Sametime
Version 8.5.2
Version 8.5.2

Sametime Advanced 8.5.2
Installation and Administration Guide
Note

Before using this information and the product it supports, read the information in "Notices."

Edition notice

This edition applies to version 8.5.2 of IBM Sametime Advanced (program number 5724-J23) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2007, 2011.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Chapter 1. Overview of Sametime Advanced

IBM® Sametime® Advanced works with a Sametime Standard deployment to extend the infrastructure. Adding Sametime Advanced to your deployment provides your users with additional collaboration features such as persistent chat rooms, real-time broadcasts, location services, and instant share.

Accessibility features for Sametime Advanced

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

IBM Sametime Advanced has the following accessibility features:

• The following features are for vision-impaired users:
  – Can be operated by using only the keyboard
  – Communicates all information independent of color
  – Supports interfaces commonly used by screen readers and screen magnifiers
  – Supports the attachment of alternate output devices
  – Provides help information in an accessible format

• The following features are for users who have mobility impairments or limited use of their hands:
  – Allows the users to request more time to complete timed responses
  – Can be operated by using only the keyboard
  – Supports the attachment of alternative input and output devices

• The following features are for the deaf and hard of hearing users:
  – Supports alternatives to audio information
  – Supports adjustable volume control

• The console does not flash the screen at rates that could induce epileptic seizures

The help system has the following accessibility features:

• Uses the accessibility support enabled by the browser that is used to display the help
• Enables navigation by using the keyboard

Tip: The Sametime Information Center and its related publications are accessibility-enabled. You can operate all features using the keyboard instead of the mouse.

Navigating the console by using the keyboard

This product uses standard Microsoft Windows navigation keys.

To move through the controls on a particular page, press Tab.

To click a link or control on a page using the keyboard, navigate to the link or control and press Enter.
To change the navigation view using the keyboard, follow these steps.
1. Navigate to the View selection list pressing Tab.
2. Use the Up Arrow and Down Arrow to change the value of the selection list.
3. Press Enter. The tasks displayed in the navigation are changed according to your selection.

Navigating help by using the keyboard

Use the following key combinations to navigate the help system by keyboard:
- To bring the Topic pane (the right side) into focus, press Alt+K, and then press Tab.
- In the Topic pane, to go to the next link, press Tab.
- To go to the previous link, press Shift+Tab.
- To go directly to the Search Results view in the left side, press Alt+R, and then press Enter or the Up Arrow to enter the view.
- To go directly to the Navigation (Table of Contents) view in the left side, press Alt+C, and then press Enter or the Up Arrow to enter the view.
- To navigate your browser history, press Alt+Left Arrow to go back. If you have navigated back to a previously view page, you can use Alt+Right Arrow to navigate forward again.
- To expand and collapse a node in the navigation tree, tab to the + or - image next to it to bring the image into focus, and then press the Right Arrow or Left Arrows
- To go to the next frame in the help system, press F6.
- To go to the previous frame in the help system, press Shift+F6. In the navigation, to move to the next topic node, press the Down Arrow or Tab.
- To move to the previous topic node, press the Up arrow or Shift+Tab.
- To go to the next link, button, or topic node from inside a view, press Tab.
- To scroll all the way up or down in a frame, press Home or End, respectively.
- To print the active pane, press Ctrl+P.
- To move to the search entry field, press Alt+S.

IBM and accessibility

See the IBM Accessibility Center for more information about the commitment that IBM has to accessibility.

What’s new in this release of Sametime Advanced?

Learn more about the new features in this release that allow IBM Sametime Advanced make communications in your organization simple and effective.

What’s new in Sametime Advanced 8.5.2
- New version of the server installer
- Integration with the Sametime System Console for centralized management
- The Advanced Client plugin is installed automatically with the Sametime Connect client and the Sametime client embedded in Notes® and can be enabled through preferences
- Consistent platform support with Sametime Standard
- Support for latest server operating system platforms for WebSphere® Application Server 7.x
- Support of LDAP groups for access control
- Improved scalability for alerting and broadcasts
- The Event Broker server has been replaced by a new WebSphere Application Server component that implements the MQTT protocol
- Compliance logging APIs: Capture chat room activity; partnering with Facetime, Permessa, Instant Technologies and others

**What is Sametime Advanced?**

IBM Sametime Advanced works with a Sametime Standard deployment to extend the infrastructure and features.

For organizations that need advanced collaboration, within specific departments or across a global enterprise, Sametime Advanced makes it easy to find information and share expertise. You can engage in ongoing conversations, share your desktop instantaneously for collaboration or help desk support, and automatically store and reuse geographic location information.

- Persistent group chat rooms
  - Users can create, enter, read, and contribute to ongoing chats at any time
  - Users can be alerted to new content, events, and people in the chat room
  - Users can participate from the Sametime Connect client or a browser
  - Persistent chat rooms can be linked to broadcast channels
- Real-time broadcast channels
  - Broadcast announcements: real-time alerts are sent to channel subscribers
  - Instant poll: subscribers can create and respond to real-time polls
  - Skill tap: subscribers can find and interact with experts; expert responses can be saved and retrieved
  - Broadcast chat: invite members of a broadcast community to an online group conversation
- Location services
  - Server-stored locations
  - Ability to see the last time and location from which an offline colleague was last online
- Instant share: share or remotely control a computer desktop with colleagues

**Component applications**

Sametime Advanced operates with several component applications, some of which can be installed on different computers to distribute the load:

- LDAP directory
  An LDAP directory stores information about all your users so that they can be authenticated at login and their data (such as buddy lists) can be properly tracked. You must have an LDAP directory installed and configured before you attempt to deploy Sametime Advanced because you need to configure several fields and port settings either while installing Sametime Advanced, or immediately afterward. The LDAP directory is not included with Sametime Advanced software components.
• DB2 relational database system
  A Sametime Advanced deployment uses a DB2 database to store data related to the function of its various features. You must have DB2 installed, and this database created, before you attempt to deploy Sametime Advanced, because you will establish a connection to the database during the Sametime Advanced installation.

• Sametime Standard and Sametime Connect client
  Sametime Standard provides the base instant-messaging features used in the deployment; users access both Sametime Standard and Sametime Advanced by means of the Sametime Connect client (or a browser for persistent group chat). You must have the Sametime Community Server installed and configured before you attempt to deploy Sametime Advanced, because you need to reference the Sametime Standard community server host name and HTTP port when installing Sametime Advanced.

### Sametime Advanced architecture

A typical IBM Sametime Advanced deployment includes a cluster of servers for instant messaging on a Domino-based platform and other clustered servers running on WebSphere Application Server that support meetings, audio-visual services, and connections to a variety of clients.

The illustration below shows the different types of servers you can have in a Sametime Advanced deployment.
PDF library (Sametime Advanced)

You can find information for IBM Sametime administrators in the documents linked below.

<table>
<thead>
<tr>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime 8.5.2 Release Notes</td>
</tr>
<tr>
<td>Sametime Advanced Client Quick Start Guide</td>
</tr>
<tr>
<td>Sametime Advanced 8.5.2 Installation and Administration Guide</td>
</tr>
</tbody>
</table>
Chapter 2. Planning a Sametime Advanced deployment

Plan your IBM Sametime Advanced installation by reviewing system requirements and the products that are included in a deployment.

System requirements (Sametime Advanced)

System requirements for installing IBM Sametime, including supported operating systems, databases, LDAP servers, IBM Sametime servers, browsers, and JDKs.

System requirements for this release of the Sametime family of products are maintained as an IBM Tech Note at the following web address:


Readme for this release

The Readme document for this release of IBM Sametime Advanced provides information about getting started with this product, descriptions of any known problems with the current release, and links to IBM Tech Notes.

Review the Release Notes before you begin deploying this product.

Planning for migration from an earlier release of Sametime Advanced

Your approach to upgrading from an earlier release of IBM Sametime Advanced depends on the version of DB2 you want to use for storing the Sametime Advanced database. Upgrading then involves updating the database components, installing Sametime Advanced Server, and registering the server with the Sametime System Console.

Before upgrading to this release of Sametime Advanced, choose your preferred DB2 upgrade path. You can either keep the DB2 server you have now, upgrade a dedicated DB2 server to the release that matches other Sametime components, or move the database to a centralized DB2 server that stores all Sametime databases. Consider the implications of each choice before making your decision.

- Keeping the DB2 Enterprise Edition Server you have now is the fastest way to upgrade to this release, but may not be supported for future releases. You must maintain two DB2 servers in your organization running different versions of DB2.
- Upgrading the DB2 server to the latest Workgroup Edition Server allows you to maintain all Sametime database components on the same version of DB2 and makes future upgrades easier. This choice requires that you uninstall the current server before installing the DB2 Workgroup Edition provided with this release. You must maintain two DB2 servers in this case also.
- Moving the Advanced database to an existing DB2 Workgroup Edition server allows you to maintain all Sametime components on one computer and makes future upgrades easier. After upgrading, you can decommission the obsolete DB2 Enterprise Edition server.
Deploying instant messaging, persistent chat rooms, and broadcast communities

To provide instant messaging and presence, use an IBM Sametime Community Server or cluster of servers running on Domino®. To provide persistent chat rooms, broadcast communities, instant share and advanced location services, use a Sametime Advanced Server or cluster of servers running on WebSphere Application Server. To provide presence support for web clients, use a Sametime Proxy Server.

Components used

The following components must be deployed in a Sametime environment that combines instant messaging and presence with persistent chat rooms and broadcast communities:

- Sametime System Console - used for managing and administering servers from a central location
- DB2
- LDAP directory
- Sametime Community Server
- Sametime Advanced Server
- Sametime Connect client, Sametime client embedded in Notes, or Sametime browser client

The following components can optionally be deployed:
- Sametime Proxy Server - provides an optional integrated web chat client and presence

Downloading Sametime files before installing

IBM enables users to download IBM Sametime installation kits from the Passport Advantage website.

About this task

Follow the steps for your operating system.

Procedure

1. AIX®, Linux, Solaris, Windows
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage®, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the
user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

2. **Linux and Windows** (Media Manager)

a. To download installation packages:

1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address:

   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

   Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

   **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

3. **IBM i:** (for Sametime community server installations from downloaded images)

a. To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

b. Open this release's Download document at the following web address:

   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers.

c. On your workstation, run the downloaded .exe file to extract the following files:
   - A short Readme document
   - Q5724J23IM: IBM i binary save file containing the Sametime *BASE option
   - Q5724J23WC: IBM i binary save file containing Sametime option 1 (not included with Sametime Entry)

Follow the instructions in Preparing to install the community server from a downloaded image on IBM to transfer the save file to the system where you plan to install the community server.

4. **IBM i** (for Sametime System Console, Meeting or Proxy server installations from downloaded images)

   a. To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

   b. Open this release's Download document at the following web address:
      https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
      Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers.

   c. Use ftp or another convenient method to transfer the installation package to the system where you plan to install the product. Store the file in an IFS directory of your choosing; for example:
      `/MySametimePackages`

5. **Sametime Advanced: AIX, Linux, Solaris, Windows**

   a. To download installation packages for Sametime Advanced:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

      2) Open this release's Download document at the following web address:
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

      **Tip**: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   **AIX**
   
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   ```
   mount -v cdrfs -o ro /dev/cd0 /cdrom
   ```
Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

**Using Passport Advantage to download files**

IBM Passport Advantage website provides access to all of your entitled software; you can download products directly to your computer for installation, and download the *Quick Start Guide* for information how to get started installing IBM Sametime.

**Before you begin**

Passport Advantage provides access to your IBM software purchases, so you can download products directly to the computers where you want to install them. For information on the Passport Advantage program, review the program overview. For assistance with Passport Advantage, contact IBM eCustomer care

Downloading products from Passport Advantage requires an IBM customer ID; if you do not have one, you must register with the site:

1. Open a browser and navigate to Passport Advantage sign-in page.
2. Complete the new customer registration form.
3. Click **Register**.

When you receive your IBM customer ID, proceed to download products as explained below.

The IBM Passport Advantage account is described at the following web address:


**Procedure**

1. Open a browser and navigate to the Passport Advantage sign-in page.
2. Click **Customer sign in**
3. Enter your IBM customer ID and password, and then click **Sign in**.
4. On the "Software and services online" page, click **Software download & media access**.
5. On the "Find downloads & media" page, click **Download finder**.

Passport Advantage displays list of your entitled downloads (products that you have purchased).

6. Click a product to select it, and then click **Continue** to search for its downloadable packages.

**Tip:** If you know a download package's part number (specified in the Download document for each product), you can search on that part number to quickly find the downloadable package.

Software products are posted “assemblies” containing different versions of the product for use with various operating systems and languages. Packaging varies depending on the size and complexity of each product.

7. Under “Select criteria”, select a language and platform (operating system) for the product you want to download.
8. Under "Download options", select Yes for the option "If available, would you like to see associated products at no additional charge?". This ensures that you can view and download optional products that are used with the primary product (for example, an LDAP directory server where you can store user names).

9. Click Continue.
   Passport Advantage displays the list of assemblies (packages) for the selected criteria.

10. Select your download:
   - Select an assembly to download all of its included packages:
Click the + to expand the assembly so you can select individual packages:

• Click the + to expand the assembly so you can select individual packages:

**Important**: You should always download a copy of the product’s *Quick Start Guide* because it provides an overview of the product installation as well as links to additional documentation.

11. Select items to download and scroll to the bottom of the page.
12. Review the license agreement, and click I agree.
13. Click Download and select a location on your computer to store the downloaded files.

**What to do next**

Review the *Quick Start Guide* for an installation overview as well as links to the product documentation, where you will find instructions on installing the product.
Chapter 3. Installing Sametime Advanced

Install IBM Sametime Advanced on AIX, Linux, Solaris, or Windows. Then deploy Sametime Advanced to clients.

Before you begin

Sametime Advanced runs on an existing Sametime server environment. Before following these steps, you should have already installed and set up the Sametime System Console, the LDAP server, the Community Server, the Proxy Server, and the Meeting Server.

For more information, see Installing on AIX, Linux, Solaris, and Windows in the Installing section of Administering Sametime Standard.

Sametime Advanced also requires DB2 and DB2 Net Search Extender.

Installing DB2 for Sametime Advanced Server on Linux or Windows

Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store information about servers, users, bandwidth configuration, and meetings.

Sametime Advanced uses DB2 to store information about persistent chats and broadcast communities.

Before you begin

These instructions explain how to install the version of DB2 integrated with the Sametime installation package. Use this version of DB2 if you are unfamiliar with DB2 and would prefer a less complex deployment on Windows and Linux operating systems. The DB2 installation provided with Sametime supports Linux 64-bit systems and Windows 32-bit or 64-bit systems.

If you are familiar with DB2 deployments or are installing on other operating systems, download and install one of the unmodified DB2 limited use installation packages that are available at the following web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

IBM i includes DB2.

Linux The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

Linux: If you are installing using the GUI mode, the full X11 desktop environment is required.
About this task

If you are running in an enterprise deployment, install DB2 on a separate computer. In a small deployment, you can install DB2 on the same computer on which you plan to install Sametime system console.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
3. Download the Sametime DB2 installation package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      Linux
      Mount the CD or DVD using a command similar to the following command:
      ```
      mount /dev/cdrom /cdrom
      ```
4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - Linux ./launchpad.sh
   - Windows \launchpad.exe
Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

`sametime_server_package/IM/platform`

`sametime_server_package` is the installation package name for this server.
`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.
6. Click Install IBM DB2, then click Install IBM DB2 again.
7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.
8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.
9. Click Install.
10. Click the I accept the terms in the license agreements option and click Next.
11. Accept the default locations and click Next.
12. Accept the default location for the package group and click Next.
13. Select Create a new package group and accept the default location. Click Next.
14. Confirm that all available features are selected, then click Next.
15. Create a DB2 application user ID that does not exist on the system. Then, supply a password that meets the operating system password policy requirements and any additional requirements imposed by your company. Confirm the password.
   The user specified, dasadm1, and the group db2admin does not exist on the system.
   For information about passwords, see the Password Rules topic in the DB2 information center.

Important: This user cannot previously exist on the system. This user will be created as a local operating system user during the DB2 installation process; if your organization does not allow creation of local operating system users for security reasons, exit this installer and install DB2 using a different package. This installer does not check to see if the user exists.

Make a note of the DB2 application user name and password. This user has database administration authority and you must supply the name and password when you install the Sametime system console and when you connect to DB2 databases later.

Click Next.
16. Review the summary, then click Install to start the installation.
   The installation can take up to 20 minutes. You receive confirmation when it is complete.
17. Click Finish.
18. Click Exit to close the Installation Manager.
19. (Linux only) The DB2 server does not start by default when you restart the computer. To start a database instance automatically when the server restarts, use the `db2iauto` command.
   For more information, see `db2iauto -Autostart instance command`.

**Results**

If the installation fails, click View Log File for more information.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media. Ignore any warning about a missing `versionInfo.properties` file. It does not apply to DB2 installations and upgrades.

Installation Manager logs are stored in the following locations.

**Linux**  
/var.ibm/InstallationManager/logs

**Windows 2008**  
%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Windows 2003**  
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

More detailed DB2 installation logs are stored in the following locations.

**Linux**  
The logs are stored in the /tmp folder and are named `db2setup.log`, `db2setup.his`, and `db2setup.err`.

**Windows**  
%My Documents%\DB2LOG\  
The log file name includes the date and time of the installation attempt; for example:

C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log

**What to do next**

If you are installing DB2 for Sametime Advanced, you must also install DB2 Net Search Extender to allow database content to be searchable and persistent. See the instructions for your operating system in the DB2 9.7 information center:

- Installing Net Search Extender on IBM DB2 9.7 for UNIX
- Installing Net Search Extender on IBM DB2 9.7 for Windows

**Related information**

- IBM DB2 Database for Linux, UNIX, and Windows Information Center

**Installing DB2 in silent mode for Sametime Advanced Server**

If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media
Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

Before you begin

Information about downloading packages for Sametime is located at the following web address:

Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128


Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

About this task

Follow these steps to install the IBM Installation Manager in silent mode. Customize each product’s response file, then install the product in silent mode using the customized response file.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.
2. Navigate to the directory where you copied and extracted the installation files: \TMP\server_offering
3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.
4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows. For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.
5. The SSCPassword value should be encoded. To generate an encoded password, use the generateEncodedPassword utility packaged with the installer.

The utility is on the installation media in the same directory as launchpad.exe or launchpad.sh.

7. Open a command window.
8. Enter the following command to install the IBM Installation Manager in silent mode.
   - AIX, Linux, or Solaris
     ```
     ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
     ```
   - Windows
     ```
     IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
     ```

9. Navigate to the Installation Manager installation directory. The default directories are shown below.
   - AIX, Linux, or Solaris
     ```
     /opt/ibm/InstallationManager/eclipse
     ```
   - Windows
     ```
     C:\Program Files\IBM\Installation Manager\eclipse
     ```

10. For all installations except DB2, start the Sametime System Console.
11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.
    - AIX, Linux, or Solaris
      ```
      ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
      ```
    - Windows
      ```
      IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
      ```

    **Tip: Generating a response file automatically**
    The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation without using `--skipInstall`.
    ```
    ./install --launcher.ini your .ini file -record response file path -skipInstall agentDataLocation
    ```
    The response file is stored in the `agentDataLocation` directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same `agentDataLocation` in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using `--skipInstall` are not stored.

---

**Creating a database for Sametime Advanced**

Before installing IBM Sametime Advanced, create a database to store its data.

**About this task**

Run the scripts that come with the Sametime Advanced Server package. They are also included with Sametime Standard in the DB2 installation package.

**Procedure**

1. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation.
2. Open a command prompt and navigate to the folder where you extracted the SametimeAdvancedServer installation package.
3. Create the database by entering one of the following commands from the SametimeDB2 folder. Wait until you see confirmation that the database has been created and the command has finished.
   - AIX, Linux, or Solaris
     ```
     ./createAdvancedDb.sh STADV dbadmin
     ```
• **Windows**: `createAdvancedDb.bat STADV dbadmin`
  
  Replace `STADV` in the command if you want to choose a different database name. Names can be from 1 - 8 characters, but cannot contain special or multibyte characters.

  Replace `dbadmin` with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.

  When naming DB2 objects, follow the rules for your operating system.

4. Close the command window.

**Results**

Verify that the new database was created either from the command line or by using the DB2 control center.

**From the command line**

View the output from running the create script and enter the following command:

```
db2 connect to STADV
```

where `STADV` represents the name of the database you created. Verify that you can connect to the database.

**From the DB2 control center**

- **AIX, Linux, or Solaris**
  
  Open the IBM DB2 folder on the desktop and click **Control Center**.

- **Windows**
  
  Click **Start > Programs > IBM DB2 > General Administration Tools > Control Center**.

---

**Creating text indexes for searching the Sametime Advanced database**

Creating text indexes is a requirement for making content in the IBM Sametime Advanced database searchable.

**Before you begin**

You must have installed the IBM DB2 server software and DB2 Net Search Extender, then started those applications, and created a database.

**About this task**

Use the `dbtext.bat` and `dbtext.sh` files provided with the Sametime Advanced software download to run the Net Search Extender services. If the indexes ever become corrupted, you can safely rerun the `dbtext` scripts at any time without losing any existing data.

**Procedure**

1. Download the appropriate version of the `dbtext` script for your operating system to the DB2 server.

   The scripts are stored in the `STAdvancedLaunchpad\disk1\DatabaseScripts` directory within the Sametime Advanced software download.

   a. To download installation packages for Sametime Advanced:
1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address:
   &uid=swg24027364
   Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

   **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   **AIX**
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   `mount -v cdrfs -o ro /dev/cd0 /cdrom`

   **Linux**
   Mount the CD or DVD using a command similar to the following command:
   `mount /dev/cdrom /cdrom`

2. With the DB2 command window open, start Net Search Extender by running the following command.

   **db2text start**
   DB2 Net Search Extender must be running to support Sametime Advanced operations. If you stop this service for any reason, be sure to restart it. To remove the need for manual restarts, you may want to set this service to start automatically:
   - AIX, Linux, Solaris: Add the text indexing service startup to the database startup script.
   - Windows: Set the "DB2TEXT" service to "Automatic" in the Windows Services control panel.

3. Run the following command to create the text indexes:
   **AIX, Linux, Solaris**
   `./dbtext.sh database_name`

   **Windows**
   `dbtext.bat database_name`
   Replace `database_name` with the name of the Advanced database; for example, STADV.

4. Once the script successfully completes, you can disconnect from the database with the following command:
   `DB2 DISCONNECT STADV`

5. Now type the following command in the DB2 Command Window:
EXIT

6. Close the DB2 Command Window.

What to do next

If the dbtext.sh script does not successfully enable text searching for AIX, Linux, or Solaris, perform the following workaround to enable text searching:
1. In a DB2 command window, change to the sqllib/adm directory:
   ```
   cd ~/sqllib/adm
   ```
2. Enter this command:
   ```
   ls -al .fenced
   ```
3. Run the dbtext.sh script again by repeating Steps 3 - 6 in the above procedure.

If the group of .fenced differs from the primary group of the database instance, follow these steps to correct the ownership:
1. In a DB2 command window, enter this command to stop the db2text service:
   ```
   db2text stop
   ```
2. Stop DB2:
   ```
   db2stop
   ```
3. Change to the sqllib/adm directory:
   ```
   cd ~/sqllib/adm
   ```
4. Enter this command:
   ```
   rm .fenced
   ```
5. Enter this command to correct the ownership:
   ```
   touch .fenced
   ```
6. Start DB2:
   ```
   db2start
   ```
7. Start the db2text service:
   ```
   db2text start
   ```
8. Run the dbtext.sh script again by repeating Steps 3 - 6 in the above procedure.

Related information

Starting and stopping Net Search Extender instance services using the command line

Logging in to the Sametime System Console after creating the Sametime Advanced database

Use the IBM Sametime system console to use guided activities to perform configuration tasks and administer any Sametime servers that are managed by the console.

Procedure

With the Sametime system console started, follow these steps to log in.
1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server. For AIX, Linux, Solaris, or Windows, specify port 8700 for HTTP and 8701 for HTTP over SSL.
During the installation process, WebSphere Application Server security is enabled. SSL is enabled as part of the security process and you are directed to another port that listens for HTTPS connections.

http://serverhostname.domain:port/ibm/console

For example:

http://sametime.example.com:8700/ibm/console

https://sametime.example.com:8701/ibm/console

**Note:** On IBM i, the port number cannot be 8700. Use the port that was listed in the system console installation results summary. To check the port, open the AboutThisProfile.txt file for the system console deployment manager profile and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:

/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/
STSCDmgrProfile/logs/AboutThisProfile.txt

2. The WebSphere Application Server Integrated Solutions Console opens. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.

   The default name is wasadmin.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

---

**Connecting to a DB2 database (Sametime Advanced)**

Use the Sametime System Console to connect to the Sametime Meeting Server, Sametime Gateway, or Sametime Advanced database before installing the server from the System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

**Before you begin**

Start the Sametime System Console if it is not already running.

**Procedure**

If you have not already opened the Connect to DB2 Databases activity, follow these steps:

1. From a browser, enter the following URL, replacing *serverhostname.domain* with the fully qualified domain name of the Sametime System Console server.

   http://serverhostname.domain:8700/ibm/console

   For example:

   http://sametime.example.com:8700/ibm/console

   **IBM i:** The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary or use the setting specified for the Administrative console secure port in the AboutThisProfile.txt file. For the Sametime System Console Deployment Manager Profile (STSCDmgrProfile), the file is located in the following path:

   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/
   STSCDmgrProfile/logs/AboutThisProfile.txt
2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Sametime Prerequisites > Connect to DB2 Databases**.

**Related tasks**

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

---

**Sametime prerequisite: Connecting to a DB2 database (Sametime Advanced)**

This activity takes you through the steps for connecting to the Meeting Server, Gateway, or Advanced Server database you created.

**Before you begin**

**AIX, Linux, Solaris, Windows**: Ensure that IBM DB2 has been installed and that you have created the Sametime Meeting Server, Gateway, or Sametime Advanced database.

**IBM i**: Ensure that you have created the required database schemas and tables.

In the **Connect to DB2 Databases** portlet, verify that the Sametime System Console database you created earlier is already displayed in the list of databases.

**About this task**

Follow these steps to connect to the Meeting Server, Gateway, or Advanced Server database. You must do this before you can install the Meeting Server or the Advanced Server using the Sametime System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

**Procedure**

1. DB2 Configuration Guided Activity.

   - Click **Add** to begin the guided activity that will connect your server to the DB2 database. If a connection already exists, you can optionally edit or delete it.

2. Add a new database.

   a. In the **Connect to DB2 Databases** portlet, click **Add**.

      - If you want to edit or delete a database instead, then select one, and click the appropriate button.

   b. Enter the fully qualified host name of the DB2 server in the **Host name** field.

      - Do not enter an IP address or a short host name.

   c. The **Port** field shows the default port of 50000. Accept the default unless you specified a different port during DB2 installation or your server is using a different port.

      - **Linux**: Check the `/etc/services` file on the DB2 server to verify the port number being used.
d. In the **Database name** field, enter the name of the database you want to connect to.

e. In the **Application user ID** field, supply the DB2 application's administrative user name that you created when you installed DB2, such as db2admin. This user has database administration authority and you will use this user ID and password whenever you work with DB2 databases for Sametime. On IBM i, this is the user profile you specified as the owner of the Meeting Server database schemas in your copy of the stms.default.response.properties file or the user profile you logged in with when you created the Gateway database schemas.

f. In the **Application password** field, enter the password for the DB2 administrative user ID.

g. (Meeting Server or Gateway databases) If you are connecting to a database on an IBM i server, click **Hosted on IBM i**.

h. Click **Finish**.

---

**Preparing to install Sametime Advanced using a deployment plan**

Use the Sametime System Console to prepare to install Sametime Advanced by pre-populating values required for installation.

**Before you begin**

Start the Sametime System Console if it is not already running.

**Procedure**

If you have not already opened the Install Sametime Advanced guided activity, follow these steps:

1. From a browser, enter the following URL, replacing `servername.domain` with the fully qualified domain name of the Sametime System Console server.

   `http://servername.domain:8700/ibm/console`

   For example: `http://sametime.example.com:8700/ibm/console`

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Sametime Guided Activities** > **Install Sametime Advanced Server**.
Related tasks
“Deploying Sametime Proxy Server, Sametime Meeting Server, or Sametime Advanced on one machine” on page 51
If you deploy the Sametime Proxy Server or Sametime Meeting Server with Sametime Advanced on one machine, configure the servers to have the same host name, then configure Sametime Advanced to use that Sametime Proxy Server for awareness because users cannot get awareness on the Sametime Advanced pages.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install Sametime Advanced using a deployment plan
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

Before you begin
You have set up an IBM DB2 database and an LDAP server, and have run the guided activities for connecting to the DB2 database and to the LDAP server.

About this task
Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Advanced.

Procedure
1. Plan a product installation.
   In the Install Sametime Advanced Server portlet, click Create a New Deployment Plan, and then click Next.
2. Deployment Name.
   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.
   The name should include the installation and node type, such as stAdv_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.
3. Choose the configuration type.
   Select Primary Node if this is the first server of its type. Select Secondary Node for additional servers. Then click Next.
   The Cell option is reserved for special-use cases in which the server must be self-contained. If you select Cell, you must provide a host name, user ID, and password when prompted to do so.
   This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click Next.
Attention: Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

5. WebSphere Profile Settings.
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click Next.
      If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

   Important: This must be a unique user ID that does not exist in the LDAP directory.

6. Chat room admin user settings
   Enter the credentials for the Sametime Advanced chat room administrator, and then click Next. Select Use the WebSphere Administrator to use the user name and password you entered in the previous screen. You can also supply a new user name and password specifically for chat room administration.

7. Choose a database for this deployment. This panel appears if you selected Primary Node or Cell as the configuration type.
   Select the Sametime Advanced database that you configured with the Sametime System Console activity, and then click Next.

8. Connect to an LDAP Server. This panel appears if you selected Cell as the configuration type.
   Select the LDAP directory that you configured with the Sametime System Console guided activity, and then click Next.

   Review the summary screen, and then click Finish.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click Modify an Existing Deployment Plan and update the plan. All changes must be made prior to running installation.

What to do next

Installing Sametime Advanced

Installing Sametime Advanced using a deployment plan

Run the installation program on the machine where you plan to install IBM Sametime Advanced.

Before you begin

You should have already created a deployment plan for the Sametime Advanced Server. Verify that the deployment plan is in the “Ready to Install” state and start
the Sametime System Console server. Be sure there are no firewalls or connectivity problems to the LDAP server or the installation will fail.

**Linux**  The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**

If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:**  Check the `hosts` file and remove any lines that start with the following:

- `127.0.0.1 fully_qualified_domain_name short_name`
- `::1 fully_qualified_domain_name short_name`

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

**About this task**

By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

**Procedure**

1. **Red Hat Enterprise Linux only:** Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the `SELINUX` setting. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.

2. **Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.**

**Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. **Prepare to use the installation package.**
   a. To download installation packages for Sametime Advanced:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
Locate the components that you need in the document's listing, then
download the packages labelled with the corresponding part numbers
to the system on which you are installing.

Tip: When extracting downloads on Windows operating systems, use a
short path location such as C:\ and not a long path location such as
the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following
command:

```
mount /dev/cdrom /cdrom
```

4. Navigate to the folder where you stored the downloaded files and start the
installation program by running one of the following commands:

- **AIX, Linux, and Solaris**: `./launchpad.sh`
- **Windows**: `launchpad.exe`

**Note**: If you do not have a web browser, go to the Installation Manager
package directory and run the installation program (**install** for Linux or
**install.exe** for Windows). Find the Installation Manager package directory
here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language**
list.

6. Click **Install IBM Sametime Advanced Server** and click **Launch IBM
Sametime Advanced Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install
Installation Manager. Do so, then click **Finish** to restart the Installation
Manager and continue with the next step of the Sametime installation.
If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the
automatic web update search to allow the installation to run successfully.

a. In the Installation Manager window, choose **File > Preferences**.

b. Uncheck **Search service repositories during installation and updates** and
   click **OK**.

9. Click **Install**.
10. Select the packages that you want to install and click **Next**.
11. Click the **I accept the terms in the license agreements** option and click **Next**.
12. Select a package group option and accept the installation directory. Then click **Next**.
   Select **Create a new package group** if you have not installed any other
   Sametime software on this machine.
   Leave **Use the existing package group** selected if you are installing several
   Sametime servers on the same machine.
13. Select **IBM Sametime Advanced Server 8.5.2** as the feature to install and
   select **Use Sametime System Console to install**. Click **Next**.
14. In the Common Configurations window, supply values for connecting to the
   Sametime System Console.
   - **Host Name**: Provide the fully qualified domain name in the Host Name
     field for the Sametime System Console. The host name was determined
     when you installed the Sametime System Console. The host name must be
     the actual host name and not a DNS alias.
   - **Use SSL**: Leave this option selected to run the server over a secure
     connection.
   - **HTTPs Port**: Leave 9443 as the default value.
   - **User ID and password**: Provide the WebSphere Application Server User ID
     and password that you created when you installed the Sametime System
     Console.
15. Provide the host name for the machine you are currently using, which is the
   same name you used when you created the deployment plan for this
   installation.
   Do not use an IP address or short host name.
16. Click **Validate** to log in to the Sametime System Console.
   The button name changes to **Validated** after you log in.
17. When you are logged in, click **Next**.
18. Select the Sametime Advanced Server deployment plan you created earlier
   with the Sametime System Console guided activity. Then click **Next**.
19. Review the deployment settings, then click **Next**.
20. Review the summary, then click **Install** to start the installation.
21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

If the installation was not successful, look at the installation log files for more
information about what occurred during the installation attempt. Fix any problems,
then uninstall all components and reinstall. Find information in the logs directory
and the ant and native subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the
root of the installation media.

**AIX, Linux, or Solaris**

   /var/ibm/InstallationManager/logs

   Console connection log: /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

   %ALLUSERSPROFILE%\IBM\Installation Manager\logs
Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Windows 2003
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.

Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 481

Starting and stopping IBM Sametime servers that run on WebSphere Application Server involves other server components such as the Deployment Manager and the node agent.

“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Installing Sametime Advanced in silent mode
If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

Before you begin

Information about downloading packages for Sametime is located at the following web address:
Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.
About this task

Follow these steps to install the IBM Installation Manager in silent mode. Customize each product’s response file, then install the product in silent mode using the customized response file.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory `\TMP` on the computer where you will be installing the server offering.

2. Navigate to the directory where you copied and extracted the installation files: `\TMP\server_offering`

3. Fully documented sample response files are contained in the `responseFiles` directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes `_ssc.rsp` in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.

4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows. For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.

5. The SSCPassword value should be encoded. To generate an encoded password, use the `generateEncodedPassword` utility packaged with the installer.

The utility is on the installation media in the same directory as `launchpad.exe` or `launchpad.sh`.


7. Open a command window.

8. Enter the following command to install the IBM Installation Manager in silent mode.

   - **AIX, Linux, or Solaris**
     ```
     SametimeOffering/IM/windows/install --launcher.ini silent-install.ini
     ```

   - **Windows**
     ```
     launchpad.exe silent-install.txt
     ```

9. Navigate to the Installation Manager installation directory. The default directories are shown below.

   - **AIX, Linux, or Solaris**
     ```
     /opt/ibm/InstallationManager/eclipse
     ```

   - **Windows**
     ```
     C:\Program Files\IBM\Installation Manager\eclipse
     ```

10. For all installations except DB2, start the Sametime System Console.

11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.

    ```
    AIX, Linux, or Solaris./IBMIM --launcher.ini silent-install.ini -input response file -log log file -acceptLicense
    ```
WindowsIBMIMc --launcher.ini silent-install.ini -input response_file
-log log_file -acceptLicense

Tip: Generating a response file automatically
The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation.

```
./install --launcher.ini your .ini file -record response file
```

The response file is stored in the `agentDataLocation` directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same `agentDataLocation` in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using `-skipInstall` are not stored.

Verifying the Sametime Advanced installation
Log in to the IBM Sametime Advanced Server to verify that the installation was successful.

About this task
Verify the installation by setting up a test client and logging in to the server.

Procedure
1. Set up a Sametime client to test the installation:
   - Install the latest Sametime client.
   - Enable the Sametime Advanced client plugin by setting this preference:
     ```
     com.ibm.collaboration.realtime/enableAdvanced=true
     ```
   - Change these preferences. Under Chat Rooms and Broadcast Tools, enter the Broadcast Tools Server name and port 1883. Enter the Sametime Advanced Server name and port 9080.
     The Advanced server HTTP port is usually 9080, but may be different.
     Specify the port for your environment.
2. From a web browser, access the Sametime Advanced server by entering the following URL:
   ```
   http://serverhostname.domain:port/stadvanced
   ```
3. Verify that chat rooms and broadcast communities connect to the Advanced server correctly.

Related tasks
“Enabling Sametime Advanced persistent chat rooms and broadcast communities after installing” on page 53

The IBM Sametime Connect client, both standalone and integrated with Lotus Notes®, includes plug-ins that were available separately in previous releases.

Clustering Sametime Advanced
Configuring a cluster of IBM Sametime Advanced servers involves several tasks, including synchronizing system clocks, configuring the cluster settings, and deploying a load balancer in front of the cluster, either deploying IBM Load Balancer or another load balancer product.
Before you begin

You can create two types of clusters:

- A **Vertical cluster** resides on the Primary node and includes two or more cluster members, which run the same application.
- A **Horizontal cluster** includes a Primary node plus one or more Secondary nodes, all running the same application.

Before you can configure a cluster of Sametime Advanced servers, you must have installed the following servers:

- **The Sametime System Console**
  This server can function as the Deployment Manager for the vertical or horizontal cluster scenarios described in this procedure.
  **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Meeting server cluster, a Media Manager cluster, and an Advanced server cluster. If you want to create additional clusters for a particular product, you must deploy additional Deployment Managers.

- **Sametime Community Servers**
  At least one Sametime Community Server must be deployed. The Community Server provides presence and awareness for chats.
• One Sametime Advanced server installed with the **Network Deployment > Primary Node** option.

Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster’s application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node’s application server. The Primary node’s application server can only belong to one cluster. The Primary Node can be used as a container for additional cluster members when creating a **vertical cluster** (multiple cluster members on the same physical system).

• (Horizontal cluster only) One or more servers installed with the **Network Deployment > Secondary Node** option.

Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as containers for additional cluster members, which can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a **horizontal cluster** (one cluster member on each Secondary Node, plus one cluster member or one vertical cluster on the Primary Node).

**About this task**

There are several tasks involved in creating a cluster; complete them in the sequence shown here:

Attention: Complete all of the tasks to ensure your cluster operates properly.

Related concepts

“Clustering Sametime servers for high enterprise availability” on page 227
In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

**Setting clocks on the Sametime Advanced servers to be clustered**

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.

**About this task**

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.

**Procedure**

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager’s (the Sametime System Console) system clock.
Clustering Sametime Advanced servers

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

Start the Sametime System Console and the servers you intend to cluster.

Note: This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.
3. On the left side of the navigation tree, click the Sametime System Console task to open it.
4. Click Guided Activities > Cluster WebSphere Application Servers.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Clustering Sametime Advanced servers

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.

   This guided activity applies to the following Sametime servers if they are installed in your deployment.
Sametime Proxy Server
Sametime Meeting Server
Sametime Media Manager

Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.

Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster's Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager’s SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.
Procedure

1. Cluster WebSphere Application Servers.
   Click Next to begin the clustering activity.

2. Select Product to Cluster.
   Select the product server to cluster, and then click Next.
   The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).

3. Select or Create a Cluster.
   To create a cluster:
   a. Click Create Cluster if you are setting up a new cluster.
   b. Type a descriptive name for the cluster in the Cluster Name field.
      For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.
   c. Click Next.
   To modify an existing cluster; for example, to add a new cluster member:
   a. Click Select Existing Cluster.
   b. Select a cluster in the Cluster Name list.
      If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.
   c. Click Next.

4. Select the Deployment Manager.
   In the Select Deployment Manager list, select the Sametime System Console as the cluster's deployment manager, and then click Next.
   Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.

5. Create the Cluster with the Primary Node.
   You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node's application server is running. Click Create cluster to configure the cluster settings, and then click Next.
   Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. Select One or More Secondary Nodes.
   If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the Secondary Node Name list, click the node you want to add to the cluster and click Next.

7. Add Cluster Members.
If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more “cluster members” to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.

The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be “Clustered” if the cluster member has been completely configured on the node. If the status is “Ready to Cluster”, select the Cluster Member and use the “Add to Cluster” button to finish configuring the cluster member.

**Vertical cluster:**

a. To add new cluster member, click **New**.

b. Select the default name generated for the cluster member or enter your own cluster member server name.

c. Select the Primary Node to create the cluster member on.

d. Click **Add to Cluster**.

   The status will change from “Ready to cluster” to “Clustered”.

e. Click **Next**.

**Horizontal cluster:**

For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.

a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.

b. One at a time, select each cluster member and click **Add to Cluster**.

   Do not proceed until the current cluster member’s status changes from “Ready to cluster” to “Clustered”; then you can add the next cluster member.

c. If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.

d. Click **Next**.

8. **Deployment Summary.**

   Click **Finish** to save the cluster configuration.

   Continue with the cluster configuration tasks described in the Sametime information center.

**Restarting the servers in the cluster**

After running the Clustering guided activity, synchronize the nodes in the cluster and restart the application servers.

**Restarting and synchronizing nodes in the Sametime Advanced cluster**

Synchronize the nodes in an IBM WebSphere Application Server network deployment.

**About this task**

Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node’s configuration.
Procedure
1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Stop the Deployment Manager:
   a. Click System Administration > Deployment manager.
   b. Click the "Configuration" tab.
   c. On the Configuration tab of the deployment manager settings, click Stop.
3. Now start the Deployment Manager:
   a. Open a command window and navigate to the app_server_root/profiles/DeploymentManagerName/bin directory.
   b. Run the following command:
      IBM AIX, Linux, or Solaris
      ./startManager.sh
      Microsoft Windows
      startManager.bat
      IBM i
      1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.
      2) At the Qshell prompt, run the following commands:
         cd app_server_root/profiles/DeploymentManagerName/bin
         startManager dmgr
4. Log in to the Integrated Solutions Console.
5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.
6. Restart all nodes in the cluster:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Node agents.
   b. Click a node agent, and then click Restart (the node agent should already be running).

Restarting the application servers in the Sametime Advanced cluster
During cluster configuration, each node's application server was stopped so that the node could be federated. Start all of the application servers now.

About this task
Use the IBM Sametime System Console to start each of the application servers in the cluster.

Procedure
1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Clusters > WebSphere application server clusters in the navigation tree.
3. Select the cluster's check box and click Start to start all cluster member servers.
Installing IBM Load Balancer in a Sametime Advanced cluster

Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.

Before you begin

Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Note: The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.

IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure

1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
      Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
   For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.

3. After you have installed IBM Load Balancer, configure two static IP addresses for it:
   • Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
   • Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

   For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:
### Table 1. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer: loadbal.example.com</td>
<td>Load balancer (Cluster address)</td>
<td>Load balancer (NFA): 192.0.2.15 Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>st-cluster.example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>Deployment Manager (Sametime System Console)</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>svr1.example.com</td>
<td>Primary Node (a Sametime server)</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td>svr2.example.com</td>
<td>Secondary Node (a Sametime server)</td>
<td>192.0.2.5</td>
</tr>
</tbody>
</table>

### Configuring IBM Load Balancer in a Sametime Advanced cluster

Configure IBM Load Balancer for a cluster of IBM Sametime servers.

#### About this task

The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

**Configuring IBM Load Balancer on AIX, Linux, or Solaris in a Sametime Advanced cluster:**

Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

**Before you begin**

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

**About this task**

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.
Procedure

1. Configure the nodes of the cluster.

   **For cluster nodes running on AIX, Linux, and Solaris**
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   **For cluster nodes running on IBM i**
   Use the `Add TCP/IP Interface` command to create a virtual IP address with the "cluster" IP address you want to use.
   For example:
   
   ```
   ADDTCPIFC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
   ```
   When the virtual TCP/IP interface is started, the server accepts packets for that address.

   **Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:

   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   **Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process with the following command:
      ```
      dsserver
      ```
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).

      **AIX**
      1) Run the following command:
         ```
         autoconf6
         ```
      2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
         ```
         start usr/bin/autoconf6 * -A
         ```

      **Linux** Run the following command (you must be logged in as root):
      ```
      modprobe ipv6
      ```

      **Solaris** Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:
      ```
      ifconfig device inet6 plumb
      ifconfig device inet6 address/prefix up
      ```
d. Start the executor function of the dispatcher:
   
   dscontrol executor start

e. Add the cluster to the service:
   
   dscontrol cluster add cluster's_fully_qualified_host_name
   
   where cluster's_fully_qualified_host_name is the fully qualified host name that
   you assigned to the cluster when you installed the load balancer; for
   example:
   
   stms-cluster.example.com

f. Add the cluster port:
   
   dscontrol port add cluster's_fully_qualified_host_name@port
   
   where cluster's_fully_qualified_host_name@port is the fully qualified host name
   that you assigned to the cluster when you installed the load balancer, with
   the HTTP/HTTPS port appended to it (typically port 80); for example:
   
   stms-cluster.example.com@80

g. Add the nodes for which this server will balance workload:
   
   dscontrol server add cluster_host@port@primary_node
   dscontrol server add cluster_host@port@secondary_node
   
   where:

   • cluster_host@port@primary_node indicates the cluster's fully qualified host
     name with the port appended as in the previous step, plus now with the
     primary node's fully qualified host name appended; for example:
     
     stms-cluster.example.com@80@meetsvr1.example.com

   • cluster_host@port@secondary_node indicates the cluster's fully qualified host
     name with the port appended (as in the previous step) plus now with the
     secondary node's fully qualified host name appended (include an
     additional line for each additional secondary node); for example:
     
     stms-cluster.example.com@80@meetsvr2.example.com

h. Now start the Load Balancer administration interface with the following
   command:
   
   ./lbadmin

   Note: If you have difficulty starting the administration interface, try
   stopping and then starting the executor and dsserver services before
   running the command again:
   
   dsserver stop
dcontrol executor stop
dcontrol executor start
dsserver start
   
   ./lbadmin

4. Continue configuring Load Balancer as follows:

   a. Add the cluster to the executor:
      
      dscontrol executor add cluster's_fully_qualified_host_name
      
      where cluster's_fully_qualified_host_name is the fully qualified host name that
      you assigned to the cluster when you installed the load balancer; for
      example:
      
      stms-cluster.example.com

   b. Start the manager:
      
      dscontrol manager start
c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
   
   
   dscontrol advisor start http 80

5. Define server affinity with a "sticky time":

   By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

   The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

   a. Open a command window on the load balancer server.
   b. Stop the service with the following command:
      
      dsserver stop
   c. Set the sticky time with the following command:
      
      dscontrol port set fully_qualified_host_name@port_number stickytime number_of_seconds

      Where:
      • fully_qualified_host_name is the fully qualified host name of the server where IBM Load Balancer runs.
      • port_number is the port that will be affected by the new sticky time setting.
      • number_of_seconds is the duration, in seconds, of the time that a client should "stick to" the specified port.

      For example:
      
      dscontrol port set myserver.com@80 stickytime 60

6. Save the load balancer settings:

   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
   b. Click **Save Configuration File as** and accept the default name (default.cfg).

      The configuration settings stored in default.cfg are restored every time the server is restarted.
   c. Click **OK**.

**Configuring IBM Load Balancer on Windows in a Sametime Advanced cluster:**

Configure IBM Load Balancer on a server running Microsoft Windows.

**Before you begin**

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.
About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

Procedure

1. Configure the nodes of the cluster.
   
   For cluster nodes running on Windows
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   For cluster nodes running on IBM i
   Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.
   For example:
   ADDTCP1FC INTNETADR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)
   When the virtual TCP/IP interface is started, the server accepts packets for that address.
   
   Note: Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.
   
   Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:
   
   a. Open a command window on the load balancer server.
   b. Start the load balancer’s Dispatcher process by clicking Start > Control Panel > Administrative Tools > Services. right-click IBM Dispatcher (ULB), and then click Start.
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Run the following command while logged in as the Windows administrator:
      netsh interface ipv6 install
      This command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.
   d. Start the executor function of the dispatcher:
dscontrol executor start

e. Add the cluster to the service:
   dscontrol cluster add cluster’s_fully_qualified_host_name
   where cluster’s_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
   stms-cluster.example.com

f. Add the cluster port:
   dscontrol port add cluster’s_fully_qualified_host_name@port
   where cluster’s_fully_qualified_host_name@port is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
   stms-cluster.example.com@80

g. Add the nodes for which this server will balance workload:
   dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node
   where:
   - cluster_host@port@primary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:
     stms-cluster.example.com@80@meetsvr1.example.com
   - cluster_host@port@secondary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
     stms-cluster.example.com@80@meetsvr2.example.com

h. Add the cluster to the executor:
   dscontrol executor add cluster’s_fully_qualified_host_name
   where cluster’s_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
   stms-cluster.example.com

i. Start the manager:
   dscontrol manager start

j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
   dscontrol advisor start http 80

k. Now you can stop the service:
   dsserver stop

l. Close the command window.

4. Define server affinity with a "sticky time":
   By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every
30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

**Windows**

a. Start IBM Load Balancer.

b. In the navigation tree, select the *Executor* (the load balancer's non-forwarding IP address, which appears under its host name).

c. Click *Configuration Settings*.

d. In "Port-Specific Settings", change the Default sticky-time settings from 0 to 60 seconds, and click *Update Configuration*.

e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:

a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).

b. Click *Save Configuration File as* and accept the default name (default.cfg).

The configuration settings stored in default.cfg are restored every time the server is restarted.

c. Click *OK*.

---

**Finishing the deployment afer installing Sametime Advanced**

After you have installed your prerequisite components and IBM Sametime Advanced, complete your deployment by configuring connections to supporting servers.

**About this task**

Finish deploying Sametime Advanced by completing these tasks:

**Configuring a mail server after installing Sametime Advanced**

Configure a mail server for use with an IBM Sametime Advanced deployment.

**About this task**

Follow these steps to configure a mail server for the Sametime Advanced deployment:

**Procedure**

1. Log in to the Integrated Solutions Console as an IBM WebSphere Application Server administrator.
   - In a single-server deployment, log in from the Sametime Advanced server.
   - In a clustered deployment, log in from the cluster's Deployment Manager.
2. Click **Resources > Mail > Mail Sessions**.
3. In the 'Mail Sessions' screen, expand the **Scope** section and select a scope:
• In a single-server deployment the scope is a server, so select your server from the list (for example: Node=node_name, Server=server1).
• In a clustered deployment the scope is a cluster, so select your cluster from the list.

4. In the table, click the New button to create a new mail session.
5. Fill out the new mail session form as follows:
   On this form, some fields have information supplied already, which you can accept or modify; you must provide values for the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the mail server; for example: Sametime Mail Notifier</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>Provide an associated JNDI name; use: mail/sametime/notifier</td>
</tr>
<tr>
<td>Mail transport host</td>
<td>Provide the fully qualified host name of your SMTP server; for example: sales.example.com</td>
</tr>
<tr>
<td>Mail transport protocol</td>
<td>Select the mail transport protocol; in this example, it would be SMTP</td>
</tr>
<tr>
<td></td>
<td>You can optionally supply a user name and password for the SMTP server; this is only necessary when your SMTP server requires them for authentication before sending email.</td>
</tr>
<tr>
<td>Mail from</td>
<td>Type the email address to be used as the “From” address when sending notifications.</td>
</tr>
</tbody>
</table>

6. Click OK to save your settings.

**Configuring connectivity to a Sametime proxy server after installing Sametime Advanced**

Connecting IBM Sametime Advanced to a Sametime Proxy server activates the awareness feature that detects when a user is online for users who are in a browser.

**Before you begin**

You must have a Sametime Proxy Server installed and configured. You must set up Single Sign-On between the Sametime Advanced and the Sametime Community Server.

**About this task**

Provide information about the Sametime Proxy Server by editing the Administrative Settings configuration page of the Sametime Advanced server.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Advanced Servers**.
3. In the **Sametime Advanced Servers** list, click the deployment name of the server with the information that you want to add or change.
4. Click the **Administrative Settings** tab.

5. In the Sametime Proxy Server section, specify the host name, port, and protocol for the proxy server you configured. If you have configured the Sametime Proxy Server behind a reverse proxy, use those connection settings here as appropriate.
   - **Host name**
     Enter the fully qualified host name of the proxy server. This is the same host name that you provided when you created a deployment plan before installing the proxy server.
     For example: `sametime_proxy.example.com`
   - **Port**
     The port the proxy server is running on.
   - **Protocol**
     Use HTTP for regular connections. Use HTTPS if the Sametime Proxy server is secured with SSL.

   **Note:** If you are configuring your environment with SSL, you should use a public certificate from a Trusted Root Certificate Authority. If you instead configure your environment with self-signed certificates, then the certificate from the Sametime Proxy server must be imported into the browser for awareness on the Sametime Advanced pages to work. You will be prompted to accept the self-signed certificate from the Sametime Advanced server when you visit the page, but you will not be prompted to accept the certificate from the Sametime Proxy server. You can either import this certificate manually, or navigate to the web client on the Sametime Proxy server where you will be prompted to accept it.

6. Click **OK**.
   Sametime Advanced automatically makes the changes without restarting the server.

**Related tasks**

- “Configuring Single Sign-On for Sametime Advanced” on page 99
  You must configure servers for single sign-on (SSO) in an IBM Sametime Advanced deployment.
- “Configuring SSL for Sametime Advanced” on page 99
  Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

---

**Deploying Sametime Proxy Server, Sametime Meeting Server, or Sametime Advanced on one machine**

If you deploy the Sametime Proxy Server or Sametime Meeting Server with Sametime Advanced on one machine, configure the servers to have the same host name, then configure Sametime Advanced to use that Sametime Proxy Server for awareness because users cannot get awareness on the Sametime Advanced pages.

**About this task**

This occurs because WebSphere Application Server sets the JSESSIONID cookie whenever an application is started, and the JSESSIONID cookie is overwritten when the Sametime Proxy Server or Sametime Meeting Server and Sametime...
Advanced share a host name. Because they have matching host names, the
WebSphere Application Server JSESSIONID does not recognize them as separate
applications. Avoid this by providing the Lotus® Sametime Proxy Server or
Sametime Meeting Server with a host alias whose host name different from the
Sametime Advanced host name.

An example of a host alias is stproxy. For more information on host alias settings,
see “Host alias settings” in the WebSphere Application Server information center:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

Procedure
1. Install Sametime Advanced, Sametime Proxy Server, or Sametime Meeting
   Server on the same server.
2. Change the host name of the Sametime Proxy Server or Sametime Meeting
   Server using a host alias:
   a. Log in to the Integrated Solutions Console on the Sametime Proxy Server or
      Sametime Meeting Server.
   b. Click Environment > Virtual Hosts > default_host > Host Aliases.
   c. Configure the host aliases of the Virtual Host, default_host, of the Lotus
      Sametime Proxy Server or Sametime Meeting Server so that their host
      names do not match either the host name of Sametime Advanced or the
      wild card character, ‘*’ (asterisk).
      The new host name alias must refer to the IP address at the DNS level, so
      that the machines will be able to ping the Web server by using the host
      name. Update the host name of all of the host alias entries to the host name
      that the Sametime Proxy Server or Sametime Meeting Server will use. Use
      the same host name for all aliases.
      1) Click the host name link associated with each port.
      2) Enter the fully qualified host name for the Sametime Proxy Server or
         Sametime Meeting Server. It must not be the same host name assigned
         to Sametime Advanced.
      3) Click Apply, and then click Save.
   d. Restart the Sametime Proxy Server or Sametime Meeting Server.
3. On the Sametime System Console, go to the configuration page for Sametime
   Advanced and update the host name to match the host name alias you created
   for the Proxy Server or Meeting Server.
   a. Log in to the Integrated Solutions Console.
   b. Click Sametime System Console > Sametime Servers > Sametime
      Advanced Servers.
   c. In the Sametime Advanced Servers list, click the deployment name of the
      server with the information that you want to add or change.
   d. Click the Administrative Settings tab.
   e. In the Sametime Proxy Server or Sametime Meeting Server section, modify
      the host name to reflect the new host alias you created.
4. Click OK.

Starting and stopping the database instance and text indexing service

The text indexing service required by IBM Sametime Advanced must be started
and stopped when the database is started and stopped using the following
commands.
About this task

The command to start the database instance on all platforms is:
\texttt{db2start}

The command to start the Net Search Extender (NSE) service is:
\texttt{db2text start}

To stop the database instance, run:
\texttt{db2stop}

To stop the NSE service, run:
\texttt{db2text stop}

Starting and stopping Sametime Advanced servers

The procedures for starting and stopping Sametime Advanced are similar to other Sametime servers running on IBM WebSphere Application Server.

About this task

For more information about ways to start and stop Sametime Advanced, see Starting and stopping servers running on WebSphere Application Server in the Installing section of Administering Sametime Standard.

Uninstalling Sametime Advanced

The procedures for uninstalling Sametime Advanced are similar to other Sametime servers running on IBM WebSphere Application Server.

About this task

For more information about ways to uninstall Sametime Advanced, see Uninstalling in the Installing section of Administering Sametime Standard.

Deploying Sametime Advanced to clients

IBM Sametime Advanced is delivered to clients as a plug-in.

About this task

For more information about ways to enable the Advanced client plug-in, see Deploying the Sametime client to users in the Installing section of Administering Sametime Standard.

Enabling Sametime Advanced persistent chat rooms and broadcast communities after installing

The IBM Sametime Connect client, both standalone and integrated with Lotus Notes, includes plug-ins that were available separately in previous releases.
About this task

Administrators have different options to enable the Advanced plug-ins for users who are licensed to use Sametime Advanced. Administrators must explicitly enable the Advanced plug-ins even for clients upgrading from earlier releases of Sametime Advanced.

`com.ibm.collaboration.realtime/enableAdvanced=false`

Set this preference to `true` to enable the Sametime Advanced client.

**Sametime Advanced client preferences**

The following table lists the preferences for the Sametime Advanced client, for sites that have installed Sametime Advanced. The Sametime Advanced client is a plugin added to the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

*Table 2. Global Preferences - com.ibm.collaboration.realtime*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableAdvanced</td>
<td>Boolean</td>
<td>Applies to Sametime Advanced only. When the value is set to <code>true</code>, the Sametime Advanced plug-ins installed with the client become active.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>enableInstantShare</td>
<td>Boolean</td>
<td>Applies to Sametime Advanced only. If <code>enableAdvanced</code> is set to <code>false</code>, but the value of <code>enableInstantShare</code> is set to <code>true</code>, the instant share feature is available. Otherwise, the value of <code>enableInstantShare</code> is ignored.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>sametimeAdvancedServer</td>
<td>String</td>
<td><strong>Required.</strong> Fully qualified WebSphere Application Server host name, for example: sales.</td>
<td></td>
</tr>
<tr>
<td>sametimeAdvancedServerPort</td>
<td>String</td>
<td><strong>Required.</strong> Sametime Advanced server port number.</td>
<td></td>
</tr>
<tr>
<td>sametimeCommunityServer</td>
<td>String</td>
<td><strong>Required.</strong> Default Sametime community host name. This is the server users log in to for awareness and chat.</td>
<td></td>
</tr>
<tr>
<td>broadcastToolsServer</td>
<td>String</td>
<td><strong>Required.</strong> Fully qualified WebSphere Application Server host name.</td>
<td></td>
</tr>
</tbody>
</table>
Table 2. Global Preferences - com.ibm.collaboration.realtime (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcastToolsServerPort</td>
<td>String</td>
<td>Required. WebSphere Application Server port number. The port number is normally 1883 for HTTP and 8883 for SSL, but can be any port specified by the administrator.</td>
<td></td>
</tr>
<tr>
<td>useHTTPS</td>
<td>Boolean</td>
<td>If you are using SSL while connecting to the server, set to true. If you are using HTTP set to false.</td>
<td></td>
</tr>
<tr>
<td>advancedServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Sametime Advanced server. Set to 0 for a direct connection to the server. Set to 1 to connect through a reverse proxy.</td>
<td></td>
</tr>
<tr>
<td>broadcastServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Broadcast tools server. Set to 1 for a direct connection to the server. Set to 2 to connect using SSL.</td>
<td></td>
</tr>
<tr>
<td>useHttpProxy</td>
<td>Boolean</td>
<td>Set to true if you are using an HTTP forward proxy, otherwise set it to false.</td>
<td></td>
</tr>
<tr>
<td>proxyHost</td>
<td>String</td>
<td>Enter the proxy IP address or host name if you are using a HTTP proxy, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>proxyPort</td>
<td>String</td>
<td>Enter the HTTP proxy port to which you are connecting.</td>
<td></td>
</tr>
<tr>
<td>proxyUserName</td>
<td>String</td>
<td>Enter the user name if the HTTP proxy requires one for authentication, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>reverseProxyBaseURL</td>
<td>String</td>
<td>Enter the reverse proxy base URL to use if connecting through a reverse proxy. For example: <a href="http://mycompany.com/mycontext">http://mycompany.com/mycontext</a>. Leave blank otherwise.</td>
<td></td>
</tr>
<tr>
<td>reverseProxyUserName</td>
<td>String</td>
<td>Enter the reverse proxy user name if the proxy is authenticating. Leave blank if you are not using reverse proxies.</td>
<td></td>
</tr>
<tr>
<td>jmsProtocol</td>
<td>String</td>
<td>Indicates whether the client connects with a secure connection using the Security Secure Sockets Layer (SSL) or not. The default is disthub (to connect without SSL). Enter disthubs to connect with SSL.</td>
<td></td>
</tr>
<tr>
<td>liveNameResolveTimeout</td>
<td>String</td>
<td>Time allowed in milliseconds for awareness names to resolve. The default is 10000.</td>
<td></td>
</tr>
<tr>
<td>notifyNewOpenCommunities</td>
<td>Boolean</td>
<td>Alert users when a new open community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewModeratedCommunities</td>
<td>Boolean</td>
<td>Alert users when a new moderated community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewPrivateCommunities</td>
<td>Boolean</td>
<td>Alert users when a new private community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnDoNotDisturb</td>
<td>Boolean</td>
<td>Blocks broadcasts when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnInMeeting</td>
<td>Boolean</td>
<td>Blocks broadcast when user is in a meeting. The default is false. Set to true to block broadcasts when user is in a meeting.</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>notifyChatRoomAddMember</td>
<td>boolean</td>
<td>Alert users when a chat room has a new member. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnDoNotDisturb</td>
<td>boolean</td>
<td>Blocks chat room notifications when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnInMeeting</td>
<td>boolean</td>
<td>Blocks chat room notifications when user is in a meeting. The default is false. Set to true to block chat room notifications when user is in a meeting.</td>
<td></td>
</tr>
<tr>
<td>broadcastServerUserIdType</td>
<td>string</td>
<td>The default is &quot;email&quot; to use the Sametime ID's email directory field. You need to use the same property value to log in to both the Sametime client and Sametime Advanced.</td>
<td></td>
</tr>
<tr>
<td>useTokens</td>
<td>boolean</td>
<td>Determines whether or not the client uses LTPA token at login. The default is true. Set this to false only if there is no way to set up Single Sign-on between the Sametime and Sametime Advanced servers.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Community Preferences - com.ibm.collaboration.community

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginTokenRefreshInterval</td>
<td>integer</td>
<td>LTPA token timeout in seconds. IBM recommends 86100000 (23 hours and 55 minutes).</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| appsharePreference     | String        | Set the *instantshare* plug-in to use the application sharing component of either the Sametime Meeting Server or the Sametime Classic meeting service:  
• 1 - Try the Sametime Meeting Server application sharing component, and if it fails try the Sametime Classic meeting service application sharing component (default).  
• 2 - Use only the Sametime Meeting Server application sharing component.  
• 3 - Use only the Sametime Classic meeting service application sharing component. |         |
<p>| useAlternateServer     | Boolean       | If the value is true, instant share uses the host name defined by alternateMeetingServer for instant share sessions. The default is false. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use. |         |
| alternateMeetingServer | String        | If the value of useAlternateServer is true, enter a host name here. Instant share uses the host name defined by alternateMeetingServer for instant share sessions. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use. |         |</p>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>useTokens</td>
<td>Boolean</td>
<td>Set to &quot;true&quot; only if InstantShare is configured to use an alternate server and LTPA token is required at login.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4. Migrating and upgrading Sametime Advanced

Migrate data from a previous version of IBM Sametime Advanced and upgrade one or more servers to take advantage of the latest features. This section contains information about installing and configuring Sametime Advanced, while maintaining as much legacy data as possible, if you have used previous versions of the product.

Upgrading from Sametime Advanced 8.0.x

First upgrade database components, then upgrade servers in an IBM Sametime Advanced deployment to take advantage of the latest features.

Related concepts
“Planning for migration from an earlier release of Sametime Advanced” on page 7

Your approach to upgrading from an earlier release of IBM Sametime Advanced depends on the version of DB2 you want to use for storing the Sametime Advanced database. Upgrading then involves updating the database components, installing Sametime Advanced Server, and registering the server with the Sametime System Console.

Backing up the DB2 database before upgrading Sametime Advanced

Before upgrading from an earlier release of IBM Sametime Advanced, back up the database.

Procedure
1. Prepare for upgrading by shutting down the servers running the current release of Sametime Advanced. Stop the Sametime Advanced server and Event Broker. Refer to the Sametime Advanced information center for instructions about starting and stopping servers.
2. Back up the existing database:
   a. Log in to the DB2 server as the DB2 administrator (or as a user in the DB2ADMNS group).
   b. Open a DB2 command window.
   c. Run the following command in the DB2 command window to locate the DB2 recovery log location for the Sametime Advanced database. This procedure assumes you used the name STADV for the database.
      
      ```
      db2 GET DB CFG FOR STADV
      ```
       Review the output for the STADV database and locate the "Path to log files" section. Write down the path and file name for the recovery log.
   d. Run the command to back up the Sametime Advanced database.
      
      ```
      db2 BACKUP DATABASE STADV
      ```
   e. As a precaution, save the backup and recovery logs to another computer or to a flash drive in case you encounter problems upgrading.
Migrating to DB2 Workgroup Edition

Unless you decided to keep the IBM DB2 Enterprise Edition Server you already have, you can either upgrade the DB2 server to the newest release and keep the Sametime Advanced database on that server or move the database to a DB2 server already in use for other Sametime components.

Upgrading a dedicated DB2 server to DB2 Workgroup Edition


Before you begin

If you are currently running DB2 on a 32-bit Linux server and want to run DB2 9.7, you must upgrade the server to 64-bit and use the 64-bit version of DB2 9.7 before proceeding.

About this task

After backing up the Sametime Advanced database, follow these steps to upgrade the DB2 server and maintain the Sametime Advanced database separately from other Sametime databases.

Procedure

1. Start the DB2 server and open a command window.
2. Run the following command to get a list of the contents of the system database directory.
   
   ```
   db2 LIST DATABASE DIRECTORY
   ```
   
   Save the information.
   
   See Uninstalling in the DB2 information center.
   
   “Installing DB2 on Linux or Windows” on page 251
5. Install DB2 Net Search Extender.
6. Run the following command to catalog the database using the information from the list database directory command.
   
   ```
   db2 CATALOG DATABASE STADV on drive c:
   ```
7. Update the database to DB2 9.7.
   
   Follow the steps in the DB2 information center for your operating system:
   
   Windows
   
   Linux
What to do next

You can now remove the Broker database from the Sametime Advanced 8.0.1 release.

**Moving the Sametime Advanced database to a shared DB2 server**

Move the existing IBM Sametime Advanced database to a DB2 server already in use for other Sametime components to keep all Sametime database components on one computer.

**About this task**

After backing up the Sametime Advanced database, follow these steps to update the Advanced database and move it to the shared DB2 server used by the Sametime System Console and the Sametime Meeting Server.

**Procedure**

1. Start the older DB2 Enterprise Edition server.
2. Log in to the DB2 server as the DB2 administrator (or as a user in the DB2ADMNS group).
3. Open a DB2 command window.
4. Run the following command to get a list of the contents of the system database directory.
   ```
   db2 LIST DATABASE DIRECTORY
   ```
   Save the information.
5. Run the following command to catalog the database using the information from the list database directory command.
   ```
   db2 CATALOG DATABASE STADV on drive c:
   ```
7. Move the database file to the shared Sametime DB2 server.
8. Use the RESTORE command to restore the database on the new server.
   ```
   db2 restore database STADV from backup_directory
   ```
   For more information about the RESTORE command, see the DB2 information center:
   ```
   RESTORE DATABASE command
   ```
   Follow the steps in the DB2 information center for your operating system:
   ```
   Windows
   Linux
   ```
10. Close the command window.

**Results**

Verify that the new database was created either from the command line or by using the DB2 control center.

**From the command line**

View the output from running the create script and enter the following command:
db2 connect to STADV

where STADV represents the name of the database you created. Verify that you can connect to the database.

From the DB2 control center
- AIX, Linux, or Solaris
  Open the IBM DB2 folder on the desktop and click Control Center.
- Windows
  Click Start > Programs > IBM DB2 > General Administration Tools > Control Center.

Updating the Advanced database schema
Before upgrading to this release of IBM Sametime Advanced, update the database schema to ensure that the latest features are stored correctly in the database.

About this task
Update the database regardless of which version of DB2 you are running.

Procedure
1. On the DB2 machine, log in with the database administrator account.
2. Open a DB2 command window.
3. From the command line, enter
   db2
4. Enter the command to connect to the Sametime Advanced database
   connect to advanced_database_name
   where advanced_database_name is the name of the Sametime Advanced database.
5. Run the following command to update the database schema:
   db2 -tf migration_ST852.ddl

Updating text indexes for searching the Sametime Advanced database
Creating text indexes is a requirement for making content in the IBM Sametime Advanced database searchable.

Before you begin
You must have installed the IBM DB2 server software and DB2 Net Search Extender, then started those applications, and created a database.

About this task
Use the dbtext.bat and dbtext.sh files provided with the Sametime Advanced software download to run the Net Search Extender services. If the indexes ever become corrupted, you can safely rerun the dbtext scripts at any time without losing any existing data.

Procedure
1. Download the appropriate version of the dbtext script for your operating system to the DB2 server.
The scripts are stored in the STAdvancedLaunchpad\disk1\DatabaseScripts directory within the Sametime Advanced software download.

a. To download installation packages for Sametime Advanced:

1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address:
   &uid=swg24027364
   Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

   Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   AIX
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   ```bash
   mount -v cdrfs -o ro /dev/cd0 /cdrom
   ```

   Linux
   Mount the CD or DVD using a command similar to the following command:
   ```bash
   mount /dev/cdrom /cdrom
   ```

2. With the DB2 command window open, start Net Search Extender by running the following command.

   `db2text` start

   DB2 Net Search Extender must be running to support Sametime Advanced operations. If you stop this service for any reason, be sure to restart it. To remove the need for manual restarts, you may want to set this service to start automatically:

   - AIX, Linux, Solaris: Add the text indexing service startup to the database startup script.
   - Windows: Set the "DB2TEXT" service to "Automatic" in the Windows Services control panel.

3. Run the following command to create the text indexes:

   **AIX, Linux, Solaris**
   ```bash
   ./dbtext.sh database_name
   ```

   **Windows**
   ```bash
   dbtext.bat database_name
   ```

   Replace `database_name` with the name of the Advanced database; for example, STADV.
4. Once the script successfully completes, you can disconnect from the database with the following command:
   
   ```
   DB2 DISCONNECT STADV
   ```

5. Now type the following command in the DB2 Command Window:
   
   ```
   EXIT
   ```

6. Close the DB2 Command Window.

**What to do next**

If the `dbtext.sh` script does not successfully enable text searching for AIX, Linux, or Solaris, perform the following workaround to enable text searching:

1. In a DB2 command window, change to the `sql1lib/adm` directory:
   
   ```
   cd ~/sql1lib/adm
   ```

2. Enter this command:
   
   ```
   ls -a .fenced
   ```

3. Run the `dbtext.sh` script again by repeating Steps 3 - 6 in the above procedure.

   If the group of `.fenced` differs from the primary group of the database instance, follow these steps to correct the ownership:

   1. In a DB2 command window, enter this command to stop the `db2text` service:
      
      ```
      db2text stop
      ```

   2. Stop DB2:
      
      ```
      db2stop
      ```

   3. Change to the `sql1lib/adm` directory:
      
      ```
      cd ~/sql1lib/adm
      ```

   4. Enter this command:
      
      ```
      rm .fenced
      ```

   5. Enter this command to correct the ownership:
      
      ```
      touch .fenced
      ```

   6. Start DB2:
      
      ```
      db2start
      ```

   7. Start the `db2text` service:
      
      ```
      db2text start
      ```

   8. Run the `dbtext.sh` script again by repeating Steps 3 - 6 in the above procedure.

**Related information**

- Starting and stopping Net Search Extender instance services using the command line

**Upgrading Sametime Advanced**

Run the installation program on the computer running an earlier release of IBM Sametime Advanced.
Before you begin

Use the Installation Manager installation program to upgrade from an earlier release of Sametime Advanced. Be sure there are no firewalls or connectivity problems to the LDAP server or the installation will fail. The DB2 server must be running.

**Linux**  The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**  If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:**  Check the hosts file and remove any lines that start with the following:

- `127.0.0.1 fully_qualified_domain_name short_name`
- `::1 fully_qualified_domain_name short_name`

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

About this task

Installing this release of Sametime Advanced upgrades the software and copies the existing WebSphere Application Server configuration to the new release.

Procedure

1. **Red Hat Enterprise Linux only:** Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the `SELINUX` setting. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Prepare to use the installation package.
   a. To download installation packages for Sametime Advanced:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
2) Open this release’s Download document at the following web address:
&uid=swg24027364
Locate the components that you need in the document’s listing, then
download the packages labelled with the corresponding part numbers
to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a
short path location such as C: \ and not a long path location such as
the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:
`mount -v cdrfs -o ro /dev/cd0 /cdrom`

Linux
Mount the CD or DVD using a command similar to the following
command:
`mount /dev/cdrom /cdrom`

4. Navigate to the folder where you stored the downloaded files and start the
installation program by running one of the following commands:
• **AIX, Linux, and Solaris.** `./launchpad.sh`
• **Windows** `launchpad.exe`

**Note:** If you do not have a web browser, go to the Installation Manager
package directory and run the installation program (`install` for Linux or
`install.exe` for Windows). Find the Installation Manager package directory
here:

`sametime_server_package/IM/platform`

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language
list.

6. Click **Install IBM Sametime Advanced Server** and click **Launch IBM
Sametime Advanced Server 8.5.2 installation.**

7. If the IBM Installation Manager is not installed, you are prompted to install
Installation Manager. Do so, then click Finish to restart the Installation
Manager and continue with the next step of the Sametime installation.
If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the
automatic web update search to allow the installation to run successfully.
a. In the Installation Manager window, choose **File > Preferences.**
b. Uncheck **Search service repositories during installation and updates** and click OK.

9. Click **Install**.

10. Select the packages that you want to install and click **Next**.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Select a package group option and accept the installation directory. Then click **Next**.

   Select **Create a new package group** if you have not installed any other Sametime software on this machine.

   Leave **Use the existing package group** selected if you are installing several Sametime servers on the same machine.

13. Select **IBM Sametime Advanced Server 8.5.2** as the feature to install. Do not select **Use Sametime System Console to install**. Click **Next**.

14. At the WebSphere Application Server Location screen, select **Use Sametime installed WebSphere Application Server** and click **Next**.

15. At the Import Existing Configuration screen, select **Import the configuration data from an existing Sametime Advanced Server 8.0.1** and provide the locations for the existing servers. Enter the fully qualified Host Name and click **Validate**.

   After validating, click **Next**.

16. At the WebSphere Application Server Configuration screen, click **Next**. The upgrade uses the profile type used by the Sametime Advanced 8.0.x server, so you do not make any selections.

17. At the credentials screen, click **Next**. The upgrade uses values from the previous release.

18. At the Configure DB2 for the Advanced Server screen, click **Next**.

19. At the LDAP screen, click **Next**.

20. Review the summary, then click **Install** to start the installation.

21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the ant and native subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**

```
/var/ibm/InstallationManager/logs

Console connection log: /tmp/SSCLogs/ConsoleUtility0.log
```

**Windows 2008**

```
%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log
```

**Windows 2003**

```
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
```
Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 481
Starting and stopping IBM Sametime servers that run on WebSphere Application Server involves other server components such as the Deployment Manager and the node agent.
“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.
“Registering and federating an upgraded Advanced server” on page 71
After upgrading an IBM Sametime Advanced server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows, register it with the Sametime System Console, so you can manage all of the Sametime servers from a central location.

Updating broadcast communities and chat rooms
After upgrading to this release of IBM Sametime Advanced, migrate broadcast communities so they are available for use after the upgrade. Update database timestamps to make timestamps correct for existing chat rooms, chat transcripts, and FAQs created before the upgrade.

Before you begin
Confirm that you have backed up the database and upgraded the server.

About this task
If you are a Sametime Advanced administrator, follow these steps to migrate broadcast communities and update database timestamps.

Procedure
1. Working on the Sametime Advanced server, copy the AdvancedMigration.jar and advancedmigration.properties files from the installation package or media to a temporary directory. The files are located in the AdvancedMigration directory.
2. Edit the advancedmigration.properties file to point to the fully qualified server host name and port running Sametime Advanced.
3. Open a command window and change directories to the temporary directory where you copied the files.
4. Enter the following commands on one line to migrate the broadcast communities:
   Linux
   Windows
   set CLASSPATH= .\AdvancedMigration.jar;WAS_HOME\plugins\com.ibm.ws.runtime.jar java com.ibm.stadvanced.cmdline.AdvancedMigration -c adminUser adminUser
   where:
 WAS_HOME is the location of the WebSphere Application Server Appserver
directory.

adminUser is the email address for the Sametime Advanced administrator.

adminUserPassword is the password for the Sametime Advanced
administrator.

5. Review the output file, communitymigration_time.xml, after the command runs.

6. Enter the following commands on one line to update the database timestamps.

    Important: Update the database timestamp one time only. Contact IBM
    Support if you run into issues with the update; do not attempt to run the
    update again.

    Linux
    CLASSPATH="./AdvancedMigration.jar:WAS_HOME/plugins/com.ibm.ws.runtime.jar" export CLASSPATH
    java com.ibm.stadvanced.cmdline.AdvancedMigration -t

    Windows
    set CLASSPATH=.\AdvancedMigration.jar;WAS_HOME\plugins\com.ibm.ws.runtime.jar java
    com.ibm.stadvanced.cmdline.AdvancedMigration -t adminUser adminUserPassword

    where:
    • WAS_HOME is the location of the WebSphere Application Server Appserver
directory.
    • adminUser is the email address for the Sametime Advanced administrator.
    • adminUserPassword is the password for the Sametime Advanced
    administrator.

7. Review the output file, updatetimestamp_time.xml, after the command runs.

Registering and federating an upgraded Advanced server

After upgrading an IBM Sametime Advanced server on IBM AIX, Linux, Sun
Solaris, or Microsoft Windows, register it with the Sametime System Console, so
you can manage all of the Sametime servers from a central location.

Before you begin

Verify that the Deployment Manager, the Sametime System Console server, and the
Sametime Advanced server are running.

About this task

During this task you will edit the following files; click the topic titles below to see
details on each file. You may want to open each topic in a new browser tab or
window so you can keep it open for reference:

• console.properties
• productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. On the server to be registered, navigate to the InstallLocation/console
directory.
   b. Make backup copies (using different names) of the console.properties and
      productConfig.properties files.

2. Update the following values in the console.properties file and save the file.
Table 5. console.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
<td>Provide the fully qualified host name of the Sametime System Console server.</td>
</tr>
</tbody>
</table>
| SSCHTTPPort           | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is “false.”
|                       | To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the “HTTP transport port.” The default profile name is STSCAppProfile. For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt |
| SSCUserName           | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin. |
| SSCPassword           | Enter the WebSphere Application Server password associated with the SSCUserName.               |
| SSCSSLEnabled         | Change this value to “true” to connect to the Sametime System Console using a secure connection. |
| SSCHTTPSPort          | Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to “true.” |

3. Verify that the following settings in the productConfig.properties file are correct. Modify them as needed before saving and closing the file. You will need to add the passwords.

Table 6. Sametime Advanced

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Manager Hostname</td>
<td>The fully qualified host name for the WebSphere Application Server Deployment Manager.</td>
</tr>
<tr>
<td>SOAP port</td>
<td>The SOAP port for the WebSphere Application Server Deployment Manager.</td>
</tr>
</tbody>
</table>

4. Now register and federate the server:
   a. Run the registration utility from the /console directory.
      - AIX, Linux, Solaris: ./registerProduct.sh -federateNode
      - Windows: registerProduct.bat -federateNode

   The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the registration is successful, a console.pid file will be added.

**Verifying a Sametime Advanced upgrade**

Log in to the IBM Sametime Advanced Server to verify that the installation was successful.

**About this task**

Verify the installation by setting up a test client and logging in to the server.
Procedure

1. Set up a Sametime client to test the installation:
   • Install the latest Sametime client.
   • Enable the Sametime Advanced client plugin by setting this preference:
     com.ibm.collaboration.realtime/enableAdvanced=true
   • Change these preferences. Under Chat Rooms and Broadcast Tools, enter the
     Broadcast Tools Server name and port 1883. Enter the Sametime Advanced
     Server name and port 9080.
     The Advanced server HTTP port is usually 9080, but may be different.
     Specify the port for your environment.

2. From a web browser, access the Sametime Advanced server by entering the
   following URL:
   http://serverhostname.domain:port/stadvanced

3. Verify that chat rooms and broadcast communities connect to the Advanced
   server correctly.

Related tasks

“Enabling Sametime Advanced persistent chat rooms and broadcast communities
after installing” on page 53

The IBM Sametime Connect client, both standalone and integrated with Lotus
Notes, includes plug-ins that were available separately in previous releases.

Removing obsolete components after upgrading Sametime Advanced

After verifying the IBM Sametime Advanced upgrade, remove the obsolete
components.

About this task

You can remove the following components, depending on the type of upgrade you
chose:
• Remove the Broker database used with Advanced 8.0.1.
• If you moved the Advanced database to a new DB2 server to share with other
  Sametime components, remove the Advanced 8.0.1 database from the original
  DB2 server.
• Uninstall Event Broker from the server that was used for that program.

Clustering Sametime Advanced after upgrading

Configuring a cluster of IBM Sametime Advanced servers involves several tasks,
including synchronizing system clocks, configuring the cluster settings, and
deploying a load balancer in front of the cluster, either deploying IBM Load
Balancer or another load balancer product.

Before you begin

You can create two types of clusters:
• A **Vertical cluster** resides on the Primary node and includes two or more cluster
  members, which run the same application.
• A **Horizontal cluster** includes a Primary node plus one or mode Secondary
  nodes, all running the same application.
Before you can configure a cluster of Sametime Advanced servers, you must have installed the following servers:

- **The Sametime System Console**
  This server can function as the Deployment Manager for the vertical or horizontal cluster scenarios described in this procedure.
  
  **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Meeting server cluster, a Media Manager cluster, and an Advanced server cluster. If you want to create additional clusters for a particular product, you must deploy additional Deployment Managers.

- **Sametime Community Servers**
  At least one Sametime Community Server must be deployed. The Community Server provides presence and awareness for chats.

- **One Sametime Advanced server installed with the Network Deployment > Primary Node option.**
  Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster’s application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node's application server. The Primary node's application server can only belong to one cluster. The Primary Node can be used as a...
container for additional cluster members when creating a vertical cluster (multiple cluster members on the same physical system).

- (Horizontal cluster only) One or more servers installed with the Network Deployment > Secondary Node option.
  
  Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as containers for additional cluster members, which can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a horizontal cluster (one cluster member on each Secondary Node, plus one cluster member or one vertical cluster on the Primary Node).

**About this task**

There are several tasks involved in creating a cluster; complete them in the sequence shown here:

**Attention:** Complete all of the tasks to ensure your cluster operates properly.

**Related concepts**

“Clustering Sametime servers for high enterprise availability” on page 227

In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

**Setting clocks on the upgraded Sametime Advanced servers to be clustered**

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.

**About this task**

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.

**Procedure**

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager's (the Sametime System Console) system clock.

**Clustering upgraded Sametime Advanced servers**

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

**Before you begin**

Start the Sametime System Console and the servers you intend to cluster.
Note: This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.
3. On the left side of the navigation tree, click the Sametime System Console task to open it.
4. Click Guided Activities > Cluster WebSphere Application Servers.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Clustering upgraded Sametime Advanced servers

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.
   This guided activity applies to the following Sametime servers if they are installed in your deployment.
   • Sametime Proxy Server
   • Sametime Meeting Server
   • Sametime Media Manager
     Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.
   • Sametime Advanced
2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster's Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager's SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

Procedure

1. Cluster WebSphere Application Servers.
   Click Next to begin the clustering activity.
2. Select Product to Cluster.
   Select the product server to cluster, and then click Next.
   The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually
register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).

3. Select or Create a Cluster.
   To create a cluster:
   a. Click **Create Cluster** if you are setting up a new cluster.
   b. Type a descriptive name for the cluster in the **Cluster Name** field.
      For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.
   c. Click **Next**.
   To modify an existing cluster; for example, to add a new cluster member:
   a. Click **Select Existing Cluster**.
   b. Select a cluster in the **Cluster Name** list.
   c. Click **Next**.

4. Select the Deployment Manager.
   In the **Select Deployment Manager** list, select the Sametime System Console as the cluster's deployment manager, and then click **Next**.
   Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters.
   Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.

5. Create the Cluster with the Primary Node.
   You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node's application server is running. Click **Create cluster** to configure the cluster settings, and then click **Next**.
   Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. Select One or More Secondary Nodes.
   If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the **Secondary Node Name** list, click the node you want to add to the cluster and click **Next**.

7. Add Cluster Members.
   If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more "cluster members" to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.
   The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be "Clustered" if the cluster member has been
completely configured on the node. If the status is "Ready to Cluster", select the Cluster Member and use the "Add to Cluster" button to finish configuring the cluster member.

**Vertical cluster:**
- a. To add new cluster member, click **New**.
- b. Select the default name generated for the cluster member or enter your own cluster member server name.
- c. Select the Primary Node to create the cluster member on.
- d. Click **Add to Cluster**.
  - The status will change from "Ready to cluster" to "Clustered".
- e. Click **Next**.

**Horizontal cluster:**
For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.
- a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.
- b. One at a time, select each cluster member and click **Add to Cluster**.
  - Do not proceed until the current cluster member's status changes from "Ready to cluster" to "Clustered"; then you can add the next cluster member.
- c. If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.
- d. Click **Next**.

8. **Deployment Summary.**
- Click **Finish** to save the cluster configuration.
- Continue with the cluster configuration tasks described in the Sametime information center.

**Restarting the servers in the Sametime Advanced cluster**
After running the Clustering guided activity, synchronize the nodes in the cluster and restart the application servers.

**Restarting and synchronizing upgraded nodes in the Sametime Advanced cluster**
Synchronize the nodes in an IBM WebSphere Application Server network deployment.

**About this task**
Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node’s configuration.

**Procedure**
1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Stop the Deployment Manager:
   - a. Click **System Administration > Deployment manager**.
   - b. Click the "Configuration" tab.
   - c. On the Configuration tab of the deployment manager settings, click **Stop**.
3. Now start the Deployment Manager:
a. Open a command window and navigate to the `app_server_root/profiles/DeploymentManagerName/bin` directory.

b. Run the following command:

- **IBM AIX, Linux, or Solaris**
  ```
  ./startManager.sh
  ```
- **Microsoft Windows**
  ```
  startManager.bat
  ```
- **IBM i**
  1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.
  2) At the Qshell prompt, run the following commands:
     ```
     cd app_server_root/profiles/DeploymentManagerName/bin
     startManager dmgr
     ```

4. Log in to the Integrated Solutions Console.

5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes in the cluster.
   c. Click **Full Resynchronize**.

6. Restart all nodes in the cluster:
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Node agents**.
   b. Click a node agent, and then click **Restart** (the node agent should already be running).

**Restarting the upgraded application servers in the Sametime Advanced cluster**

During cluster configuration, each node's application server was stopped so that the node could be federated. Start all of the application servers now.

**About this task**

Use the IBM Sametime System Console to start each of the application servers in the cluster.

**Procedure**

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.

2. Click **Servers > Clusters > WebSphere application server clusters** in the navigation tree.

3. Select the cluster's check box and click **Start** to start all cluster member servers.

**Installing IBM Load Balancer in an upgraded Sametime Advanced cluster**

Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.
Before you begin

Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Note: The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.

IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure

1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
      Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
   For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.

3. After you have installed IBM Load Balancer, configure two static IP addresses for it:
   - Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
   - Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

   For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer:</td>
<td>Load balancer</td>
<td>Load balancer (NFA): 192.0.2.15</td>
</tr>
<tr>
<td>loadbal.example.com</td>
<td>(Cluster address)</td>
<td>Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>Cluster:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>st-cluster.example.com</td>
<td>Deployment Manager</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>(Sametime System Console)</td>
<td></td>
</tr>
</tbody>
</table>

| Table 7. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer |
Table 7. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer (continued)

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>svr1.example.com</td>
<td>Primary Node (a Sametime server)</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td>svr2.example.com</td>
<td>Secondary Node (a Sametime server)</td>
<td>192.0.2.5</td>
</tr>
</tbody>
</table>

**Configuring IBM Load Balancer in an upgraded Sametime Advanced cluster**
Configure IBM Load Balancer for a cluster of IBM Sametime servers.

**About this task**
The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

**Configuring IBM Load Balancer on AIX, Linux, or Solaris in an upgraded Sametime Advanced cluster:**
Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

**Before you begin**
Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

**About this task**
Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.

**Procedure**
1. Configure the nodes of the cluster.
   - **For cluster nodes running on AIX, Linux, and Solaris**
     Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   - **For cluster nodes running on IBM i**
     Use the **Add TCP/IP Interface** command to create a virtual IP address with the "cluster" IP address you want to use.
For example:
ADDTCPIFC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)

When the virtual TCP/IP interface is started, the server accepts packets for that address.

**Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFERENCES parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:

   IBM Load Balancer requires every node in the cluster to use the same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   **Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process with the following command:
      dsserver
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).
      **AIX**
      1) Run the following command:
         autoconf6
      2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
         start usr/bin/autoconf6 " " -A
      **Linux** Run the following command (you must be logged in as root):
      modprobe ipv6
      **Solaris** Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:
      ifconfig device inet6 plumb
      ifconfig device inet6 address/prefix up
   d. Start the executor function of the dispatcher:
      dscontrol executor start
   e. Add the cluster to the service:
      dscontrol cluster add cluster’s_fully_qualified_host_name
      where *cluster’s_fully_qualified_host_name* is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
      stms-cluster.example.com
   f. Add the cluster port:
dscontrol port add cluster's_fully_qualified_host_name@port
where cluster's_fully_qualified_host_name@port is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
stms-cluster.example.com@80

g. Add the nodes for which this server will balance workload:
dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node
where:

- cluster_host@port@primary_node indicates the cluster's fully qualified host name with the port appended as in the previous step, plus now with the primary node's fully qualified host name appended; for example:
stms-cluster.example.com@80@meetsvr1.example.com
- cluster_host@port@secondary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
stms-cluster.example.com@80@meetsvr2.example.com

h. Now start the Load Balancer administration interface with the following command:
./lbadmin

Note: If you have difficulty starting the administration interface, try stopping and then starting the executor and dsserver services before running the command again:
dsserver stop
dscontrol executor stop
dscontrol executor start
dsserver start
./lbadmin

4. Continue configuring Load Balancer as follows:
a. Add the cluster to the executor:
dscontrol executor add cluster's_fully_qualified_host_name
where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
stms-cluster.example.com

b. Start the manager:
dscontrol manager start
c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
dscontrol advisor start http 80

5. Define server affinity with a "sticky time":
By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.
The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

a. Open a command window on the load balancer server.
b. Stop the service with the following command:
   ```
   dsserver stop
   ```
c. Set the sticky time with the following command:
   ```
   dscontrol port set fully_qualified_host_name@port_number stickytime number_of_seconds
   ```
   Where:
   - `fully_qualified_host_name` is the fully qualified host name of the server where IBM Load Balancer runs.
   - `port_number` is the port that will be affected by the new sticky time setting.
   - `number_of_seconds` is the duration, in seconds, of the time that a client should "stick to" the specified port.
   
   For example:
   ```
   dscontrol port set myserver.com@80 stickytime 60
   ```

6. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
   b. Click Save Configuration File as and accept the default name (default.cfg).
      The configuration settings stored in default.cfg are restored every time the server is restarted.
   c. Click OK.

Configuring IBM Load Balancer on Windows in an upgraded Sametime Advanced cluster:

Configure IBM Load Balancer on a server running Microsoft Windows.

Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.
Procedure
1. Configure the nodes of the cluster.
   
   **For cluster nodes running on Windows**
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   **For cluster nodes running on IBM i**
   Use the **Add TCP/IP Interface** command to create a virtual IP address with the "cluster" IP address you want to use.
   For example:
   
   ```
   ADDTCPIFC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
   ```
   When the virtual TCP/IP interface is started, the server accepts packets for that address.

   **Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the **PREFIFC** parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   **Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process by clicking **Start > Control Panel > Administrative Tools > Services.** right-click **IBM Dispatcher (ULB),** and then click **Start.**
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      
      Run the following command while logged in as the Windows administrator:
      ```
      netsh interface ipv6 install
      ```
      This command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.
   d. Start the executor function of the dispatcher:
      ```
      dscontrol executor start
      ```
   e. Add the cluster to the service:
      ```
      dscontrol cluster add cluster's_fully_qualified_host_name
      ```
      where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
      ```
      stms-cluster.example.com
      ```
   f. Add the cluster port:
dscontrol port add cluster's_fully_qualified_host_name@port

where \textit{cluster's_fully_qualified_host_name@port} is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:

\texttt{stms-cluster.example.com@80}

g. Add the nodes for which this server will balance workload:

dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node

where:

- \textit{cluster_host@port@primary_node} indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:

\texttt{stms-cluster.example.com@80@meetsvr1.example.com}

- \textit{cluster_host@port@secondary_node} indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:

\texttt{stms-cluster.example.com@80@meetsvr2.example.com}

h. Add the cluster to the executor:

dscontrol executor add cluster's_fully_qualified_host_name

where \textit{cluster's_fully_qualified_host_name} is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

\texttt{stms-cluster.example.com}

i. Start the manager:

dscontrol manager start

j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):

dscontrol advisor start http 80

k. Now you can stop the service:

dsserver stop

l. Close the command window.

4. Define server affinity with a "sticky time":

By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

\textbf{Windows}

a. Start IBM Load Balancer.
b. In the navigation tree, select the Executor (the load balancer's non-forwarding IP address, which appears under its host name).

c. Click Configuration Settings.

d. In "Port-Specific Settings", change the Default sticky-time settings from 0 to 60 seconds, and click Update Configuration.

e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:

a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).

b. Click Save Configuration File as and accept the default name (default.cfg).

   The configuration settings stored in default.cfg are restored every time the server is restarted.

c. Click OK.

---

**Finishing the deployment after upgrading Sametime Advanced**

After you have installed your prerequisite components and IBM Sametime Advanced, complete your deployment by configuring connections to supporting servers.

**About this task**

Finish deploying Sametime Advanced by completing these tasks:

**Configuring a mail server after upgrading Sametime Advanced**

Configure a mail server for use with an IBM Sametime Advanced deployment.

**About this task**

Follow these steps to configure a mail server for the Sametime Advanced deployment:

**Procedure**

1. Log in to the Integrated Solutions Console as an IBM WebSphere Application Server administrator.
   - In a single-server deployment, log in from the Sametime Advanced server.
   - In a clustered deployment, log in from the cluster's Deployment Manager.

2. Click Resources > Mail > Mail Sessions.

3. In the "Mail Sessions" screen, expand the Scope section and select a scope:
   - In a single-server deployment the scope is a server, so select your server from the list (for example: Node=node_name, Server=server1).
   - In a clustered deployment the scope is a cluster, so select your cluster from the list.

4. In the table, click the New button to create a new mail session.

5. Fill out the new mail session form as follows:
   - On this form, some fields have information supplied already, which you can accept or modify; you must provide values for the following fields:
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the mail server; for example: Sametime Mail Notifier</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>Provide an associated JNDI name; use: mail/sametime/notifier</td>
</tr>
<tr>
<td>Mail transport host</td>
<td>Provide the fully qualified host name of your SMTP server; for example: sales.example.com</td>
</tr>
<tr>
<td>Mail transport protocol</td>
<td>Select the mail transport protocol; in this example, it would be SMTP</td>
</tr>
<tr>
<td></td>
<td>You can optionally supply a user name and password for the SMTP server; this is only necessary when your SMTP server requires them for authentication before sending email.</td>
</tr>
<tr>
<td>Mail from</td>
<td>Type the email address to be used as the &quot;From&quot; address when sending notifications.</td>
</tr>
</tbody>
</table>

6. Click OK to save your settings.

### Configuring connectivity to a Sametime proxy server after upgrading Sametime Advanced

Connecting IBM Sametime Advanced to a Sametime Proxy server activates the awareness feature that detects when a user is online for users who are in a browser.

**Before you begin**

You must have a Sametime Proxy Server installed and configured. You must set up Single Sign-On between the Sametime Advanced and the Sametime Community Server.

**About this task**

Provide information about the Sametime Proxy Server by editing the Administrative Settings configuration page of the Sametime Advanced server.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Advanced Servers.
3. In the Sametime Advanced Servers list, click the deployment name of the server with the information that you want to add or change.
4. Click the Administrative Settings tab.
5. In the Sametime Proxy Server section, specify the host name, port, and protocol for the proxy server you configured. If you have configured the Sametime Proxy Server behind a reverse proxy, use those connection settings here as appropriate.
   * Host name
Enter the fully qualified host name of the proxy server. This is the same host
name that you provided when you created a deployment plan before
installing the proxy server.
For example: sametime_proxy.example.com

- Port
  The port the proxy server is running on.

- Protocol
  Use HTTP for regular connections. Use HTTPS if the Sametime Proxy server
  is secured with SSL.

Note: If you are configuring your environment with SSL, you should use a
public certificate from a Trusted Root Certificate Authority. If you instead
configure your environment with self-signed certificates, then the certificate
from the Sametime Proxy server must be imported into the browser for
awareness on the Sametime Advanced pages to work. You will be prompted
to accept the self-signed certificate from the Sametime Advanced server when
you visit the page, but you will not be prompted to accept the certificate
from the Sametime Proxy server. You can either import this certificate
manually, or navigate to the web client on the Sametime Proxy server where
you will be prompted to accept it.

6. Click OK.
   Sametime Advanced automatically makes the changes without restarting the
   server.

Related tasks
"Configuring Single Sign-On for Sametime Advanced” on page 99
You must configure servers for single sign-on (SSO) in an IBM Sametime Advanced
deployment.
"Configuring SSL for Sametime Advanced” on page 99
Communications between Sametime servers are encrypted when they are set up to
run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on
IBM WebSphere Application Server install with SSL enabled, but you can change
the SSL certificates they use.

Upgrading Sametime Advanced clients
The IBM Sametime Connect client, both standalone and integrated with Lotus
Notes, includes a Sametime Advanced plug-in.

About this task
After you upgrade Sametime Advanced servers, enable the plug-in to make it
available to Sametime Connect clients by setting the enableAdvanced client
preference to true.

Note: The default broadcast server port has changed from 1506 to 1883. If you
provide default values through customized install packages, change the value of
com.ibm.collaboration.realtime.bcs/broadcastToolsServerPort= to 1883.
Related concepts

“Configuring Sametime Advanced client preferences after upgrading”

The following table lists the preferences for the Sametime Advanced client, for sites that have installed Sametime Advanced. The Sametime Advanced client is a plugin added to the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Deploying Sametime Advanced to clients after upgrading

IBM Sametime Advanced is delivered to clients as a plug-in.

About this task

For more information about ways to enable the Advanced client plug-in, see Deploying the Sametime client to users in the Installing section of Administering Sametime Standard.

Enabling Sametime Advanced persistent chat rooms and broadcast communities after upgrading

The IBM Sametime Connect client, both standalone and integrated with Lotus Notes, includes plug-ins that were available separately in previous releases.

About this task

Administrators have different options to enable the Advanced plug-ins for users who are licensed to use Sametime Advanced. Administrators must explicitly enable the Advanced plug-ins even for clients upgrading from earlier releases of Sametime Advanced.

com.ibm.collaboration.realtime/enableAdvanced=false

Set this preference to true to enable the Sametime Advanced client.

Configuring Sametime Advanced client preferences after upgrading

The following table lists the preferences for the Sametime Advanced client, for sites that have installed Sametime Advanced. The Sametime Advanced client is a plugin added to the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableAdvanced</td>
<td>Boolean. Default is false.</td>
<td>Applies to Sametime Advanced only. When the value is set to true, the Sametime Advanced plug-ins installed with the client become active.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>enableInstantShare</td>
<td>Boolean</td>
<td>Applies to Sametime Advanced only. If enableAdvanced is set to false, but the value of enableInstantShare is set to true, the instant share feature is available. Otherwise, the value of enableInstantShare is ignored.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>sametimeAdvancedServerName</td>
<td>String</td>
<td>Required. Fully qualified WebSphere Application Server host name, for example: sales.</td>
<td></td>
</tr>
<tr>
<td>sametimeAdvancedServerPort</td>
<td>String</td>
<td>Required. Sametime Advanced server port number.</td>
<td></td>
</tr>
<tr>
<td>sametimeCommunityServer</td>
<td>String</td>
<td>Required. Default Sametime community host name. This is the server users log in to for awareness and chat.</td>
<td></td>
</tr>
<tr>
<td>broadcastToolsServerName</td>
<td>String</td>
<td>Required. Fully qualified WebSphere Application Server host name.</td>
<td></td>
</tr>
<tr>
<td>broadcastToolsServerPort</td>
<td>String</td>
<td>Required. WebSphere Application Server port number. The port number is normally 1883 for HTTP and 8883 for SSL, but can be any port specified by the administrator.</td>
<td></td>
</tr>
<tr>
<td>useHTTPS</td>
<td>Boolean</td>
<td>If you are using SSL while connecting to the server, set to true. If you are using HTTP set to false.</td>
<td></td>
</tr>
<tr>
<td>advancedServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Sametime Advanced server. Set to 0 for a direct connection to the server. Set to 1 to connect through a reverse proxy.</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>broadcastServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Broadcast tools server. Set to 1 for a direct connection to the server. Set to 2 to connect using SSL.</td>
<td></td>
</tr>
<tr>
<td>useHttpProxy</td>
<td>Boolean</td>
<td>Set to true if you are using an HTTP forward proxy, otherwise set it to false.</td>
<td></td>
</tr>
<tr>
<td>proxyHost</td>
<td>String</td>
<td>Enter the proxy IP address or host name if you are using a HTTP proxy, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>proxyPort</td>
<td>String</td>
<td>Enter the HTTP proxy port to which you are connecting.</td>
<td></td>
</tr>
<tr>
<td>proxyUserName</td>
<td>String</td>
<td>Enter the user name if the HTTP proxy requires one for authentication, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>reverseProxyBaseURL</td>
<td>String</td>
<td>Enter the reverse proxy base URL to use if connecting through a reverse proxy. For example: <a href="http://mycompany.com/mycontext">http://mycompany.com/mycontext</a>. Leave blank otherwise.</td>
<td></td>
</tr>
<tr>
<td>reverseProxyUserName</td>
<td>String</td>
<td>Enter the reverse proxy user name if the proxy is authenticating. Leave blank if you are not using reverse proxies.</td>
<td></td>
</tr>
<tr>
<td>jmsProtocol</td>
<td>String</td>
<td>Indicates whether the client connects with a secure connection using the Security Secure Sockets Layer (SSL) or not. The default is disthub (to connect without SSL). Enter disthubs to connect with SSL.</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>liveNameResolveTimeoutString</td>
<td>String</td>
<td>Time allowed in milliseconds for awareness names to resolve. The default is 10000.</td>
<td></td>
</tr>
<tr>
<td>notifyNewOpenCommunities</td>
<td>Boolean</td>
<td>Alert users when a new open community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewModeratedCommunities</td>
<td>Boolean</td>
<td>Alert users when a new moderated community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewPrivateCommunities</td>
<td>Boolean</td>
<td>Alert users when a new private community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnDoNotDisturb</td>
<td>Boolean</td>
<td>Blocks broadcasts when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnInMeeting</td>
<td>Boolean</td>
<td>Blocks broadcast when user is in a meeting. The default is false. Set to true to block broadcasts when user is in a meeting.</td>
<td></td>
</tr>
<tr>
<td>notifyChatRoomAddMember</td>
<td>Boolean</td>
<td>Alert users when a chat room has a new member. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnDoNotDisturb</td>
<td>Boolean</td>
<td>Blocks chat room notifications when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnInMeeting</td>
<td>Boolean</td>
<td>Blocks chat room notifications when user is in a meeting. The default is false. Set to true to block chat room notifications when user is in a meeting.</td>
<td></td>
</tr>
</tbody>
</table>
Table 8. Global Preferences - com.ibm.collaboration.realtime (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcastServerUserIdType</td>
<td>String</td>
<td>The default is &quot;email&quot; to use the Sametime ID's email directory field. You need to use the same property value to log in to both the Sametime client and Sametime Advanced.</td>
<td></td>
</tr>
<tr>
<td>useTokens</td>
<td>Boolean</td>
<td>Determines whether or not the client uses LTPA token at login. The default is true. Set this to false only if there is no way to set up Single Sign-on between the Sametime and Sametime Advanced servers.</td>
<td></td>
</tr>
</tbody>
</table>

Table 9. Community Preferences - com.ibm.collaboration.community

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginTokenRefreshInterval</td>
<td>String</td>
<td>LTPA token timeout in seconds. IBM recommends 8610000 (23 hours and 55 minutes).</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>appsharePreference</td>
<td>String</td>
<td>Set the <em>instantshare</em> plug-in to use the application sharing component of either the Sametime Meeting Server or the Sametime Classic meeting service:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 - Try the Sametime Meeting Server application sharing component, and if it fails try the Sametime Classic meeting service application sharing component (default).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 - Use only the Sametime Meeting Server application sharing component.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3 - Use only the Sametime Classic meeting service application sharing component.</td>
<td></td>
</tr>
<tr>
<td>useAlternateServer</td>
<td>Boolean</td>
<td>If the value is true, instant share uses the host name defined by alternateMeetingServer for instant share sessions. The default is false. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use.</td>
<td></td>
</tr>
<tr>
<td>alternateMeetingServer</td>
<td>String</td>
<td>If the value of useAlternateServer is true, enter a host name here. Instant share uses the host name defined by alternateMeetingServer for instant share sessions. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10. Instant Share Preferences - com.ibm.collaboration.realtime.instantshare (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>useTokens</td>
<td>Boolean</td>
<td>Set to &quot;true&quot; only if InstantShare is configured to use an alternate server and LTPA token is required at login.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 5. Configuring Sametime Advanced

Configure connections and security in an IBM Sametime Advanced deployment.

About this task

Complete the configuration tasks in the order shown here:

Configuring SSL for Sametime Advanced

Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

About this task

For more information, see Working with Sametime servers that are enabled for SSL in the Configuring security section of Administering Sametime Standard.

Configuring Single Sign-On for Sametime Advanced

You must configure servers for single sign-on (SSO) in an IBM Sametime Advanced deployment.

About this task

For more information, see Setting up single sign-on (SSO) for Sametime clients in the Configuring security section of Administering Sametime Standard.

Integrating SiteMinder with Sametime Advanced

This section describes how to configure CA eTrust SiteMinder 6 for authentication with IBM Sametime Advanced.

Before you begin

Note: IBM recommends that you use the latest available version of the CA eTrust SiteMinder, as well as the latest available hot fix that is certified by Computer Associates to work with the version of the HTTP server that you are using. Use this documentation as a guide, but you will probably need to refer to the SiteMinder documentation, too.

SiteMinder uses agents to intercept HTTP requests in Sametime Advanced, and then forwards them to the SiteMinder Policy Server for authentication. There are two types of SiteMinder agents used when you configure SiteMinder to work with Sametime Advanced.

- SiteMinder Web Agent - Installed on the Lotus Sametime Advanced HTTP server and the Sametime 8 server
  Web agents control access to web content and deliver a user’s security credentials directly to any web application being accessed by the user. By placing an agent in a web server that is hosting protected web content or...
applications, administrators can coordinate security across a heterogeneous environment of systems and create a single sign-on domain for all users. For web servers, the web agent integrates through each web server’s extension API. It intercepts all requests for resources (URLs) and determines whether each resource is protected by SiteMinder. If the resource is not SiteMinder protected, the request is passed through to the web server for regular processing. If it is protected by SiteMinder, the web agent interacts with the policy server to authenticate the user and to determine if access to the specific resource is allowed.

- **Application Server Agents - Installed on the IBM WebSphere Application Server**
  To secure more finely-grained objects such as servlets, JSPs, or EJB components, which could comprise a full-fledged distributed application, SiteMinder provides a family of SiteMinder application server agents (ASAs). ASAs are plug-ins that communicate with the SiteMinder Policy Server to extend single sign-on (SSO) across the enterprise, including J2EE application server-based applications. ASAs also enable SiteMinder to centralize security policy management by externalizing J2EE authorization policies through standard interfaces such as those based on JSR 115.

**About this task**

Similar to other WebSphere Application Server environment configurations, you need to configure the following objects in SiteMinder to successfully protect your Sametime environment:

- An agent for the SiteMinder Web Agent
- An agent for the SiteMinder TAI
- An Agent Conf Object for the SiteMinder web Agent
- An Agent Conf Object for the SiteMinder TAI
- A Host Conf Object for the SiteMinder Web Agent
- A Host Conf Object for the SiteMinder TAI
- A User Directory Definition for SiteMinder to use to validate user credentials
- An Authentication Scheme
- A domain for the web agent in your Sametime environment
- A domain for the TAI in your Sametime environment
- Realm definitions for both domains
- Rules for the realms responses, if required, for the rules that you have defined
- A policy or policies for the domains

To configure SiteMinder to work with your Sametime Advanced server, complete the following integration steps:

**Creating configuration objects for SiteMinder (Sametime Advanced)**

Follow these steps to create configuration objects for your IBM Sametime Advanced environment on the CA eTrust SiteMinder Policy server.

**Procedure**

1. Open the SiteMinder Policy Server console.
2. To create the web agent objects, follow these steps.
   a. Click the **System** tab.
Chapter 5. Configuring Sametime Advanced
Sametime Advanced server can access the appropriate LDAP server to authenticate your Sametime Advanced users. This must be the same LDAP server that has been configured with your Sametime Advanced server. To create a user directory:

a. Under System Configuration, right-click the User Directories icon.

b. Click **Create User Directory**.

c. In the SiteMinder User Directory Dialog, type a unique value in the **Name** field.

d. Optional: Type a description.

e. Select **LDAP** from the **Namespace** drop-down list.

f. Type the fully qualified host name of your LDAP server in the **Server** field.

g. Complete the LDAP Search and LDAP User DN Lookup fields as appropriate for your LDAP users.

**Note:** Depending on your LDAP server configuration, you might need to add required credentials on the Credentials and Connection tab so that the SiteMinder Policy Server can bind with your LDAP server. Refer to the eTrust SiteMinder documentation for details.

h. Click **OK**.

### Configuring domains and realms for Sametime Advanced

Follow these steps to configure the domains and realms for your IBM Sametime Advanced environment on the CA eTrust SiteMinder Policy Server.

**Procedure**

1. Open the SiteMinder Policy Server console.

2. Define a domain for the web agent in your Sametime Advanced environment:
   a. Right-click **Domains** under System Configuration, and choose **Create Domain**.
   b. In the SiteMinder Domain Dialog, type a unique value in the **Name** field, for example, **Sametime_WA**.
   c. Optional: Type a description.
   d. In the drop-down list at the bottom of the dialog, select the user directory to use in this domain.
   e. Click **Add** to add it to the User Directories Tab.
   f. Click **OK**.

3. Define a domain for the TAI in your Sametime Advanced environment:
   a. Click **Create Domain**.
   b. In the SiteMinder Domain Dialog, type a unique value in the **Name** field, for example, **Sametime_TAI**.
   c. Optional: Type a description.
   d. Click **OK**.

4. Define the realm definition for the web agent domain that you created in step 2:
   a. Click the Domains tab.
   b. Right-click the domain you created, and click **Create Realm**.
   c. In the SiteMinder Realm Dialog, type a unique value in the **Name** field, for example, **Sametime_WA**.
   d. Optional: Type a description.
e. Click the Resource tab.

f. In the Agent field, type the name of the agent that you created for the web agent in this environment. You can also select it using Lookup.

g. Type the Resource Filter as /

h. Under Default Resource Protection, select Protected. Leave all the other fields on the Resource, Session and Advanced tabs as their default values.

i. Click OK.

5. Define the realm definition for the TAI domain that you created in step 3:

   a. Right-click the domain you created, and click Create Realm.

   b. In the SiteMinder Realm Dialog, type a unique value in the *Name field, for example, SM TAI Validation.

   c. Optional: Type a description for the realm.

   d. Click the Resource tab.

   e. In the Agent field, type the name of the agent that you created for the TAI in this environment. You can also select it using Lookup.

   f. Type the Resource Filter as /siteminderassertion.

   g. From the Authentication Scheme drop-down list, select the scheme that you will use for this environment.

   h. Under Default Resource Protection, select Protected. Leave all the other fields on the Resource, Session and Advanced tabs as their default values.

   i. Click OK.

6. Define rules for the realm that you created for the Web Agent domain.

   a. Right-click the realm that was created for the web agent domain (for example Sametime_WA), and select Create Rule under Realm.

   b. Use the SiteMinder Rule dialog to create the following rules:

   **GetPostPut rule properties**
   - *Name - GetPostPut Rule
   - Realm - For example, Sametime_WA
   - Resource: - *
   - Web Agent actions - Get,Post,Put
   - When this Rule fires - Allow Access
   - Enable or Disable this Rule - Enabled

   **OnAuthAccept rule properties**
   - *Name - OnAuth
   - Realm - For example, Sametime_WA
   - Resource: - *
   - Authentication events - OnAuthAccept
   - When this Rule fires - Allow Access
   - Enable or Disable this Rule - Enabled

7. Define a policy to control the webagent domain.

   a. Under the domain that was previously created, right-click on policies, and select Create Policy.

   b. In the SiteMinder Policy Dialog, type a unique value in the *Name field, for example, STADVWAPolicy.

   c. Optional: Type a description.
Installing and configuring the SiteMinder Web Agent (Sametime Advanced)

IBM recommends that you install the latest available version of the CA eTrust SiteMinder Web Agent as well as the latest available hot fix that is certified by Computer Associates to work with the version of the HTTP server that you are using.

**Before you begin**

Before you begin, you must download the SiteMinder V6-QMR5 W32 web agent installation files from the SiteMinder support site at .http://support.netegrity.com.

**About this task**

Refer to the SiteMinder platform support matrices for more details. These matrices can be obtained from the SiteMinder support site. You can also refer to the SiteMinder WebAgent Installation Guide for details about configuring the web agent to work with the HTTP server that you are using. The application agent for Sametime Advanced should be v6.0 CR005 or later to ensure support of IBM WebSphere Application Server 6.1.

**Note:** To install the SiteMinder Web Agent on platforms other than Microsoft Windows, you can use the relevant Win32 instructions as a reference document. The same configuration information needs to be provided, regardless of platform. There are also additional instructions included with the web agent installation files that indicate platform-specific steps that are required for installing and configuring the web agent on a specific platform.

Follow these steps to install and configure the Win32 6x Web Agent for your HTTP server.

**Procedure**

1. If necessary, extract all the files from the ZIP file provided by SiteMinder.
2. Start the Web Agent executable. The format is nete-wa-6qmrX-platform.exe.
   
   For example:
   nete-wa-6qmr5-win32.exe

   The CA SiteMinder Web Agent Introduction screen appears.
3. Click Next.
4. On the License Agreement screen, scroll down and select **I accept the terms of the License Agreement**, and click Next.
5. Click Next on the Important Information screen.
6. On the Choose Install Location screen, accept the default location for installing the web agent or click Choose to select a different location, then click Next.
7. Click **Next** on the Choose Shortcut Folder screen.
8. Click **Install** on the Pre-Installation Summary screen.
9. On the Install Complete screen, accept the defaults selection and click **Done**. Your system restarts.
10. Click **Start > Programs > Siteminder > Web Agent Configuration Wizard** to start the Web Agent Configuration Wizard.
11. On the Host Registration screen, select **Yes, I would like to do Host Registration now**, but do not select the **Enable PKCS11 DLL Cryptographic Hardware** check box. Click **Next**.
12. On the Admin Registration screen, type the SiteMinder administrator name and password provided by your SiteMinder contact. Do not select the **Enable Shared Secret Rollover** check box. Click **Next**.
13. On the Trusted Host Name and Configuration Object screen, type the trusted hostname and Host Conf Object provided by your SiteMinder contact. Click **Next**.
14. On the Policy Server IP Address screen, type the SiteMinder Policy Server IP address provided by your SiteMinder contact and click **Add**. Click **Next**.
15. On the Host Configuration file location screen, accept the default file name and location and click **Next**.
16. On the Select Web Server(s) screen, select the check box next to the http server that you wish to configure with the web agent, and then click **Next**.
17. On the Agent Configuration Object screen, enter the Agent Conf Object provided by the SiteMinder contact and click **Next**.
18. On the Web Server Configuration Summary screen, click **Install**. The web agent configuration process starts, and then the Configuration Complete screen appears.
19. Click **Done** to complete the configuration process.

**Note:** You can ignore messages indicating that some warnings occurred during the installation. These warnings appear by default and do not affect the functionality of the web agent.

**What to do next**

There are additional steps that must be completed to enable the web agent to function properly for your server. Follow the additional instructions that are provided by your SiteMinder contact in order to complete this setup.

**Installing and configuring the SiteMinder TAI (Sametime Advanced)**

IBM recommends that you install the latest available version of the CA eTrust SiteMinder Trust Association Interceptor (TAI) as well as the latest available hot fix that is certified by Computer Associates to work with the version of the IBM WebSphere Application server that you are using.

**About this task**

Refer to the SiteMinder platform support matrices for more details. These matrices can be obtained from the SiteMinder support site. After TAI installation perform the following configuration steps:
Procedure
1. Copy the smagent.properties file from the TAI installation \conf folder to the WebSphere Application Server profile properties folder. For example:
   c:\program files\IBM\websphere\appserver\ST_Advanced_Profile\properties
2. Verify that your system path includes a path to the TAI bin directory, typically c:\smwasasa\bin.
5. Click Trust Association.
6. Select the Enable Trust Association check box, and click Apply
7. Click Interceptors.
8. Delete any interceptors that you do not require.
10. In the Interceptor Classname field, type the following SiteMinder TAI class name and click Apply:
    com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor
11. Click Save on the next two screens.
12. Log out of the Integrated Solutions Console.

Enabling and testing the SiteMinder Web Agent and TAI (Sametime Advanced)
Follow these steps to enable the CA eTrust SiteMinder Web Agent and Trust Association Interceptor (TAI) for your IBM Sametime Advanced deployment. You also need to test that the integration is working.

Procedure
1. In the local web agent configuration file (WebAgent.conf) of the SiteMinder Web Agent that has been configured with your HTTP server, set the EnableWebAgent parameter to YES.
2. In the local Web Agent configuration file (typically c:\smwasasa\conf\ASAAgent-Assertion.conf) of the eTrust SiteMinder TAI that has been configured with your server, set the EnableWebAgent parameter to YES
3. Restart your HTTP and Sametime Advanced Servers.
4. To test that your integration is working, enter the url for your deployment of Sametime Advanced into a browser. For example:
   http://host_name/stadvanced

   Verify that eTrust SiteMinder authentication is invoked. When valid user credentials are entered, the user should be successfully logged into Sametime Advanced. The user should not be prompted for authentication credentials by Sametime Advanced.
   If you are directed to the Sametime Advanced login screen then there is a problem with the TAI configuration, and you must revisit the setup to determine the cause.

Configuring logout in SiteMinder (Sametime Advanced)
The IBM Sametime Advanced log out link in the user interface is not configurable for logging out from CA eTrust SiteMinder.
About this task

You have two options to log out from SiteMinder.

- Restart the browser to clean all SiteMinder cookies, or
- Configure SiteMinder with a link, which when accessed within the same browser session, logs out the user.

To configure SiteMinder with a link, complete the following steps:

Procedure

1. Create a file named Logout.html on your HTTP server. The file can have no content or have something simple such as "Logged Out of SiteMinder."
2. Add the following parameter to the SiteMinder Web Agent Webagent.conf file, or, if the local configuration is not enabled, set it in the appropriate Agent Configuration Object on the SiteMinder Policy Server.
   
   LogOffURI="Path\to\Logout.html"

3. Restart the HTTP Server.

Configuring SiteMinder for the Sametime Community Server in a Sametime Advanced deployment

This section describes how to configure CA eTrust SiteMinder for the IBM Sametime Community server.

About this task

You installed the Lotus Sametime Community Server as part of the process for installing Sametime Advanced. The Sametime Community server is managed with the Sametime Advanced server. When you configure SiteMinder to work the Sametime Community server, you create a new agent object, agent configuration object, Host configuration object, realm, and sub-realms. You should use the same user directory and domain that you created when you configured SiteMinder for Sametime Advanced. See Configuring the domains and realms for your Sametime Advanced environment.

Creating configuration objects for the Sametime Community Server in a Sametime Advanced deployment

Follow these steps to create configuration objects for IBM Sametime Community Server on the CA eTrust SiteMinder Policy server.

Before you begin

Open the SiteMinder Policy Server console.

Procedure

1. To create an Agent object, follow these steps.
   a. Click the System tab.
   b. Under System Configuration, right-click the Agents icon.
   c. In the SiteMinder Agent Dialog, type a unique value not used previously for an existing agent in the Name field.
   d. Optional: Type a description such as "Sametime Agent."
   e. Under Agent Type, select SiteMinder, and select Web Agent from the drop-down list.
f. Click OK.

2. Create a duplicate of the existing DominoDefaultSettings Agent Conf object on the SiteMinder Policy Server and modify the duplicate as appropriate. To create an Agent Conf object for your HTTP Server:
   a. Under System Configuration, click the Agent Conf Objects icon.
   b. Right-click the DominoDefaultSettings Agent Conf object in the Agent Conf Object list on the right side of the console, and select Duplicate Configuration Object.
   c. In the SiteMinder Agent Configuration Object dialog, type a unique value not used previously for an existing agent in the *Name field.
   d. Optional: Type a description such as "Domino Configuration Agent."
   e. In the Configuration Values list, set the following parameters to the values indicated or to the appropriate values for your server. Clicking each parameter, and select the Edit:
      • DefaultAgentName - Name given to agent created in step c.
      • AllowLocalConfig - Yes
      • CssChecking - No
      • BadUrlChars - remove // and /,%00-%1f,%7f-%ff,%25 from the default list of Bad Url Characters
      • SkipDominoAuth - No. All other parameters can be left at their default settings..
   f. Click OK.

3. IBM recommends that you create a duplicate of the existing DefaultHostSettings Host Conf Object on the SiteMinder Policy Server and modify the duplicate as appropriate. To create a Host Conf object for your HTTP Server:
   a. Under System Configuration, click the Host Conf Objects icon.
   b. Right-click the DefaultHostSettings object in the Host Conf Object List on the right side of the console, and select Duplicate Configuration Object.
   c. In the SiteMinder Host Configuration Object dialog, type a unique value in the *Name field.
   d. Optional: Type a description such as "Sametime Advanced Host."
   e. In the Configuration Values list, edit the #Policy Server value by removing the # from in front of the parameter name and entering the IP address of your SiteMinder Policy Server in the appropriate place in the value field.
   f. Click OK.

**Configuring realms for the Sametime Community Server in a Sametime Advanced deployment**

Follow these steps to configure the realms for IBM Sametime Community Server on the CA eTrust SiteMinder Policy Server.

**About this task**

You should use the same user directory and web agent domain that you created when you configured SiteMinder for Sametime Advanced. See Configuring the domains and realms for your Sametime Advanced environment.

**Procedure**

1. Open the SiteMinder Policy Server console.
2. Define the realm definition for the web agent domain:
a. Click the Domains tab in the left side of the SiteMinder Policy Console.
b. Right-click the web agent domain that you previously created.
c. Click Create Realm.
d. In the SiteMinder Realm Dialog, type a unique value in the *Name field, for example, Sametime.
e. Optional: Type a description.
f. Click the Resource tab.
g. In the Agent field, type the name of the agent that you created for the web agent for Sametime Community Server. You can also select it using Lookup.
h. Type the Resource Filter as /.
i. In Authentication Scheme list, select Basic.
j. Under Default Resource Protection, select Protected. Leave all the other fields on the Resource, Session and Advanced tabs as their default values.
k. Click OK.

3. Create sub-realms under the realm you just created.
   a. Click the Domains tab in the left side of the SiteMinder Policy Console.
   b. Right-click the realm that you created in step 2.
   c. Click Create Realm.
   d. Create the following sub-realms for your configuration, with the values indicated in each dialog:

<table>
<thead>
<tr>
<th>Name</th>
<th>Resource Filter</th>
<th>Authentication Scheme</th>
<th>Default Resource Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST Test</td>
<td>stlinks</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST AdminConfig</td>
<td>servlet/auth/scs</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST AdminPage</td>
<td>servlet/auth/admin</td>
<td>Basic</td>
<td>Protected</td>
</tr>
<tr>
<td>ST Src</td>
<td>stsrc.nsf/join</td>
<td>Basic</td>
<td>Protected</td>
</tr>
<tr>
<td>ST Domino</td>
<td>STDomino.nsf</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Applets</td>
<td>sametime/applets</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Applet</td>
<td>Sametime/Applet</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>IMI Sametime</td>
<td>sametime/hostAddress.xml</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST MAPI</td>
<td>servlet/auth/mapi</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Admin CGI</td>
<td>cgi-bin/StAdminAct.exe</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST UserInfoServlet</td>
<td>servlet/UserInfoServlet</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
</tbody>
</table>

4. Create rules for the protected realm (Sametime) and the two protected sub-realms (ST AdminPage and ST Src).
   a. Right-click the realm that was created for the web agent domain (for example Sametime), and select Create Rule under Realm.
   b. Use the SiteMinder Rule dialog to create the following rules named Rule 1 and Rule 2:
      
      **Rule 1 properties**
      - *Name - GetPost Rule
      - Realm - Sametime
c. Right-click the ST AdminPage sub-realm, and select Create Rule under Realm.

d. Use the SiteMinder Rule dialog to create the following rule named Rule 1:

Rule 1 properties
- *Name - GetPost Rule
- Realm - Sametime.ST AdminPage
- Resource: *
- Web Agent actions - Get,Post,
- When this Rule fires - Allow Access
- Enable or Disable this Rule - Enabled

Rule 2 properties
- *Name - OnAuthAccept
- Realm - Sametime
- Resource: *
- Authentication events - OnAuthAccept
- When this Rule fires - Allow Access
- Enable or Disable this Rule - Enabled

e. Right-click the ST Src sub-realm, and select Create Rule under Realm.

f. Use the SiteMinder Rule dialog to create the following rules named Rule 1 and Rule 2:

Rule 1 properties
- *Name - GetPost Rule
- Realm - Sametime.ST Src
- Resource: *
- Web Agent actions - Get,Post,
- When this Rule fires - Allow Access
- Enable or Disable this Rule - Enabled

Rule 2 properties
- *Name - OnAuthAccept
- Realm - Sametime.ST Src
- Resource: *
- Authentication events - OnAuthAccept
- When this Rule fires - Allow Access
- Enable or Disable this Rule - Enabled

5. Add the rules to the SiteMinder policy that you created for Sametime Advanced.

a. Double-click the policy you created for Sametime Advanced, for example, STADVWAPolicy.

b. Click the Rules tab, and then click Add/Remove Rules. Add all the rules you created previously for the realm and sub-realms to the current members list. Click OK.
Installing and configuring the SiteMinder Web Agent for use with
the HTTP server
IBM recommends that you install the latest available version of the CA eTrust
SiteMinder Web Agent as well as the latest available hot fix that is certified by
Computer Associates to work with the version of the HTTP server that you are
using.

Before you begin
Before you begin, you must download the Siteminder V6-QMR5 W32 web Agent

About this task
Refer to the SiteMinder platform support matrices for more details. These matrices
can be obtained from the SiteMinder support site. You can also refer to the
SiteMinder WebAgent Installation Guide for details about configuring the web agent
to work with the HTTP server that you are using. The application agent for
Sametime Advanced should be v6.0 CR005 or later to ensure support of IBM
WebSphere Application Server 6.1.

Note: To install the SiteMinder Web Agent on platforms other than Microsoft
Windows, you can use the relevant Win32 instructions as a reference document.
The same configuration information needs to be provided, regardless of platform.
There are also additional instructions included with the web agent installation files
that indicate platform-specific steps that are required for installing and configuring
the web agent on a specific platform.

Follow these steps to install and configure the Win32 6x Web Agent for your HTTP
server.

Procedure
1. If necessary, extract all the files from the ZIP file provided by SiteMinder.
2. Start the Web Agent executable. The format is nete-wa-6qmrX-platform.exe.
   For example:
   nete-wa-6qmr5-win32.exe
   The CA SiteMinder Web Agent Introduction screen appears.
3. Click Next.
4. On the License Agreement screen, scroll down and select I accept the terms of
the License Agreement, and click Next.
5. Click Next on the Important Information screen.
6. On the Choose Install Location screen, accept the default location for installing
the web agent or click Choose to select a different location, then click Next.
7. Click Next on the Choose Shortcut Folder screen.
8. Click Install on the Pre-Installation Summary screen.
9. On the Install Complete screen, accept the defaults selection and click Done.
Your system restarts.
10. Click Start > Programs > Siteminder > Web Agent Configuration Wizard to
start the Web Agent Configuration Wizard.
11. On the Host Registration screen, select Yes, I would like to do Host
Registration now, but do not select the Enable PKCS11 DLL Cryptographic
Hardware check box. Click Next.
12. On the Admin Registration screen, type the SiteMinder administrator name and password provided by your SiteMinder contact. Do not select the Enable Shared Secret Rollover check box. Click Next.

13. On the Trusted Host Name and Configuration Object screen, type the trusted hostname and Host Conf Object provided by your SiteMinder contact. Click Next.

14. On the Policy Server IP Address screen, type the SiteMinder Policy Server IP address provided by your SiteMinder contact and click Add. Click Next.

15. On the Host Configuration file location screen, accept the default file name and location and click Next.

16. On the Select Web Server(s) screen, select the check box next to the http server that you wish to configure with the web agent, and then click Next.

17. On the Agent Configuration Object screen, enter the Agent Conf Object provided by the SiteMinder contact and click Next.

18. On the Web Server Configuration Summary screen, click Install. The web agent configuration process starts, and then the Configuration Complete screen appears.

19. Click Done to complete the configuration process.

Note: You can ignore messages indicating that some warnings occurred during the installation. These warnings appear by default and do not affect the functionality of the web agent.

What to do next

There are additional steps that must be completed to enable the web agent to function properly for your server. Follow the additional instructions that are provided by your SiteMinder contact in order to complete this setup.

Adding the DSAPI filter file name to the Domino Directory in a Sametime Advanced deployment

Your IBM Sametime server will run on a Lotus Domino server. When you integrate Sametime with CA eTrust SiteMinder, the SiteMinder Web Agent is implemented as a Domino Web Server Application Programming Interface (DSAPI) filter file.

About this task

Follow these steps to add the DSAPI filter file name to the Domino Directory.

Procedure


2. Edit the server document for the Domino server as follows:

   a. Click the Internet Protocols tab, then click the HTTP tab. In the DSAPI filter file names field, type the full path and name of the SiteMinder Web Agent (typically c:\Program Files\Netegrity\Siteminder Web Agent\bin\dominowebagent.dll)

   b. Click the Domino Web Engine tab, then set the Session authentication field to Disabled.

3. Save and close the server document.
Enabling SiteMinder on the Sametime Community Server in a Sametime Advanced deployment

Follow these steps to enable the CA eTrust SiteMinder Web Agent for the IBM Sametime server.

Procedure

1. Locate the local Web Agent configuration file for the SiteMinder Web Agent that has been configured with your HTTP server. For example:
   
   C:\Program Files\IBM\HTTPServer\conf\WebAgent.conf

2. Use a text editor to open the file and set the EnableWebAgent parameter to YES.

3. Restart your HTTP and Lotus Domino Servers. When you start or stop the Domino server, you are starting and stopping the Sametime server as well.

Awareness and SiteMinder in a Sametime Advanced deployment

CA eTrust SiteMinder cookies are not compatible with Sametime Links. Sametime Links enables awareness in IBM Sametime Advanced through the Sametime Community Server server. To display awareness in the Sametime Advanced user interface on the Web, you must perform the following tasks.

- Enable IBM WebSphere LtpaToken (Single Sign-on)
- Export the keys
- Import the keys into the Web SSO configuration document on the Sametime Community Server

With this solution, both the LtpaToken and SiteMinder cookies are in use. The SiteMinder tokens are used for SSO and authentication into the Lotus Sametime environment, and the LtpaToken is used by Lotus Sametime Advanced to provide awareness for your environment. For other possible solutions using SiteMinder cookies contact IBM support and consider opening a case against the SiteMinder SDK (https://support.netegrity.com).

The instructions for enabling LtpaToken, exporting keys, and importing them into Lotus Sametime are in the Enabling Single Sign-on and Configuring connectivity to a proxy server topics.

SiteMinder automatically logs users into the Lotus Sametime Advanced server when the context root "stadvanced" is accessed. In order to log in to Lotus Sametime, you must explicitly access the host_name/stadvanced/logon.jsp URL and select the check box for Log in to Sametime instant messaging.
Chapter 6. Administering Sametime Advanced

Set up and begin using IBM Sametime Advanced to let users create and use persistent chat rooms and broadcast communities. After installing Sametime Advanced, you can manage user access, enable workflow, set anonymous access, and integrate Sametime Advanced servers with other products.

Controlling access in Sametime Advanced

You can control access in IBM Sametime Advanced at the application level or at the feature level.

About this task

You control access at the application level by editing the security role to user/group mappings in the Integrated Solutions Console. This is where you grant administrator privileges to other users, assign workflow approvers, and assign broadcast community creators. IBM does not recommend changing the authenticated user or the all user mappings.

You control access at the feature level by editing role settings in the broadcast communities, chat rooms, and folders.

- **Broadcast communities.** Access to broadcast communities is determined by membership role and by broadcast type: public, private, restricted recipient, or restricted publisher.
- **Chat rooms.** Access to chat rooms is determined by assigning roles to folders in the chat room folder hierarchy and by chat room owner/creators.

See the following topics for instructions on controlling access in Sametime Advanced.

Configuring the user access level to Sametime Advanced

Access to IBM Sametime Advanced is determined by user roles.

About this task

When you install Sametime Advanced, default access levels or roles are assigned to users and groups. You can change these assignments to fit the needs of your organization.

Follow these instructions to change role assignments.

Procedure

1. In the WebSphere Integrated Solutions Console, click **Applications > Enterprise Applications.**
2. Click **Sametime Advanced application.**
3. Under Detail Properties, click **Security role to user/group mapping.**
4. Use the following list to determine how you want to assign users to roles.
   - **AllUsers** - Any user assigned to this role has access to non-authenticated areas of the application - All Chat Rooms and Search tabs. This role is assigned to **Everyone** by default and should not be changed.
AllAuthenticatedUsers - Authenticated users are users that have been authenticated with the LDAP directory. Authenticated users have access to All Chat Rooms, My Chat Rooms, Broadcast Communities, and Search tabs. This role is assigned to All authenticated by default and should not be changed.

CommunityCreators - Broadcast communities can be created by any user assigned to this role.

WorkflowApprovers - Users who can approve or deny chat rooms and communities waiting for approval. If workflow has been enabled, then once a community or chat room has been created, it has to be approved for use.

AdminUser - These users are administrators and have access to the entire system. They have full access to manage (create/edit/delete/archive) any folder or chat room in Sametime Advanced.

5. Assign a role to a user by following these steps. In this procedure, an administrator is added to Sametime Advanced by assigning a user to the AdminUser role.
   a. Under the Select column, select the check box next to the AdminUser role.
   b. Click Look up users.
   c. In Search String, type the name of the user you want to assign the administrator role.
   d. Select a name in the Available box, and then click the right arrow button to add the name to the Selected box.
   e. Click OK. The user name is added to the Mapped users box next to the AdminUser role.
   f. Click OK.

Setting up a folder hierarchy for chat rooms

In IBM Sametime Advanced, create a folder hierarchy for chat rooms and grant access to other users.

About this task

When IBM Sametime Advanced is installed, a single root folder named "Chat Rooms" is created on the All Chat Rooms page. This folder cannot be renamed or removed. Initially, all users have permission to create and edit new folders and chat rooms in this folder. You can limit users' ability to create new folders and chat rooms by designating specific users as managers of the Chat Rooms folder. Managers of a folder automatically are granted manager permissions in all subfolders.

Procedure

1. Log in to Sametime Advanced as an administrator.
2. Click the All Chat Rooms tab.
3. Next to the Chat Rooms folder (the root folder), click Edit.
4. Click the Managers tab.
5. Select the Users specified below have manager access to this folder check box.
6. Click Edit.
7. Use the Edit Users dialog to search for, add, and remove users.
8. Repeat the previous three steps for Authors and Readers.
9. Click Save.

What to do next

After you have designated managers, you and the other managers can create new folders and subfolders to build a hierarchy of folders for your organization.

Folder and chat room roles

The following table describes the roles associated with folders and chat rooms in IBM Sametime Advanced.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Administrator       | This super user can manage the complete folder hierarchy  
|                     | - Create, edit, delete, archive, restore, enable, disable all chat rooms.  
|                     | - View all archived chat rooms.  
|                     | - Create, edit, delete all global folders  
|                     | - Move chat rooms from one global folder to another.  
|                     | - Cannot delete the root Chat Rooms folder.                                                                                           |
| Folder Manager:     | This user can do anything an Administrator can do, except only in the folder where he is a manager.  
|                     | - Can enter any chat room in a folder he manages.  
|                     | - Create, edit, delete, archive, restore, enable, disable all chat rooms under the folders he manages.  
|                     | - View all archived chat rooms under the folders he manages.  
|                     | - Create, edit, delete all global folders under the folders he manages.  
|                     | - Edit or delete the immediate folder.  
|                     | - Move chat rooms from one global folder to another. He must have writing access to the two folders.  |
| Folder Author       | - Can enter those chat rooms he created, but not others in the folder.  
|                     | - Create, edit, delete, enable, or disable chat rooms that he created in the folder where he is an author.  
|                     | - May not edit or delete the immediate folder where he is an author. For example, if I am writer for Folder A1, then I can’t edit or delete A1.  
|                     | - Move chat rooms from one global folder to another. He must have authoring access to the two folders.                                                                 |
| Folder Reader       | - Can enter a chat room if he is the owner, or an invitee, or if the chat room has open access to him.  
|                     | - Can view the folder and only view chat rooms which have open access, or he is a member of the folder.                                                                                   |
| Chat Room Owner     | - Can enter chat room that he owns.  
|                     | - Edit, delete, enable, or disable the chat room  
|                     | - When choosing chat room owners, if the owner has no writing access to the folder that the chat room resides in, then system gives the owner writing access automatically. The owner will have writing access to the folder, but no access to other chat rooms in the folder, only the ones he creates. The owner will be only a reader of the parent folders above. |
| Chat Room Invitee   | - Can enter chat room.  
|                     | - Cannot edit, delete, archive, restore, enable or disable the chat room.  
|                     | - After the chat room is created, he is a reader to all the folders he can navigate to in the chat room.                                                                                   |
## Role Description

**Unauthenticated User**
- This user has not logged in.
- Can view All Chat Rooms and Search tabs; cannot view the other tabs.
- Can only view folders which allow unauthenticated access.
- Can join chat rooms that are not limited to invitees, or logged in users.
- Can enter chat room details page.

## Assigning creators for broadcast communities

In IBM Sametime Advanced, administrators can create and manage broadcast communities. Before other users can create or manage a broadcast community, they must be assigned the CommunityCreators role. By default, all authenticated users are assigned the role.

### About this task

Assign or change CommunityCreators in the IBM WebSphere Integrated Solutions Console.

### Procedure

1. From Integrated Solutions Console, click **Servers > Application Servers** > `stadvanced_server_name`.
2. Under Applications on the Configuration tab, click **Installed applications**.
3. Click **Sametime Advanced application**.
4. Under Detail Properties, click **Security role to user/group mapping**.
5. In the Mapped Users and Mapped Groups column of the CommunityCreators row, enter the users that you want to grant permission to create broadcast communities.
6. Optional: If you have written the code to enable the workflow community API, then a designated workflow approver must be assigned the WorkflowApprovers role. In the Mapped Users and Mapped Groups column of the WorkflowApprovers row, enter the users that you want to grant permission to approve community creation. This setting also lets them approve chat room creation. You can find information on writing the workflow API calls in the *Sametime Advanced Software Development Kit* at IBM developerWorks® at [http://www.ibm.com/developerworks/lotus/downloads/toolkits.html](http://www.ibm.com/developerworks/lotus/downloads/toolkits.html).
7. Click **OK**.

## Broadcast community types and roles

Different types of IBM Sametime Advanced broadcast communities have different roles. These roles determine what you can do in the community.

<table>
<thead>
<tr>
<th>Community type</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open</strong></td>
<td>Manager - Can edit or delete a broadcast community. Can edit the manager list.</td>
</tr>
<tr>
<td>Any authenticated Sametime Advanced user can join.</td>
<td></td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>Manager - Can edit or delete a broadcast community. Can edit the manager list.</td>
</tr>
<tr>
<td>You must be a community member to participate in this community.</td>
<td></td>
</tr>
<tr>
<td><strong>Member</strong></td>
<td>Member - Can join the community and can send and receive broadcasts.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Community type Roles

**Restricted recipients**

Any authenticated Sametime Advanced user can send a broadcast. You must be a community member to receive a broadcast.

- **Manager** - Can edit or delete a broadcast community. Can edit the manager list.
- **Recipient** - Can join the community and can receive broadcasts.

**Restricted publishers**

Any authenticated Sametime Advanced user can receive a broadcast. You must be a community member to send a broadcast.

- **Manager** - Can edit or delete a broadcast community. Can edit the manager list.
- **Publisher** - Can join the community and can send broadcasts.

### Limiting anonymous access

You can limit anonymous access to IBM Sametime Advanced.

**About this task**

By default, users can access chat rooms without logging in first, but they cannot access broadcast communities. Once users have logged in to Sametime Advanced they can access all the features that their licenses allow, including broadcast communities.

If you want to prevent these anonymous users from accessing any Sametime Advanced features, follow these instructions.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Advanced Servers**.
3. In the **Sametime Advanced Servers** list, click the deployment name of the server with the information that you want to add or change.
4. Click the **Administrative Settings** tab.
5. Under Anonymous Access, clear the **Allow anonymous access** check box.
6. Click **OK**.

**What to do next**

Since anonymous users are not issued licenses, they are not counted in the number of licenses issued figure in the **Counts** page of the **License Management** view.

### Configuring licensing management

You can configure settings related to license management for IBM Sametime Advanced.

**About this task**

- Limit the number of licenses supported
- Count the licenses that are already in use and how many are still available.
- Automatically issue licenses at login.

Follow these steps to configure licensing.
**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Advanced Servers**.
3. In the **Sametime Advanced Servers** list, click the deployment name of the server with the information that you want to add or change.
4. Click the **License Management** tab.
5. Type the number of licenses that you want to allocate in the **Allocated licenses** box. This setting overrides the default number of licenses, which is 1000.
6. If you would like to limit unlicensed users' ability to use Sametime Advanced, select **Enable license counting**. When a valid user that has not been issued a license logs in, the user receives a message that a license is required. The user cannot use any features in Sametime Advanced.
7. If you enabled license counting in the previous step and you would like to allow users to automatically receive a license when they login, select **Enable automatic licensing**.
8. Click **OK**.

**What to do next**

You can also monitor the number of licenses using the **Count** tab.

**Issuing licenses to users**

Users' access to features in IBM Sametime Advanced is controlled by the license issued to them. You can issue licenses to individual users or groups in the LDAP directory or to users listed in an upload file you create.

**Before you begin**

To use a file to issue licenses, create a file with users' unique identifiers, one user per line.

**About this task**

A license is persistent and assigned to a specific user. The user is not allocated a limited time or session-based license from a pool of available licences.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Advanced Server**.
3. In the Sametime Advanced Servers list, click the deployment name of the Sametime Advanced Server.
4. Click the License Management tab.
5. Click **Set License Settings**.
6. Confirm that automatic license issuing is enabled.
7. Click **Issue**.
8. Search for and select users or groups to issue licenses to or upload the user list you created earlier.
9. Click **Grant licenses**.
What to do next

To revoke a license, open the License Management tab, select the licensed users whose licenses you want to revoke and click Revoke.

1.

Command line user management

You can manage users in IBM Sametime Advanced by running the stlicadmin command line tool. The tool has commands for adding and removing users.

Purpose

The tool has commands for adding and removing users. The stlicadmin command is available in the AppServer/bin directory.

Syntax

- Windows
  stlicadmin.bat {--add | --delete} {--user Uid | --group Gid | --batch Fname}

- UNIX
  ./stlicadmin.sh {--add | --delete} {--user Uid | --group Gid | --batch Fname}

Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a new user or group of users</td>
</tr>
<tr>
<td>delete</td>
<td>Delete a user or group of users</td>
</tr>
</tbody>
</table>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Syntax</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>-u</td>
<td>UserName</td>
<td>The user being referenced. Required unless -b or -g is specified. The UserName parameter is specified as the email address.</td>
</tr>
<tr>
<td>group</td>
<td>-g</td>
<td>GroupName</td>
<td>An LDAP group. Required unless -u or -b is specified.</td>
</tr>
<tr>
<td>batch</td>
<td>-b</td>
<td>FileName</td>
<td>Batch mode. Specify a file containing a list of users, required unless -u or -g is specified.</td>
</tr>
<tr>
<td>host</td>
<td>-h</td>
<td>HostName</td>
<td>The server that hosts the license service</td>
</tr>
<tr>
<td>port</td>
<td>-p</td>
<td>PortNumber</td>
<td>The port of the server to be connected</td>
</tr>
</tbody>
</table>
#### Turning on workflow

IBM Sametime Advanced supports workflow APIs for approving chat room and broadcast community creation.

**About this task**

When you turn on workflow APIs, and a user creates a chat room or a broadcast community, it is not automatically created, but it is placed in a queue. A designated workflow approver must monitor the queue, and then approve or deny the request to create a chat room or community. Queue monitoring and chat room and community approval can only be done by writing your own code using the workflow APIs. You can find information on using the workflow API calls in the *Sametime Advanced Software Development Kit* at IBM developerWorks at [http://www.ibm.com/developerworks/lotus/downloads/toolkits.html](http://www.ibm.com/developerworks/lotus/downloads/toolkits.html).

Follow these instructions for turning on workflow APIs.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Advanced Servers**.
3. In the **Sametime Advanced Servers** list, click the deployment name of the server with the information that you want to add or change.
4. Click the **Administrative Settings** tab.
5. Select one or both of the following check boxes:
   - Enable chat room workflow API
   - Enable community workflow API
6. Click **OK**.

**What to do next**

Assign or change workflow approvers in the WebSphere Integrated Solutions Console. Go to **Servers > Application servers > server_name > Installed applications > Sametime Advanced Application > Security role to user/group mapping**.

---

### Changing the administrator password for Sametime Advanced

The following topics explain how to change your administrator passwords.
**Updating your DB2 password for Sametime Advanced**

If you change your administrator password in IBM DB2, you must update your password in the Sametime System Console, as well as the Meeting Server and, if applicable, Sametime Advanced. If you do not update your password, IBM Sametime stops working.

**Procedure**

1. Log in to the Integrated Solutions Console for the Sametime System Console.
2. Click **Resources > JDBC > Data sources**.
3. Click the data source in the table.
4. Under Related Items, click **JAAS - J2C authentication data**.
5. Click your DB2 administrator alias.
6. Under General Properties, type your new password.
7. Click **Apply** and then click **OK**.
8. Repeat this procedure for the Sametime Meeting Server and, if applicable, the Sametime Advanced server.
9. Restart the Sametime System Console and Meeting Server or Advanced Server.

The changed password only takes effect after you restart the server, so be sure to restart the server.

**Updating your LDAP Bind password for Sametime Advanced**

You can change the LDAP Bind password that you defined when you first connected the LDAP server.

**About this task**

Change your LDAP Bind password by running the Connect to LDAP Servers prerequisite in the Sametime System Console. Changing the password updates the Sametime Community Server database, stconfig.nsf and the WebSphere Application Server. Then send the update to any other Deployment Managers in the environment and to the Directory Assistance database on the Sametime Community Server.

**Procedure**

1. From the Sametime System Console, run the Connect to LDAP Servers prerequisite. Update the LDAP Bind password when you are prompted to do so and save the changes.
   The change updates the LDAP repository configured for WebSphere Application Server.
2. Wait for the next scheduled update task to run, which updates the LDAP Server document in the Sametime Community Server configuration database (stconfig.nsf) with the password change.
3. If the Sametime System Console is the Deployment Manager for all Sametime servers, proceed to the next step.
   If there are other Deployment Managers in the Sametime environment, update the Bind password on each Deployment Manager. Make the change by editing the LDAP repository as described in the WebSphere Application Server information center topic Lightweight Directory Access Protocol repository configuration settings.
a. From the Notes client, open the Directory Assistance database (usually named da.nsf) on the Community Server.

b. Open the Directory Assistance document for the LDAP server.

c. On the LDAP tab, under Connectivity Settings, update the Administrator password.

d. Save and close the document.

5. Restart the Community Servers, Deployment Managers, and Application Servers that share the LDAP repository.

Related tasks
“Connecting to an LDAP server” on page 265
Use the IBM Sametime system console to connect IBM Sametime servers to an LDAP server that has already been installed and configured. An LDAP server is required for these server offerings: community server, meeting server, media manager, and gateway.

“Creating a Directory Assistance document” on page 710
The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the LDAP server.

Updating your WebSphere Application Server administrator password for Sametime Advanced
You can change your WebSphere Application Server administrator password.

About this task
You can change your WebSphere Application Server administrator (wasadmin) password on the following WebSphere-based Sametime servers. If you change the wasadmin password on any of these servers, then you must also update the wasadmin password for that server that is stored in the Sametime System Console.

- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Gateway Server
- SIP Proxy and Registrar
- FIPS Proxy Server
- Sametime Advanced

The complete Sametime Media Manager installations are listed under both the Media Manager and the SIP Proxy and Registrar administration listings. There is only one entity and changing the connection properties in one place is reflected in the other.

A FIPS Proxy Server uses the same credentials as the Sametime Proxy Server on which it was installed. Changing the credentials in either location affects both administrative connections. The FIPS Proxy Server list depends on a valid server connection, so if the connection information is not correct, the FIPS Proxy server is not be listed. You can correct this by editing the connection properties in the Sametime Proxy Server listing.
Procedure
1. Change the wasadmin password of the WebSphere-based Sametime application server.
   a. Log in to the Integrated Solutions Console on the WebSphere-based Sametime application server.
   b. Click Users and Groups > Manage Users.
   c. Under Search for Users, select User ID in the Search by field, and then enter wasadmin in the Search for field. Click Search.
   d. Click wasadmin in the results dialog.
   e. Enter a new password in the Password and Confirm Password fields.
   f. Click Apply and then click OK.
2. Update the wasadmin password that you changed in the previous step on the Sametime System Console.
   a. Log in to the Integrated Solutions Console for the Sametime System Console.
   b. Click Sametime System Console > Sametime Servers.
   c. Click the Sametime application server that has the wasadmin password that you changed in step 1.
   d. Locate the deployment name and click Edit under Connection Properties.
   e. Enter a new password.
   f. Click Save and then click Done.

Integrating Sametime Advanced with Connections

You can integrate your IBM Connections communities into IBM Sametime Advanced. Integrating Connections with Sametime Advanced provides users with a unified list of Connections communities and broadcast communities on the Broadcast Communities tab in Sametime Advanced.

Granting an administrator rights to Connections 1.0.2 communities

Before you can integrate your IBM Sametime Advanced communities with IBM Connections 1.0.2 communities, you need to grant superuser access to a Sametime Advanced administrator in Connections. You do this by adding a grant access statement to the community.policy file.

Procedure
1. You need to determine your realm name.
   a. In the Integrated Solutions Console, click Security > Secure administration, applications, and infrastructure.
   b. Select Federated Repositories, and then click Configure.
   c. On the main Federated repositories page note the realm name for your Connections server.
2. Determine the location of the community.policy file.
   a. In the Integrated Solutions Console, click Servers > Application Servers
   b. Click Connections_server_name.
   d. Click Java Virtual Machine.
Under Additional Properties, click Custom Properties. The communities.policy file location is contained in the 'java.security.auth.policy' custom property.

3. Open the community.policy file from the location you determined in the previous step with a text editor.

4. Add a new grant statement like the one in the following example:

```python
grant Principal com.yourcompany.ws.security.common.auth.WSPrincipalImpl
"<YOUR_REALM_NAME>/<YOUR_ADMINISTRATIVE_USER_LOGIN_ID>"
  permission com.yourcompany.tango.auth.permission.CommunityManagementPermission "*";
  permission com.yourcompany.auth.permission.CommunityMembershipPermission "*";
  permission com.yourcompany.tango.auth.permission.CommunityAccessPermission "*";
  permission com.yourcompany.tango.auth.permission.CommunityReferencePermission "*";
};
```

- **YOUR_REALM_NAME** was determined in step 1.
- **YOUR_ADMINISTRATIVE_USER_LOGIN_ID** should be the same as the one in Connections administrative settings of the Server Integration view of the Administration page in Sametime Advanced.

The login id is case sensitive, and it should be exactly the same as in LDAP.

5. Save the community.policy file.

### Granting an administrator rights to Connections 2.5 communities

To grant an administrator rights to IBM Connections 2.5 communities, you need to create a superuser who has access to all communities, public and restricted.

### About this task

With additional configuration on the Connections server, you can create a superuser who can see all communities, public and restricted. For IBM Sametime Advanced integration, you need to create a user of this type, and add their login and password credentials to the Sametime Advanced server so that you can connect on their behalf to list all of the communities.

### Procedure

1. To determine the user realm for the new administrative user, do the following:
   a. In the IBM WebSphere Application Server Integrated Solutions Console, select Security > Secure Administration, applications and infrastructure > Federated Repositories.
   b. Click Configure.
   c. On the main Federated repositories page, note the value for the realm name for your application server.

2. Open a command window and start the wsadmin command line tool. See Starting the wsadmin client in the Connections 2.5 information center:

3. Use one of the following commands to access the Communities configuration files:
   - Stand-alone deployment:
     ```
     execfile("/communitiesAdmin.py")
     ```
   - Network deployment:
     ```
     execfile("<WAS_HOME>/profiles/<DMGR>/bin lc_admin/communitiesAdmin.py")
     ```
4. Check out the Communities policy configuration file using the following command:

```
CommunitiesConfigService.checkOutPolicyConfig("working_directory", "cell_name")
```

where:
- `working_directory` is the temporary working directory to which the configuration XML and XSD files are copied. The files are kept in this working directory while you make changes to them. △
- `cell_name` is the name of the WebSphere Application Server cell hosting the Connections feature. This argument is required even in stand-alone deployments. This argument is also case-sensitive, so type it with care.

For example:

```
CommunitiesConfigService.checkOutPolicyConfig("/temp", "foo01Cell01")
```

5. From the temporary directory to which you just checked out the Connections configuration files, open the `communities-policy.xml` file in a text editor.

6. To add an administrative user with rights to access all Connections communities, add the following grant statement to the file:

```
<comm:grant>
  <comm:principal class="com.ibm.ws.security.common.auth.WSPrincipalImpl" name="YOUR_REALM_NAME/YOUR_LOGIN_ID" />
  <comm:permission class="com.ibm.tango.auth.permission.CommunityManagementPermission" communityType="*" action="*" />
  <comm:permission class="com.ibm.tango.auth.permission.CommunityMembershipPermission" communityType="*" action="*" />
  <comm:permission class="com.ibm.tango.auth.permission.CommunityAccessPermission" communityType="*" action="*" />
  <comm:permission class="com.ibm.tango.auth.permission.CommunityReferencePermission" communityType="*" action="*" />
  <comm:permission class="com.ibm.tango.auth.permission.CommunityBroadcastPermission" communityType="*" action="*" />
</comm:grant>
```

where:
- `YOUR_REALM_NAME` is the realm name you identified in step 1.
- `YOUR_LOGIN_ID` is the login ID of the user who you want to set up as the administrator for communities.

7. Save your changes to the `communities-policy.xml` file.

8. Check in the updated file using the following wsadmin client command:

```
CommunitiesConfigService.checkInPolicyConfig("<working_directory>", "<cell_name>")
```

9. To exit the wsadmin client, type exit at the prompt.

10. Stop and restart the server hosting the Communities feature.

**Results**

When the user specified in the policy file logs in to Communities, they will be able to view and edit all communities and community resources.

**Synchronizing Sametime Advanced with Connections**

You can synchronize IBM Connections communities with IBM Sametime communities just once, or set up automatic daily synchronization.

**Before you begin**

Connections 2.5 and 2.5.0.1 require fixes for communities synchronization.
- Connections 2.5 fix
- Connections 2.5.0.1 fix
About this task

Integration and synchronization is "one-way": from Connections to Sametime Advanced. Therefore, users can see their Connections communities in Sametime Advanced, but they do not see broadcast communities in Connections. These communities cannot be edited in Sametime Advanced; they can only be edited in Connections.

Synchronization does not support HTTP redirection. If the Connections server is configured to redirect from one port to another, for example from HTTP to HTTPS, then synchronization fails.

You must be an administrator for both Sametime Advanced and Connections before you can synchronize the communities. Before you begin, you must grant a Sametime Advanced administrator access rights to Connections communities in the connection.policy file. See the previous topic for more information. This administrator must also be a member of the LDAP directory.

Procedure

1. Log in to the Sametime System Console.
2. Click Sametime Servers > Sametime Advanced Server.
3. Select the Sametime Advanced server.
4. On the Administrative Settings tab, find the Connection settings
5. Select the protocol type.
6. Type the fully qualified host name in Host name.
7. Type the port number in Port.
8. Enter the administrator user name and password. This is the administrator ID that was granted superuser rights to access Connections communities in the Connections community.policy file. See the previous topic, "Granting an administrator rights to access Connections communities."
9. If you want to automate community synchronization so that it happens daily, select Enable daily community synchronization. The servers will synchronize daily at 2 AM in the time zone of the Sametime Advanced server.
10. If you want to synchronize immediately, click Synchronize Now.

Setting up community synchronization with HTTPS

Since IBM Connections authentication uses HTTPS, you need to follow these instructions to set up synchronization between IBM Sametime Advanced and Connections communities.

Procedure

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console of the Connections server.
2. Click Security SSL Certificate and key management.
3. Under Related Items, click Key store and certificates.
4. Click NodeDefaultTrustStore.
5. Under Additional Properties, click Signer Certificates.
6. In the table, select the certificate that has a "default" alias issued to CN=connections_server_host,O=..., and then click Extract.
7. Enter a file name, and click OK.
Note: This file name is saved to the file system of the Connections server.

9. Copy the file containing the certificate from the Connections server file system to the Sametime Advanced server file system.
10. Log in to the WebSphere Application Server Integrated Solutions Console of the Sametime Advanced server.
11. Click **Security SSL Certificate and key management**.
12. Under Related Items, click **Key store and certificates**.
13. Click **NodeDefaultTrustStore**.
14. Under Additional Properties, click **Signer Certificates**.
15. Click **Add**.
16. Enter an alias for the certificate such as **Connection Server Certificate**.
17. Enter the path of the file where the certificate is saved.
18. Click **OK**.
19. Save the changes.

**Monitoring Sametime Advanced**

You can monitor chat room and community usage.

**About this task**

The following topics describe how you can monitor statistics in chat rooms and broadcast communities. In addition, if you want to monitor IBM Sametime Advanced at a more detailed level, you can write instructions using the monitoring API calls defined in the *Sametime Advanced Software Development Kit*. You can find the SDK on IBM developerWorks at [http://www.ibm.com/developerworks/lotus/downloads/toolkits.html](http://www.ibm.com/developerworks/lotus/downloads/toolkits.html).

**Monitoring chat room statistics**

IBM Sametime Advanced users can view statistics for all chat rooms in the folder hierarchy.

**About this task**

Administrators, folder managers, chat room owners, and chat room creators can view statistics for all chat rooms they have access to. Administrators have access to everything, so the summaries they see reflect an accurate calculation for all chat rooms. Because individual users can only view statistics for chat rooms to which they have manager or author access, they may see smaller totals depending on how many chat rooms and folders are private. For example, if a user does not have access to a chat room, the chat room owner for that chat room would not be included in the total count.

Statistics are shown in the following views:

- **Summary** - Statistics are summarized by chat room, participant, and folder. Some of the statistics are described below.
  - **Added as My chat rooms by users**
    This statistic displays the number of chat rooms that have been added by users to their My chat rooms lists. Assume two users have created My chat rooms list at your site. Betty has ten chat rooms in her list and Jerry has four chat rooms in his list, so the total is 14.
- **Archived chat rooms**
  This statistic shows the total number of chat rooms that are archived. Archived chat rooms are not physically archived (from the database), but are put into a different view in the All Chat Rooms tab.

- **Participants**
  This statistic shows the total number of members that have access for all chat rooms, whether or not they have gone into the chat rooms. Invited participants are the total number of members and managers for all chat rooms.

- **Chat room owners**
  This statistic shows the total number of unique users who created chat rooms.

- **FAQs for chat rooms**
  This statistics shows the total number of persistent chat FAQs for all chat rooms.

- **Total folders**
  This statistic shows the total number of global folders.

- **Usage** - Chat rooms are listed alphabetically. The number of entries, active participants, and last logins are listed for each chat room.
- **Owners** - Owners are listed by the chat room owner’s user ID. The number of chat rooms owned, entries, and bookmarks are listed for each chat room owner.

### Procedure

Follow these steps to view chat room statistics:

1. In Sametime Advanced, click the **All Chat Rooms** tab.
2. Click **Chat Room Statistics**.
3. Click the tab for how you want to display statistics.

### Monitoring broadcast community statistics

You can monitor the number of IBM Sametime broadcast communities and the number by type of broadcast community: open, private, restricted recipient, and restricted publisher. Only administrators and community creators can view broadcast community statistics. Users will see items on this page to which they have author access.

### About this task

Follow these steps to view broadcast community statistics:

**Procedure**

1. In Sametime Advanced, click the **Broadcast communities** tab.
2. Click **Communities Statistics**.

### Archiving chat rooms

IBM Sametime administrators, folder managers, and chat room owners can archive chat rooms. Archiving the chat room will place it in the archive view and remove it from other views for all participants.
**About this task**

When a chat room is archived, it is moved from the Chat Rooms view of the All Chat Rooms tab and placed in the Archived Chat Rooms view. Only administrators, folder managers, and chat room owners with archived chat rooms can see or access the Archived Chat room view. Other users can no longer enter or even see the chat room. If the chat room was in a user’s My Chat Rooms tab, then it is removed from that view after it have been archived.

If you would rather temporarily suspend participation and end access to a chat room without removing it from the Chat Rooms view, you should disable it instead of archiving it.

Follow these steps to archive a chat room.

**Procedure**

1. In Sametime Advanced, click **All Chat Rooms**.
2. Click the name of the chat room that you want to archive.
3. Click **More Actions > Archive**.
4. When the confirmation message appears, click **OK**.

**Results**

The chat room is moved to the **Archived Chat Rooms** view.

---

**Disabling chat rooms**

IBM Sametime administrators, folder managers, folder authors, and chat room owners can disable chat rooms. Disabling the chat room prevents users from entering it, posting new content or reading the chat history.

**About this task**

If you would rather prevent users from entering a chat room as well as automatically removing it from the All Chat Rooms view so that users can no longer see it, you should archive the chat room instead of disabling it.

Follow these steps to disable a chat room.

**Procedure**

1. In Sametime Advanced, click **All Chat Rooms**.
2. Click the name of the chat room that you want to archive.
3. Click **More Actions > Disable**.
4. When the confirmation message appears, click **OK**.

---

**Backing up user data**

All IBM Sametime Advanced user data is stored in an IBM DB2 database, and can be backed up using the DB2 backup commands.
Before you begin

About this task

The default Sametime Advanced configuration requires that DB2 be shut down for backup. This is because by default, DB2 is configured to reuse the recovery logs. If you want online backup, the database can be configured to archive the recovery logs. In that case, the database is backed up, and all archived recovery logs are backed up. The recovery logs that have been backed up must also be periodically removed. If the database runs out of space to archive the recovery logs, the database will stop accepting changes until space is available.


The only special backup consideration for Sametime Advanced is that because the full text indexes are maintained outside of the database tablespaces, after a restore operation the `dbtext.sh` or `dbtext.bat` scripts should be run to drop and recreate the text indexes to match the restored data in the database. You can find these scripts at CD1/SupportingFiles/DB2.
Chapter 7. Tuning Sametime Advanced

Complete the following tuning procedures to enhance performance.

Tuning WebSphere Application Server in a Sametime Advanced deployment

When you installed the IBM Sametime server software, the IBM WebSphere Application Server was installed automatically. Complete the following tuning procedures to enhance performance of the WebSphere Application Server. Some procedures must be repeated on each server in a cluster.

Setting thread pool values in a Sametime Advanced deployment

Set the thread pool values for an IBM Sametime Advanced server to improve performance. By using a thread pool, server components can reuse existing threads, which helps improve performance by reducing the overhead of creating new threads at run time.

Procedure

1. From the Integrated Solutions Console, click Servers > Application Servers > \textit{stadvanced\_server\_name}, and then under Additional Properties, click Thread Pools.
2. Click Default.
3. Change the values for Minimum Size and Maximum Size to 50.
4. Click OK, and click Save to save changes to the master configuration.
5. If Sametime Advanced is clustered, repeat the preceding steps for each node of the cluster.

Tuning the JVM in a Sametime Advanced deployment

The IBM WebSphere Application Server is a Java based process and requires a Java virtual machine (JVM) environment to run and support IBM Sametime Advanced. You can tune the Java runtime environment for performance by turning on verbose garbage collection and setting the heap size.

About this task

Note: The following instructions contain settings that were tested in IBM labs. These are just a starting point. Since your deployment might have a configuration unique to your site, these settings might require more adjustment.

Procedure

1. From Integrated Solutions Console, click Servers > Application Servers > \textit{stadvanced\_server\_name}.
4. Select the Verbose garbage collection check box.
5. In the **Generic JVM arguments** field, type the following values. These values may vary depending on the amount of memory on the machine, operating system, and the load for the Sametime Advanced server.

   -Xgcpolicy:gencon -Xms1536m -Xmx1536m -Xms1344 -Dsun.nio.MaxDirectMemorySize=524288000

   **Note:** Solaris does not support this setting.

6. Click **OK**, and click **Save** to save changes to the master configuration.

7. Click **Custom properties**.

8. Click **New**.

9. Add the property com.ibm.websphere.security.util.authCacheMaxSize, with a value of 120000.

10. If Sametime Advanced is clustered, repeat the preceding steps for each node of the cluster.

### Tuning access to the LDAP server in a Sametime Advanced deployment

Set the context pool parameters to improve the performance of concurrent access to an LDAP server.

**About this task**

The context pool is used in virtual member manager to improve the performance of concurrent access to an LDAP server. Use the Integrated Solutions Console on the Deployment Manager. You can also edit values in the wimconfig.xml file stored here:

C:\ProgramFiles\IBM\WebSphere\AppServer\profiles\ST_Advanced_Profile\config\cells\machineNameCell\wim\config\wimconfig.xml

**Note:** The following instructions contain settings that were tested in IBM labs. Adjust these settings as needed for your specific environment.

**Procedure**

1. In the Integrated Solutions Console for the Deployment Manager, click **Security** > **Global security**.

2. Under User account repository, select **Federated repositories** from the Available realm definitions field and click **Configure**.

3. Under Related items, click **Manage repositories**.

4. Select the configured LDAP repository.

5. Under Additional properties, click **Performance**.

6. Set the following context pool parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size (maxPoolSize): 200</td>
<td>Specifies the maximum number of live connections. If there is no available connection in the pool when the request is submitted, the request waits the number of milliseconds specified in poolTimeOut. After this amount of time has passed, if no connection is available and the current number of live connections is less than the maxPoolSize, a new connection is created. If the total number of live connections is equal to or larger than maxPoolSize, an exception is thrown.</td>
</tr>
<tr>
<td>(Can be set only in the wimconfig.xml file) poolWaitTime=&quot;5000&quot;</td>
<td>Specifies the number of seconds a connection can exist in the connection pool. When requesting a connection from the pool, if this connection already exists in the pool for more than the time defined by poolWaitTime, this connection is closed and a new connection is created for the request. After the connection is used it is returned to the pool. If this parameter is set to 0, a new connection is created for each request and no connection are put into the pool for reuse. If this parameter is set to -1 or any negative number, the connection does not expire and is reused until the connection is turned off (for example by a firewall or a socket timeout). The default value is -1.</td>
</tr>
<tr>
<td>Preferred size (prefPoolSize): 20</td>
<td>Specifies the preferred number of context instances that the context pool will maintain. Context instances that are in use and those that are idle contribute to this number. When there is a request for the use of a pooled context instance and the pool size is less than the preferred size, the context pool creates and uses a new pooled context instance regardless of whether an idle connection is available. When a request finishes with a pooled context instance and the pool size is greater than the preferred size, the context pool closes and removes the pooled context instance from the pool. The valid range for this parameter is from 0 to 100. Setting the value of this parameter to 0 means that there is no preferred size and a request for a pooled context instance results in a newly created context instance only if no idle ones are available. The default value is 3.</td>
</tr>
<tr>
<td>Cache the attributes Cache size: 80000</td>
<td>Specifies the number of LDAP attributes that are cached by the server.</td>
</tr>
<tr>
<td>Cache the search results Cache size: 80000</td>
<td>Specifies the number of LDAP search results that are cached by the server.</td>
</tr>
</tbody>
</table>
7. Save the changes.

Tuning the web container in a Sametime Advanced deployment

You can set the time that the HTTP transport channel allows a socket to remain idle between requests.

About this task

The IBM WebSphere Application Server web container manages all HTTP requests to servlets, JavaServer Pages and web services. Requests flow through a transport chain to the web container. WebSphere Application Server will close a given client connection after a number of requests or a timeout period. You can set a value for persistent timeouts to specify the amount of time, in seconds, that the HTTP transport channel allows a socket to remain idle between requests.

Note: The following instructions contain settings that were tested in IBM labs. These are just a starting point. Since your deployment might have a configuration unique to your site, these settings might require more adjustment.

Procedure

1. From the Integrated Solutions Console, click Servers > Application Servers > stadvanced_server_name > Web Container Settings > Web container transport chains > WCInboundDefault > HTTP inbound channel (HTTP_2).
2. Under General Properties, enter the following timeout values:
   - Persistent timeout: 60
   - Read timeout: 90
   - Write timeout: 90
3. Under Persistent connections, select Unlimited persistent requests per connection.
4. Click OK and save the master configuration.
5. From the Integrated Solutions Console, click Servers > Application Servers > stadvanced_server_name > Web container transport chains > WCInboundDefault > TCP inbound channel (TCP_2).
6. Under General Properties, enter the following values:
   - Maximum open connections: 60000
   - Inactivity timeout: 600
7. Click OK and save the master configuration.
8. From the Integrated Solutions Console, click Servers > Application Servers > stadvanced_server_name > Web container > Session management.
9. Under General Properties, for the Maximum in-memory session count, enter 5000.
10. Click OK and save the master configuration.

Tuning database connections in a Sametime Advanced deployment

To improve performance for an IBM Sametime Advanced server, change the default database connection pool values.
Tuning cache instances in a Sametime Advanced deployment

To improve performance for an IBM Sametime Advanced server, change the default size of cache instances.

Procedure
1. From the Integrated Solutions Console, click Resources > Cache instances > Object Cache instances.
2. From the dropdown list, select Node and stadvanced_server_name.
3. Click New.
4. For Name, enter WSsecureMap.
5. For JNDI name, enter ws/WSSecureMap.
6. For the Cache size, enter 80000.
7. Leave all the other default values as is. Click OK, and click Save to save changes to the master configuration.
8. If Sametime Advanced is clustered, repeat the preceding steps for each node of the cluster.

Tuning security in a Sametime Advanced deployment

Enabling security decreases performance. Authentication information persists in the system for a limited amount of time before it expires and must be refreshed.

About this task

Use the following procedure to tune performance without compromising your security settings.

Procedure
1. From the Integrated Solutions Console, click Security > Global security > LTPA.
2. Increase the LTPA timeout to be 720 minutes (12 hours).
3. Click Apply, and then click OK.

Tuning DB2 for Sametime Advanced

IBM DB2 is a database management system that stores information used by IBM Sametime Advanced. A database that has the potential to grow large requires some ongoing tuning by a database administrator.

About this task

Periodically, as the dataset grows, the database administrator should reorganize the objects that need attention, and update the statistics so that the DB2 optimizer can make optimal plans for accessing the data. Sametime Advanced provides an example script that reorganizes the indexes that are most likely to require attention.
and then updates the statistics in the catalog. The script is called stadv_reorg.sql and is stored in the STAdvancedLaunchpad\disk1\DatabaseScripts directory within the Sametime Advanced software download. This script or one like it should be run periodically when the system is lightly loaded, as it will lock the tables as it runs.

Procedure

Follow these steps to reorganize the indexes by running a version of the stadv_stadv_reorg.sql script that you have customized for your site.

1. On the DB2 machine, log in with the database administrator account.
2. Open a DB2 command window.
3. From the command line, enter
   
   ```
   db2
   ```
   
   4. Enter the command to connect to the Sametime Advanced database
   
   ```
   connect to advanced_database_name
   ```
   
   where `advanced_database_name` is the name of the Sametime Advanced database.

5. Run the script with the following command:

   ```
   db2 -tf stadv_reorg.sql
   ```

6. Enter the following commands to update relevant tables and columns in the database:

   ```
   update sysstat.tables set card=100000,npages=10000,fpages=15000 where tabname = 'USER_CONNECTION';
   update sysstat.tables set card=100000,npages=10000,fpages=15000 where tabname = 'COMMUNITY_SUBSCRIPTION';
   update sysstat.columns set colcard = 50000 where tabname = 'USER_CONNECTION' and colname = 'MEMBERID';
   update sysstat.columns set colcard = 50000 where tabname = 'COMMUNITY_SUBSCRIPTION' and colname = 'CLIENTID';
   update sysstat.columns set colcard = 5 where tabname = 'USER_CONNECTION' and colname = 'NODEID';
   update sysstat.columns set colcard = 50000 where tabname = 'COMMUNITY_SUBSCRIPTION' and colname = 'TOPIC';
   ```

Tuning DB2 text indexes for Sametime Advanced

IBM DB2 is a database management system that stores information used by IBM Sametime Advanced. A database that has the potential to grow large requires some ongoing tuning by a database administrator.

About this task

The database administrator should monitor the DMS tablespaces and add additional storage as needed. The default tablespace creation scripts allow the tablespaces to automatically grow to a set size. This set size can be changed, or additional files can be added to the tablespace as needed.

The database administrator may wish to do additional maintenance on the full text indexes that are maintained outside of the database. The text indexes can be altered after they are created to modify the frequency of updates. Incremental commits can be configured if the update transactions become too large, and the indexes can be reorganized. If for any reason, a text index becomes corrupted, re-running dbtext.bat or dbtext.sh will drop all text indexes and recreate them.

Dropping a database does not automatically drop the text indexes. If the database administrator decides to drop a database that contains text indexes, the administrator should also run the script dropdbtext.bat or dropdbtext.sh to drop the text indexes first. If the indexes are not dropped, entries for them should be cleaned out of the DB2 ctedem.dat file.
Related information

- Maintaining text indexes
- Dropping a database

---

Setting open file limits in a Sametime Advanced deployment

If you have a high volume of users logged in to IBM Sametime Advanced running on a Linux server, you might encounter too many files exception messages.

About this task

After 1000 or more users log in, the following exception starts appearing in the SystemOut.log, and no more users can log in:

```
```

```
```

This problem is caused when a high number of concurrent users get a connection to the Sametime Advanced server. Java opens many files and Sametime Advanced uses a lot of file descriptors. Eventually, the server runs out of file descriptors. You can fix this by editing the file descriptor limit in the limits configuration file in Linux.

Procedure

1. Use a text editor and open `/etc/security/limits.conf`.
2. Add the following lines to set these limits for all users.
   ```
   * soft nofile 65535
   * hard nofile 65535
   ```
3. Save the file.
4. Stop and restart the machine running the server.
Chapter 8. Troubleshooting Sametime Advanced

Use the following topics to troubleshoot problems.

Other sources of information

Use the following links to find other hints and tips when troubleshooting IBM Sametime Advanced:

- Sametime wiki:
  www-10.lotus.com/ldd/stwiki.nsf/dx/Sametime_Advanced_Troubleshooting_Guide
- Tech Notes for Sametime Advanced:
  www.ibm.com/support/search.wss?q=Sametime%20Advanced&rs=477&tc=SSKTXQ&dc=DB520&dtm

Setting a diagnostic trace for Sametime Advanced

You can specify how the server handles IBM Sametime Advanced log records. You can select a Sametime Advanced server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and trace.
2. Click the Sametime Advanced Server.
3. Under General Properties click Diagnostic Trace
4. Under Additional Properties, click Change Log Detail Levels.
5. Choose whether to make configuration or runtime changes.
   - Click the Configuration tab if you want to save the changes after a server restart.
   - Click the Runtime tab to make changes that are not saved, but will apply until the server is restarted.
6. In the text box, append the following settings:
   **=info: com.ibm rtc.messaging.=fine: com.ibm rtc.poll.==fine: com.ibm rtc.servlet.==all

   To get even more detailed traces, use this setting instead:
   **=info: com.ibm rtc.==all
7. Click Apply, and then Save.
8. Monitor the log file in IBM\WebSphere\AppServer\profiles\HostName_STADV_deploymentType_Profile_Number\logs
9. If you made changes in the Configuration tab, restart the server.

Logging and tracing in Sametime Advanced

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem
A determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

---

### Gathering logs and traces for Sametime Advanced

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

**About this task**

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

**Procedure**

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   
   For more information, see the following topic in the WebSphere Application Server information center:
   
   Gathering information with the collector tool (deprecated)

2. Run the collector on the IBM Sametime Advanced server.
   
   - Run collector on the WebSphere Application Server profiles.
     
     The profiles are stored in the `\profiles` directory; for example on Microsoft Windows:
     
     ```
     C:\Program Files\ibm\WebSphere\AppServer\profiles
     ```
     
     - The collector resides in the `\bin` directory below the profile; for example:
     
     ```
     C:\Program Files\ibm\WebSphere\AppServer\profiles\HostName_STADV_deploymentType_Profile_Number\bin\collector.bat
     ```
     
     The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
     
     ```
     HostName_STADV_deploymentType_Profile_Number-WASenv.jar
     ```
     
     **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. Submit the collector generated log files to IBM support.
Troubleshooting Sametime Advanced using JVM logs

To start troubleshooting a problem on IBM Sametime Advanced, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the Sametime Advanced Server.

   Note: Any configuration changes to the JVM logs that are made to a running Sametime server do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting WebSphere Application Server failed startup

In the event that a change is made to an IBM WebSphere Application Server component of IBM Sametime Advanced, WebSphere Application Server could fail to start.

Procedure

1. Use a text editor to open the WebSphere Application Server file here:
   `<was_home>\Appserver\profiles\<st_adv_profile>\config\cells\<cellName>\nodes\<node_name>\servers\<st_adv_server>\server.xml`.
2. In the server.xml file, search for jvmEntries. For example:
   ```xml
   <jvmEntries xmi:id="JavaVirtualMachine_1190064977109" verboseModeClass="false" verboseModeGarbageCollection="false" verboseModeJNI="false" initialHeapSize="1024" maximumHeapSize="1280" runHProf="false" debugMode="false"```
If the JVM arguments are incorrect, you must modify the `genericJvmArguments` attribute of the `jvmEntries` element of server.xml. You could leave it blank, to eliminate all errors, or try modifying the value of the attribute until it is correct. Two value here are the heap sizes. These values are set when you set the JVM garbage collection policy. But you can set them in the server.xml as well. These values are the `initialHeapSize` with a recommended value of 1024, and `maximumHeapSize`, set to a recommended value of 1280.

3. Save the file and restart the server.

### Troubleshooting authentication with Sametime Advanced

If users are having difficulties authenticating with IBM Sametime Advanced, check their browser settings for cookies and language.

**About this task**
- Authenticated users cannot enter chat rooms unless they accept cookies. If a user logs in to Sametime Advanced and cannot enter a chat room where the user is listed as a member, the user should be sure that the browser is accepting cookies.
- Users might have be unable to authenticate if their user IDs and passwords contain characters that are not part of the character set of the language that their browsers use.

Follow these instructions to enable cookies and set the language for your browser:

**Procedure**
1. Open your browser.
2. If you are using Microsoft Internet Explorer, follow these steps:
   a. Click **Tools > Internet Options**.
   b. Click the **Privacy** tab.
   c. Move the slider to an appropriate selection for your site that accepts cookies.
   d. Click the **General** tab.
   e. Click **Languages**.
   f. Use the **Remove** and **Add** controls to set your browser to the language whose character set you use in your ID and password.
   g. Click **OK**.
3. If you are using Mozilla Firefox, follow these steps:
   a. Click **Tools > Options**.
   b. Click the **Privacy** button.
   c. Under Cookies, select **Accept cookies from sites**.
   d. Click the **Advanced** button.
   e. Click the **General** tab.
   f. Click the **Choose** button.
   g. Select the language whose character set you use in your ID and password.
h. Click OK.
4. Click OK.
Chapter 9. Overview

Learn more about how to install and configure IBM Sametime for instant messaging and web conferences.

This section contains an overview of the components of IBM Sametime for installers and administrators.

Accessibility features for Sametime

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully. IBM strives to provide products with usable access for everyone, regardless of age or ability.

Accessibility features

The Lotus Sametime System Console is based on the IBM WebSphere Application Server Integrated Console, and shares the same accessibility features, described below.

Note: The best accessible experience can be had using the latest versions of both the screen reader and browser.

• The following features are for vision-impaired users:
  – Can be operated by using only the keyboard
  – Communicates all information independent of color
  – Supports interfaces commonly used by screen readers and screen magnifiers
  – Supports the attachment of alternate output devices
  – Provides help information in an accessible format
  – Supports high contrast using a white background (some icons may not display properly on a colored background)

  Attention: If you modify the level of contrast, you must restart the Sametime client for the change to take effect.

When a Sametime web browser user chooses to share the screen, the user is prompted with three options: to share the entire screen, part of the screen, or a particular application. For this prompt to be accessible to a screen reader, the user must install the Java access bridge. For installation instructions, see the Oracle web site.

• The following features are for users who have mobility impairments or limited use of their hands:
  – Allows the user to request more time to complete timed responses
  – Can be operated by using only the keyboard
  – Supports the attachment of alternative input and output devices

• The following features are for the deaf and hard of hearing users:
  – Supports alternatives to audio information
  – Supports adjustable volume control

• The console does not flash the screen at rates that could induce epileptic seizures
The help system for Integrated Solutions Console has the following accessibility features:

- Uses the accessibility support enabled by the browser that is used to display the help
- Enables navigation by using the keyboard

The Sametime Information Center is accessibility-enabled. The accessibility features of the information center are described at: Accessibility and keyboard shortcuts in the information center.

**Keyboard navigation**

To move through the controls on a particular page, use the Tab key.

To click a link or control on a page using the keyboard, navigate to the link or control and press Enter.

To make a selection in a checkbox, use the Space key.

To change the navigation view using the keyboard, follow these steps:
1. Navigate to the View selection list using the Tab key.
2. Use the up and down arrows to change the value of the selection list.
3. Press Enter.

The tasks displayed in the navigation are changed according to your selection.

**Related accessibility information**

When you administer WebSphere Application Server settings, you work in the Integrated Solutions Console. Detailed information on console accessibility is provided in the WebSphere Application Server information center.

**IBM and accessibility**

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility:

---

**What's new in this release?**

Learn more about the new features in this release that allow IBM Sametime to make unified communications in your organization simple and effective.

**What's new in Sametime 8.5.2**

**New platforms**
- Microsoft Windows 2008 R2
- Novell SLES 11 Linux
- IBM Websphere Application Server 7.0.0.3
- IBM DB2 9.7

**Web browser meetings improvements to extend access and reach**
- Browser plug in installs on demand or pre-installed; also supports third party video integration
- New Call & video controls
• List of participants: shows connection, presence & muted status
• Call Controls: Connect/disconnect, Adjust Volume, Hold/Resume
• Moderator Controls: Mute/Unmute all, Mute another person, Lock call, End call for everyone, Hang up participant
• Video Controls: Show/Hide own video, Hold/Resume, Pause/Resume

New meetings tools for web browser users
• Meetings open in a new tab or window
• Jump forward or backwards in the slide deck
• Create and send polls
• Click to return to the meeting room center
• Pointer and highlighters

Manage access to meeting rooms
• Prevent entry without room owner or manager present
• Eject users from a meeting room
• End meeting session for all
• Room delete for system administrators

Chat and contact list improvements
• Chat history viewer enhancements
  – Two tabs: one for Transcripts and one for Files and Links
  – Search all transcripts or just those of the selected contact
  – Find files and links sent by the selected contact
  – View All Chats by date
• Live text and widget support can be enabled in Sametime Connect client to allow chatting or calling a recognized person, as well as allowing creation or installation of widgets
• Live text and widget support is enabled in the Sametime embedded client for Lotus Notes
• Public group subscription control in the Sametime Connect client is controlled by new preferences

Audio / video management
• NAT traversal for audio/video
  – Enables audio and video connectivity across firewalls
  – Supports ICE/STUN/TURN standards
• Bandwidth Manager
  – Protects network by restricting bandwidth used for Sametime audio/video
  – Manages calls to available bandwidth at each location
  – Uses bandwidth policies based on classes of users
• Multiple A/V partner integration
  – Allows Sametime native and a third-party audio and a third-party video service
  – Lets users select appropriate service for each call or conference
  – Manages access to each service via policies
Mobile access - new devices and capabilities
- Instant messaging and presence for Android client
- Meetings client for BlackBerry devices
- Initiate® Sametime Unified Telephony calls from Android devices

Collaboration integration
- Sametime contact list in iNotes® sidebar
- Contact list portlet
- Microsoft Office 2010 support with Office Ribbin UI model to allow the user to leverage Sametime real-time functionality from Outlook, Word, Excel and PowerPoint.
- Sametime presence in Lotus Connections

Administration Improvements
- Sametime System Console
  - Federated deployment: share a common deployment manager instance across Sametime servers
- Compliance APIs for Sametime Meetings and chat room data capture
  - Working closely with partners – Facetime, Permessa, Instant Technologies
- Monitoring
  - More monitoring APIs
  - New IBM Tivoli® Monitoring solution for Sametime

What was new in Sametime 8.5.1
Enhancing the features introduced with Sametime 8.5, this release adds:
- Windows 7, Mac OS 10.6 (Snow Leopard), and Linux client support
- Improved video quality and stability
- Lotus Notes version 8.5.1 FP2 is required to run Sametime Embedded and Sametime Unified Telephony 8.5.1 in Notes
- Mobile devices added for this release: Blackberry Storm2 (9520/9550) and Bold2 (9700)

What was new in Sametime 8.5
Unified communications consolidate various synchronous communications channels (voice, video, meetings) with asynchronous channels (email, voicemail, social networks) on a common data network, thereby reducing communications and infrastructure costs. Unfortunately, however unified on the back end, unified communications solutions are rarely unified for the end user. It is not uncommon for an “integrated” solution to require users to learn four or more software clients. And the clients rarely integrate with each other, forcing users to switch contexts as their communication needs change, disrupting the task at hand. In the end, this complexity slows adoption and the business fails to recognize the expected return on investment.

The focus of Sametime 8.5 is to make unified communications seamless to the user by introducing a range of new capabilities and improvements:
A new online meeting experience is fully integrated into the Sametime Connect client.

A new Sametime Meetings panel provides a consolidated view of a user’s meetings and calendar and makes starting or joining a meeting a single-click process. Users can easily invite others to meetings by dragging their names from the Contact list. They can accept meeting invitations with a single click, just like joining a group chat. Users can move seamlessly from a text chat to a voice or video chat to a meeting. To upload meeting materials, they simply drag and drop the items they need.

New, zero-download, browser-based chat and meeting clients extend the desktop experience to wherever the user is working.

Improved audio and video capabilities make it easier to interoperate with existing audio and video conferencing systems and increase their utilization.

New audio and video codecs provide higher quality native voice and video services for a more compelling collaborative experience out of the box.

New Web 2.0 APIs let developers embed Sametime capabilities into websites and applications so users do not have to switch context as often.

For mobile users, there is a new browser-based Apple iPhone chat client, support for the Blackberry Storm, and an improved mobile client for Microsoft Windows Mobile devices.

New social views make it easier for users to find the people they collaborate with the most.

You can now select an existing geographic location that you have previously used and copy the location data to your current location.

Improved integration with Microsoft Outlook and Office puts more Sametime capabilities at users’ fingertips.

This release also continues to focus on enhancing Sametime as a platform, making it easier to manage and less expensive to operate.

A new Sametime System Console centralizes infrastructure configuration, deployment, and management and centralizes policy management for all Sametime services.

A new Sametime Media Manager with SIP-based interfaces and APIs interoperates with third-party video and audio conferencing systems. It also offers new video (H.264) and audio (G.722.1) codecs that deliver a better user experience at a fraction of the bandwidth and provides administrative controls over the video experience (size, bitrate, and so on).

A new online meeting infrastructure no longer requires add-on servers for high availability and improves firewall friendliness through the use of HTTP/S to connect users.

A new Sametime Proxy Server with Web 2.0 APIs simplifies integration into websites and applications.

New operating systems and platforms are supported for this release: IBM Lotus Domino 8.5, Microsoft Windows 2008 (32-bit and 64-bit editions) and 64-bit Linux operating systems.

**What is Sametime?**

IBM Sametime consists of client and server applications that enable a community of users to collaborate through instant messaging and online meetings over an intranet or the Internet. Sametime Entry is an offering targeted at helping organizations get started with instant messaging.
Members of the Sametime community use collaborative activities such as awareness, chat, screen sharing, and real-time audio/video capabilities to work together.

**Awareness** – Sametime awareness technology lets members who have logged in to Sametime to see all other members who are logged in. The names of online users display in "awareness lists" in Sametime applications. From these awareness lists, members of the community can chat through instant messaging sessions or start meetings that include chat, screen-sharing, polls, the ability to send web pages to other users, and audio/video capabilities.

**Meeting rooms** – While awareness lists support instant collaboration with other online users, the Sametime Meeting Room Center provides a central meeting place for members of the community. In the Meeting Room Center, users can create meeting rooms and use them whenever they want to meet with their colleagues. Users access the Sametime Meeting Room Center with web browsers or from the Meetings panel in the Sametime Connect client.

**Instant messaging** – The Sametime client is a Java application that uses the Eclipse-based IBM Lotus Expeditor. The Sametime client leverages the Eclipse plug-in framework to provide developers with extensibility features that go far beyond those available in previous Sametime releases. Partners, independent software vendors (ISVs), customers, and internal developers use these features to integrate with the Sametime client to extend its capabilities.

**Instant meetings** – Instant meetings are meetings that Sametime Connect users can create on the fly, and are perfect for quick meetings when you don't need to save the meeting room, its content, and related information.

**Voice chat** – The Sametime client allows users to talk to other Sametime users through their computer's audio features and Voice-over-IP (VoIP) technology. VoIP is becoming increasingly popular, since it allows users anywhere in the world to talk inexpensively. Voice-over-IP allows users to click the microphone icon to call another user for instant voice chats over the intranet.

**Telephony** – Voice chat is one of two telephony capabilities in the Sametime IM client. The other is click-to-call (also called click-to-dial), which allows a user to instantly create a telephone conference with one or more other users. In both cases, a user invites other users in a chat window or on the buddy list to join a call, and the invitees are given the opportunity to either join or decline. Those users who choose to join can connect to the call by clicking an icon. If voice chat is used to initiate the call, all connected parties communicate using their computer's microphone and speakers. If click-to-call is used, a third-party telephony service calls each user at the appropriate number.

**Video chat** – Users who are equipped with video components can see each other on their screens during a chat.

**Location awareness** – Sametime includes location awareness of the user, and an extensible resource area at the bottom of the left pane that can be customized to reflect different locations.

**Connect to public IM networks** – Sametime provides for connectivity to outside instant messaging providers such as AOL's AIM, Microsoft Office Communications
Server, and Google Talk communities through IBM’s Sametime Gateway. Through the gateway, users can share presence information and can participate in text-based IM conversations.

**Contact information** – The Business Card features provides the user with telephone number, email address, photo, name, title, and location displayed in the Business Card hover-over feature and in the chat window. Business cards can be provided by the Sametime Community Server or a Lotus Connections server.

**Emoticons** – Sametime includes emotionally-expressive icons such as smiley faces.

**Customizing** – Your company name can be added to the Instant Messaging window.

**File transfer** – Users can send files.

**Quick find** – Users can start typing name in the Quick Find box to find a person they want to chat with, and then click the name to initiate a chat.

**Time stamp** – The time of day is provided in the Chat window along side the text.

**Polling** – A user can poll members of a group to provide brief feedback to questions.

**Policy** – Users can be assigned access to different features in Instant Messaging, such as voice chat, creating meetings, transferring files, IP telephony. Policy settings govern their access.

The two primary Sametime client applications are the Sametime Connect client and the Sametime Meeting Room. The Sametime Connect client contains a presence list that displays selected members of the community who are online. From Sametime Connect, a user can collaborate by sending instant messages or by starting an instant meeting with any other online member of the community.

The Sametime Meeting Room runs in a user’s web browser whenever the user attends a meeting. The Sametime Meeting Room contains components that support the full range of Sametime collaborative activities, including interactive audio and video.

**Sametime Standard and Sametime Entry**

Sametime Standard is the full Sametime product offering, Sametime Standard provides awareness, instant messaging, and meeting room functionality.

Sametime Entry is a limited offering, providing a core set of awareness and instant messaging capabilities either from stand-alone Sametime clients or from within Lotus Notes. Sametime Entry does not support meeting rooms. In addition, Sametime Entry is sometimes packaged with other IBM products.

You can expand your real-time collaboration capabilities in Sametime Entry by purchasing the Sametime Standard server to add meeting room capabilities and a richer instant messaging client to your environment.

The following table compares the features of Sametime Entry and Sametime Standard.
<table>
<thead>
<tr>
<th>Capability</th>
<th>Available with Sametime Entry</th>
<th>Available with Sametime Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Instant Messaging chat</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>N-way (group) chat</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Sort contact list</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Show short names</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Show those online only</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Time stamps on chats</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Chat history</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Rich text</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Emoticons</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Emoticon palettes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Business card display</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Contact type ahead</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Spell check in chat</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Standalone Sametime Connect client</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Microsoft Office integration</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Meeting rooms and instant meetings</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Sametime toolkits</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Sametime gateway (to public IM)</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Sametime mobile access</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Selective ‘who can see me’</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Alerts setting</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>File transfer</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Telephony (with 3rd party)</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Voice chat</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Video chat (native point-to-point)</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Multiple communities</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Geographic locating</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Screen capture tool</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Selective do-not-disturb status</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Sametime plug-ins</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Sametime server architecture**

A typical Sametime server includes a cluster of servers for instant messaging on a Domino-based platform and other clustered servers running on WebSphere Application Server that support meetings, audio-visual services, and connections to a variety of clients.
The illustration below shows the different types of servers you can have in a Sametime deployment.

**Sametime System Console**

The Sametime System Console is a Web-based application that provides a central location for installing, configuring, administering, and monitoring the Sametime family of products.

In an enterprise deployment, install the console on a dedicated machine. The machine also becomes the Deployment Manager in a clustered environment, managing activity in all server clusters in the Sametime environment.
Sametime Community Server
The Sametime Community Server runs on Lotus Domino. It supports all presence (or awareness) and text chat activity in a Sametime community. Any Sametime client that contains a presence list must connect to the Sametime Community server.

Basic functionality supported by the server includes:
- Handling client login requests.
- Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP, HTTPS, or SOCKS proxy servers.
- Providing directory access for user name search and display purposes.
- Providing directory access to compile lists of all Sametime servers and users in the community.
- Dissemination of presence and chat data to all users connected to Community Services.
- Maintenance and storage of privacy information, user preference settings, and presence lists for online users.
- Handling connections from the Community Services on other Sametime servers when “Using multiple non-clustered Sametime Community Servers” on page 921. Server-to-server connections for the Sametime Community Server occur on default TCP/IP port 1516.
- Logging of server events to the “General log settings” on page 1140 (stlog.nsf).
- Enabling a name entry prompt to appear when the ACL settings of a Domino database enabled with IBM Lotus instant messaging technology allows anonymous access. This name entry prompt ensures that the presence list in the Sametime database can display a name for the user.

Sametime Proxy Server
The IBM Sametime Proxy Server runs on IBM WebSphere Application Server. It requires a Sametime Community Server.

The Sametime Proxy Server communicates with the Sametime Community Server, Sametime Meeting server, Lotus Connections Server, and Sametime Unified Telephony Server or other TCSP-enabled server.

The Proxy Server is responsible for the following activities:
- It hosts the Sametime client for browsers.
- It provides live names awareness for Sametime meetings, Business Cards, and custom applications.
- It replaces the Sametime Java Connect and Sametime Connect for Browsers clients.
- It replaces the Sametime Links Toolkit.

Sametime Media Manager
The IBM Sametime Media Manager runs on WebSphere Application Server to provide audio visual services for chats and meetings. It requires a Sametime Community Server.
The Sametime Media Manager uses the Session Initiation Protocol (SIP) to provide support for point-to-point and multipoint calls. It is designed to support standard audio and video codecs so that it works with other external audio and video vendors.

The Sametime Media Manager uses three components. In a small deployment, the Sametime Media Manager components can all be installed on one server, but in an enterprise deployment, you should install each of the components on its own server.

- **Conference server**
  The Conference server manages all conferences, including point-to-point and multipoint. It works with the client to establish the SIP session for the call. It hosts the internal TCSP1 adapter and optionally an external TCSP1 adapter.
  The Conference server requires access to LDAP, Meetings (optional), and Proxy/Registrar (including transport protocol: UDP, TCP, TLS). The Conference server will handle workload management for conference sessions among the switchers.

- **Proxy and Registrar**
  The Proxy and Registrar is responsible for location service and forwarding SIP messages to a destination. It requires access to LDAP. You may also install and configure a database to be used with it.

- **Packet switcher**
  The Packet switcher is responsible for receiving and sending media streams from endpoints to other endpoints in a conference. The Switcher works on audio streams to determine the active video stream to send to the participants, a process known as Voice-Activated Switching (VAS).
  The Packet switcher requires access to LDAP, Conference server, and media ports (1 or a range of ports for audio, and 1 or a range of ports for video). If the switchers are installed on the same machine, ensure that there are no port conflicts.

Security is enabled by default. Use TLS or SSL to allow servers to communicate. TLS transport is recommended when using media encryption.

**Sametime Bandwidth Manager**

Administrators manage bandwidth to ensure that sufficient network capacity is available to high-priority audio and video users when needed. Bandwidth management also ensures that as many users as possible can use audio and video features at the same time without interfering with other network traffic. IBM Sametime Bandwidth Manager allows you to centrally configure and monitor bandwidth for Sametime calls by declaring limits for various parts of the network, placing constraints on how bandwidth is used on your network, and monitoring that usage.

The Sametime Bandwidth Manager optimizes bandwidth by calculating the call route for each call at call setup time and reserving the required bandwidth for the duration of the call. If sufficient bandwidth is not available, the call is either modified (through codec, bandwidth, or media reduction), or it is not allowed and the user is presented with a "resources in use" message.

The Bandwidth Manager also supports networks containing internal NATs (Network Address Translators).
To fully understand how bandwidth management works, review the following topics on bandwidth management concepts:

**Sites and links**
In a network managed by IBM Sametime Bandwidth Manager, a site is any network entity that corresponds to a range of IP addresses and to a physical location on your network. It can represent a city, a building, a campus, or a LAN within your managed network. A link constrains the bandwidth connecting two sites, such as network traffic that leaves one building on a wide-area network on its way to a second location.

**Configuring site properties**
Configuring properties for a site constrains bandwidth for the individual site and affects any audio and video calls made within the site.

*Table 11. Site properties*

<table>
<thead>
<tr>
<th>Site property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled or Disabled</td>
<td>You can set the Disabled property to disable a site while you are configuring it. You can also disable it during normal operations when you need to suspend bandwidth constraints temporarily.</td>
</tr>
<tr>
<td>Default</td>
<td>A site can be designated as the &quot;default site,&quot; which is the site that handles all endpoints that do not fit within the IP ranges of any modeled site.</td>
</tr>
<tr>
<td>IP ranges</td>
<td>This value defines the site by specifying which endpoints belong to a site based on the endpoints' IP addresses.</td>
</tr>
<tr>
<td>Maximum bandwidth</td>
<td>This setting allows administrators to define the maximum bandwidth for a site. Bandwidth in a site is consumed anytime a call is initiated, ends, or routes through a site. Whenever the maximum bandwidth is reached, future calls are prevented until the current bandwidth usage falls below that maximum setting.</td>
</tr>
<tr>
<td>Peak utilization</td>
<td>Optionally, you can specify a percentage of the total bandwidth capacity in a bandwidth pool to define peak utilization, and set special bandwidth allocation policies to be used in that circumstance. For example, you can set a bandwidth policy that reduces the amount of bandwidth allocated to new calls.</td>
</tr>
</tbody>
</table>

**Configuring link properties**
Associating a link with a site allows you to constrain the bandwidth between that site and another. A link is implicitly associated with the site you are configuring and determines the second site through the destination site name property. By configuring bandwidth constraints for links, you control bandwidth at network bottlenecks for which the interconnected sites are unnecessary.
Table 12. Link properties

<table>
<thead>
<tr>
<th>Link property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled or Disabled</td>
<td>You can set the Disabled property to disable a link while you are configuring it. You can also disable it during normal operations when you need to suspend bandwidth constraints temporarily.</td>
</tr>
<tr>
<td>Destination site name</td>
<td>The destination site is the one that the implicit site links to. The destination site must also be a configured site.</td>
</tr>
<tr>
<td>Link type</td>
<td>A link can be physical or virtual. Physical links represent the real (physical) connection between sites. Virtual links represent a virtual circuit within a physical link. Multiple virtual links share or are mapped to a given physical link.</td>
</tr>
<tr>
<td>Distance</td>
<td>This metric controls which route is taken by media when multiple possible routes exist.</td>
</tr>
<tr>
<td>Maximum bandwidth and Peak Utilization</td>
<td>Similar to sites, physical links have maximum bandwidth and peak utilization constraints. Virtual links have a nominal capacity expressed as a percentage of the capacity of the shared physical link.</td>
</tr>
</tbody>
</table>

Site types

A network managed by IBM Sametime Bandwidth Manager can work with several different types of sites. All IP ranges that have been configured for a site are maintained if you change the site’s type.

Sites provide an anchor for links in the topology model. However, there are distinct differences and uses for the three types of sites:

- **Regular sites**
  - Use regular sites to model physical locations, such as buildings, campuses, or cities, in the enterprise network topology model.
  - They are represented by the IP addresses or ranges of endpoints that are supported in them.
  - They can have associated bandwidth pools and constraints.

- **Cloud sites**
  - Use cloud sites to model intermediate connection points for multiple virtual circuits in the network topology model.
  - They do not have any IP ranges associated with them.
  - They cannot have any endpoints associated with them.
  - They cannot have any bandwidth constraints associated with them.

- **VPN**
  - Use VPN sites to model home and mobile user VPNs as users of the physical enterprise network in the topology model.
  - Like regular sites, they are represented by the IP addresses or ranges of endpoints that are supported in them and they also have bandwidth constraints.
  - They cannot have physical links with other sites.
  - They can have virtual links to other sites only via the Internet site.
For examples of different site types, see Network topology examples.

**Call rate policies**

In a network managed by IBM Sametime Bandwidth Manager, you can customize bandwidth usage by creating call rate policies. When a call is established, a call rate policy determines whether any changes must be made, such as reducing audio media to a lighter weight codec, reducing video bandwidth by reducing resolution or frame rate, removing video media, or denying the call completely. A call rate policy can be associated with a site, a group of sites, or a group of users. In addition, call rate policies associated with specific users can use the directory identifier or the media IP address (endpoint address).

Call rates are defined for normal circumstances and for times when audio and video traffic on the network is heavy:

- **Normal call rate**: A call rate policy for a given call specifies the normal call rate for video or audio-only calls.
- **Peak utilization call rate**: Administrators can specify an alternate call rate when the call consumes bandwidth from a site or link that has or will exceed its configured peak utilization value.

You can define hundreds of different call rate policies, specifying policies for different classes of users, calls between different locations, and for periods of both normal use and peak utilization. You can also precisely control the order by which policies are searched and selected for the case where there are multiple potential matching policies. Examples of typical call rate policies are provided in Call rate policy examples.

**Applying call rates to endpoints**

You can apply call rate policies to different classes of endpoints:

- Conference rooms might be configured to request calls at 1 Mbps (resulting in HD video).
- Desktop systems might be configured to use a maximum of 512 kbps.

MCUs (devices that connect users with audio and video conferencing) are incorporated as endpoints that are contained within a specific class of user. MCU users are then incorporated into profile definitions like any other class of users. Therefore, multi-party calls are treated like point-to-point calls between a user and the MCU.

**Applying call rates to groups**

Using groups is a convenient way to apply different call rate parameters to different classes of users. For example, the following call rate policies could be easily configured if users were organized into three groups, VIP users, standard users, and support staff:

- **VIP users** could be authorized to place calls at 768kb/s calls (resulting in a high-resolution experience).
- **Standard users** could be limited to 384kb/s calls using CIF (Common Interchange Format), which specifies a speed of 30 frames per second.
- **Support staff** could be prohibited from using video altogether through bandwidth policies that specify audio-only calls.

You can apply policies to existing Sametime groups or you can use the Sametime Bandwidth Manager to create groups. Groups or classes can be defined by
matching a variety of attributes associated with users. Users in groups are selected from the user directory configured for the Bandwidth Manager.

**Sametime TURN Server**

The IBM Sametime TURN Server enables Sametime clients to send audio and video communications across a NAT (Network Address Translator) or firewall when direct peer-to-peer communications are not possible. In earlier releases, this feature was called the Sametime Reflector.

Normally, Sametime clients communicate directly using a peer-to-peer connection. If either or both of the clients is situated behind a NAT or a firewall and a peer-to-peer multimedia session cannot be established, the clients will utilize the Sametime TURN Server to relay the media. The TURN Server resolves problems with media connections by using a technology called ICE (Interactive Connectivity Establishment). The ICE methodology uses STUN (Session Traversal Utilities for NAT) and TURN (Traversal Using Relay NAT) protocols to traverse a NAT and ensure that audio/video connections can be completed between users on either side. ICE determines the most logical and efficient network paths between remote endpoints, using all available network interfaces. This greatly improves the ability of clients to negotiate audio/video sessions across complex network topologies.

**Sametime Meeting Server**

The IBM Sametime Meeting Server runs on WebSphere Application Server. It requires an IBM DB2 database and an LDAP server. The Meeting Server provides a central meeting place for members of the community. When combined with the Sametime Media Manager, meeting rooms can be enhanced with audio-visual features.

**Sametime Classic Meetings**

The Sametime Meeting server running on WebSphere Application Server replaces the meeting features included in Sametime Standard 8.0.x and 7.5.1. To defer your migration of meetings to the new platform, you can upgrade Sametime 8.0.x and 7.5.1 servers, while maintaining your existing “Classic” meetings until you are ready to migrate them to the new platforms. When you download the Sametime 85x installation package, the Classic Meeting server is part of the community server installation zip/tar file.

**Related concepts**

“Planning a Sametime Meeting Server installation” on page 244

Follow these guidelines when planning the deployment of IBM Sametime Meeting servers.

**Sametime Gateway**

IBM Sametime Gateway runs on WebSphere Application Server. It is a platform for sharing presence and real-time collaboration with external instant messaging communities.

Use Sametime Gateway to connect with any of the following gateways or communities:

- Sametime communities deployed outside of your firewall
- AOL Instant Messenger
- Google Talk
- Jabber
• Microsoft Office Communications Server communities

You can install one Sametime Gateway server or cluster of Sametime Gateway servers for a local Sametime community. A local community can be made up of one Sametime server, or a cluster of Sametime servers connected by a common LDAP directory. Sametime Gateway does not support more than one local Sametime community and uses the same LDAP directory used by the local Sametime community.

Sametime Gateway is delivered with out-of-the-box functionality, such as presence and instant messaging, filtering of blacklisted domains, user access control, and logging of user content, presence, and instant messaging events. In addition, all interactions with external domains are logged. Built upon a plug-in technology, the Sametime Gateway allows IBM and third-party developers to enrich and customize message handlers for spam control and virus checking.

**How Gateway connections work**

Instant messaging and presence through the Sametime Gateway depend on direct connections between companies. The following illustration shows a local IBM Sametime community behind a firewall. The community connects with Company A, B, C, and D and vice versa, but these companies do not connect with each other.
Sametime Gateway follows these steps to deliver an instant message to another community.

1. Gateway confirms that the other community is on its list of communities.
2. Gateway checks each message to see if it has a route to the desired destination.
3. Gateway checks if there is permission to interact with the other system by means of an Access Control List (ACL).

4. If necessary, Gateway translates the message into a protocol, either SIP or XMPP (Extensible Messaging and Presence Protocol) that the community can understand.

AOL Instant Messenger and Microsoft Office Communications server.

Jabber and Google Talk use XMPP.

Sametime Gateway also bridges Sametime communities that use the same protocol, as is the case with Company A and Company B in the illustration above.

5. Finally, Gateway sends the message to its destination.

**Sametime clients**

To collaborate in instant messaging and online meetings, people in your organization use IBM Sametime clients that interact with services on Sametime servers.

- Sametime Connect - desktop instant messaging client that can be stand-alone or embedded in Lotus Notes
- Sametime browser client - instant messaging client in a browser
- Sametime mobile client - instant messaging features in a mobile device
- Sametime iPhone client - optimized browser client for iPhone
- Sametime Meetings - meeting room plugin for Sametime Connect or Lotus Notes
- Sametime Meeting Room Center in a browser - online access to Sametime meeting rooms
- Sametime Classic Meetings client - Java-based meeting room client interacts with the Sametime Classic Meeting Server.

**Sametime offering features by client type**

The features available to users depend on the type of client they use and the Sametime offering installed on their home servers.

The following tables compare features of IBM Sametime Entry, Sametime Standard, and Sametime Advanced by client type.

- Presence
- Instant Messaging
- Meetings
- Voice and Video
- Community Collaboration
- Mobile Access
- Communications Enabled Business Processes
- Administration and Security

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Adv</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Notes</td>
<td>Embedded</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
</tr>
<tr>
<td>Presence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 13. Presence feature comparison (continued)

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Adv</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Presence status</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Availability status icons</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Custom status message</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>View Other’s geographic location</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Automated Geographic location awareness</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Status</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Set alerts to notify when users are available</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Selective do not disturb/privacy lists</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Set presence state and status message on start-up</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Set presence status from system tray, chat window or Connect, web and Mobile clients</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Table 13. Presence feature comparison (continued)

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Adv</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto status update based on PC inactivity</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Auto status update based on calendar</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Auto status update when entering or leaving a Sametime Meeting</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Server-based geographic location services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

### Table 14. Instant Messaging feature comparison

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Adv</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Notes Embedded Connect</td>
<td>Connect Web</td>
<td>Mobile Connect Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Messaging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log in to multiple and external Sametime Communities</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Anonymous or “Guest Access”</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Business Card Display</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Table 14. Instant Messaging feature comparison (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>x</th>
<th>x</th>
<th>x</th>
<th>x</th>
<th>x</th>
<th>x</th>
<th>x</th>
<th>x</th>
</tr>
</thead>
<tbody>
<tr>
<td>ahead</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Contact Search /</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Quick Find</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Primary Contacts</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>View</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Frequent Contacts</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>View</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Recent Contacts</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>View</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Initiate chats</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>with users not in</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>contact list</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>User created</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>personal groups</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>and nested groups</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Administrator</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>created public</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>contact list</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>groups</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Contact List</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Sorting Options</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Contact list</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>scrubber to remove</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>infrequently used</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>contacts</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Automatically</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>send email if</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>contact is offline</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Secure One-on-one</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>text chat</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Feature</td>
<td>Sametime</td>
<td>Message</td>
<td>Instant</td>
<td>Sametime</td>
<td>Message</td>
<td>Instant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------</td>
<td>---------</td>
<td>----------</td>
<td>----------</td>
<td>---------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Multi-party text chat</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Video</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Integration</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Announcements (to selected users and groups)</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent accidentally starting large multi-party chats</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabbed Chat Windows</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display user information and photo in chat window</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display chat partner status in chat window</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rich text formatting</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emoticons</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emoticon Palettes</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Capture Tool</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Screen Share</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfer</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 14. Instant Messaging feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send hyperlinks and Notes doclinks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Spell Check</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Time and Date Stamps</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Chat History</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Automatically populate recent chat history in chat window</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Off the record mode / disable transcript save</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Print Transcript</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Send transcript as email</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Zero-download browser chat client</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Table 15. Meetings feature comparison

<p>| Offering                  | Entry | Entry | Standard | Standard | Standard/Advanced | Advanced | Advanced |
|---------------------------|-------|-------|----------|----------|-------------------|----------|
| Client                    | Notes Embedded | Connect | Connect | Web | Mobile | Connect | Web |
| Meetings                  |       |       |          |          |                   |          |
| Reservationless, persistent meeting rooms, available 24 x 7 for participant use | x | x | x | x | x | x | x |</p>
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instantly create a Sametime Meeting Room from Sametime Connect Client or browser based Meeting Room Center</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Join or create a Sametime Instant Meeting from a 1-on-1 or group chat</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Assign and enter meeting rooms from Notes, Outlook invitations</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View your calendar from Sametime Connect with one click access to meeting rooms</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>One click access to Meeting rooms you own</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>One click access to your recently used Meeting Rooms</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Tool A</td>
<td>Tool B</td>
<td>Tool C</td>
<td>Tool D</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Find Meeting Rooms by owner or room name</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Set passwords and hide meeting rooms</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Anonymous or &quot;Guest Access&quot;</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Set permissions to control whether users can share their screens or just observe</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Control who else can manage room permissions</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Invite users to meeting by drag and drop from contact list</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Browser users can participate in meetings without any client download</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Photo and list view of attendees</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Sort participant list alphabetically or by users with raised hands</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>App / Screen sharing (Windows only; Mac and Linux to come in follow on release)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>App sharing remote control (peer-to-peer)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Each meeting room has its own, private file library</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Load files into library by Drag and Drop</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High quality conversion and presentation of PDF, ODF, and Microsoft Office files</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Local, background, high-fidelity file conversion</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control whether users can download documents from meeting library</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Fit to screen view</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Edge-to-edge full screen view</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Presenter tools (highlighter, pointer)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>View slide thumbnails during presentation</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Create Polls Immediately or Store for Future Use</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Immediately share poll results with participants</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Screen Capture tool</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Paste an item from your clipboard to the meeting library</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Share URL's</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Raise Hand</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Initiate private chat</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Group discussion</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Feature</td>
<td>Sametime</td>
<td>Sametime Express</td>
<td>Sametime Advanced</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>Emoticon Support</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Breakout sessions and simultaneously participate in multiple meetings</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Join Call function to enter audio portion of meeting</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Client-side meeting recordings in standard file formats</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Control whether users can record a meeting</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Conferencing Integration/Voice and Video</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>User re-arrangeable interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Capture Minutes, Questions, Action Items, Answered questions and Follow Up Items</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Detailed Meeting reports</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Historical Meeting Reports</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Table 15. Meetings feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset room by clearing out all room content</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Administrators can use policies to control in-meeting discussion and file sharing</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Reporting tool for Administrators to generate Meeting statics and usage reports</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Use HTTP/HTTPS to connect all users, simplifying internal and external collaboration</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Built in failover and clustering</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zero Download browser meetings client</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Table 16. Voice and Video feature comparison

<table>
<thead>
<tr>
<th>Voice and Video</th>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Client</td>
<td>Notes</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
</tr>
<tr>
<td>Embedded</td>
<td>Notes</td>
<td></td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
</tr>
<tr>
<td>Feature Description</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A single audio / video interface delivers both built-in and partner media capabilities in voice and video chats or in Sametime online meetings</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sametime Video supports variable video window size, full screen mode and resolutions up to high definition</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP and video chats with multiple participants</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Administrative controls over the video experience (size, bitrate, quality, and so on)</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 16. Voice and Video feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>New H.264 video and G.722.1 audio codecs provide a higher quality multimedia experience at lower bandwidths</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio/video based on the industry standard Session Initiation Protocol (SIP), improving interoperability with third-party audio/video conferencing systems.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 17. Community Collaboration feature comparison

<table>
<thead>
<tr>
<th>Offering Description</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Collaboration</td>
<td>Notes</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
<td>Web</td>
</tr>
<tr>
<td>Exchange presence and chat with other Sametime communities, public IM services through Sametime Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature Description</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange presence and chat with Microsoft OCS users through the connectors built into the Sametime Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Community Channels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Tap</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Polls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Chat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Announcements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create FAQs from Broadcast community content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persistent Group Chat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chats history stored on the server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to store and share files with others</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 17. Community Collaboration feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swarming tools - notifications triggered by keywords or number of participants - drive real time use</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create FAQs from Persistent Group Chat content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Table 18. Mobile Access feature comparison

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry Notes Embedded</th>
<th>Entry Connect</th>
<th>Standard Connect</th>
<th>Standard Web</th>
<th>Standard/Advanced Mobile</th>
<th>Advanced Connect</th>
<th>Advanced Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIM Blackberry 8700, 7100, 8300 (Curve), 9000 (Bold and Storm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia Enterprise eSeries: E51, E60, E61, E62, D65, E70, E90</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Mobile 2003 SE, Windows Mobile 5 and 6 (Standard and Professional)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
### Table 18. Mobile Access feature comparison (continued)

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sony Ericsson P1i</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple iPhone and iPod Touch (browser)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 19. Communications Enabled Business Processes feature comparison

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Enabled Business Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded Note Embedded</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect Web</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect Web</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web client customization via style sheets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web 2.0 APIs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere Portal Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

180  
Sametime Advanced: Installation and Administration Guide
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Lotus Connections and Quickr® Integration</th>
<th>Lotus Notes Integration</th>
<th>Microsoft SharePoint Integration</th>
<th>Microsoft Outlook and Office Toolbar Extensions</th>
<th>Contact presence, location and status messages</th>
<th>Generate dynamic contact list from email recipient list</th>
<th>Open Sametime Quick Find Search</th>
<th>Click to text chat</th>
<th>Click to talk (VoIP)</th>
<th>Click to talk (3rd party telephony)</th>
<th>Instant meetings</th>
<th>Instant screen share</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Table 20. Administration and Security feature comparison

<table>
<thead>
<tr>
<th>Offering</th>
<th>Entry</th>
<th>Entry</th>
<th>Standard</th>
<th>Standard</th>
<th>Standard/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Notes Embedded</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
<td>Web</td>
</tr>
<tr>
<td>Administration</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Security</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Integrated Installation Manager</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Central policy management of features and user settings</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Auto-provision client updates</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Serviceability Management</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Security and Encryption</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Chat monitoring and archiving integration</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Related concepts

“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 248

A mixed-license environment includes a combination of IBM Sametime Entry servers, along with Sametime Standard servers and possibly Sametime Advanced. When you deploy IBM Sametime Entry servers with other types of servers, plan for additional steps to meet the licensing requirements for Sametime Entry, which offers only instant messaging features and does not offer meetings. Sametime Entry users are licensed for instant messaging features only and not Web conferencing. Fully-licensed users for Sametime Standard or Sametime Advanced have access to instant messaging and Web conferencing.

**Sametime screen sharing and remote control features available to clients**

The screen sharing and remote control features available to clients depend on the type of server that is hosting meetings and the operating system clients are running on.
Users who have sharing abilities can share their screens with others during a meeting. Users who have Remote Control Hosting ability can share the screen while others send keyboard and mouse commands to the machine sharing the screen. Users who have Remote Control Driving ability can send keystroke and mouse commands to a remote machine.

The following table shows the screen sharing and remote control features that are available when you host meetings on a Sametime meeting server. Sametime clients running on a browser must have Java installed and enabled to have screen-sharing ability.

For information on Sametime system requirements, see the system requirements at the following web address:


Table 21. Features available when using Sametime meeting server

<table>
<thead>
<tr>
<th>Client Operating system</th>
<th>Screen Sharing Hosting</th>
<th>Remote Control Hosting (P2P Connection only)</th>
<th>Remote Control Driving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Connect client</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Sametime browser client</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Linux</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The following table shows the sharing and remote control features that are available when you host meetings on a Sametime classic server running on Lotus Domino, either using the Java applet-based meeting client, or the Instant Share feature in Sametime Connect. Instant Share is a Sametime Advanced plugin that works with Sametime Meeting servers and Sametime classic meetings.

Table 22. Features available when using Sametime classic meetings on a Domino server

<table>
<thead>
<tr>
<th>Client Operating system</th>
<th>Screen Sharing Hosting</th>
<th>Remote Control Hosting</th>
<th>Remote Control Driving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Related concepts

“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 248

A mixed-license environment includes a combination of IBM Sametime Entry servers, along with Sametime Standard servers and possibly Sametime Advanced. When you deploy IBM Sametime Entry servers with other types of servers, plan for additional steps to meet the licensing requirements for Sametime Entry, which offers only instant messaging features and does not offer meetings. Sametime Entry users are licensed for instant messaging features only and not Web conferencing. Fully-licensed users for Sametime Standard or Sametime Advanced have access to instant messaging and Web conferencing.

Meeting features in Connect versus web clients

The table below compares meeting features available to the Sametime Connect client (rich client) and the web client.

<table>
<thead>
<tr>
<th>Features</th>
<th>Connect client</th>
<th>Web client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reservationless, persistent meeting rooms, available 24 x 7 for participant use</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Instantly create a Sametime Meeting Room from Sametime Connect Client or browser based Meeting Room Center</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Join or create a Sametime Instant Meeting from a 1-on-1 or group chat</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Assign and enter meeting rooms from Notes, Outlook invitations</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>View your calendar from Sametime Connect with one click access to meeting rooms</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>One click access to Meeting rooms you own</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>One click access to your recently used Meeting Rooms</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Find Meeting Rooms by owner or room name</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Set passwords and hide meeting rooms</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Anonymous or guest access to meetings</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Set permissions to control whether users can share their screens or just observe</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Control who else can manage room permissions</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Invite users to meeting by drag and drop from contact list</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Features</td>
<td>Connect client</td>
<td>Web client</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Browser users can participate in meetings without any client download</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Photo and list view of attendees</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Sort participant list alphabetically or by users with raised hands</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Each meeting room has its own, private file library</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Load files into library by drag and drop</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>High quality conversion &amp; presentation of PDF, ODF, and Microsoft Office files</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Local, background, high-fidelity file conversion</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Control whether users can download documents from meeting library</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fit to screen view</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Edge-to-edge full screen view</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Presenter tools (highlighter, pointer)</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>View slide thumbnails during presentation</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Create Polls Immediately or Store for Future Use</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Immediately share poll results with participants</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Screen capture tool</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Paste an item from your clipboard to the meeting library</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Share URLs</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Raise hand</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Initiate private chat</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Group discussion</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Emoticon support</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Breakout sessions and simultaneously participate in multiple meetings</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Join a conference call to enter audio portion of meeting</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Client-side meeting recordings in standard file formats (mpeg4 .mov)</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
### Features

<table>
<thead>
<tr>
<th>Features</th>
<th>Connect client</th>
<th>Web client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control whether users can record a meeting</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Conferencing with voice and video</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>User can rearrange interface</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Capture minutes, questions, action items, answered questions and follow up items</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Detailed meeting reports</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Historical meeting reports</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Reset meeting room by clearing out all room content</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Administrators can use policies to control in-meeting discussion and file sharing</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Reporting tool for administrators to generate meeting statics and usage reports</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Use HTTP/HTTPS to connect all users, simplifying internal and external collaboration</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Built-in failover and clustering</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

### Related reference

“Sametime screen sharing and remote control features available to clients” on page 182

The screen sharing and remote control features available to clients depend on the type of server that is hosting meetings and the operating system clients are running on.

### Integrating Sametime with Microsoft Office applications

You can integrate Sametime with Microsoft Office to enable Windows users to talk and meet without leaving their Microsoft Office applications. You can also integrate Sametime with the Office SharePoint Server to enable Sametime users to communicate with Office SharePoint Server users from a SharePoint site.

The administrator decides which features to make available to clients. If you enable all features for clients, they have access to the following Sametime features from Microsoft Outlook, Microsoft Word, Microsoft PowerPoint, Microsoft Excel, and a Microsoft Sharepoint web page.

- **Presence awareness**
  
  Names within Microsoft documents are instant-messaging-aware, which means users can see if a document author—or any name included in a document—is online. This is helpful, for example, if a user is reviewing a client proposal and cannot proceed without verifying a project estimate with the writer. Presence awareness allows the user to see immediately—directly from the proposal—that the writer is online and available to answer questions.
• **Business-class instant messaging**
  Instant-messaging capabilities within Microsoft documents can help users get information and answers quickly, so they can work unimpeded. For example, to verify a data point in an Excel spreadsheet, a user can start a chat directly from the spreadsheet. There's no need to leave the spreadsheet to start a chat or even a Voice over Internet Protocol (VoIP) call.

• **web conferencing**
  Users can also initiate web conferences directly from Microsoft Office applications, for those projects that require collaboration to move them along. A user working on a chart within a PowerPoint presentation, seeing that it needs some refining, can use web conferencing to collaborate with team members. Sharing the presentation in real time, and even jointly editing it live, saves time that would otherwise be spent sending emails or managing multiple versions of the content.

**Related tasks**
“Enabling installation of optional client features such as Microsoft Office Integration” on page 551
IBM Sametime ships with a number of optional client features that are not included in the default installation package. You can add features to the installation package for new client installs and update already-installed clients by updating the installation manifest file.

“Installing Sametime Integration for Microsoft Office” on page 579
IBM Sametime integration with Microsoft Office allows you to collaborate, create meetings, and chat with coworkers through Microsoft Office applications. Sametime integration with the Microsoft Office SharePoint Server allows similar collaboration features with coworkers who use Office SharePoint Server as their instant messaging application.

**PDF library**
You can find information for IBM Sametime administrators in the documents linked below.

<table>
<thead>
<tr>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime 8.5.2 Release Notes</td>
</tr>
<tr>
<td>Sametime Client Quick Start Guide</td>
</tr>
<tr>
<td>Sametime Client Preview Guide</td>
</tr>
<tr>
<td>Sametime Installation, Migration, and Configuration Guide</td>
</tr>
<tr>
<td>Sametime Administration Guide</td>
</tr>
</tbody>
</table>

**Glossary**
Familiarize yourself with terminology used in IBM Sametime.

**Terms**

**breakout sessions**
Users who are attending a meeting see a list of all meeting participants in the Participant List component of the Meeting Room client. While the meeting is in progress, a user who has Instant Meeting Policy permission can start a "breakout session" with any user displayed in the Participant list.
List. A breakout session is an instant meeting that is started from the Participant List of a meeting that is currently active.

Users must also be allowed by their Policy to create instant meetings in order to create a breakout session.

candidate/candidate pair
A candidate is any possible network end-point for an audio/video call. A candidate may be a transport address consisting of an IP address and a port.

A candidate pair is a combination of a local candidate and a remote candidate. The pair is a possible path for the media stream between the two end-points on a call. As part of the ICE process, all candidate pairs are tested and the best is selected to exchange the media.

chat
Sametime supports text-based chat and instant messaging. A chat session can consist of two (or more) users exchanging instant messages. Chat or instant messaging sessions can be initiated from any contact list in a Sametime client.

There are three basic kinds of voice chat that can be used with Sametime Instant Messaging and Instant Meetings, and with scheduled meetings. These are: the traditional Codec-style voice that comes with the client workstation that is equipped with sound card and speakers, the Sametime-ready third-party IP telephony, and the new IBM community tools plug-in that uses voice-over-IP technology. For IP telephony, Sametime provides a new client-side telephony application program interface (API) that allows partners to easily integrate their telephony service with the Instant Messaging client.

All instant messaging and chat activity is supported by Community Services on the Sametime server.

clearinghouse
A federated community of users linked by an enterprise’s message router that translates protocols and routes messages. When a message contains destination domains not found elsewhere in a routing configuration, the message is routed to a clearinghouse. A route to a clearinghouse enables Sametime Gateway users to connect to a much wider community.

community
The Sametime community refers to all users that have web browser access to a Sametime server (or servers) and all Sametime servers that support those users. The Sametime community can be maintained in the Domino Directory on the Sametime Server or in an LDAP Directory on a third-party LDAP-compliant server. Specifically, the Sametime community can be described as a shared directory, or set of directories, that lists the people and groups of the community, and as one or more Sametime servers that each have access to the shared directory or set of directories.

connectivity (firewall and proxy support)
To engage in collaborative activities, the Sametime clients must connect to various services on the Sametime server. The HTTP Services, Community Services, Meeting Services, Recorded Meeting Broadcast Services, and Audio/Video Services on the Sametime server listen for connections from clients on different TCP/IP ports. Because of the number of ports required to support the full range of collaborative activities, Sametime includes specially-designed connectivity features that enable Sametime clients to establish connections through firewalls and proxy servers.
DMZ  A DeMilitarized Zone is a physical or logical subnetwork that contains and exposes an organization’s external services to a larger untrusted network, usually the Internet.

Domino Directory  The Sametime server uses the Domino Directory of the Domino server on which Sametime is installed. The Domino Directory is a database that serves as a central repository for information about Sametime users (or members of the Sametime community). The Domino Directory contains a separate Person document for each Sametime user. The Person document contains the User Name and Internet password required for authentication with the Sametime server. The Person document also contains a “Sametime server” field that is used to specify a user’s home Sametime server. The home “Sametime server” is the Sametime server a user connects to when logging in to the Community Services for presence and chat activity. The Domino Directory also contains Group documents that hold lists of users that perform similar tasks. Group documents also define the Public Groups that users can add to the Sametime Connect client presence list.

hand raise  Hand raise is a collaborative activity that allows users to raise a hand at any time during a meeting. When users raise their hands, a hand icon appears next to their names in the Participant List.

ICE  The Interactive Connectivity Establishment process is used by two participants in a call to determine the best path for exchanging media streams (audio/video). ICE is based on the STUN and TURN protocols, and utilizes the TURN server. These related RFCs which were implemented in the Sametime NAT traversal feature:
- ICE protocol RFC
- STUN protocol RFC
- TURN protocol RFC

IP audio  Interactive IP Audio is a Sametime collaborative activity that enables multiple (two or more) users to transmit and receive audio over an IP network. In a meeting that includes interactive IP audio, the audio can operate in either the “automatic microphone” or the “request microphone” mode. The request microphone mode is the more controlled mode. Only one user can speak at a time and a user must request the microphone before speaking. The automatic microphone mode enables two users to speak simultaneously. In the automatic microphone mode, the person speaking is automatically detected by the Audio/Video Services on the Sametime server (it is not necessary to request the microphone before speaking). Automatic microphone mode offers a more natural form of conversation but provides less control.

IP video  Interactive IP video is a Sametime collaborative activity that enables multiple users to transmit and receive video packets over an IP network. In a meeting that includes interactive IP video, the video follows the audio. The video component of the Sametime Meeting Room client includes a Remote and Local video window. The Remote window displays images from the camera of the person who is speaking and the Local window displays the image from a user’s local camera.

LDAP directory  The administrator can configure the Sametime server to connect to a
Lightweight Directory Access Protocol (LDAP) server. This capability enables an administrator to integrate Sametime into an environment in which LDAP servers and LDAP directories are already deployed. When Sametime is configured to connect to an LDAP server, the Sametime server searches and authenticates user names against entries in the LDAP directory on the third-party LDAP server. The LDAP directory replaces the Domino Directory as the user repository in the community. The community is defined by the users in the LDAP directory.

**LITE and FULL ICE modes**

ICE supports two modes, called LITE and FULL:

- **LITE mode**: Only local candidates from a specific local IP address will be considered when gathering possible connection pairs. No connection will be made to the Sametime TURN server.

- **FULL mode**: All possible candidates are included, including those behind a NAT. Ports are allocated on the Sametime TURN server. Most clients use FULL ICE mode to ensure connections to users behind a NAT and firewall; this is the default mode in Sametime.

**logging**

The Sametime server logging tools include the Sametime log and the Domino® log. The Sametime log records events in the Sametime log database (stlog.nsf). The Sametime Administration Tool includes logging settings that enable you to control whether activities are logged to a database or to text files and to determine which activities are logged. If you log Sametime information to a database, you can view the Sametime log from the Sametime Administration Tool.

The Sametime Administration Tool also allows an administrator to launch the Domino Web Administration Tool to view the Domino log. The Domino log includes information about available memory and disk space, server performance, and databases that need maintenance.

**MCU**

A Multipoint Control Unit (MCU) is a device commonly used to bridge video-conferencing connections. The MCU is an endpoint on the LAN that provides the capability for 3 or more terminals and gateways to participate in a multipoint conference.

**meetings**

Sametime meetings are either "instant" or "scheduled." An instant meeting is started immediately from a presence list in any Sametime client. Whiteboard files cannot be saved during instant meetings. Instant meetings cannot be recorded. A scheduled meeting is scheduled to start at a particular time and date. Scheduled meetings are created in advance in the Sametime Meeting Center application (stconf.nsf) on the Sametime server.

The Meeting Services and the Community Services support the starting, stopping, and creation of meetings on the Sametime server. Components of the Sametime Meeting Room clients interact with the Meeting Services, Community Services, and Audio/Video Services when participating in Sametime meetings. The Meeting Room Client provides telephony and video features for meetings (web conferences). When attending a meeting, a participant can click the 'Join the call' button on the Meeting page. Teleconferencing services are extensible through the use of Telephony Conferencing SPI (TCSIPI). For Audio teleconferencing, telephone services can be made available for meetings and chats, allowing the user to initiate a call for selected users or for everyone in the meeting/chat, using telephone network or voice over IP (VoIP). Server establishes the phone
Audio/video services include VoIP and video services for meetings, using G.711 and G.723 audio codecs, and H.263+, and can be selected when a user schedules a meeting or launches an instant meeting.

**monitoring**

The Sametime server includes charts that allow you to monitor current Sametime server statistics. The monitoring charts, which are presented as tables, provide up-to-the-second information about Community Services, Meeting Services, Recorded Meeting Broadcast Services, Audio/Video Services, web statistics, and free disk space on the server.

**NAT**

A Network Address Translator creates address binding between internal (private) and external (public) addresses. This enables a user with an address on a private network to receive communications from someone outside of their network, through the published external address.

**Packet Switcher**

A Sametime Media Manager component that provides MCU (Multipoint Control Unit) capabilities for audio/video conferencing. The Packet Switcher plays an end-point in the conference, receiving all audio and video data from each client and sending it to all other clients connected to the conference.

**polling**

Polling is a Sametime collaborative activity that enables a Room Owner or Manager to use polls (or ask questions) to gather feedback from meeting participants. For example, the Moderator might ask meeting participants to vote to approve or reject a proposal. Any Sametime Connect users can send polls. Users with share permission for the Sametime Connect can create polls.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

**presence**

Presence refers to the ability of a user to detect when other users are online. A user can view a presence list in a Sametime client or application that displays the names of other online users. Presence is sometimes called "awareness" or "online awareness."

A presence list (or contact list) is a starting point for immediate or "instant" collaboration. Presence lists in Sametime clients display the names of online users in bold green text. Instant messaging sessions and instant meetings can be started immediately from a contact list. A user simply double-clicks or right-clicks an online user's name to send an instant message or start an instant meeting.

Contact lists are found in all Sametime clients. The Sametime Connect client includes a contact list that can display the names of all users in the community who are online. The Sametime Meeting Room client contains a Participant List that displays the names of all users attending a particular meeting.

A user logs in to the Community Services on the Sametime server to become present in the community or an online place (such as a Sametime meeting or website enabled with Sametime technology). The Community Services on the Sametime server support all presence functionality in Sametime.
record and playback (recorded meetings)
Sametime includes a Record and Playback feature that enables a user to record meetings. When scheduling a meeting, the user selects a check box labeled "Record this meeting so that others can replay it later" to record the meeting.

reverse proxy and portal server support
A Sametime server can be deployed behind a reverse proxy server or a portal server. When a Sametime server is deployed on an internal network behind a reverse proxy server, the reverse proxy server operates as an intermediary between the Sametime server and the Sametime clients. All Sametime data flowing between the Sametime server and its clients passes through the reverse proxy server. To accomplish its security objectives, a reverse proxy server manipulates the data that passes through it. The manipulation of Sametime data by the reverse proxy server imposes specific requirements and limitations on the use of reverse proxy servers with the Sametime server.

Sametime Administration Tool
The Sametime® Administration Tool is an HTML and XML based application that runs in a web browser. You open the Sametime Administration Tool by clicking "Administer the Server" on the Sametime server home page. The Sametime Administration Tool is the primary administration tool for the Sametime server.

Sametime Gateway
IBM Sametime Gateway serves as the clearinghouse of presence, using Extensible Messaging and Presence Protocol (XMPP), Virtual Place (VP) protocol, and Session Initiation Protocol (SIP) to connect clients both inside and outside your corporate environment. The Sametime Gateway opens Sametime to external instant messaging access. You can enable this functionality to allow users in your community to communicate with users in another Sametime community that contains a Sametime server with the Sametime Gateway functionality enabled. Enabling the Sametime Gateway functionality requires the installation of separate components.

Sametime Meeting Center (stconf.nsf)
The Sametime Meeting Center is an application (a Lotus Notes® database named stconf.nsf) on the Sametime server that is accessed by a web browser. This application is a central meeting place for members of the Sametime community. From the Sametime Meeting Center, you can schedule a meeting, start a meeting immediately, attend a meeting, and view information about scheduled and finished meetings. All scheduled meetings in Sametime are created in the Sametime Meeting Center. A user who starts an instant meeting from a contact list does not access the Sametime Meeting Center. Anonymous access is allowed to the Sametime Meeting Center database by default. With anonymous access, users are not required to authenticate when accessing the Sametime Meeting Center.

Sametime server
The term Sametime server is used throughout the documentation to refer to a server that has both Sametime and Domino installed.

Sametime server clusters
The Sametime server supports Sametime server clustering. Sametime server clusters enhance server scalability and reliability to enable Sametime to meet the demands of large user populations, and provide load balancing and failover capabilities for Sametime Community Services and Meeting Services.
Sametime server home page (stcenter.nsf)

The Sametime server home page is an HTML page that exists in the Sametime Center database (stcenter.nsf). The Sametime server home page can only be accessed by a web browser and is the user entry point to the Sametime server. After installing the Sametime server on the Domino server, you must set stcenter.nsf as the Home URL for the server. To do this, open the Server document for the Domino server that includes Sametime, select the Internet Protocols tab, select the HTTP tab, and enter stcenter.nsf in the Home URL field of the Mapping section of the Server document.

Sametime TURN Server

A Sametime server used by clients to relay audio/video packets. The Sametime TURN Server uses STUN/TURN functionality. In previous releases, this feature was called the Sametime Reflector.

screen sharing

Screen sharing is a Sametime collaborative activity that enables multiple users to work within a single application on one user's computer. Geographically dispersed users in remote locations can collaborate within a single application to produce a document, spreadsheet, blueprint, or any other file generated from a Windows application. Screen sharing is sometimes also referred to as "application sharing."

In a meeting that includes screen sharing, one user uses the screen-sharing tool in the Sametime Meeting Room client to share a screen or application on the user's local computer with other meeting participants in remote locations. The other meeting participants also use the screen-sharing tools of the Sametime Meeting Room client on their local computers to view and make changes to the shared screen or application. It is not necessary for the remote users to have the application that is being shared installed on their local systems. (The remote users share a single instance of the application that is running on only one meeting participant's computer.)

Only one user at a time can be in control of the shared screen. Most users see the initials of the user who controls the shared screen beside the cursor. The person who is sharing the screen does not see the initials when someone else controls the shared screen. The person who is sharing the screen must view the Participant List details to confirm who controls the shared screen.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General tab of the Sametime Administration Tool.

The administrator controls whether screen sharing is available for meeting participants by setting the Policies - "Allow screen sharing" options of the Sametime Administration Tool. Note that policy is group or user-specific.

Screen sharing is supported by T.120 components of the Meeting Services on the Sametime server. For more information about using this collaborative activity in a meeting, see the Sametime user online help.

security

The Sametime server uses the Internet and intranet security features that are available on the Domino server on which it is installed. Generally, you use the Access Control Lists (ACLs) of databases on the Sametime server to provide users with anonymous access or basic password authentication to individual databases on the server. In addition to the Domino Internet and intranet security features, the Sametime server requires "authentication by
token” security mechanisms to ensure that Sametime clients that establish connections to the Sametime services are authenticated. These security mechanisms include the Sametime Secrets and Tokens authentication databases and the Domino Single Sign-On (SSO) authentication feature.

**self-registration**
The Sametime server includes a self-registration feature. This feature allows an user to create a Person document that contains a User Name and Internet password in the Domino Directory on the Sametime server. The self-registration feature is available to users from the Register link of the Sametime server home page. The administrator has the option of allowing or not allowing self-registration. Self-registration can reduce the workload for the administrator because it enables users to add themselves to the Domino Directory (create a Person document in the directory containing a User Name and Internet password). Allowing self-registration can involve security risks because it enables anonymous users to create records in the Domino Directory. These records permit anonymous users to authenticate with databases on the server. Self-registration is not allowed by default. Also, self-registration cannot be used if Sametime is configured to operate with an LDAP directory.

**send web pages**
Send Web Pages is a Sametime collaborative activity that enables a Meeting Moderator to send a web page URL to all participants in a meeting. When the Moderator sends a web page URL to the meeting participants, a browser window opens on each participant’s screen and displays the web page. If the Moderator sends an additional Web page URL to the meeting participants, the new web page replaces the previous web page in the web browser window.

The administrator controls whether this collaborative activity is available for meetings on the Sametime server from the Configuration - Meeting Services - General settings of the Sametime Administration Tool.

**shared whiteboard and slides tools**
The slides and shared whiteboard tools are Sametime collaborative activities. The slides tab in the meeting room supports uploaded presentations and other documents, while the whiteboard tab provides a white page on which meeting participants can draw. Both activities provide annotation tools that can be used for drawing and highlighting.

In a slides presentation of a web conference or e-meeting, the meeting chair or other presenter displays a slide visible to participants on their computers. Remote meeting participants can view the images and annotate the images using the annotation tools in the Sametime Meeting Room. Before slides can be presented in a meeting, a file containing the slide(s) must be attached to the meeting.

The meeting chair or creator can attach files before or during meetings, and any presenter can attach files during meetings.

**SIP Proxy and Registrar**
A Sametime Media Manager component consisting of two SIP applications: SIP Registrar: Responsible for location service. SIP Proxy: Forwards SIP messages by determining the destination address, using the location service or standard SIP routing procedures. The SIP Proxy/Registrar implements the SIP standard RFC3261.

**StdebugTool.exe utility**
You can use the StdebugTool.exe utility to produce trace files and create
new trace file sets for troubleshooting purposes. These trace files contain debug messages that aid IBM Technical Support in troubleshooting Sametime server problems. If you have never worked with Sametime trace files before, you should use the StdebugTool.exe utility only under the guidance of IBM Technical Support.

**STUN** The Session Traversal Utilities for NAT protocol enables audio/video communications with a client behind a NAT or firewall by providing that client with a transport address (an IP address and port) for receiving packets from a caller. STUN is used by the ICE process to perform connectivity checks on the different available routes between the endpoints on a call.

**transfer files**
Transferring files is a Sametime collaborative activity that enables users to send a file to another user via a contact list in the Sametime Meeting Room or the Sametime Connect client. Users must transfer one file at a time to one person at a time. File transfers are automatically encrypted. The administrator can enable or disable this feature. When you enable this feature, both authenticated and anonymous users can transfer files. The administrator can also disallow certain file types such as .exe file types.

The file transfer feature does not work with Sametime Links. For more information about Sametime Links, see the Sametime Directory and Database Access Toolkit documentation available from IBM DeveloperWorks (http://www.ibm.com/developerworks/lotus/products/instantmessaging/).

**TURN** The Traversal Using Relay NAT protocol enables audio/video communications with a client behind a NAT or firewall by routing communications to the client's external address through a server (the TURN server) residing on the public Internet. TURN is integrated into the Sametime NAT traversal feature to enable clients to exchange audio/video data when direct peer-to-peer communications are not possible. Deploying the NAT traversal feature involves installing a stand-alone TURN server.
Chapter 10. Planning

This section contains information about planning for information technology departments, including installers and administrators.

Skills needed for Sametime administration

Administering a Sametime deployment calls for skills in several different technologies. There are many IBM learning resources that can help you develop the skills you need.

**WebSphere Application Server administration**

Understand application server configurations

Understand cells, nodes, and servers

**Resources for information:**

- WebSphere Application Server V7.0: Technical Overview

**WebSphere Application Server configuration and maintenance**

View performance information about server and application components

WAS proxy, SIP, and HTTP servers

Use problem determination tools and log files to troubleshoot problems

**Resources for information:**

- System Administrator skills for IBM WebSphere Application Server 7
- Education Assistant for WebSphere Application Server 7
- WebSphere Application Server education
- WebSphere Application Server V7 Administration and Configuration Guide

**WebSphere Application Server application management**

Use WebSphere Application Server administrative tools to configure and manage enterprise applications

Configure security for server-side application resources

**Resources for information:**

- WebSphere Application Server V7.0: Technical Overview

**WebSphere Application Server clustering**

Deploy applications in clustered environments

**Resources for information:**

- IBM Certified System Administrator - WebSphere Application Server Network Deployment V7.0
LDAP directory management

Install and set up an LDAP directory

Manage users

Resources for information:
- Best Practices for using LDAP with Sametime

DB2 database management

Creating and managing DB2 databases

Resources for information:
- DB2 education
- DB2 9.5 for Linux, UNIX, and Windows Transition from DB2 9

Domino server administration

Domino is required for Sametime. The administrator should know:
- Notes and Domino basics (what they are, how used)
- Installation and setup of Notes and Domino.
- How to monitor the Domino server tasks (logs, alerts)
- Basic Domino networking (setup/configuration).
- Security (levels, including how ACLs work, server security)
- Server tasks (what are they, how to change, how used, access)
- Administrator client (how to use, accessing from the web)

Resources for information:
- Lotus Domino product home page
- Education Offerings on IBM Lotus Notes Domino 8/8.5

Secure Sockets Layer (SSL) configuration

Knowledge of certificate management

SSL management in Domino and WebSphere Application Server environments

Resources for information:
- WebSphere Application Server V7.0 Security Guide

Audio/Video technology

Audio/Video transmission protocols (STUN, TURN, ICE)

Audio/Video codecs (Media Manager)
Readme

The Readme document for this release of IBM Sametime provides information about getting started with this product, descriptions of any known problems with the current release, and links to IBM Tech Notes.

Review the Release Notes before you begin deploying this product.

System requirements

System requirements for installing IBM Sametime, including supported operating systems, databases, LDAP servers, IBM Sametime servers, browsers, and JDKs.

System requirements for this release of the Sametime family of products are maintained as an IBM Tech Note at the following web address:


Resources for IBM Sametime Standard and Sametime Entry users

You can help your IBM Sametime Standard and Sametime Entry users get started quickly and easily using the informational and learning resources in the Sametime wiki.

For starters, the Administrators: Previewing IBM Sametime Standard and IBM Sametime Entry for your users provides your users with a preview of the new features coming to their desktops. This ready-to-distribute PDF file gives a quick overview of what is new and changed in this release. The Lotus Symphony™ file includes the same information as the PDF file, with instructions on how to customize the file with information specific to your site and how to create your own PDF. Note: Be sure to read the customization instructions in blue text.

The Learning Center page links you to all of the informational and educational material you’ll need, including Getting started pages and the Media Gallery. These resources include links to Flash demonstrations, videos, reference cards, Web seminars, product tours, and other materials for learning Sametime.

Finally, you can provide your users with desktop access to Web seminars, reference cards, and other learning materials by giving them the Sametime Learning Widget. You can find this widget in the Sametime Learning Widget page.

Supporting IPv6 addressing in a Sametime deployment

IPv6 addresses use a different format from IPv4 addresses to support a greater range of direct addresses to computers on the internet. Enabling IPv6 addressing reduces the need for Network Address Translators while improving the efficiency of routing and providing for greater security. Beginning with release 8.0.2, IBM Sametime servers and clients support the use of IPv6 addresses.

Note: For more information on IPv6 addressing with Sametime, see the article Best practices for moving to IPv6.

In this release of Sametime, some components have some limitations when supporting IPv6 addressing:

- Sametime System Console
When installing the Sametime System Console on a system that supports both IPv4 and IPv6 addressing, the IPv4 and IPv6 addresses associated with the Sametime System Console must be mapped to the same host name. Additional host names cause problems in the Sametime System Console because SSL certificates can be generated using either the IPv4 or IPv6 host name, which might not match during authentication.

- **Sametime Gateway**
  You must install the Gateway with a special parameter to enable it for IPv6 addressing; you cannot enable it for support after deployment. The instructions for installing a Sametime Gateway server include information on the parameter and how to use it.

- **Sametime Media Manager**
  The Media Manager does not support IPv6 addressing in this release. If your Sametime deployment includes a Media Manager server, you cannot enable IPv6 addressing at this time. IPv6 addressing will be supported in an upcoming release of Sametime Media Manager.

- **Sametime Connect clients**
  If you support only IPv6 addressing, clients from releases earlier than 8.0.2 will not generate error messages but will appear “broken” to users because they cannot communicate with the IPv6-enabled servers. To avoid lengthy investigations of problems caused by attempts to use older clients with servers where only IPv6 addressing is enabled, you should only use clients from release 8.0.2 or later. If you support both IPv4 and IPv6 addressing, all Sametime clients can communicate all Sametime servers provided you configure those servers to listen for IPv4-format addresses as well as IPv6-format addresses.

- **Sametime Advanced**
  Sametime Advanced does not yet support IPv6 addressing. If your Sametime deployment includes Sametime Advanced, you cannot enable IPv6 at this time. IPv6 addressing will be supported in an upcoming release of Sametime Advanced.

- **Sametime Unified Telephony**
  Sametime Unified Telephony does not yet support IPv6 addressing. If your Sametime deployment includes Sametime Unified Telephony, you cannot enable IPv6 at this time. IPv6 addressing will be supported in an upcoming release of Sametime Unified Telephony.

Enabling support for IPv6 addressing in Sametime products requires configuration changes to various components of a deployment, as described in the following topics:

### Supporting IPv4, IPv6, or both protocols

Your IBM Sametime deployment can support IPv4 addressing, IPv6 addressing, or both protocols. The option you choose will determine how you configure the servers in your deployment.

Existing Sametime deployments use IPv4 addressing only. Rather than completely switch over to IPv6 addressing, you will probably want to phase it in and support both protocols for some time until you are satisfied with your IPv6 support. There are some requirements and limitations for each type of addressing, so review the sections below before implementing any changes.
IPv4 and IPv6 protocols

IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are names of protocols that define how you address computers on the Internet. The IPv6 protocol was introduced to provide not only a larger number of addresses for the increasing number of computers on the Internet, but also to enhance the security of Internet communications.

When entering an IPv4 address, you format it using four sets of digits, separated with dots like this:
205.188.21.22

IPv6 addresses use eight sets of hexadecimal digits separated with colons like this:
2001:0db8:85a3:0000:0000:8a2e:0370:7334

You may see IPv6 addresses abbreviated, for example:
• 2001:db8:85a3:0:0:8a2e:370:7334 where the leading zeros in each group are omitted
• 2001:db8:85a3::8a2e:370:7334 where two consecutive groups containing only zeros are represented by a double colon
• [2001:db8::]/64 where the suffix (/64) indicates the portion of the address that represents the network (the remainder of the address represents computers within that network)

If the URL includes a port, add the :port value outside of the brackets like this:
https://[2001:db8:85a3:08d3:1319:8a2e:0370:7348]:443

Supporting IPv4—only addressing

Prior to release 8.0.2, Sametime products supported only IPv4 addresses, listening only for connections from clients using the IPv4 protocol and ignoring connections using the IPv6 protocol. An IPv4—only deployment requires no special configuration and can combine Sametime components from release 8.0.2 and later with those from prior releases.

Supporting both IPv4 and IPv6 addressing

Sametime release 8.0.2 introduced support for IPv6 addressing, but additionally continued support for IPv4 addressing. This allows you to update your Sametime deployment gradually by combining servers that support both protocols.

Even if a particular Sametime component is enabled only for IPv4 addressing, it can still communicate with IPv6—enabled servers within the deployment provided those servers also support IPv4 addressing (known as dual-support).

Enabling support for IPv6 addressing requires some additional configuration in your deployment. If you upgrade from an IPv6—enabled server in your Sametime deployment, you should verify that your IPv6 settings are still in place and modify them if needed.

When installing the Sametime System Console on a system that supports both IPv4 and IPv6 addressing, the IPv4 and IPv6 addresses associated with the Sametime System Console must be mapped to the same host name. Additional host names cause problems in the Sametime System Console because SSL certificates can be
generated using either the IPV4 or IPV6 host name, which might not match during authentication.

**Supporting IPv6–only addressing**

If you choose to support only IPv6 addressing in your Sametime deployment, use the instructions in this section to enable IPv6. You will additionally need to disable support for IPv4 addressing by ensuring that your settings use values recommended for "IPv6 only" wherever that option is offered.

Enabling support for IPv6 addressing requires some additional configuration in your deployment. If you upgrade from an IPv6-enabled server in your Sametime deployment, you should verify that you IPv6 settings are still in place and modify them if needed.

**Enabling support for IPv6**

Enabling IPv6 support in an IBM Sametime deployment involves configuration changes to the operating system and networks as well as the Sametime components themselves.

**About this task**

Enable support for the IPv6 addressing protocol in your server and client operating systems before you install Sametime:

**Enabling IPv6 on your operating systems**

Before enabling IPv6 support for IBM Sametime, you must enable it for your server and client operating systems.

**About this task**

The configuration changes needed for supporting IPv6 with Sametime vary with the operating system and whether you are using it as a server or a client:

**Enabling IPv6 on a server operating system:**

Consult your server operating system's documentation for instructions on configuring support for IPv6 addressing. In addition, implement the specific changes described here to ensure that your operating system can properly communicate with IBM Sametime while using IPv6 addressing.

**About this task**

The configuration changes needed for supporting IPv6 with Sametime vary with the server's operating system:

*Configuring an AIX server to support IPv6:*

Configure support for IPv6 addressing on a computer running an IBM AIX operating system.

**About this task**

To see which versions of AIX are supported by IBM Sametime, see the system requirements for this release at the following Web address:
For complete instructions on configuring support for IPv6 addressing on a computer running an IBM AIX operating system, see the Upgrading to IPv6 with IPv4 configured in the AIX information center:

**Important:** Some of the components of a Sametime server require the use of an IPv4-formatted loopback address. To ensure that your Sametime server functions properly, do not disable IPv4 support in your server operating system – instead, enable support for both IPv4 and IPv6 addressing.

*Configuring an IBM i server for IPv6:*

Configure support for IPv6 addressing on a computer running an IBM i operating system.

**Before you begin**

You must be using IBM i V6R1 with Sametime if you want to support IPv6 addressing; if you are using an older version of i5/OS®, upgrade to V6R1 before configuring the operating system to support IPv6 as described below. To see the complete list of IBM i and i5/OS versions supported by Sametime, see the system requirements for this release at the following web address:


For information on the IBM i operating system, visit the IBM System i information center.

**About this task**

These instructions describe how to enable support for IPv6 addressing on a functioning Sametime server that is currently using IPv4 addressing.

Follow the steps below to update the IBM i TCP/IP configuration for the IPv6 address you will use for your Sametime server:

**Important:** Some of the components of a Sametime server require the use of an IPv4-formatted loopback address. To ensure that your Sametime server functions properly, do not disable IPv4 support in your server operating system – instead, enable support for both IPv4 and IPv6 addressing.

**Procedure**

1. Add the IPv6–formatted IP address that you will use for your Sametime server. For more information, see Adding a TCP/IP address on IBM i.
2. Add an entry in the local host table for the IPv6 IP address. For more information, see Updating the host table on IBM i. Specify the same fully qualified host name that you used for the original IPv4 address.
3. Update the Domain Name Server. The contents of the Domain Name Server should be similar to the local host table, with two DNS entries for the host name of your Sametime server: one entry that maps the host name to the IPv4 address and another that maps it to the IPv6 address.
See Updating the Domain Name Server for IBM i for special considerations when TCP/IP is configured to check the DNS before the local host table.

**Configuring a Linux server for IPv6:**

By default, the versions of Linux SUSE and Linux RHEL required by IBM Sametime are enabled for IPv6 addressing; however, you should verify that support is enabled before attempting to configure IPv6 support in Sametime.

**Before you begin**

Some of the components of a Sametime server require the use of an IPv4-formatted loopback address. To ensure that your Sametime server functions properly, do not disable IPv4 support in your server operating system – instead, enable support for both IPv4 and IPv6 addressing.

**About this task**

To see which versions of Linux are supported by Sametime, see the system requirements for this release at the following web address:


- **Red Hat Enterprise Linux**

  Red Hat Enterprise Linux supports IPv6 firewall rules using the Netfilter 6 subsystem and the ip6tables command. In Red Hat Enterprise Linux 5, both IPv4 and IPv6 services are enabled by default. For more information on IPv6 support in Red Hat, visit the Red Hat website.

- **SUSE Linux**

  SUSE Linux supports IPv6 addressing, which is enabled by default; for more information on IPv6 support in Linux SUSE, see the SUSE Linux 10 Reference Guide.

A Linux SUSE operating system supports IPv6 addressing by default; however it support was disabled for some reason, you will need to enable it before installing Sametime:

**Configuring Linux SUSE to support IPv6:**

Configure support for IPv6 addressing on a computer running a Linux SUSE operating system.

**About this task**

IPv6 addressing is enabled by default on Linux SUSE servers, but may have been disabled to improve performance while running applications that did not support this protocol.

**Procedure**

1. If you suspect that IPv6 addressing was disabled on your Linux SUSE server, you can check by logging in as the root user and running the following command:
   ```
   ifconfig
   ```
   The system output will look like this:
If the system output includes statements containing the string `inet6` as shown above, then IPv6 support is currently enabled and you can proceed directly to the next topic.

If the output does not contain this string, you must enable IPv6 support now as explained in the next step.

2. Edit the configuration file of the kernel module loader and add the following statement:

   The configuration file is typically located in one of these locations:
   - `/etc/modules.conf`
   - `/etc/conf.modules`
   ```
   alias net-pf-10 ipv6  # automatically load IPv6 module on demand
   ```

3. Save and close the file.

**Configuring a Solaris server for IPv6:**

Configure support for IPv6 addressing on a computer running a Sun Solaris operating system.

**About this task**

To see which versions of Solaris are supported by Sametime, see the system requirements for this release at the following web address:


Support for IPv6 addressing can be enabled during installation of a Solaris server. For information on enabling and verifying IPv6 support on Sun Solaris servers, see the Sun IPv6 Administration Guide:

**Important:** Some of the components of a Sametime server require the use of an IPv4-formatted loopback address. To ensure that your Sametime server functions properly, do not disable IPv4 support in your server operating system – instead, enable support for both IPv4 and IPv6 addressing.

**Configuring a Microsoft Windows server to support IPv6:**

Configure support for IPv6 addressing on a computer running a Microsoft Windows operating system.
Before you begin

Some of the components of a Sametime server require the use of an IPv4-formatted loopback address. To ensure that your Sametime server functions properly, do not disable IPv4 support in your server operating system – instead, enable support for both IPv4 and IPv6 addressing.

About this task

To see which versions of Windows are supported by Sametime, see the system requirements for this release at the following web address:


The Microsoft TechNet website includes information on how IPv6 addressing affects Microsoft operating systems.

Enable IPv6 addressing for your Windows operating system by following the steps below. Note that the names of commands and dialog boxes may be different for your particular Windows operating system.

Procedure

1. Open the "Network Connections" dialog box; for example, by clicking Start > Control Panel > Network Connections.
2. In the "Network Connections" dialog box, right-click on Local Area Connection, and click Properties.
   a. In the "Local Area Connection Properties" dialog box, make sure you are viewing the "General" tab.
   b. On the "General" tab, click the Install button (below the list of connection items).
   c. In the "Select Network Component" dialog box, click Protocol in the list of network components, and then click the Add button.
   d. In the "Select Network Protocol" dialog box, click Microsoft TCP/IP version 6, and then click OK.
      Support for IPv6 is installed immediately, and the "Network Component" and the "Network Protocol" dialog boxes close automatically.
      Back in the "Local Area Connection Properties" dialog box, you can enable or disable the IPv6 protocol on your computer using the checkbox that appears next to Microsoft TCP/IP version 6.
   e. Close the "Local Area Connection Properties" dialog box by clicking the Close button.
3. To assign an IP address to your computer, use the netsh command.
   The Microsoft TechNet website contains a Netsh Technical Reference section that explains how to use the netsh command.

Enabling IPv6 on a client operating system:

Consult your server operating system’s documentation for instructions on configuring support for IPv6 addressing. In addition, implement the specific changes described here to ensure that your operating system can properly communicate with IBM Sametime while using IPv6 addressing.
About this task

To see which operating systems are supported by Sametime Connect, see the system requirements for this release at the following web address:


The configuration changes needed for supporting IPv6 with Sametime vary with the client computer’s operating system:

Configuring a Linux client for IPv6:

Configure Linux on a client computer to support IPv6 addressing.

Procedure
1. Click System > Administration > Network.
2. Select the network interface you want to change, and click Edit.
3. Click Enable IPv6 configuration for this interface, and then close the dialog box.
   This enables IPv6 support for the current session on this computer.
4. To enable IPv6 each time the computer is started, open a command console and run the following command:
   "alias net-pf-10 ipv6" >> /etc/modprobe.conf
5. If you later want to disable IPv6 support on the Linux client, reverse the above settings as follows:
   a. Click System > Administration > Network.
   b. Select the network interface you want to change, and click Edit.
   c. Click Enable IPv6 configuration for this interface, and then close the dialog box.
   d. Open a command console and run the following command:
      "alias net-pf-10 off" >> /etc/modprobe.conf

Configuring a Mac client for IPv6:

Configure a Macintosh computer to support IPv6 addressing.

Procedure
1. Click System Preference.
2. Select the network interface you want to change, and click Advanced.
3. Set "Configure IPv6" to off, and close the dialog box.
4. If you later want to disable IPv6 support on the Mac client, reverse the above settings as follows:
   a. Click System Preference.
   b. Select the network interface you want to change, and click Advanced.
   c. Set "Configure IPv6" to on, and close the dialog box.

Configuring a Windows client operating system for IPv6:

Configure a Microsoft Windows client operating system to support IPv6 addressing.
Procedure

1. Open the "Network Connections" dialog box; for example, in Windows XP Professional, by clicking Start > Control Panel > Network Connections.

2. In the "Network Connections" dialog box, right-click on Local Area Connection, and click Properties.
   a. In the "Local Area Connection Properties" dialog box, make sure you are viewing the "General" tab.
   b. On the "General" tab, click the Install button (below the list of connection items).
   c. In the "Select Network Component" dialog box, click Protocol in the list of network components, and then click the Add button.
   d. In the "Select Network Protocol" dialog box, click Microsoft TCP/IP version 6, and then click OK.
      Support for IPv6 is installed immediately, and the "Network Component" and the "Network Protocol" dialog boxes close automatically.
      Back in the "Local Area Connection Properties" dialog box, you can enable or disable the IPv6 protocol on your computer using the checkbox that appears next to Microsoft TCP/IP version 6.
   e. Close the "Local Area Connection Properties" dialog box by clicking the Close button.

3. If you later want to disable IPv6 support on the Windows client, reverse the above settings as follows:
   a. Open the "Network Connections" dialog box; for example, in Windows XP Professional, by clicking Start > Control Panel > Network Connections.
   b. In the "Local Area Connection Properties" dialog box, make sure you are viewing the "General" tab.
   d. Click Uninstall.
   e. Close the "Local Area Connection Properties" dialog box by clicking the Close button.

Ports used by Sametime servers

IBM Sametime uses a number of ports on the servers in your deployment. This topic lists the default ports and their uses; a range of ports means that the application can select any port in that range, in case one or more of those ports are already in use by other applications.

Sametime System Console

The following ports are used on the Sametime System Console.

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>50000</td>
<td>Installation manager utilities, post-registration utilities, and the Sametime Meeting Server access the Sametime System Console database port. The database port number is determined by the DB2 server configuration.</td>
</tr>
</tbody>
</table>
Table 23. Sametime System Console ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9080</td>
<td>The Sametime Community Server accesses the Sametime System Console HTTP port. This is determined by the WebSphere Application Server configuration. You can find this port number in AboutThisProfile.txt or in the Integrated Solutions Console.</td>
</tr>
<tr>
<td>9443</td>
<td>The Sametime Community Server accesses the Sametime System Console HTTPS port. This is determined by the WebSphere Application Server configuration. You can find this port number in AboutThisProfile.txt or in the Integrated Solutions Console.</td>
</tr>
<tr>
<td>8700</td>
<td>Provides HTTP browser access to the Sametime System Console for administrators. This is determined by the WebSphere Application Server configuration. You can find this port number in AboutThisProfile.txt or in the Integrated Solutions Console.</td>
</tr>
<tr>
<td>8701</td>
<td>Provides HTTPS browser access to the Sametime System Console for administrators. This is determined by the WebSphere Application Server configuration. You can find this port number in AboutThisProfile.txt or in the Integrated Solutions Console.</td>
</tr>
</tbody>
</table>

DB2 server

The following ports are used on the DB2 server.

Table 24. DB2 server ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>50000</td>
<td>The DB2 port is accessed by the Sametime System Console. The port number is configured by the DB2 server configuration.</td>
</tr>
</tbody>
</table>

LDAP server

The following ports are used on the LDAP server.

Table 25. LDAP server ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>389 or 636</td>
<td>The LDAP port is accessed by the Sametime System Console. The port number is configured by the LDAP server configuration.</td>
</tr>
</tbody>
</table>
**Sametime Community Server**

The following ports are used on the Sametime Community Server. The first table lists ports used by HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports, and the second table lists ports used by Community Services.

*Table 26. HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports*

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>The Sametime Community Server listens for the Sametime System Console on port 80. If you allow HTTP tunneling on port 80 during the Sametime Community Server installation, the Community Services multiplexer on the Sametime Community Server listens for HTTP connections from web browsers, and Sametime Connect clients on port 80. If the you do not allow HTTP tunneling on port 80 during the Sametime Community Server installation, the Domino HTTP server listens for HTTP connections on this port.</td>
</tr>
<tr>
<td>389</td>
<td>If you configure the Sametime Community Server to connect to an LDAP server, the Sametime Community Server connects to the LDAP server on this port.</td>
</tr>
</tbody>
</table>

**Alternate HTTP port (8088)**

If you allow HTTP tunneling on port 80 during the Sametime Community Server installation or afterward, the Domino HTTP server on which the Sametime Community Server is installed must listen for HTTP connections on a port other than port 80. The Sametime installation changes the Domino HTTP port from port 80 to port 8088 if the administrator allows HTTP tunneling on port 80 during a Sametime Community Server installation.

**Note:** If you allow HTTP tunneling on port 80 during the Sametime Community Server installation, web browsers make HTTP connections to the Community Services multiplexer on port 80, and the Community Services multiplexer makes an intraserver connection to the Sametime HTTP server on port 8088 on behalf of the web browser. This configuration enables the Sametime Community Server to support HTTP tunneling on port 80 by default following the server installation.

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>The Domino HTTP server listens for HTTPS connections from the Sametime System Console on this port by default. This port is used only if you have set up the Domino HTTP server to use Secure Sockets Layer (SSL) for web browser connections.</td>
</tr>
</tbody>
</table>
Table 26. HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1352</td>
<td>The Domino server on which Sametime is installed listens for connections from Notes clients and Domino servers on this port.</td>
</tr>
<tr>
<td>9092</td>
<td>The Event Server port on the Sametime Community Server is used for intraserver connections between Sametime components. Make sure that this port is not used by other applications on the server.</td>
</tr>
<tr>
<td>9094</td>
<td>The Token Server port on the Sametime Community Server is used for intraserver connections between Sametime components.</td>
</tr>
</tbody>
</table>

Table 27. Community Services ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1516</td>
<td>Community Services listens for direct TCP/IP connections from the Community Services of other Sametime Community Servers on this port. If you have installed multiple Sametime Community servers, this port must be open for presence, chat, and other Community Services data to pass between the servers.</td>
</tr>
</tbody>
</table>
| 1533         | The Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients (such as Sametime Connect and Sametime Meeting Room clients) on this port.  
  
  **Note:** The term "direct" TCP/IP connection means that the Sametime client uses a unique Sametime protocol over TCP/IP to establish a connection with the Community Services.  
  
  The Community Services also listen for HTTPS connections from the Community Services clients on this port by default. The Community Services clients attempt HTTPS connections when accessing the Sametime Community Server through an HTTPS proxy server. If a Sametime client connects to the Sametime Community Server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted.  
  
  If you do not allow HTTP tunneling on port 80 during the Sametime installation, the Community Services clients attempt HTTP-tunneled connections to the Community Services on port 1533 by default. |
### Table 27. Community Services ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>If you allow HTTP tunneling on port 80 during the Sametime Community Server installation, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80. <strong>Note:</strong> When HTTP tunneling on port 80 is allowed during the Sametime installation, the Community Services multiplexer listens for HTTP-tunneled connections on both port 80 and port 1533. The Community Services multiplexer simultaneously listens for direct TCP/IP connections on port 1533. Port 80 ensures backward compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime Community Server, the client might attempt this connection on port 80.</td>
</tr>
<tr>
<td>8082</td>
<td>When HTTP tunneling support is enabled, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 8082 by default. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. Port 8082 ensures backward compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime Community Server, the client might attempt this connection on port 80.</td>
</tr>
</tbody>
</table>

### Table 28. Sametime Classic Meetings

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1533,</td>
<td>The Sametime Classic Meeting Room client loads in a user's web browser when the user attends an instant or scheduled meeting. The Meeting Room client must establish connections with the Community Services on the Sametime Community Server (on default port 1533).</td>
</tr>
<tr>
<td>8081,</td>
<td>The Meeting Room client must establish connections with the Meeting Services on the Sametime Community Server (on default port 8081).</td>
</tr>
<tr>
<td>554</td>
<td>The Sametime Classic Recorded Meeting client attempts a direct RTSP TCP/IP connection to the Recorded Meeting Broadcast Services on the Sametime Community Server on default port 554. Over this connection, the Broadcast client negotiates with the server to receive the streams that transmit the recorded meeting data.</td>
</tr>
</tbody>
</table>
The following ports are used on the Sametime Media Manager.

### Table 29. Media Manager ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9080</td>
<td>HTTP port for control and general management of audio/video calls. In a cluster, HTTP ports are proxied through a WebSphere Proxy Server. This lets you open these ports only between the firewall and the WebSphere Proxy. WebSphere may change this ports depending on the install environment.</td>
</tr>
<tr>
<td>42000-43000</td>
<td>The Packet Switcher component of the Sametime Media Manager routes audio data to participant endpoints through a range of ports starting with 42000 through 43000. It uses values in this range as needed, as it services multiple calls. It chooses new ports in increments of 2. If encryption is enabled (SRTP), the range starts with an odd port number. RTCP starts with the next port available, which is the RTP or SRTP port incremented by 1.</td>
</tr>
<tr>
<td>46000-47000</td>
<td>The Packet Switcher component of the Sametime Media Manager routes video data to participant endpoints through a range of ports starting with 46000 through 47000. It uses values in this range as needed, as it services multiple calls. It chooses new ports in increments of 2. If encryption is enabled (SRTP), the range starts with an odd port number. RTCP starts with the next port available, which is the RTP or SRTP port incremented by 1.</td>
</tr>
<tr>
<td>5060 and 5061</td>
<td>The Conference Manager, and Packet Switcher are SIP applications, so they use WebSphere SIP container ports. By default, they are 5060 and 5061, but they are dependent on WebSphere during install to determine the available port numbers to use. In a cluster, SIP ports are proxied through a WebSphere Proxy Server. This lets you open these ports only between the firewall and the WebSphere Proxy.</td>
</tr>
<tr>
<td>8880</td>
<td>This is for server to server communication. The Sametime System Console accesses the Deployment Manager SOAP port. This port number varies, depending on how WebSphere was installed. The port number can be determined by looking at AboutThisProfile.txt’s SOAP connector port value in the profile log directory or the Integrated Solutions Console.</td>
</tr>
</tbody>
</table>
**SIP Proxy and Registrar**

The following ports are used on the SIP Proxy and Registrar.

*Table 30. SIP Proxy and Registrar ports*

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5080-5081</td>
<td>SIP messaging uses these ports in a single server Media Manager deployment where SIP Proxy and Registrar runs in a separate virtual host. The value is defined in the WebSphere Application Server instance on which the Sametime Proxy &amp; Registrar is running.</td>
</tr>
<tr>
<td>5060-5061</td>
<td>The default ProxyRegistrar installer does not use these ports. It uses the two above. Therefore, this is only true if the administrator changes the virtual host to use the default, which is defined on port 5060/5061. SIP messaging uses this port in a multiple server Media Manager deployment where SIP Proxy and Registrar runs in on a separate machine. The value is defined in the WebSphere Application Server instance on which the Sametime Proxy &amp; Registrar is running.</td>
</tr>
</tbody>
</table>

**Sametime Meeting Server**

The following ports are used on the Sametime Meeting Server. Most of these ports are configurable.

*Table 31. Meeting Server ports*

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9080</td>
<td>In a single node environment using HTTP that bypasses the WebSphere Application Server proxy, the Sametime Meeting Server listens for data from the Sametime Meeting Room client over this connection.</td>
</tr>
<tr>
<td>443</td>
<td>In a single node environment using HTTPS that bypasses the WebSphere Application Server proxy, the Sametime Meeting Server listens for data from the Sametime Meeting Room client over this connection.</td>
</tr>
<tr>
<td>9080</td>
<td>In a multiple node environment using HTTP, the Sametime Meeting Server listens for data from the Sametime Meeting Room client that is passed through the WebSphere Application Server proxy.</td>
</tr>
<tr>
<td>9443</td>
<td>In a multiple node environment using HTTPS, the Sametime Meeting Server listens for data from the Sametime Meeting Room client that is passed through the WebSphere Application Server proxy.</td>
</tr>
</tbody>
</table>
Table 31. Meeting Server ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8880</td>
<td>This is for server to server communication. The Sametime System Console accesses the Deployment Manager SOAP port. This port number varies, depending on how WebSphere was installed. The port number can be determined by looking at AboutThisProfile.txt’s SOAP connector port value in the profile log directory or the Integrated Solutions Console. See also the following section: Note about SOAP ports for complex deployments.</td>
</tr>
</tbody>
</table>

Note about SOAP ports for complex deployments Deploying WebSphere Application Server SOAP port is complicated and might include ports besides 8880, especially if there is more than one Sametime product on a specific machine. Usually the firewall openings are configured prior to the deployment, when your understanding of the port configuration is still incomplete. In order to have a smoother deployment you can add port ranges – for example 8880 - 8890 and 8600 - 8610. For example, when a Sametime Proxy node in the DMZ is federated into the internal Sametime System Console cell, it needs one port for Sametime System Console to Sametime Proxy Deployment Manager communication and another port for the Sametime Proxy primary node communication – which is on the same machine. You might also need port 8601 when you want to update the Sametime Proxy configuration through the Sametime System Console.

**Sametime Proxy Server**

The following ports are used on the Sametime Proxy Server.

Table 32. Proxy Server ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8880</td>
<td>This is for server-to-server communication. The Sametime System Console accesses the Deployment Manager SOAP port. This port number varies, depending on how WebSphere was installed. The port number can be determined by looking at AboutThisProfile.txt’s SOAP connector port value in the profile log directory or the Integrated Solutions Console. See also the previous section: Note about SOAP ports for complex deployments.</td>
</tr>
</tbody>
</table>

**Sametime Advanced**

The following ports are used on Sametime Advanced. Most of these ports are configurable.

Table 33. Advanced server ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9080</td>
<td>The default http port for the Sametime Advanced web application.</td>
</tr>
</tbody>
</table>
Table 33. Advanced server ports  (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9443</td>
<td>The default https port for the Sametime Advanced web application.</td>
</tr>
<tr>
<td>1883</td>
<td>The default MQTT port. The broadcast community alerts and notifications are sent over this port.</td>
</tr>
<tr>
<td>8883</td>
<td>The default MQTT SSL port. The broadcast community alerts and notifications are sent over this port.</td>
</tr>
</tbody>
</table>

**Note about SOAP ports for complex deployments**
Deploying WebSphere Application Server SOAP port is complicated and might include ports besides 8880, especially if there is more than one Sametime product on a specific machine. Usually the firewall openings are configured prior to the deployment, when your understanding of the port configuration is still incomplete. In order to have a smoother deployment you can add port ranges – for example 8880 - 8890 and 8600 - 8610. For example, when a Sametime Proxy node in the DMZ is federated into the internal Sametime System Console cell, it needs one port for Sametime System Console to Sametime Proxy Deployment Manager communication and another port for the Sametime Proxy primary node communication – which is on the same machine. You might also need port 8601 when you want to update the Sametime Proxy configuration through the Sametime System Console.

**Sametime Connect client**

The following ports are used on the Sametime Connect client.

Table 34. Sametime Connect client ports

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>The client listens for HTTP traffic over this port. This cannot be configured in preferences.</td>
</tr>
<tr>
<td>22222</td>
<td>The installed meeting client uses this port for peer-to-peer application sharing.</td>
</tr>
<tr>
<td>20830 to 20930</td>
<td>This range of ports is used by the audio and video channels to receive RTP and RTCP packets over UDP.</td>
</tr>
<tr>
<td>5060</td>
<td>Sametime Connect client SIP port. The Sametime Connect client will start with the initial port value, finding the first port available in increments of 2. This search is up to and including the starting port value plus 100. The starting value is implemented as a preference, but is not currently exposed for update via any user interface.</td>
</tr>
<tr>
<td>5656.</td>
<td>Sametime Connect client port used for peer-to-peer file transfer.</td>
</tr>
<tr>
<td>59449</td>
<td>Sametime Connect client Web API port for HTTP</td>
</tr>
<tr>
<td>59669</td>
<td>Sametime Connect client Web API port for HTTPS</td>
</tr>
</tbody>
</table>
Finding ports for WebSphere Application Server-based applications

Follow these instructions to determine the ports used by the WebSphere Application Server-based application servers: IBM Lotus Sametime Meeting Server, Sametime Media Manager, and Sametime Proxy Server.

Procedure
1. Log in to the Integrated Solutions Console for the WebSphere Application Server-based Sametime application server.
2. Click **Application servers** > **STMeetingServer or STMediaSever or STproxyServer** > **Ports**.
3. The following ports are used by Sametime application servers:

<table>
<thead>
<tr>
<th>Port</th>
<th>Application server</th>
</tr>
</thead>
<tbody>
<tr>
<td>WC_defaulthost, WC_defaulthost_secure</td>
<td>Sametime Meeting Server, Sametime Proxy Server</td>
</tr>
<tr>
<td>SIP_DEFAULTHOST, SIP_DEFAULTHOST_SECURE</td>
<td>Sametime Media Manager</td>
</tr>
<tr>
<td>SOAP_CONNECTOR_ADDRESS</td>
<td>Server/server connection</td>
</tr>
<tr>
<td>PROXY_HTTP_ADDRESS, PROXY_HTTPS_ADDRESS</td>
<td>Http server for Sametime Meeting Server and Sametime Proxy Server</td>
</tr>
</tbody>
</table>

Planning deployments with the Sametime Standard features you want

Read about the topology that includes the IBM Sametime Standard features you plan to deploy to users. To extend the deployment to include persistent chat rooms and broadcast communities, purchase and deploy Sametime Advanced.

Related information

- What is Sametime Advanced?
- Deploying instant messaging, persistent chat rooms, and broadcast communities

Deploying instant messaging and presence only

To provide instant messaging and presence only, use a Sametime Community Server or cluster of servers running on Domino.

The following components are deployed in a Sametime environment that contains instant messaging and presence only:

- Sametime Community Server
- Sametime Connect client, Sametime client embedded in Notes, or Sametime browser client
- LDAP directory
  - An LDAP directory is required to integrate the Sametime Community server with the Sametime System Console, Meeting Server, and Media Manager.

To extend instant messaging to external communities, also deploy Sametime Gateway. To provide audio-visual features in the Sametime client, also deploy Sametime Media Manager.
Deploying instant messaging and meetings
To provide instant messaging and presence, use an IBM Sametime Community Server or cluster of servers running on Domino. To provide meeting rooms, use a Sametime Meeting Server or cluster of servers running on WebSphere Application Server.

Components used
The following components must be deployed in a Sametime environment that combines instant messaging and presence with meetings:

- Sametime System Console - used for managing and administering servers from a central location
- DB2
- LDAP directory
- Sametime Community Server
- Sametime Meeting Server
- Sametime Connect client, Sametime client embedded in Notes, or Sametime browser client
- Sametime Proxy Server - provides an integrated web chat client and presence; required for Sametime browser clients

The following components can optionally be deployed:

- Sametime Gateway - extends instant messaging to external communities
- Sametime Media Manager - provides audio and video features in the Sametime client and in meetings

Deploying instant messaging, meetings, and web clients
To provide instant messaging and presence, use a Sametime Community Server or cluster of servers running on Domino. To provide meeting rooms, use a Sametime Meeting Server or cluster of servers running on WebSphere Application Server. To provide support for web chat clients, use a Sametime Proxy Server.

Components used
The following components must be deployed in a Sametime environment that combines instant messaging and presence with meetings:

- Sametime System Console - used for managing and administering servers from a central location
- DB2
- LDAP directory
- Sametime Community Server
- Sametime Meeting Server
- Sametime Connect client, Sametime client embedded in Notes, or Sametime browser client
- Sametime Proxy Server - provides an integrated web chat client and presence; required for Sametime browser clients
The following components can optionally be deployed:

- Sametime Gateway - extends instant messaging to external communities

**Deploying instant messaging, meetings, web clients, audio, and video**

To provide all client features to users, plan to deploy Sametime Community Servers, Sametime Meeting Servers, Sametime Proxy Servers, and Sametime Media Manager components.

**Components used**

The following components must be deployed in a Sametime environment that combines instant messaging and presence with meetings that enable audio and video features:

- Sametime System Console - used for managing and administering servers from a central location
- DB2
- LDAP directory
- Sametime Community Server
- Sametime Meeting Server
- Sametime Connect client, Sametime client embedded in Notes, or Sametime browser client
- Sametime Proxy Server - provides an integrated web chat client and presence; required for Sametime browser clients
- Sametime Media Manager - provides audio and video features in the Sametime client and in meetings

The following components can optionally be deployed:

- Sametime Gateway - extends instant messaging to external communities
- Sametime Bandwidth Manager - enables you to assign maximum levels of bandwidth usage to users based on policy settings
- Sametime TURN Server - enable clients to exchange audio and video data when direct peer-to-peer communications are not possible

**Audio-visual components provided with the Sametime Media Manager**

The Sametime Media Manager comprises three components, which are installed on separate systems in a production environment.

- **Packet Switcher**
  Based on voice-activated switching, the Packet Switcher functions as an MCU (Multipoint Conferencing Unit) by routing audio and video data between participant endpoints. There can be one or more Packet Switchers in a deployment; the Conference Manager will distribute conferences over the available Packet Switchers. A Packet Switcher can only be registered with one Conference Manager (or cluster of Conference Managers). A Packet Switcher should not be a member of a WebSphere Application Server cluster; instead, each Packet Switcher is deployed as a non-clustered (primary) node.

- **Conference Manager**
Manages multipoint conferences by maintaining a dialog with each participant, and ensuring that all media flows between those participants. You can install multiple Conference Manager components and cluster them for high availability and failover.

- **SIP Proxy/Registrar**
  Directs conference participants to Conference Manager servers and provides high availability and failover functionality. You can install multiple SIP Proxy/Registrar components and cluster them for high availability and failover.

## Deploying instant messaging to external messaging communities

Use IBM Sametime Gateway to connect Sametime clients with other instant messaging clients. Several options are available for setting up a single server or a cluster of Sametime Gateway servers in a network deployment. You can install Sametime Gateway securely in the network DMZ. In some cases, Network Address Translators (NAT) is supported.

In addition to the topologies described here, you can read about deploying Sametime Gateway on the wiki, available at the following web address:

http://www.ibm.com/developerworks/wikis/display/sametime/Sametime+Gateway+deployments

### Deploying Sametime Gateway in the DMZ

Sametime Gateway is an enterprise solution that requires a clustered deployment in the network DMZ. DMZ is a networking term that comes from the military term "demilitarized zone." DMZ refers to an area of a network, usually between two firewalls, where users from the Internet are permitted limited access over a defined set of network ports and to predefined servers or hosts. A DMZ is used as a boundary between the Internet and your company’s internal network. The network DMZ is the only place on a corporate network where Internet users and internal users are allowed at the same time.

There is no risk of data being compromised as Sametime Gateway itself does not contain data. There is no need to install reverse proxies or other servers, such as IP sprayers or load balancers in front of Sametime Gateway. Sametime Gateway is secure because:

- **Firewall restrictions** make it impossible for users from the Internet to directly access a Sametime community server on your corporate intranet, but Internet users can access Sametime Gateway in the network DMZ.
- Sametime community servers, behind the internal firewall, are accessible only over an encrypted VP protocol.
- DB2 is behind the internal firewall, restricted by host and port access.
- LDAP is behind the internal firewall, accessible over SSL and restricted by host and port access.
- Sametime Gateway exchanges with other instant messaging providers over SIP can be encrypted with SSL.

Components perform best when installed on their own machines and are most secure when behind the internal firewall.

### Topologies for a standalone server

A standalone Sametime Gateway server has its own administrative console. Standalone servers do not require a SIP or XMPP proxy server. In the following
configuration, the Sametime Gateway server is deployed outside the internal firewall in the DMZ, while DB2 and LDAP servers are behind the firewall.

Topologies for a managed group of servers

Each of the following deployments consists of a cluster of servers that work together in a cell to provide high availability and failover. There is one administrative console to manage all servers. The following cluster deployments are considered:

- Scenario: Two-machine installation of a cell of Sametime Gateway servers
  - Machine 1: DB2, Deployment Manager, primary node
  - Machine 2: secondary node, proxy servers
- Scenario: Three-machine installation of a cell of Sametime Gateway servers
  - Machine 1: DB2
  - Machine 2: Deployment Manager, primary node
  - Machine 3: secondary node, proxy servers
- Scenario: Four-machine installation of a cell of Sametime Gateway servers
  - Machine 1: DB2
  - Machine 2: Deployment Manager, primary node
  - Machine 3: secondary node
  - Machine 4: proxy servers
- Scenario: Five-machine installation of a cell of Sametime Gateway servers
  - Machine 1: DB2
  - Machine 2: Deployment Manager, primary node
  - Machine 3: secondary node
  - Machine 4: secondary node
  - Machine 5: proxy servers

The following illustration shows a typical of Sametime Gateway cluster and the ports that must be open in the firewalls to connect with DB2 and LDAP, and exchange instant messages and presence between the local Sametime community and external instant messaging communities.
WebSphere Application Server and DB2

IBM Sametime Gateway runs on IBM WebSphere Application Server. WebSphere Application Server provides the following capabilities:

- Clustering support, robust failover capability using the High Availability Manager
- Session Initiation Protocol (SIP) Infrastructure, including stateless SIP Proxy and SIP IP sprayer provided by the platform
- Open, extensible platform support. Additional plug-in services can configured in a flexible manner
- A central place to administer system configuration and monitoring and security policies through the Integrated Solutions Console and wsadmin script commands.

DB2 is the storage for the Sametime Gateway policies and logging. DB2 can be clustered for failover and load-balancing purposes. DB2 is part of the Lotus common storage strategy. Lotus Domino can use DB2 as an alternative repository, and Sametime Enterprise Meeting Server also uses DB2 for storing and sharing configuration data across servers. DB2 should be installed on a separate machine behind the internal firewall.

**Typical deployment when connecting to instant messaging communities**

Sametime Gateway can connect to the following instant messaging communities:

- AOL, Google Talk, and XMPP communities
- Other Sametime communities
- Other Sametime companies using AOL clearinghouse
You can set up any or all configurations as needed. Sametime Gateway allows
selected individuals in your company to send instant messages to users on one or
more public networks, giving your users immediate access to millions of users
worldwide.

**Note:** When you set up a connection with AOL, you have the option of connecting
with AOL users only, or connecting with the AOL clearinghouse community that
includes AOL, ICQ, iChat, and other users from AOL Enterprise Federation Partner
communities, including external Sametime communities. IBM recommends that
you do not configure both communities, as users served by the AOL clearinghouse
are a superset of users served by the AOL community. If you set up AOL only, and
later decide to connect with the AOL clearinghouse community, delete the AOL
community first before adding the AOL clearinghouse community to Sametime
Gateway.

When you connect to other Sametime companies, you can connect business users
of different companies. This deployment is very useful in case of acquisitions when
IT infrastructure is still separate, when you want to interconnect vendors over the
Internet. Connections are made secure by using an SSL certificate exchange.

**Recommended deployment**

For small, test configurations only, you can install Sametime Gateway on the same
computer as Sametime Community Server, DB2, or other applications. For a
production environment, your Sametime Community Server should be installed on
a separate computer from your Sametime Gateway.

**Multiple Network Interface Cards**

To simulate a NAT (Network Address Translator), you can use two Network
Interface Cards (NICs), one for an internal IP address and the other for an external
IP address. If you use this configuration, you must update the default host using
the Integrated Solutions Console. See Configuring network interface cards to
simulate a NAT.
Note: The use of a NAT is only supported with a clustered configuration. Setting up a NAT is described in Configuring the Gateway cluster and SIP proxy for a NAT environment.

**Deploying meetings to external Internet users**

Use internal and external Sametime Meeting servers to allow users within your organization to meet with external users from the Internet. One Sametime Meeting server is installed on the corporate intranet and another Sametime Meeting server is installed on another machine outside the firewall or in the network DMZ if you have one. DMZ, or "demilitarized zone," refers to an area of a network, usually between two firewalls, where users from the Internet are permitted limited access over a defined set of network ports and to predefined servers or hosts. A DMZ is used as a boundary between the Internet and your company's internal network.

Deploying meetings without a DMZ

When you set up two independent Meeting servers without a DMZ, the external Meeting server is not connected to your internal Meeting server. The room-based URLs are simpler with this configuration. Browser clients access the external server with anonymous logins. Each Meeting server is maintained separately.
Deploying meetings in a DMZ

The network DMZ is the only place on a corporate network where Internet users and internal users are allowed at the same time. When internal users are not allowed to address servers outside the corporate firewall, set up a reverse proxy that allows internal users to connect to the external Meeting Servers. The reverse proxy provides the routing services and allows a single entity to be configured in the firewall. It controls access to external servers and can be set up to limit usage.

<table>
<thead>
<tr>
<th>Internal Sametime Client (any type)</th>
<th>Internal Meetings</th>
<th>Reverse-Proxy</th>
<th>External Meetings</th>
<th>External Sametime Client (browser-based)</th>
</tr>
</thead>
</table>

Planning the size of your deployment on AIX, Linux, Solaris, or Windows

Before you install any Sametime components, know whether you are installing a small-scale deployment or an enterprise-scale deployment. In the case of an enterprise-scale deployment, you must also decide if you will be using clustered servers to distribute the load or multiple separate servers that function independently. The size of your deployment affects installation choices.

After you install the Sametime System Console, you create deployment plans for the Sametime Community Server, Sametime Proxy Server, Sametime Media Manager components, Sametime Meeting Server and, if needed, Sametime Advanced. Deployment plans are the blueprints for each server's installation, so you must know at that point whether you want to install on the same machine or a separate machine. Your decision determines the choice you make for the configuration type. The Sametime Community Server is always installed on its own machine running Lotus Domino. For the other servers, you have a choice of installing them on one machine or multiple machines.

In a pilot deployment or a small deployment, you can use one machine for the Sametime System Console, Sametime Proxy Server, Sametime Media Manager components, and Sametime Meeting Server and if needed, Sametime Advanced, as long as the hardware, RAM, and processing speed are sufficient. You can also use separate machines for each of the servers.
In a **non-clustered production deployment**, you should install each of these Sametime servers on its own machine for the best performance. Only consider installing multiple Sametime components on one machine if its hardware, RAM, and processing speed are superior.

A **clustered production deployment** consists of multiple servers of the same type, so you may have a cluster of Sametime Proxy Servers, a cluster of Meeting Servers, and so on. You can either create a horizontal cluster or vertical cluster. In a horizontal cluster, you install each of the Sametime servers on its own machine. In a vertical cluster, you install each Sametime server on the same machine as long as it can provide good performance.

Decide which type of deployment you are rolling out before you begin to install any server.

**Planning a small deployment on AIX, Linux, Solaris, and Windows**

Before installing the Sametime System Console, Sametime Proxy Server, Sametime Meeting Server, Sametime Media Manager, Sametime Bandwidth Manager, Sametime Advanced Server, and DB2, decide if you will install everything on one machine as a single-server configuration or on separate machines as a multiple-server configuration. The minimum RAM for a small deployment on a single server is 6 GB, but IBM recommends 8 GB. You will always install Sametime Community Servers and Sametime Gateway on their own machines because of their underlying legacy architecture.

For optimal memory usage and simplified administration, install the Sametime System Console with the "Cell Profile" option. Install each new type of server as a Primary Node and allow the installation program to integrate it immediately with the console.
Related concepts

“How installing cell profiles affects starting and stopping servers” on page 481
If you chose the configuration type “Cell Profile” when you installed a Sametime Proxy Server, Sametime Media Manager components, or a Sametime Meeting Server, you installed a self-contained set of WebSphere Application Server components for each server. You have this configuration type if you installed different Sametime servers on the same machine or on multiple machines that are not clustered.

Related tasks

“Preparing to install a Sametime Proxy Server” on page 346
Use the Sametime System Console to prepare to install an IBM Sametime Proxy Server by pre-populating values required for installation.

“Preparing to install a Sametime Media Manager on Linux or Windows” on page 372
Use the Sametime System Console to prepare to install a Sametime Media Manager by pre-populating values required for installation. The media manager runs on Linux or Microsoft Windows only.

“Preparing to install a Sametime Meeting Server” on page 436
Use the Sametime System Console to prepare to install a Sametime Meeting Server by pre-populating values required for installation.

Clustering Sametime servers for high enterprise availability

In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

Clusters are groups of servers that are managed together and participate in workload management. A cluster can contain nodes or individual application servers. A node is usually a physical computer system with a distinct host IP address that is running one or more application servers. Clusters can be grouped under the configuration of a cell, which logically associates many servers and clusters with different configurations and applications with one another depending on the discretion of the administrator and what makes sense in their organizational environments.

Clusters are responsible for balancing workload among servers. Servers that are a part of a cluster are called cluster members. When you install an application on a cluster, the application is automatically installed on each cluster member. You can configure a cluster to provide workload balancing with service integration or with message driven beans in the application server.

Important: It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

How you create a cluster for a Sametime server depends on the type of server you’re working with.

• **Sametime Community Server**
Unlike other Sametime products, the community server is not hosted on WebSphere Application Server. Instead, you install the community server on a Lotus Domino server and use the replication feature to create a cluster.

- **Sametime Gateway**
  The gateway is hosted on WebSphere Application Server, but installs and clusters differently from other WebSphere-based Sametime servers. A Sametime Gateway cluster always requires a dedicated Deployment Manager, and additionally uses a dedicated WebSphere SIP proxy server and XMPP server.

- **Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, Sametime Advanced**
  These servers all run on WebSphere Application Server and can use the Sametime System Console as a cluster’s Deployment Manager. When you cluster these servers, you administer the WebSphere Application Server through the cluster’s Deployment Manager, using its Integrated Solutions Console. You administer the Sametime server applications using the centralized Sametime System Console.

If you intend to cluster two or more Sametime servers, you have several decisions to make before you begin installation:

- **Where will you install the Deployment Manager?**
  The type of server you are clustering determines the role of the Deployment Manager.
  - **Sametime Community Server**
    If you are clustering Sametime Community Servers, you will not require a Deployment Manager. Instead, select one community server to function as the "master" server for replication purposes; any additional community servers will function as "slaves" and receive copies of data from the master server.
  - **Sametime Gateway**
    If you are clustering Sametime Gateway servers, you must install a dedicated Deployment Manager for the cluster, and then manage the WebSphere Application Server nodes using the Deployment Manager’s Integrated Solutions Console.
  - **Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, Sametime Advanced**
    The Sametime System Console can function as the Deployment Manager for any, and all, clusters of these Sametime servers. This documentation assumes that you will use the Sametime System Console as the Deployment Manager for all clusters and provides instructions appropriate to that deployment. You can also deploy a dedicated Deployment Manager for a cluster, by installing that server using the “Deployment Manager” option and selecting the dedicated Deployment Manager when configuring the cluster.

  **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

- **Which kind of cluster are you creating: vertical or horizontal?**
  The Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Advanced support two types of clusters, called vertical clusters and horizontal clusters.
- A vertical cluster contains multiple instances of one type of Sametime server hosted on the same physical machine (or node). A vertical cluster distributes the load as appropriate across servers. Machine maintenance in a vertical cluster is easier and more convenient because everything is on one machine.

- A horizontal cluster contains multiple physical machines (or nodes), each with one type of Sametime server. A horizontal cluster distributes the load across servers on multiple machines as needed. The advantage of a horizontal cluster is that users can still use the Sametime application even if one machine in the cluster fails. A horizontal cluster includes a Deployment Manager, a Primary Node, and at least one Secondary Node. The Primary Node and each Secondary Node has only one Application Server configured to run on it as part of the cluster.

**How will you cluster Media Manager components?**

Clustering the Sametime Media Manager works differently from clustering other Sametime products. When you install the media manager, you have the option of installing its three components on separate computers, but you can only cluster two of them:

1. **SIP Proxy and Registrar:** You can deploy either a vertical or a horizontal cluster for this component. You must configure this cluster before you configure a cluster of Conference Managers.

2. **Conference Manager:** You can deploy either a vertical or a horizontal cluster for this component.

The Packet Switcher cannot be clustered; however you can install multiple Packet Switchers for a deployment and associate them with a Conference Manager or with a cluster of Conference Managers. The Conference Managers will balance the load among multiple Packet Switchers.

**Will you need a dedicated load balancer?**

When you create a cluster, you may need to deploy a dedicated WebSphere proxy server or a load balancer in front of the cluster to direct traffic for load balancing and failover purposes. If this is necessary for a particular Sametime product, the clustering instructions for that product explain what is needed and how to install it.
Related concepts

“Planning to deploy a vertical cluster on AIX, Linux, Solaris, and Windows”
In a vertical cluster, you install multiple Sametime servers of the same type on one machine as long as the machine’s hardware, RAM, and processing speed are superior.

“Planning to deploy a horizontal cluster on AIX, Linux, Solaris, and Windows” on page 231
You can create horizontal clusters for these types of servers: Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Advanced. In a horizontal cluster, you install each of the same type of Sametime server on its own machine. In this release, a horizontal cluster can include only a Deployment Manager, a Primary Node, and one Secondary Node.

Related tasks

“Adding a server to the Community Server cluster” on page 320
You can add IBM Sametime Community servers to an existing cluster.

“Clustering Sametime Proxy Servers” on page 357
Configuring a cluster of IBM Sametime Proxy Servers involves several tasks, including synchronizing system clocks, configuring the cluster settings, and optionally deploying an IBM Load Balancer in front of the cluster.

“Clustering Sametime Media Manager components” on page 383
The IBM Sametime Media Manager includes several components. You can install the components separately and optionally cluster some of them.

“Clustering Sametime Meeting Servers” on page 445
Configuring a cluster of IBM Sametime Meeting Servers involves several tasks, including synchronizing system clocks, configuring the cluster settings, and configuring an IBM WebSphere proxy server for the cluster, as well as optionally deploying an IBM Load Balancer in front of the cluster.

Planning to deploy a vertical cluster on AIX, Linux, Solaris, and Windows

In a vertical cluster, you install multiple Sametime servers of the same type on one machine as long as the machine’s hardware, RAM, and processing speed are superior.

Setting up a vertical cluster of servers of the same type involves these steps. These instructions apply to creating vertical clusters for these types of servers: Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Advanced. Only one Sametime Community server can be installed on a particular instance of Lotus Domino, so you cannot configure vertical clusters for community servers.

1. Decide what you will use as the cluster’s Deployment Manager and if necessary, install one using the “Deployment Manager” option.
   This documentation assumes that you will use the Sametime System Console as the Deployment Manager for all clusters and provides instructions appropriate to that deployment. You can also deploy a dedicated Deployment Manager for a cluster, by installing that server using the “Deployment Manager” option and selecting the dedicated Deployment Manager when configuring the cluster.

2. Install the first Sametime server of its type. When you create the deployment plan, select Primary Node and choose to federate the node at install time to the Sametime System Console cell.

3. Install another instance of the same application on the same computer. When you create the deployment plan, select Secondary Node and choose to federate the node at install time to the same cell as the primary node.
4. Then configure the cluster by identifying the Deployment Manager and selecting the Primary Node and adding a "cluster member" to the same server. The cluster member will be another instance of the same Sametime application.

Related tasks
“Preparing to install a Sametime Proxy Server” on page 346
Use the Sametime System Console to prepare to install an IBM Sametime Proxy Server by pre-populating values required for installation.
“Preparing to install a Sametime Media Manager on Linux or Windows” on page 372
Use the Sametime System Console to prepare to install a Sametime Media Manager by pre-populating values required for installation. The media manager runs on Linux or Microsoft Windows only.
“Preparing to install a Sametime Meeting Server” on page 436
Use the Sametime System Console to prepare to install a Sametime Meeting Server by pre-populating values required for installation.

Planning to deploy a horizontal cluster on AIX, Linux, Solaris, and Windows
You can create horizontal clusters for these types of servers: Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Advanced. In a horizontal cluster, you install each of the same type of Sametime server on its own machine. In this release, a horizontal cluster can include only a Deployment Manager, a Primary Node, and one Secondary Node.

Setting up a horizontal cluster of servers of the same type involves several steps. These instructions apply to creating horizontal clusters for these types of servers: Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Advanced.

1. Decide what you will use as the cluster’s Deployment Manager and if necessary, install one using the “Deployment Manager” option.
This documentation assumes that you will use the Sametime System Console as the Deployment Manager for all clusters and provides instructions appropriate to that deployment. You can also deploy a dedicated Deployment Manager for a cluster, by installing that server using the "Deployment Manager" option and selecting the dedicated Deployment Manager when configuring the cluster.

Attention: Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

2. Install the first Sametime server of its type. When you create the deployment plan, select Primary Node and choose to federate the node at install time to the Sametime System Console cell.

3. Install another instance of the same application on a different computer. When you create the deployment plan, select Secondary Node and choose to federate the node at install time to the same cell as the primary node.

4. Then configure the cluster by identifying the Deployment Manager and selecting which Primary Node and Secondary Node make up the cluster.
Related tasks
“Preparing to install a Sametime Proxy Server” on page 346
Use the Sametime System Console to prepare to install an IBM Sametime Proxy Server by pre-populating values required for installation.

“Preparing to install a Sametime Media Manager on Linux or Windows” on page 372
Use the Sametime System Console to prepare to install a Sametime Media Manager by pre-populating values required for installation. The media manager runs on Linux or Microsoft Windows only.

“Preparing to install a Sametime Meeting Server” on page 436
Use the Sametime System Console to prepare to install a Sametime Meeting Server by pre-populating values required for installation.

Planning for an LDAP directory
The IBM Sametime 8.5 multiple-server environment requires an LDAP directory for user authentication. The LDAP server should be set up and running before deploying Sametime.

System requirements
Sametime works with V3-compliant LDAP servers. See the "LDAP Servers" section of the System requirements tech note for a list of LDAP server products that are supported in this release:


Planning for specific operating systems
Follow the guidelines for your operating system before setting up an LDAP server:

- **AIX, Linux, Solaris, and Windows:**
  To avoid resource conflicts that may degrade performance, do not host the directory on the same computer as the Sametime Community Server.

- **IBM i:**
  The directory and the Sametime Community Server can reside on the same system. If using LDAP to access the contents of the Domino directory, the LDAP service and the community server must run on separate Domino servers.

  **Note:** System capacity planning for anticipated workloads must be performed.

Multiple directory support
Support for multiple directories with the following restrictions:

- Groups may only contain members present on the same directory server and base DN specified in the LDAPServer document. Sametime does not support mixed groups at this time.

- Multiple replicas of the same directory in the stconfig.nsf database are not supported. For effective load balancing, you should route LDAP traffic through a load balancer.

- If the browse feature is enabled on the server, certain features such as LDAP timeouts or the maximum number of search results returned may need to be disabled.
If you use multiple LDAP repositories, you must ensure that the base entries do not overlap, as that causes problems when Secure Socket Layer (SSL) is enabled. For example, the following base entries have a field in common, so they overlap:

- `o=lotus`
- `o=sales,o=lotus`

These base entries use different fields and are acceptable:

- `o=ibm,c=us`
- `o=lotus`

**An LDAP Server connection is a prerequisite for some servers**

After installing the Sametime System Console, you will be instructed to connect it to the LDAP server. These other servers require that an LDAP directory be set up and running to be able to complete the installation:

- The Sametime Meeting Server
- The IBM Sametime Community Server, when installed with a deployment plan through the Sametime System Console
  - An IBM Sametime Community Server integrated with the Sametime System Console must connect to a user directory in LDAP format.
- Sametime Advanced

**Contact lists**

Sametime might experience difficulties when users include large public groups in their contact lists. To avoid problems, limit the size of public groups used with Sametime to 1000 users.

**Sametime servers and the LDAP mail attribute**

Sametime 8.5 and later requires authenticated users to have a `mail` attribute assigned in the LDAP directory. The mail attribute must be a unique string, which preferably follows the syntax and length restrictions of email addresses.

The softphone provided by Sametime uses the email field for user identification. To support audio video communications, the LDAP directory must have the email field populated for every user.

This attribute is not used for email purposes, and does not have to be assigned as a user name for logging into Sametime. Instead, the “mail” attribute serves as a common attribute between the various Sametime subsystems, such as Calendar Integration, Business Cards, LDAP, and REST APIs. This attribute is also used when generating a URL for a user's persistent meeting room (for example, `http://meetings.company.com/stmeetings/room/user@company.com/users-room`). In addition, using the “mail” attribute provides certain performance advantages since translation between attributes is not required; it also provides consistency and integrity by using a common and well-understood attribute.

**Note:** Not all users need to be authenticated to use the server; the `mail` attribute is not required for anonymous (guest) users.

Therefore, IBM recommends that the user repository (LDAP server) create a mail attribute for users who plan to authenticate with the Sametime servers. The `mail` attribute must be a unique string, which preferably follows the syntax and length restrictions of email addresses.
Upgrade considerations

If you used a Lotus Domino Directory in its native format with a release prior to Sametime 8.5, you have two options for setting up your user directory:

- Convert the existing Lotus Domino Directory to LDAP format. The LDAP service and the community server must run on separate Domino servers.
- Set up a dedicated LDAP directory for use with Sametime.

**Policy assignments use the UUID (Universally Unique ID) LDAP attribute by default.**

With this release, Sametime uses the UUID LDAP attribute by default. After upgrading servers, you must upgrade policies to use the UUID attribute before they can be used.

The LDAP attribute used for UUID is different for every LDAP Server type. For example, Domino LDAP uses a String attribute named dominounid and Active Directory uses a Binary attribute named objectguid. If the UUID attribute does not exist or is invalid, then the DN can also be used by selecting to use the DN by creating or editing the LDAP Deployment Plan Advanced Person Settings.

New and existing custom Java classes for searching the Community Server’s LDAP directory must include the appropriate UUID attribute for the LDAP directory if UUID is used with policy assignments or Sametime user login IDs:

- Lotus Domino LDAP: dominounid
- IBM Tivoli Directory Server: ibm-entryuuid
- Microsoft Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

**Best Practices**

Best Practices for using LDAP with Sametime article on the Sametime wiki contains an overview of LDAP components and describes how the Sametime Community Server works with LDAP to provide authentication, name lookups, and name resolution. The article describes best practices for creating search filters, setting `sametime.ini` parameters, and enhancing Sametime and LDAP performance.
Planning a Community Server installation

You should review the following considerations before installing an IBM Sametime Community Server.

Directory type

An LDAP directory is required if your Community Server will be integrated with the Sametime System Console. The LDAP server must be connected to the Sametime System Console and the Community Server itself must also be configured to use an LDAP server (instead of a native Lotus Domino Directory). You can configure additional user directories, including Lotus Domino Directories, later.

Directory limitations

Sametime might experience difficulties when users include large public groups in their contact lists. To avoid problems, limit the size of public groups used with Sametime to 1000 users.

Network performance

For optimal performance, the Community Server should be placed at a centrally located network backbone, to reduce the number of network hops between clients and the server. Ideally, there should be no more than one WAN hop for every possible client-to-server connection. Clients that make multiple WAN hop to connect to the server will experience slower performance than clients connecting through a LAN or making one WAN hop to the server. For organizations that have large networks, it may be necessary to install multiple community servers to reduce the number of WAN hops for clients.

Clustering Community Servers

If you have a large number of Sametime users, you can install multiple community servers and cluster them for load balancing and to reduce network usage.

Installing multiple community servers

Even if you have decided not to cluster your community servers, there are special considerations when installing more than one Community Server; for example, you must synchronize all of the community servers to operate as a single community.
National language considerations

You do not need to select a language when installing a Community Server. The language displayed for Sametime interfaces is primarily determined by the individual user's language settings. However, it is recommended that you install the Lotus Domino language pack that corresponds to the language used by the majority of your Sametime users. If no language pack exists for your language on your preferred platform, see the IBM Technotes, available at www.ibm.com/software/support, for information on how to localize the Lotus Domino server.

Related concepts

“Clustering Sametime servers for high enterprise availability” on page 227
In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

Planning for the dedicated Lotus Domino server

Unlike other IBM Sametime servers that run on WebSphere Application Server, the Sametime community server runs on a Lotus Domino server. You must install the Lotus Domino server before you install the Sametime community server. The Lotus Domino Server that runs the community server should be completely dedicated to supporting the real-time, interactive communication services of Sametime. Lotus Domino must use a 32-bit version even if you are installing on a 64-bit Microsoft Windows system. Lotus Domino must use a 32-bit version when installing on AIX, x86 Linux, or Solaris even if you are installing on a 64-bit version operating system.

The Sametime community server uses the directory, security, and replication features of the Lotus Domino server. Do not use the community server for other high-demand Lotus Domino services such as mail storage and routing, application and database storage, or centralized directory and administration services.

IBM AIX, Linux, Sun Solaris and IBM i can run multiple partitioned Lotus Domino servers on the same system. For these server platforms, you can create a new Lotus Domino server on the same system as your existing production server. This configuration is not supported in Microsoft Windows. Adding Sametime to an existing production server is not supported.

To add a server to an existing Lotus Domino domain for use as a Sametime community server, register the server to create a Server document before installing Lotus Domino. For more information, see "Installing a Lotus Domino server" for your operating system.

To find out which Lotus Domino releases are supported for Sametime, see the system requirements for this release:


Directory considerations

If your community server will be integrated with the Sametime System Console, then you must initially configure the console with an LDAP server. The community server must also use the LDAP server. If your user information is stored in a Lotus
Domino Directory, you can configure Sametime to access the Domino Directory using LDAP. However, the LDAP service and the community server must run on separate Domino servers.

While an LDAP directory is highly recommended, you can configure the Sametime community server to directly access the Lotus Domino Directory if you do not plan to use the Sametime System Console. Keep in mind that changing the community server to use an LDAP server at a later time is more complicated than initially configuring it to use LDAP.

- If you install the Lotus Domino server in a new domain, no users are in the Lotus Domino Directory at the time the server is created, other than the server administrator. Therefore, if you select the Lotus Domino Directory as the user repository for your Sametime community server, you will need to add all of your Sametime users to the Lotus Domino Directory. When you install the Domino server into an existing domain, you will not need to add these users to the directory. However, before a user can use Sametime, the user's directory entry must be updated with the name of a home Sametime server and an Internet password.

- To add a new Sametime user to the Lotus Domino Directory, create a Person document for the user in the directory that includes (at minimum) a Last Name, a User Name and an Internet password. The Person document must also include a home Sametime server. You can use any of the following tools to create a Person document: an IBM Lotus Notes client, a Lotus Domino Administrator client, or the Sametime server self-registration feature.

### Deploying a stand-alone Community Server Mux

Optionally install an IBM Sametime Community Server Mux (multiplexer) on a separate computer to remove the connection-handling load from the Sametime Community Server. Configuring a stand-alone multiplexer enables the Community Server to handle a larger number of users and improves its stability.

### About this task

Every Sametime Community Server contains a multiplexer (“mux”) component that maintains connections from Sametime clients. The Community Server Mux is installed automatically and comes configured for immediate use. You can optionally deploy a stand-alone Community Mux by installing it on a separate computer, so that clients connect to the stand-alone multiplexer instead of to the Community Server. This configuration frees the Community Server from the burden of managing the live client connections; the stand-alone multiplexer is dedicated to this task.

You can deploy a stand-alone Community Mux to operate with one or more unclustered Community Servers, or to operate with a cluster. You can also deploy multiple stand-alone multiplexers and use a load-balancer to distribute client connections among them.

### Deploying stand-alone multiplexers in front of a Community Server cluster

If you intend to deploy one or more stand-alone Community Server multiplexers in front of a cluster of Community Servers, there are some issues to consider.

The stand-alone multiplexer maintains a single IP connection to each Community Server in the cluster. The data for all Community Server clients is transmitted over this single IP connection to the Community Server on the Sametime server. The
The illustration below shows stand-alone Community Services multiplexers deployed in front of clustered Community Servers to reduce the client connection load on the clustered servers.

In the illustration, note the following:
- The Community Server multiplexers are installed on separate computers and handle the connections from the clients.
- If you want to distribute connections among the multiplexers, you can set up a load-balancing mechanism such as IBM Load Balancer.
- Each Community Server multiplexer maintains a single IP connection to Sametime server 1, and a single IP connection to Sametime server 2. The Community Server data is passed from the multiplexer computers to the Sametime Community Servers over these IP connections. Each Sametime Community Server maintains only two IP connections to handle all data.
- The scenario shown above can significantly increase the load-handling capabilities of the Sametime Community Servers. The table below illustrates the advantages of deploying stand-alone multiplexers.

<table>
<thead>
<tr>
<th>Multiplexer deployment</th>
<th>Number of Community Services connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Sametime servers with the multiplexer installed on the same machines as the servers (default installation)</td>
<td>If the servers have multi-core processors, each Sametime Community Server can handle approximately 20,000 connections, for a total of 40,000 connections. Using the servers to host Sametime classic meetings rather than using Sametime meeting servers reduces the number of connections each server can support.</td>
</tr>
</tbody>
</table>
### Multiplexer deployment
Two Sametime servers with the multiplexers installed on different computers (as seen in the illustration above)

<table>
<thead>
<tr>
<th>Number of Community Services connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Each Sametime Community Server can service approximately 100,000 active connections.</td>
</tr>
<tr>
<td>- Each Community Server multiplexer machine can handle as many as 20,000 to 30,000 live IP port connections, for a possible total of 60,000 connections.</td>
</tr>
<tr>
<td>- The machines in the illustration above might be able to handle 160,000 active connections. You can increase the load handling capability further by adding additional Community Server multiplexers in front of the two Sametime Community Servers. For example, adding two more Community Server multiplexers to the cluster shown above might accommodate as many as 120,000 active connections (4 x 30,000 connections per Community Server multiplexer).</td>
</tr>
</tbody>
</table>

**Note:** The server capacity numbers used above are approximations meant to provide a rough estimate of the possible load-handling improvement if you deploy Community Server multiplexers on separate computers. The actual server capacity is affected by variables such as:
- The average number of users in the contact lists of all Sametime clients
- The number of instant messages that users send

Server capacity is also reduced if you use Sametime Classic meetings, which are legacy meetings hosted on a Sametime server, rather than using a Sametime Meeting server.

### Deploying a stand-alone Community Mux for a single Sametime Community Server
This section discusses the performance advantages and procedures associated with deploying a stand-alone multiplexer in front of a Sametime server machine (or machines) that does not operate as part of a Community Server cluster.

Each Sametime server contains a Community Server multiplexer (or MUX) component. The function of the Community Server multiplexer is to handle and maintain connections from Sametime clients to the Community Server.

During a normal Sametime server installation, the Community Server multiplexer is installed with all other Sametime components on the Sametime server machine. The Sametime server CD provides an option to install only the Community Server multiplexer component. This option enables the administrator to install the Community Server multiplexer on a different machine than the Sametime server.

When the Sametime Community Server multiplexer is installed on a different machine than the Sametime server:
- The Sametime Connect clients connect to the Community Server multiplexer machine, not the Sametime server. This configuration frees the Sametime server from the burden of managing the live client connections; the multiplexer machine is dedicated to this task.
The Community Server multiplexer maintains a single IP connection to the Sametime server. The data for all Community Server clients is transmitted over this single IP connection to the Community Server.

In this scenario, the Community Server connection-handling load is removed from the Sametime server. The Sametime server does not need to employ system resources to maintain thousands of client connections. Removing the connection-handling load from the Sametime server ensures these system resources can be dedicated to other Community Server processing tasks.

The Community Server multiplexer machine dedicates its system resources to handling client connections but does not perform other Community Server processing. Distributing the Community Server workload between multiple servers in this way enables the Community Server to handle a larger number of connections (users) and to function more efficiently.

**Performance improvements with a stand-alone multiplexer**

If the Community Server multiplexer operates on the same machine as the Sametime server, the Sametime server can handle approximately 8,000 to 10,000 Community Server connections and also perform other Community Server processing tasks adequately.

However, if the Sametime server is not required to expend system resources to maintain client connections, the server can service approximately 100,000 connections. (The Sametime server is capable of processing the Community Server data that is passed over 100,000 connections if it does not have to maintain the connections themselves.)

When a Sametime Community Server multiplexer is installed on a separate machine, the Community Server multiplexer can support approximately 20,000 live IP port connections. You can also deploy multiple Community Server multiplexers in front of a Sametime server.

To summarize the performance benefits of a stand-alone multiplexer deployment, consider the following example:

- You can install three separate Community Server multiplexers in front of a single Sametime server. If each Community Server multiplexer handles 20,000 connections, as many as 60,000 users can be connected to a single Sametime server at one time.
- If the Sametime server is capable of servicing 100,000 connections, the server performance will not degrade under the load produced by 60,000 connections.
- If the multiplexer operates on the Sametime server instead of being deployed separately, the Sametime server can service a maximum of 10,000 users. By deploying three stand-alone multiplexers in front of a single Sametime server, you can service 50,000 more users (assuming one connection per user) than if the multiplexer operates on the same machine as the Sametime server.
- If you deploy stand-alone multiplexers in the manner described above, you can also implement a rotating DNS system, or IBM WebSphere Edge Server, in front of the multiplexers to load balance connections to the stand-alone multiplexers.
Planning a Sametime Media Manager installation on Linux or Windows

The Sametime Media Manager is available for installing on the Linux or Microsoft Windows platforms only. You should review the following considerations before installing components of an IBM Sametime Media Manager. Audio and video are managed with the Sametime Media Manager server. Audio and video services provided by the Sametime Media Manager have been tested and optimized for sessions with 20 participants. The actual number of participants per session will vary up or down based on network and environmental conditions.

Important: In this release, a Sametime deployment can support only one stand-alone Media Manager server, or one cluster of Media Manager servers. This restriction is due to a limitation with the current version of the Sametime System Console.

A Media Manager deployment consists of a Conference Manager, a SIP Proxy and Registrar, and a Packet Switcher. A standalone Media Manager deployment can have multiple Packet Switchers to support a higher number of simultaneous audio and video conferences. Each Packet Switcher runs on a separate WebSphere node and is not clustered; the Conference Manager handles the workload distribution among them.

The Sametime System Console can only administer one Media Manager instance. The individual components of the Media Manager instance may be individually clustered to provide failover and high availability, deployed as stand-alone servers, or installed on the same server – but only one Media Manager deployment can be administered from a given Sametime System Console.

The Packet Switcher is not administered from the console, so it is not affected by this limitation; however the Conference Manager and the SIP Proxy and Registrar components are administered from the console, so your planning must take this limitation into consideration.

Example 1: Two standalone Conference Manager servers cannot be administered from the same Sametime System Console.

Example 2: A Conference Manager cluster and a SIP Proxy and Registrar cluster can both be administered from the same console. This is the recommended topology for enterprise customers.

Example 3: A Conference Manager cluster and a standalone SIP Proxy and Registrar server can be administered from the same console.

Related concepts
“Sametime Media Manager” on page 156
The IBM Sametime Media Manager runs on WebSphere Application Server to provide audio visual services for chats and meetings. It requires a Sametime Community Server.

Audio and video considerations
If your IBM Sametime deployment will include one or more Sametime Media Manager servers, you should review this information about A/V (audio/video) features.

Bandwidth considerations
Sametime Media Manager allows configuration of several parameters that effect the bandwidth and performance of audio and video conferences. These parameters default to values which should work for most environments, but they can be tuned to meet the specific needs of the organization deploying Sametime Media Manager.

In the Sametime System Console, the codecs used for audio and video transfer can be tuned to the values required. The selected audio and video codec will effect the bandwidth used and the processing power required to encode and decode the information streams. Consult the specification of those codecs to determine which one best suits any specific needs of the deployment.

Within the specification of the video codec, it is also possible to adjust the video resolution and bit-rate which will be used for video streams. Generally, the lower the resolution and the bit-rate, the lower the bandwidth used and the lower the processing power required to send and receive the video streams. However, the lower resolutions and bandwidth, the lower the quality of the video. Likewise, the higher the bit-rate and resolution, the higher the required bandwidth and processing power, and the higher the quality of the video.

For example, if you are using low bandwidth networks and older machines with less processing power, it might be necessary to select a lower video bit rate. If the quality of the video image is important, and enough processing power and network bandwidth is available, a higher video bit-rate can be used.

Sametime video codecs provide many resolution choices, from SQCIF to Wide Full HD (1080p). The higher the resolution, the more CPU, display memory, and graphics card power are required. HD requires Intel Core 2 Quad or better CPU and at least 256 megabytes of display memory.

Another configuration parameter which can be adjusted is the number of switched audio streams. This is the total number of audio streams that will be sent from the server to the client when participating in a audio conference call. The higher the number of audio streams to each client, then the higher the number of people on the call who can speak at the same time and be heard by all participants. The number of streams sent to each client also affects bandwidth and server load.

The total number of participants in audio and video conferences can also be capped, limiting the amount of bandwidth that any single call can use as a sum of the other parameters and the number of people participating in the conference.

**Video Conferencing**

As the number of participants in a video conference increases, so does the demand on the network. To ensure that a given network can support this new collaborative feature, administrators have the ability to restrict the maximum number of participants. Administrators should work directly with their network team to identify the maximum number of participants that works best for their organization and their respective network policies. The default maximum number of participants in a single audio-only or video conferences is set to 20; however, this can be adjusted up or down to accommodate specific network consumption requirements. As a best practice, the moderator has the option to mute all participants. To ensure the best experience possible, the mute all feature should be exercised to keep background noise to a minimum. Once a user has been muted by the moderator, the user has the option to un-mute themselves at any time.
Another consideration for networks is latency, which can cause undesirable results. Latency of less than 150 ms end-to-end is normally acceptable in interactive real-time audio video conferencing.

**Video considerations**

- **Video driver**
  It is strongly recommended that you use the up-to-date driver that comes with the video camera, as some cameras do not work well with the generic video driver.

- **Video memory**
  256 MB of video memory required for VGA and above; Minimal 128 MB of video memory for QVGA resolution and below.

**IPv6 addressing**

IPv6 addressing is not supported for the Sametime Media Manager or its components.

**Sametime Reflector**

Starting with release 8.5.2, the Sametime Reflector has been replaced with the Sametime TURN Server. The TURN Server enables Sametime clients to send audio and video communications across a NAT (Network Address Translator) or firewall when direct peer-to-peer communications are not possible.

**Audio/video bandwidth consumption considerations**

The table below outlines maximum bandwidth consumption for Sametime clients using the default audio and video codecs:

<table>
<thead>
<tr>
<th>Client type</th>
<th>Connect client</th>
<th>Web meeting client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Video (H.264)</td>
<td>384 kbps</td>
<td>384 kbps</td>
</tr>
<tr>
<td>Max Audio (iSAC)</td>
<td>32 kbps</td>
<td>32 kbps</td>
</tr>
</tbody>
</table>

**Client considerations**

- All 8.5.x clients (8.5.0, 8.5.1, and 8.5.2) can interoperate with each other and use any 8.5.0, 8.5.1, or 8.5.2 servers.
- IBM Sametime Connect clients or Sametime embedded clients require a Sametime Media Manager server running Release 8.5.1 or later to be able to make or receive computer audio (voice chat) or video calls.
- Microsoft Windows XP Tablet PC is not supported.
- Sametime Media Manager includes additional security and audio-visual quality features that work with clients running Release 8.5.1 or later only. To support 7.5.x, 8.0.x, or 8.5 clients running on an 8.5.1 or later server, disable these features until all clients are running 8.5.1 or later:
  - SRTP
  - TLS
  - RTCP for N-way
- If you leave these features enabled, 8.5 and earlier clients cannot use audio-visual features provided by the Media Manager.
LDAP

The softphone provided by Sametime uses the email field for user identification. To support audio video communications, the LDAP directory must have the email field populated for every user.

Best Practices

For information on using the best practices for ensuring a good audio/visual experience, see Audio/Visual Best Practices in the Sametime wiki.

Related tasks

“Changing the default number of maximum users” on page 1151
As demands on video conferencing change, you can update the maximum number of participants to ensure that your network can support this feature.

Planning a Sametime Meeting Server installation

Follow these guidelines when planning the deployment of IBM Sametime Meeting servers.

Security

For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server deployments.

LiveNames

If you will be supporting the use of LiveNames in your Sametime deployment, you should deploy all Sametime Meeting Servers, Sametime Proxy Servers, and Sametime Advanced Servers within the same subnet. It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Sametime Classic Meetings

Sametime Classic meetings are legacy meeting features that run on Sametime 8.0.x and 7.5.1 servers on the Domino platform. When you download the Sametime 85x installation package, the Classic Meeting server is part of the community server installation zip/tar file. This product documentation focuses on information about the Sametime Meeting Server running on WebSphere Application Server, but you will find some references to classic meetings for features that can be configured for either type of meeting server.

For other information about administering Sametime Classic Meetings, refer to the information center that was included with your release of Sametime.

Planning for migration from an earlier release

Planning an upgrade from an earlier release of IBM Sametime takes into account which release of Sametime you are upgrading from and whether you want to upgrade all servers and clients to this release in phases or at one time.

Planning server upgrades

The tasks involved in planning an upgrade from an earlier release of IBM Sametime will vary, depending on your current release of Sametime, whether you have enabled online meetings, and how you want to support those meetings in the future.

Upgrading from Release 8.5 or 8.5.1

IBM DB2 9.7 is included with the Sametime download kit. Upgrade DB2 and existing databases first, before proceeding with other server updates.

Existing Sametime 8.5 and 8.5.1 servers can be upgraded to this release of Sametime. Install the servers using the Update option.

Upgrading from Sametime 8.0.x and 7.5.1

Starting with Sametime 8.5, meeting services and community services moved to separate servers. Legacy Sametime servers and Sametime Gateway servers can be upgraded to this release of Sametime. In addition, you may choose to install additional components to take advantage of new features and capabilities.

Upgrading Sametime with no online meetings

You can upgrade a legacy Sametime server running release 7.5.1 or later directly to this release of Sametime Community Server, preserving legacy data and supporting instant messaging just as in earlier releases.

Note: If your Sametime server is running a release prior to 7.5.1, you will need to complete an interim upgrade to release 7.5.1 or later before upgrading to this release of Sametime.

Upgrading Sametime with online meetings enabled

If your legacy Sametime server has the online meetings feature enabled, you have two options:

- Continue creating and hosting online meetings on the upgraded server
If the online meetings feature was enabled in your previous release of Sametime, it remains enabled when you upgrade and features work just as in the earlier release.

**Note:** The Sametime Enterprise Meeting Server is not supported by this release of Sametime. If your meeting rooms are clustered with Sametime Enterprise Meeting Server, you will have to remove the servers from the cluster.

- Install additional components to support this release of Sametime Meeting Server
  All your legacy meeting data is still preserved, but rather than continue creating and hosting meetings on the upgraded server, you can set up URL redirects to route users to this release of the Sametime Meeting Server for creating and attending meetings. Expanding the deployment to include a stand-alone Meeting Server requires that you install these additional components:
    - LDAP user directory
      Because the new components in this release of Sametime run on IBM WebSphere Application Server, you must use an LDAP directory to ensure all components can authenticate users. If your previous deployment used the native Lotus Domino Directory for user management, you can convert it to LDAP format for use with the expanded deployment.
    - IBM DB2 database
      The database stores information used by the Sametime System Console and the Sametime Meeting Server.
    - Sametime System Console
      The Sametime System Console provides a central point for administering all servers in the deployment. If you cluster any of the WebSphere-based servers, you can use the system console as the Deployment Manager; the console can serve as Deployment Manager for multiple clusters.
    - Sametime Proxy Server
      The Sametime Proxy Server enables browser-based clients to participate in Sametime instant messaging and online meetings. In addition, the Sametime Proxy Server works with Sametime Community Server or Lotus Connections to enable the business card feature in Sametime, and with Sametime Unified Telephony or other TCSPI-enabled products to enable the Sametime click-to-call feature. The Sametime Proxy Server also provides live names awareness, and can replace the Links Toolkit used in earlier releases of Sametime.
    - Sametime Meeting Server
      The Sametime Meeting Server provides an online meeting feature in a stand-alone server, rather than combining them with community services as in the past. Because it runs on WebSphere Application Server, the meeting server can be clustered using a WebSphere network deployment.

If you choose to expand your deployment this way, you may additionally choose to install these remaining components:
- Sametime Media Manager
  The Sametime Media Manager provides audio and video features for instant messaging and online meetings.
- Sametime Gateway
  Sametime Gateway provides instant messaging with external communities, including Sametime communities deployed outside of your firewall, AOL Instant Messenger, and Google Talk.
Upgrading Sametime Gateway

You can upgrade Sametime Gateway 8.0.2 directly to this release; if you have an earlier release you will need to complete an interim upgrade before you can upgrade to this release. Upgrading Sametime Gateway includes upgrading the WebSphere Application Server on which it runs from version 6 to version 7.

Although a new deployment of Sametime Gateway uses DB2 9.5 Limited Use, an upgraded gateway will continue to use DB2 9.1 Enterprise Server Edition; the database schema will be updated automatically by scripts that run during gateway product installation.

Before upgrading Sametime Gateway servers in a cluster, you will have to remove each node from the cluster. Once the server upgrades are complete, you can add the nodes back into the cluster.

Note: In this release, a Sametime Gateway cluster can only have one Secondary Node.

Planning for a mixed-release server environment

If you are planning a phased approach to upgrading servers, you will have a mix of servers running different versions of Sametime in the same production environment. Keep the following considerations in mind as you plan for this type of migration.

Deferring migration of Sametime meetings

The Sametime Meeting server running on WebSphere Application Server replaces the meeting features included in Sametime Standard 8.0.x and 7.5.1. To defer your migration of meetings to the new platform, you can upgrade Sametime 8.0.x and 7.5.1 servers, while maintaining your existing “Classic” meetings until you are ready to migrate them to the new platforms.

Maintaining Sametime 8.0.2 community servers

You can extend configuration support from the Sametime System Console to environments that are still using 8.0.2 Community servers, while taking advantage of new features offered in this release. For instructions, see the following article on the Sametime wiki: Configuring Sametime 8.5.1 Media and Proxy Servers with an 8.0.2 Community Server using Sametime System Console.

Establishing connections with older Sametime community servers on AIX, Linux, Solaris, or Windows

To ensure that new and upgraded community servers can still connect to older community servers, update the VP_SECURITY LEVEL parameter in the sametime.ini file on the older servers as explained in Connecting with older Community Servers on AIX, Linux, Solaris, or Windows.

Planning client upgrades

Sametime Connect and Sametime embedded clients running release 7.5.1 or later can be upgraded directly to this release.
If you are planning a phased approach to upgrading clients, you will have a mix of clients running different releases of Sametime in the same organization. Keep the following considerations in mind as you plan for this type of migration.

- **Clients must be running release 7.5.1 or later to upgrade to this release.**
  If your users are running clients older than release 7.5.1, their workstations must be upgraded to release 7.5.1 or later before you can upgrade them to this release.

- **Allow upgraded servers to accept login requests from older client versions until client upgrades are complete.**
  Configure upgraded servers to allow logins from clients running a variety of releases.

- **Audio/video (A/V) interoperability between releases**
  - All 8.5.x clients (8.5.0, 8.5.1, and 8.5.2) can interoperate with each other and use any 8.5.0, 8.5.1, or 8.5.2 servers.
  - IBM Sametime Connect clients or Sametime embedded clients require a Sametime Media Manager server running Release 8.5.1 or later to be able to make or receive computer audio (voice chat) or video calls.
  - Microsoft Windows XP Tablet PC is not supported.
  - Sametime Media Manager includes additional security and audio-visual quality features that work with clients running Release 8.5.1 or later only. To support 7.5.x, 8.0.x, or 8.5 clients running on an 8.5.1 or later server, disable these features until all clients are running 8.5.1 or later:
    - SRTP
    - TLS
    - RTCP for N-way
  - If you leave these features enabled, 8.5 and earlier clients cannot use audio-visual features provided by the Media Manager.

**Related concepts**

“Audio and video considerations” on page 241
If your IBM Sametime deployment will include one or more Sametime Media Manager servers, you should review this information about A/V (audio/video) features.

**Related tasks**

“Upgrading Sametime clients” on page 770
Use the information in this section to help users upgrade their Sametime Connect or Notes Embedded 8.0.2 clients to this release.

“Considerations for upgrading the Sametime Connect client” on page 770
There are several things you need to know before users upgrade the IBM Sametime Connect client.

“Specifying the minimum allowed client version” on page 772
Each IBM Sametime Community Server is configured to allow logins from a minimum client version.

---

**Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers**

A mixed-license environment includes a combination of IBM Sametime Entry servers, along with Sametime Standard servers and possibly Sametime Advanced. When you deploy IBM Sametime Entry servers with other types of servers, plan for additional steps to meet the licensing requirements for Sametime Entry, which offers only instant messaging features and does not offer meetings. Sametime Entry
users are licensed for instant messaging features only and not Web conferencing.
Fully-licensed users for Sametime Standard or Sametime Advanced have access to
instant messaging and Web conferencing.

You have a mixed-license environment if you have Sametime Entry, as well as any
combination of these offerings in the same production environment.

- Sametime Standard
- Sametime Standard/Advanced
- Sametime Advanced

When you configure a mixed-license environment to comply with licensing
limitations involving Sametime Entry servers, some people cannot create or attend
meetings. It is important to let everyone in your organization know about the
mixed environment so users who have access to meetings through Sametime
Standard or Sametime Advanced servers can decide how to work with users
whose Sametime Entry home servers prevent them from using meetings.

**Configuring the mixed-license environment on IBM i**

On IBM i, you have some choices about how to configure Sametime Entry home
servers.

- When you install the Sametime Entry offering (only *BASE option of 5724J23),
  any servers you configure are Sametime Entry servers and meetings are disabled
  automatically.
- When you install the Sametime Standard offering (both *BASE and Option 1 of
  5724J23), the servers are Sametime Standard Community servers by default, but
  you can elect to make some of them Entry servers by running a command that
disables meetings. For any server that will be assigned to Sametime Entry users,
you must disable meetings on that server to create the mixed-license
environment.

  When you upgrade, meetings are re-enabled on all Sametime servers and you
  must disable meetings again on any servers that are assigned to Sametime Entry
  users.

**Information for Sametime Standard or Sametime Advanced users**

Here are some of the issues Sametime Standard or Sametime Advanced users
should be aware of when working with Sametime Entry users:

- The client contact list does not indicate what type of home server another user
  has.
- It is not possible to have instant meetings with Sametime Entry users. If
  someone sends an invitation to join a meeting, the invited user should click the
  Respond button on the meeting invitation to let the meeting initiator know that
  it is not possible to join the meeting. Otherwise, the meeting initiator does not
  know why the Sametime Entry user cannot join the meeting.

**Information for Sametime Entry users**

It is not possible to use meeting features even though the user interface in the
client may suggest otherwise. Here are some of the issues Sametime Entry users
should be aware of:

- Sametime Entry users receive meeting invitations, but cannot actually join
  meetings.
In attempting to join meetings, users see a message indicating the Sametime Meeting Room is being prepared but they are never allowed to join the meeting and must manually close the window.

Tell users to click the Respond button on a meeting invitation to let the meeting initiator know that it is not possible to join the meeting. Otherwise, the meeting initiator does not know why Sametime Entry users cannot join the meeting.

- Sametime Entry users who open the Sametime Meeting Center on a Sametime Standard server and click **Attend a Meeting** or **Schedule a Meeting** receive a message that tells them they are not authorized to perform that action.
- Sametime Entry users receive an error message when they try to start an instant meeting through an action such as right-clicking a name in the Contact list and selecting a "Collaborate" option.

**Related tasks**

“Configuring a mixed-license environment with clients that connect to Sametime Entry servers” on page 343

To comply with licensing limitations involving Sametime Entry servers, take steps to configure the mixed environment for two types of clients – those who are licensed to use instant messaging and meetings and those who are licensed only for instant messaging.

**Related reference**

“Sametime offering features by client type” on page 164

The features available to users depend on the type of client they use and the Sametime offering installed on their home servers.
Chapter 11. Installing

Install and configure prerequisites, install IBM Sametime servers and complete basic server configuration, then deploy the clients you want.

Installing on AIX, Linux, Solaris, and Windows

Install and configure prerequisites, then install IBM Sametime servers and complete basic server configuration on AIX, Linux, Solaris, and Windows.

This section contains information about system requirements, Sametime prerequisites, server installation and required configuration tasks to do after installation.

You should install Sametime servers by installing a Sametime system console first and then using the console to create a deployment plan for the server you want to install server. If you cannot install a Sametime server in the recommended way, read about an alternate way to install in this Sametime wiki article:

Installing Sametime 8.5.x servers without using deployment plans

Restriction: There are known issues with using Cygwin/X to run Eclipse-based applications on remote AIX machines, which may affect installation. For details of existing Bugzilla reports on these issues, see the information at https://bugs.eclipse.org/bugs/show_bug.cgi?id=36806. If a different X server (such as Hummingbird Exceed) is used, these problems do not occur.

Related concepts
Chapter 12, “Migrating and upgrading,” on page 605
Migrate data from a previous version of Sametime and upgrade one or more servers to take advantage of the latest features.

Related tasks
“Troubleshooting installation or uninstallation” on page 1219
Use the following topics to troubleshoot problems that occur after installing and uninstalling IBM Sametime servers.

Installing DB2 on Linux or Windows

Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store information about servers, users, bandwidth configuration, and meetings. Sametime Advanced uses DB2 to store information about persistent chats and broadcast communities.

Before you begin

These instructions explain how to install the version of DB2 integrated with the Sametime installation package. Use this version of DB2 if you are unfamiliar with DB2 and would prefer a less complex deployment on Windows and Linux operating systems. The DB2 installation provided with Sametime supports Linux 64-bit systems and Windows 32-bit or 64-bit systems.
If you are familiar with DB2 deployments or are installing on other operating systems, download and install one of the unmodified DB2 limited use installation packages that are available at the following web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

IBM i includes DB2.

**Linux**  The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**Linux**: If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

If you are running in an enterprise deployment, install DB2 on a separate computer. In a small deployment, you can install DB2 on the same computer on which you plan to install Sametime system console.

**Procedure**

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

3. Download the Sametime DB2 installation package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

      **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**Linux**

Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **Linux** ./launchpad.sh
- **Windows** launchpad.exe

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

*platform* is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM DB2, then click Install IBM DB2 again.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

a. In the Installation Manager window, choose File > Preferences.

b. Uncheck Search service repositories during installation and updates and click OK.

9. Click Install.

10. Click the I accept the terms in the license agreements option and click Next.

11. Accept the default locations and click Next.

12. Accept the default location for the package group and click Next.

13. Select Create a new package group and accept the default location. Click Next.

14. Confirm that all available features are selected, then click Next.

15. Create a DB2 application user ID that does not exist on the system. Then, supply a password that meets the operating system password policy requirements and any additional requirements imposed by your company. Confirm the password.

The user specified, dasadm1, and the group db2admin does not exist on the system.
For information about passwords, see the Password Rules topic in the DB2 information center.

**Important:** This user cannot previously exist on the system. This user will be created as a local operating system user during the DB2 installation process; if your organization does not allow creation of local operating system users for security reasons, exit this installer and install DB2 using a different package. This installer does not check to see if the user exists.

Make a note of the DB2 application user name and password. This user has database administration authority and you must supply the name and password when you install the Sametime system console and when you connect to DB2 databases later.

Click **Next**.

16. Review the summary, then click **Install** to start the installation.
    The installation can take up to 20 minutes. You receive confirmation when it is complete.

17. Click **Finish**.

18. Click **Exit** to close the Installation Manager.

19. (Linux only) The DB2 server does not start by default when you restart the computer. To start a database instance automatically when the server restarts, use the `db2iauto` command.
    For more information, see `db2iauto - Autostart instance command`.

**Results**

If the installation fails, click **View Log File** for more information.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media. Ignore any warning about a missing `versionInfo.properties` file. It does not apply to DB2 installations and upgrades.

Installation Manager logs are stored in the following locations.

**Linux**  /var.ibm/InstallationManager/logs

**Windows 2008**  %ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Windows 2003**  %ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

More detailed DB2 installation logs are stored in the following locations.

**Linux**  The logs are stored in the /tmp folder and are named `db2setup.log`, `db2setup.his`, and `db2setup.err`.

**Windows**  %My Documents%\DB2LOG\%

The log file name includes the date and time of the installation attempt; for example:

C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log
What to do next

If you are installing DB2 for Sametime Advanced, you must also install DB2 Net Search Extender to allow database content to be searchable and persistent. See the instructions for your operating system in the DB2 9.7 information center:

- Installing Net Search Extender on IBM DB2 9.7 for UNIX
- Installing Net Search Extender on IBM DB2 9.7 for Windows

Related information

IBM DB2 Database for Linux, UNIX, and Windows Information Center

Installing DB2 in silent mode

If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

Before you begin

Information about downloading packages for Sametime is located at the following web address:

Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128


Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

About this task

Follow these steps to install the IBM Installation Manager in silent mode. Customize each product’s response file, then install the product in silent mode using the customized response file.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.
2. Navigate to the directory where you copied and extracted the installation files: \TMP\server_offering
3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp
in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.

4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows.

For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.

5. The SSCPassword value should be encoded. To generate an encoded password, use the `generateEncodedPassword` utility packaged with the installer.

The utility is on the installation media in the same directory as `launchpad.exe` or `launchpad.sh`.


7. Open a command window.

8. Enter the following command to install the IBM Installation Manager in silent mode.

   - **AIX, Linux, or Solaris**
     
     ```
     /opt/ibm/InstallationManager/eclipse
     ```

   - **Windows**
     
     ```
     C:\Program Files\IBM\Installation Manager\eclipse
     ```

9. Navigate to the Installation Manager installation directory. The default directories are shown below.

   - **AIX, Linux, or Solaris**
     
     ```
     /opt/ibm/InstallationManager/eclipse
     ```

   - **Windows**
     
     ```
     C:\Program Files\IBM\Installation Manager\eclipse
     ```

10. For all installations except DB2, start the Sametime System Console.

11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.

    - **AIX, Linux, or Solaris**
      
      ```
      ./IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
      ```

    - **Windows**
      
      ```
      IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
      ```

**Tip: Generating a response file automatically**

The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation.

```
./install --launcher.ini your .ini file -record response_file path -skipInstall agentDataLocation
```

The response file is stored in the `agentDataLocation` directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same `agentDataLocation` in the next recording session to record updating or modifying the product. The products that you installed, the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using `-skipInstall` are not stored.
Installing the Sametime System Console

The IBM Sametime System Console is your focal point for administering and configuring all Sametime servers.

About this task

Install and configure prerequisite applications, then install the IBM Sametime System Console, which you use for preparing for server installations and for managing your Sametime deployment.

Creating a database for the system console on AIX, Linux, Solaris, or Windows

Before installing the IBM Sametime System Console on AIX, Linux, Solaris, or Windows, create a database to store its data.

Before you begin

Make sure that you have installed DB2. To install the Sametime System Console server, the DB2 application user ID must have administrator rights to be able to create and update tables in the database. If the user does not have administrator rights, you must perform an additional step after creating the database to create tables needed for installation.

About this task

Run the scripts that come with the Sametime System Console package. They are also included with Sametime in the DB2 installation package.

Procedure

1. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation.
   - If you are logging in for the first time, create a DB2 profile if you are prompted to do so, then close the Welcome to First Steps window.
2. Open a command prompt and navigate to the folder where you extracted the SametimeSystemConsole installation package.
3. Create the database by entering one of the following commands from the SametimeDB2 folder. Wait until you see confirmation that the database has been created and the command has finished.
   - AIX, Linux, or Solaris: `./createSCDb.sh STSC dbadmin`
   - Windows: `createSCDb.bat STSC dbadmin`
   - Replace STSC in the command if you want to choose a different database name. Names can be from 1 - 8 characters, but cannot contain special or multibyte characters.
   - Replace dbadmin with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.
   - When naming DB2 objects, follow the rules for your operating system.
4. Close the command window.
5. Open the DB2 control center.
   - AIX, Linux, or Solaris
     - Open the IBM DB2 folder on the desktop and click Control Center.
   - Windows
Click Start > Programs > IBM DB2 > General Administration Tools >
Control Center.

6. Find the database name to verify that the new database was created.

What to do next

If corporate policy prevents the DB2 application user ID from having administrator
rights to the DB2 server, perform these additional steps after creating the database
and before installing the Sametime System Console.

Connect to the system console database (for example, STSC). Then enter the
createSchedTable.dd1 command to create additional tables in the database.

AIX, Linux, or Solaris

db2 connect to STSC

db2 -tf createSchedTable.dd1

Windows

db2cmd

db2 connect to STSC

db2 -tf createSchedTable.dd1

Related tasks

“Installing DB2 on Linux or Windows” on page 251
Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing
with this release of IBM Sametime. The Sametime system console, the Sametime
Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store
information about servers, users, bandwidth configuration, and meetings.
Sametime Advanced uses DB2 to store information about persistent chats and
broadcast communities.

Installing the console on AIX, Linux, Solaris, or Windows
Run the installation program to set up the system console on AIX, Linux, Solaris,
or Windows.

Before you begin

Ensure that your IBM DB2 server is installed and running with the db2start
command, and that the Sametime System Console database has been created. If
you are upgrading, make sure that you have completed the database update before
proceeding.

IPv4 and IPv6 addressing: When installing the Sametime System Console on a
system that supports both IPv4 and IPv6 addressing, the IPv4 and IPv6 addresses
associated with the system console must be mapped to the same host name.
Additional host names cause problems in the system console because SSL
certificates can be generated using either the IPv4 or IPv6 host name, which might
not match during authentication.

Linux  The launchpad installation program launches a web browser to start. You
need to be on the console or have an X server and a web browser installed
and configured. (VNC or a remote X term session works as well). The
graphical library pages must also be installed for Linux so that the
Installation Manager works correctly. The /home directory must be
writable so that the home directories for the users created by the install are
created on the system.

**AIX, Linux, and Solaris:**

If you are installing using the GUI mode, the full X11 desktop environment
is required.

**Attention:** Check the hosts file and remove any lines that start with the
following:

- 127.0.0.1 fullyQualifiedDomainName shortName
- ::1 fullyQualifiedDomainName shortName

These lines must be removed before installing any Sametime server running on
WebSphere Application Server. An issue with WebSphere Application Server causes
the server installation to fail if these lines are in the file. Save the file if you make
changes.

**Procedure**

Follow these steps to install the system console.

1. **Red Hat Enterprise Linux only:** Disable Security Enhanced Linux on any Red
   Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the
      software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or
      permissive.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows
   operating systems or as root on Linux operating systems.

   **Solaris only:** The installation must be performed by the root user using su
   or a normal login session. Independent sudo packages are not supported on
   Solaris.

3. Prepare to use the installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport
         Advantage account. For information on using Passport Advantage, see
         the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         &uid=swg24029128
         Locate the components that you need in the document’s listing, then
         download the packages labelled with the corresponding part numbers
         to the system on which you are installing.

   **Tip:** When extracting downloads on Windows operating systems, use a
   short path location such as C:\ and not a long path location such as
   the user’s desktop or TEMP directories. When extracting to long path
   locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
`mount -v cdrfs -o ro /dev/cd0 /cdrom`

Linux
Mount the CD or DVD using a command similar to the following command:
`mount /dev/cdrom /cdrom`

Solaris
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**.: `/launchpad.sh`
   - **Windows**: `launchpad.exe`

   **Note**: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (`install` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

   `sametime_server_package/IM/platform`

   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM Sametime System Console and click Launch IBM Sametime System Console 8.5.2 installation.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.

9. Click Install.

10. Select the packages that you want to install and click Next.

11. Click the I accept the terms in the license agreements option and click Next.

12. Accept the location for shared installation files and click Next.

13. Select Create a new package group. Accept the installation directory and click Next.
14. Verify that **IBM Sametime System Console server 8.5.2** is selected as the feature to install and click **Next**.

15. In the Common Configurations window, verify the cell, node, and host name.

   The Sametime System Console is a deployment manager and administers a cell and any nodes federated into the cell for other Sametime servers. In an enterprise deployment, the servers are in one geographic region and in a small deployment, the servers are all installed on one computer.

   **Windows**

   Avoid using a node name that is longer than 10 characters if possible. Installation creates a profile name based on the selection you make here. The maximum number of characters for a profile is 80 characters. If installation fails, reinstall the product using a shorter directory path and a shorter node name.

   - **Cell**: The name of the WebSphere Application Server cell that is created for the system console, such as `systemNameSSCCell`.
   - **Node**: The name of the WebSphere Application Server node that runs the Sametime applications in the system console. It is federated into the cell during the installation process.
   - **Host Name**: Use the fully qualified DNS name of the server that you are installing the system console on. Make sure this DNS name is resolvable from other servers you will be installing products on. Do not use an IP address, a short host name, or localhost.

16. Create the WebSphere Application Server user ID. Avoid a name that contains spaces. Supply a password and confirm it. Click **Next**.

   If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

   This user must be one that is not on the operating system or in an LDAP directory. The user is created in a WebSphere Application Server local file system repository and is used to administer the Sametime System Console server.

   Make a note of the ID and password because you use them later for additional product installations and configuration. You also use them to administer the Sametime System Console server.

17. In the Configure DB2 for the System Console window, provide information for connecting to the system console database.

   - **Host Name**: Use the fully qualified domain name of the server where you installed DB2. Do not use an IP address or a short host name.
   - **Port** field shows the default port of 50000. Accept the default unless you specified a different port during DB2 installation or your server is using a different port.
     
     On Linux, the default is typically 50000, but varies based on port availability. Check the `/etc/services` file on the DB2 server to verify the port number that is being used.
   - **Database Name for the System Console/Policy**: Enter the name of the database that you want to connect to. If you used the suggested name when you created the system console database, the name is STSC.
     
     Use only upper- and lower-case English characters, numbers, and the following punctuation characters:


```plaintext
! ( ) _ \ ^ ` ~
```
- **Application user ID**: Enter the name of the database administrator that you created when installing DB2. The default is db2admin.
- **Application password**: Specify the password that you created when you installed DB2, such as db2password.

18. Click **Validate**.

19. When the button label changes to **Validated**, click **Next**.

   If the database connection is not successful, use the dbverify.log file to debug the problem. The log can be found in the temporary directory for your operating system.

   **AIX, Linux, or Solaris**
   
   /tmp
   
   **Windows**
   
   %TEMP%

20. Review the summary, then click **Install** to start the installation.

21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

After a successful installation, three components must be started before using the console: the deployment manager, the node agent, and the Sametime System Console server.

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var.ibm/InstallationManager/logs

**Console connection log**: /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Console connection log**: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

**Console connection log**: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**What to do next**

“Logging in to the console” on page 483
Related tasks
“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

Logging in to the Sametime System Console after creating the Sametime Advanced database
Use the IBM Sametime system console to use guided activities to perform configuration tasks and administer any Sametime servers that are managed by the console.

Procedure
With the Sametime system console started, follow these steps to log in.
1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server. For AIX, Linux, Solaris, or Windows, specify port 8700 for HTTP and 8701 for HTTP over SSL.
   During the installation process, WebSphere Application Server security is enabled. SSL is enabled as part of the security process and you are directed to another port that listens for HTTPS connections.
   http://serverhostname.domain:port/ibm/console
   For example:
   http://sametime.example.com:8700/ibm/console
   https://sametime.example.com:8701/ibm/console
   Note: On IBM i, the port number cannot be 8700. Use the port that was listed in the system console installation results summary. To check the port, open the AboutThisProfile.txt file for the system console deployment manager profile and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:
   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt
2. The WebSphere Application Server Integrated Solutions Console opens. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.
   The default name is wasadmin.
3. On the left side of the navigation tree, click the Sametime System Console task to open it.

Installing the Sametime System Console in silent mode
If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.
Before you begin

Information about downloading packages for Sametime is located at the following web address:

&uid=swg24029128

&uid=swg24027364

Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

About this task

Follow these steps to install the IBM Installation Manager in silent mode.
Customize each product's response file, then install the product in silent mode using the customized response file.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.
2. Navigate to the directory where you copied and extracted the installation files: \TMP\server_offering
3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.
4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows.
For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.
5. The SSCPassword value should be encoded. To generate an encoded password, use the generateEncodedPassword utility packaged with the installer.
The utility is on the installation media in the same directory as launchpad.exe or launchpad.sh.
7. Open a command window.
8. Enter the following command to install the IBM Installation Manager in silent mode.
   • AIX, Linux, or Solaris$ SametimeOffering/IM/windows/install
     --launcher.ini silent-install.ini
9. Navigate to the Installation Manager installation directory. The default directories are shown below.
- **AIX, Linux, or Solaris**
  /opt/ibm/InstallationManager/eclipse
- **Windows**
  C:\Program Files\IBM\Installation Manager\eclipse

10. For all installations except DB2, start the Sametime System Console.
11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.
   **AIX, Linux, or Solaris**
   ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
   **Windows**
   IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense

   **Tip: Generating a response file automatically**
   The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation.
   .install --launcher.ini your .ini file -record response file path -skipInstall agentDataLocation
   The response file is stored in the agentDataLocation directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same agentDataLocation in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using -skipInstall are not stored.

### Connecting to an LDAP server

Use the IBM Sametime system console to connect IBM Sametime servers to an LDAP server that has already been installed and configured. An LDAP server is required for these server offerings: community server, meeting server, media manager, and gateway.

#### Before you begin

Start the LDAP server and the Sametime system console.

#### Procedure

If you have not already opened the Connect to LDAP Servers activity, follow these steps:
1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified host name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
   For example: http://sametime.example.com:8700/ibm/console
   If you are prompted with a security exception, accept the certificate, and continue.
   **IBM i**: The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open
the AboutThisProfile.txt file for the Sametime System Console Deployment Manager Profile and use the setting specified for the “Administrative console secure port.” For the default profile name (STSCDMgrProfile), the file is located here:

/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDMgrProfile/logs/AboutThisProfile.txt

2. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Expand **Sametime Prerequisites**, and click **Connect to LDAP Servers**.

**Related concepts**

“Planning for an LDAP directory” on page 232

The IBM Sametime 8.5 multiple-server environment requires an LDAP directory for user authentication. The LDAP server should be set up and running before deploying Sametime.

**Related tasks**

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Sametime prerequisite: Connecting to an LDAP server**

This activity takes you through the steps for identifying users and groups in an LDAP directory that need access to IBM Sametime.

**Before you begin**

An LDAP server must be installed and configured.

**About this task**

Connect IBM Sametime servers to the LDAP server. After your Sametime server connects to the LDAP server, it can search the LDAP directory and authenticate Sametime users. If you have already connected Sametime to an LDAP server, but now you want to edit or delete a connection, use this activity.

**Procedure**

1. Connect to LDAP server.

   In **Connect to LDAP servers**, click **Add**.

   If you want to edit or delete an LDAP connection instead, then click the appropriate button.

   If you edit an LDAP connection for a Cell-based WebSphere Application Server product that is already installed, you must manually update the product’s LDAP configuration. The System Console Cell’s LDAP is updated and the changes are also pushed to a connected LDAP server. You can delete an LDAP connection if it is not being used by an installed product.

2. Bind to LDAP.

   a. Click **Authenticated access** to ensure that the Sametime server uses credentials to authenticate with the LDAP server.

      Provide the **Bind distinguished name (DN)** and **Password** when you are prompted to enter this information.
Select **Anonymous access** only if you are certain that all attributes are accessible when the Sametime server binds to the LDAP server.

b. Enter a **Deployment Name** for this LDAP connection to identify the connection for future reference. It does not need to map to any existing server name or value.

c. Enter the fully qualified domain name of the LDAP server that you want to connect to in the **Host name** field. Do not use an IP address or a short host name.

d. Enter the **Port** of the LDAP server. The default value is 389. If your LDAP server is running on a different port, enter the correct port value here.

e. To use an SSL connection with the LDAP server, click **Is secure LDAP connection**.

   **Attention:** Selecting this option requires additional configuration for Sametime Community Servers. When you set up the deployment plan for either of these servers, you must elect to configure the LDAP server manually. After installation, set up trust with the LDAP server’s SSL certificates and then manually configure the LDAP directory to finish setting up the secure LDAP connection. See “Enabling encryption between Sametime and the LDAP server” for more information.

f. If you selected **Is secure LDAP connection**, click **Import SSL Certificate**.

   This action imports the LDAP server’s SSL certificate into the Default Cell Trust Store. You only need to do this once.

g. If you selected **Authenticated access**, enter the **Bind distinguished name (DN)** and **Password** fields. These are the user credentials you will use to authenticate with your LDAP server. If you have selected **Anonymous Access**, these fields are not shown. For example:

   `cn=John Smith,ou=managers,o=example,st=Massachusetts,c=US`

h. **Click Next.**

   When designating an authenticated user, create a unique directory entry that is used only for the purpose of authenticating connections from the Sametime server to the LDAP server. After creating the directory entry, you must ensure that this directory entry has at least read access to the attributes of the LDAP directory entries.

3. **Base Distinguished Name and Filter for Searches.**

   Enter the base distinguished name and filter for searches information.

   a. Select your base distinguished name and filter for searches from the list or enter a value. You specify the basic LDAP parameters required to conduct searches for people and groups in the LDAP directory. Some of these parameters are also necessary for displaying the names of users in the Sametime user interface.

   Failure to specify a base distinguished name prevents authenticated users from creating and attending meetings on the meeting server.

   **Restriction:** The list displays a base DN that is detected by the guided activity; however, the list does not display for a Lotus Domino LDAP directory. Additionally, Lotus Domino LDAP is the only LDAP directory that uses a blank base DN. WebSphere Application Server requires a base DN for federating repositories and does not let you use an empty base DN. It sets the base DN to `C=US`. The LDAP repositories are listed by base DN after they are federated.

   b. **Optional:** To specify the search filter and basic LDAP settings for person and group entries, click **Configure advanced LDAP settings**.
c. Click Next.

4. Collect Person Settings. To search for a user name, users enter a text string in the Sametime user interface. This setting defines the LDAP search filter responsible for selecting a user name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory person entries.

a. Enter the attributes of an LDAP person entry.

Table 36. Person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>Specifies a set of attributes used to describe an object that identifies the entry as a person. Sametime determines whether a directory entry returned by a search is a person or a group. Groups are represented by entries with a unique object class. The name of the object class specified in this setting is compared to the object class values.</td>
</tr>
<tr>
<td>LDAP user search base</td>
<td>Specifies which ID to search for when the administrator selects User ID as the search criteria for managing policies. UUID is the default. Select Distinguished Name to use the distinguished name of users and groups instead if the default UUID attribute does not exist in the LDAP server. New and existing custom Java classes for searching the Community Server’s LDAP directory must include the appropriate UUID attribute for the LDAP directory if UUID is used with policy assignments or Sametime user login IDs: • Lotus Domino LDAP: dominounid • IBM Tivoli Directory Server: ibm-entryuuid • Microsoft Active Directory: objectguid • Novell eDirectory: guid • Sun ONE: nsuniqueid</td>
</tr>
<tr>
<td>Display name</td>
<td>Displays a user's name in Sametime user interfaces. The attribute must not be the same as the one you use for Similar name distinguisher or Email address due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Differentiates between two users that have the same common name (cn) attribute. The attribute must not be the same as the one you use for Display name or Email address due to WebSphere Application Server configuration rules.</td>
</tr>
</tbody>
</table>
Table 36. Person attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>Contains the user's email address in the field. The attribute must not be the same as the one you use for Display name or Similar name distinguisher due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td>Home Sametime server</td>
<td>Enter the name of the LDAP Attribute that contains a user's Home Sametime server. The Home Sametime server is a community server Domino name or a community server cluster name that indicates which community server or cluster a user should use. If your environment includes multiple community servers or you have deployed other applications enabled with Sametime technology, every user must be assigned to a home community server or cluster.</td>
</tr>
<tr>
<td>Membership attribute</td>
<td>Enter the attribute that specifies which groups a user belongs to if your LDAP server supports this feature.</td>
</tr>
</tbody>
</table>

b. Enter the search and authentication attributes of an LDAP person entry.

Table 37. Search and filter

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication attributes</td>
<td>Allows the user to authenticate with more than one attribute of the user's entry. For example, if this field is set to mail;cn the user can authenticate with either of these names. The guided activity allows the use of any of these three properties: mail, cn, and uid. When forming the search filters, the mail, cn, and uid properties are replaced with the attributes specified above. For example if the &quot;Similar name distinguisher&quot; or uid is set to sAMAccountName, the attribute sAMAccountName is used in the filter. Similarly, if 'Display Name' maps to &quot;cn&quot;, the attribute &quot;cn&quot; is used in the filter and if &quot;Email address&quot; maps to &quot;mail,&quot; the attribute &quot;mail&quot; is used in the filter. <strong>Important:</strong> For the meeting server to work, the first field of the Authentication attribute must be set to mail and must be listed first. Add other fields, separated by a semicolon (;). For example, the Authentication attribute can be set to mail;cn;uid.</td>
</tr>
<tr>
<td>Search attributes</td>
<td>Specifies the fields used for searching the directory for users. The fields must be separated by a semicolon (;). For example, the Search attribute can be set to mail;cn;uid.</td>
</tr>
</tbody>
</table>

c. Click Next.
5. Collect Group Settings. To search for a group name, users enter a text string in the Sametime user interface. This setting defines the LDAP search filter responsible for selecting a group name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory group entries.

a. Enter the attributes of an LDAP group entry.

Table 38. Group attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>Specifies the attribute of a directory entry that identifies the entry as a group. Sametime determines whether a directory entry returned by a search is a person or a group. Groups are represented by entries with a unique object class. The name of the object class specified in this setting is compared to the object class values.</td>
</tr>
<tr>
<td>LDAP group search base</td>
<td></td>
</tr>
<tr>
<td>Display name</td>
<td>Displays a group’s name in Sametime user interfaces.</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Differentiates between two groups that have the same common name (cn) attribute.</td>
</tr>
<tr>
<td>Group membership attribute</td>
<td>Specifies the name of the attribute in the group entry that contains that names of individual people or subgroups that belong to the group. If users add a group to a presence list, privacy list, or a list that restricts meeting attendance, Sametime must obtain the list of members within the group.</td>
</tr>
</tbody>
</table>

b. Click Next.

6. Task Completion Summary.

   Review the configuration details in the Task Completion Summary table, and click Finish to connect to the LDAP server.

7. If you selected the Import SSL Certificate, restart the system console deployment manager.

8. Restart the system console deployment manager to complete the LDAP federation process.

9. (Optional) To push the LDAP changes to all nodes, go to System Administration > Nodes. Select all nodes and click Synchronize.
Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Assign users and groups to policies” on page 1051
You can assign users and groups to specific user polices to grant or limit access to features in IBM Sametime.

“Enabling encryption between Sametime and the LDAP server” on page 805
Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

Related reference

“LDAP directory settings”
Find more details about LDAP settings for the guided activity, “Sametime prerequisite: Connecting to an LDAP server.”

“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

LDAP directory settings

Find more details about LDAP settings for the guided activity, “Sametime prerequisite: Connecting to an LDAP server.”

The tables below correspond to the tasks in the guided activity:

- “Bind to LDAP”
- “Base Distinguished Name and Filter for Searches” on page 273
- “Collect Person Settings” on page 274
- “Collect Group Settings” on page 276

Bind to LDAP

Bind to LDAP settings determine whether the system console binds to the LDAP server as an anonymous or authenticated user. Also specify the host name of the LDAP server, the port that the server is using, and whether to use SSL when connecting to the LDAP server.

Table 39. Bind to LDAP settings for the LDAP directory

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated access</td>
<td>Requires the Sametime servers to use credentials to authenticate with the LDAP server.</td>
<td></td>
</tr>
</tbody>
</table>
Table 39. Bind to LDAP settings for the LDAP directory (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
</table>
| **Anonymous access**| Select this type of access only if you are certain all attributes are accessible when the Sametime server binds to the LDAP server. Anonymous bind operations must be able to search on a unique ID attribute specific to the LDAP server in use. Use these attributes:  
  - Lotus Domino LDAP: dominounid  
  - IBM Directory Server: ibm-entryuuid  
  - Microsoft Active Directory: objectguid  
  - Novell eDirectory: guid  
  - Sun ONE: nsuniqueid | To accept anonymous access, the LDAP server must allow anonymous binding and anonymous access to the same attributes of the LDAP person and group entries that are required for the bind distinguished name (DN) and password as described later in this table. |
| Deployment Name for this LDAP connection | Specified a name that you provide to this LDAP connection for easy reference. It does not need to map to any existing server name or value. It is an easy way to identify this object when you reference it in the future. | Sample deployment name: ST_LDAP |
| Host name           | Enter the fully qualified domain name of the LDAP server or Network Dispatcher serving the LDAP servers that you want to connect to. Do not use an IP address or a short host name. | Sample host name ldap1.example.com |
| Port of the LDAP server | The port number is the one on which the LDAP server listens for TCP/IP connections. The default port for LDAP access is TCP/IP port 389. | Default 389 |
Table 39. Bind to LDAP settings for the LDAP directory (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind distinguished name (DN) and Password</td>
<td>If you have selected Authenticated Access, specify the distinguished name of an LDAP directory entry that the Sametime servers use when binding to the LDAP directory, and then enter the password associated with that user. The server transmits this user name and password to the LDAP server when making its initial connection to the LDAP server. The LDAP server verifies this user name and password against an entry in the LDAP directory to authenticate the connection. When designating an authenticated user, create a unique directory entry that is used only for the purpose of authenticating connections from the Sametime servers to the LDAP server. After creating the directory entry, you must ensure that this directory entry has at least read access to the attributes of the LDAP directory entries. If you have selected Anonymous Access, these fields are not shown.</td>
<td>If you use a person entry for the authenticated user, the Sametime server must have access to the following attributes: • person name • person description • home Sametime server • email address • location • telephone number • title • photo (if used for business card) • object class • Any LDAP directory entry attribute that is specified in any search filter in the Collect Person Settings section of the guided activity. If you use a Group entry for the authenticated user, the Sametime server must have access to the following attributes: • group name • group description (if this setting is not empty) • group members • ObjectClass • Any LDAP directory entry attribute that is specified in any search filter in the Collect Group Settings section of the guided activity.</td>
</tr>
</tbody>
</table>

Base Distinguished Name and Filter for Searches

The Base Distinguished Name and Filter for searches settings ensure that Sametime users' names are found in the appropriate LDAP directory when they authenticate through the browser client.
### Table 40. Base Distinguished Name and Filter for Searches settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detected LDAP Base DNs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For stconfig.nsf, edit the ldapservr document as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Search Base and Scope</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Base Objects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Base object when searching for person entries:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DC=austin,DC=ibm,DC=com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Base object when searching for group entries:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DC=austin,DC=ibm,DC=com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The base distinguished name is detected according to the LDAP type. The one exception is the Lotus Domino LDAP server, for which the base distinguished name is empty by default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sample Base distinguished name:dc=example,dc=com</td>
<td></td>
</tr>
<tr>
<td><strong>LDAP user search base</strong></td>
<td>Specify the base object of the directory or level of the directory from which to start a search for person or group entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Configure advanced LDAP settings</strong></td>
<td>Select this option to see additional settings that allow you to provide detailed authentication and search attributes for person and group entries in the LDAP directory.</td>
<td></td>
</tr>
</tbody>
</table>

### Collect Person Settings

To search for a user name, users enter a text string in the Sametime user interface. This setting defines the LDAP search filter responsible for selecting a user name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory person entries.

### Table 41. Collect Person Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search filter attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Comments and sample values</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Authentication Attributes | Allows the user to authenticate with more than one attribute of the user's entry. Use any of these properties: mail, cn, or uid. The properties must be separated by a semicolon (;). **Important:** For the Meeting Server to work, the first field of the Authentication attribute must be set to `mail` and it must be listed first. | Sample authentication attributes:  
  - `mail;cn`  
  - `mail;cn;uid`  
  Consider an LDAP person entry containing the following attributes:  
    - mail: jlock@example.com  
    - cn: James Lock  
    If the authentication attribute is `mail`, the user authenticates with jlock@example.com. If the authentication attribute is `cn`, the user authenticates with James Lock.  
    When forming the search filters, the mail, cn, and uid properties are replaced with the attributes specified above. For example if the "Similar name distinguisher" or uid is set to sAMAccountName, the attribute sAMAccountName is used in the filter. Similarly, if "Display Name" maps to "cn", the attribute "cn" is used in the filter and if "Email address" maps to "mail," the attribute "mail" is used in the filter. |
| Search Attributes        | Specifies the fields used for searching the directory for users. The fields must be separated by a semicolon (;). | Sample search attributes:  
  - `mail;cn;uid`  
    | |
| Object Class             | Individual users are represented by entries with a unique object class. Enter the object class attribute used for people in the LDAP schema of the LDAP directory in your environment. The name of the object class specified in this setting to the object class values of each entry to decide whether the entry is a person or a group. | The value is set automatically to a default value based on the type of LDAP directory detected. |

**Table 41. Collect Person Settings (continued)**
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy ID for users and groups</td>
<td>Specifies which ID to search for when the administrator selects User ID as the search criteria for managing policies. UUID is the default. Select Distinguished Name to use the distinguished name of users and groups instead if the UUID attribute does not exist or is invalid.</td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td>Displays a user’s name in Sametime user interfaces.</td>
<td>Sample display name: cn</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Specify the attribute of a person entry that is used to differentiate between two users that have the same common name (cn) attribute.</td>
<td>For example, a search for the name John Smith returns two person entries with the common name (cn) John Smith. Because the two John Smiths have different email addresses, the mail attribute can be displayed to enable the user to determine which John Smith is the correct one.</td>
</tr>
<tr>
<td>Email address</td>
<td>Contains the user’s email address in the field.</td>
<td></td>
</tr>
<tr>
<td>Home Sametime Server</td>
<td>Specifies the name of the field within the LDAP person entries that contains the name of each user’s home Sametime server.</td>
<td>Format for Sametime server distinguished name: CN=servername/ ou=organizational_unit/ o=organization HomeServer1/Sales/Company</td>
</tr>
</tbody>
</table>

### Collect Group Settings

To search for a group name, Sametime users enter a text string in the Sametime user interface. This setting defines the LDAP search filter responsible for selecting
a group name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory group entries.

**Table 42. Collect Group Settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
</table>
| **Object Class**      | Groups are represented by entries with a unique object class. Enter the object class attribute used for groups in the LDAP schema of the LDAP directory in your environment. The name of the object class specified in this setting is compared to the object class values of each entry. | Microsoft Active Directory group  
Netscape Directory groupOfUniqueNames  
Microsoft Exchange 5.5 and Lotus Domino directories groupOfNames  
SecureWay™ Directory groupOfUniqueNames |
| **Group Attributes**  |                                                                             |                                                                  |
| **Display Name**      | Displays a group’s name in Sametime user interfaces.                        | Sample display name: cn                                        |
| **Similar name**      | Specifies the attribute of a group entry that can differentiate between two groups that have the same common name (cn) attribute. In many LDAP directories, the "description" attribute contains descriptive information about a group. If a search on the name "Marketing" returns two group entries, the information contained in the description attribute (such as "West region" or "East region") can be used to distinguish between the two groups. | Microsoft Exchange 5.5 Directory info  
All other directories description |
| **Group membership attribute** | Specifies the name of the attribute in the group entry that contains that names of individual people or subgroups. If users add a group to a presence list, privacy list, or a list that restricts meeting attendance, Sametime must obtain the list of members within the group. | member uniquemember |

Related tasks
“Sametime prerequisite: Connecting to an LDAP server” on page 266
This activity takes you through the steps for identifying users and groups in an LDAP directory that need access to IBM Sametime.

**Installing a Sametime Community Server and supporting software**

To install an IBM Sametime community server on a Lotus Domino server, you must have already connected the system console to an LDAP server. After installing a community server, install and set up optional components, such as a multiplexer or components that integrate with Microsoft Office.
Related concepts
Chapter 12, “Migrating and upgrading,” on page 605
Migrate data from a previous version of Sametime and upgrade one or more
servers to take advantage of the latest features.
“Configuring a Sametime Community Server” on page 892
This section describes how to configure an IBM Sametime Community Server.

Related tasks
“Connecting to an LDAP server” on page 265
Use the IBM Sametime system console to connect IBM Sametime servers to an
LDAP server that has already been installed and configured. An LDAP server is
required for these server offerings: community server, meeting server, media
manager, and gateway.

Installing a Lotus Domino server
Install a Lotus Domino server and prepare the environment before installing a
Sametime community server.

Before you begin
If you have never installed and set up a Lotus Domino server, see the Lotus
Domino documentation to get an understanding about how to install and set up a
Lotus Domino server.

Installing a Lotus Domino server on Windows:
If you are installing a new IBM Lotus Domino server for your IBM Sametime
server, use these general directions to remind you of the necessary steps to install
Lotus Domino; this procedure assumes that you have a working knowledge of
Lotus Domino administration. Lotus Domino must use a 32-bit version even if you
are installing on a 64-bit Microsoft Windows system.

Before you begin
If you are adding a server to an existing Lotus Domino domain, you need to
register the server before you can install Lotus Domino. The registration process
creates a Server document in the Lotus Domino directory.

Specify the following settings during registration:
1. Store the server ID file that is created during registration somewhere on the
   system where you will configure the Lotus Sametime server. Record the path
   name; you need to specify it when you configure the Lotus Sametime server.
2. Use the same network name as the first Lotus Domino server in the Lotus
   Domino domain.

Procedure
To install Lotus Domino on Windows operating systems, follow these steps.
1. Run the installation program (setup.exe), which is on the Lotus Domino
   server installation CD.
2. Read the Welcome window, and click Next. Then read the License Agreement
   and click Yes.
3. Enter the administrator’s name and the company name. Do not elect to install
   Lotus Domino on partitioned servers.
4. Select the program and data directory in which to copy the software. Make
note of the locations that you provide for the Lotus Domino program and data
directories. You need this information when you install Sametime. Click **Next**.

5. Select **Domino Enterprise Server** as the server type.

6. Click **Next** to accept all components.

7. Specify the program folder or accept **Lotus Applications** as the program
folder that contains the software.

8. Click **Finish**.

9. For Lotus Domino 8.5 and 8.5.1 only: Create a file to modify XML transforms
needed by Sametime.
   For more information about this step, read the technote:
   a. Navigate to the `Domino_program_directory\jvm\lib` directory.
   b. Create a file called `jaxp.properties`.
   c. Add the following line to the file:
      ```
      javax.xml.transform.TransformerFactory=
      org.apache.xalan.processor.TransformerFactoryImpl
      ```
   d. Save and close the file.

10. Click **Start > Programs > Lotus Applications > Lotus Domino Server** to start
the Server Setup program.
   Answer the questions to finish setting up the Lotus Domino server.

**Preparing to install Lotus Domino on AIX, Linux, or Solaris:**

Set up the environment on a computer running IBM AIX, Linux, or Sun Solaris
before installing IBM Lotus Domino.

**Procedure**

1. You must log in as the root user to install the Lotus Domino and Sametime
server.

2. You must have a designated operating system user who can start the Sametime
server, and this user must be a part of a designated operating system group.
   The default user is notes and the default group is also notes, but any user
   name other than root and any group name can be used. To verify that the
designated operating system user is part of the operating system group, type
the following command, where `dominoUserName` is the name of the Lotus Notes
user groups `dominoUserName`
   For example, if you type `groups notes` and get the return value of `notes`,
   the return value indicates that the user name notes is a part of the group notes.

3. Verify that the file system has at least 1 GB of disk space, then enter the
following command:
   ```
   type "df -k"
   ```
   If you are installing from a downloaded image rather than a CD, you must also
consider the disk space required for the *.tar installation files and the unpacked
installation files, which require approximately 2 GB of disk space.

4. On AIX only: The input/output completion ports (IOCP) must be installed and
configured.
   If not, the Lotus Domino setup cannot begin, and you get the following error
message:
Your system is not configured with I/O Completion Ports. I/O Completion Ports must be installed in order to run the Domino 7 Server. Install and make available I/O Completion Ports and restart your system. Refer to Lotus Knowledgebase Technote 1086556 for detailed instructions on how to install/configure IOCP.

5. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.

6. On partitioned servers only: Additional preparation is necessary if you plan to install Sametime on a partitioned Lotus Domino server:
   a. Ensure that each partitioned server has a unique IP address.
      You can map multiple IP addresses to one network card using the `ifconfig` command:
      `ifconfig device alias new_IP_address netmask subnet`
      For example: `ifconfig en0 alias 192.0.2.10 netmask 255.255.255.128`
   b. Ensure that each partitioned server has a DNS name that maps to its unique IP address.
      If a DNS name can be resolved to multiple IP addresses, enter all IP addresses into the Host name field when you edit the Domino server document, as described in Configuring partitioned Domino servers on AIX, Linux, or Solaris to.
   c. Run each partitioned server using a unique user account.
      Create a UNIX Lotus Notes user for each partitioned server that you plan to install. You can use a single Lotus Notes group for all partitions.

**Installing a Lotus Domino server on AIX, Linux, or Solaris:**

If you are installing a new IBM Lotus Domino server, use these general directions to remind you of the steps for installing Lotus Domino. This procedure assumes that you have a working knowledge of Lotus Domino administration. Lotus Domino must use a 32-bit version when installing on AIX, x86 Linux, or Solaris even if you are installing on a 64-bit version operating system.

**Before you begin**

If you are adding a server to an existing Lotus Domino domain, you need to register the server before you can install Lotus Domino. The registration process creates a Server document in the Lotus Domino directory.

Specify the following settings during registration:
1. Store the server ID file that is created during registration somewhere on the system where you will configure the Lotus Sametime server. Record the path name; you need to specify it when you configure the Lotus Sametime server.
2. Use the same network name as the first Lotus Domino server in the Lotus Domino domain.
Procedure

The Lotus Domino installation programs for AIX, Linux, and Solaris use scripts that need configuration information to install the software in the appropriate directories.

1. Place the CD or DVD in the drive.
2. Log in as root.
3. Mount the Lotus Domino CD or DVD with execution privileges.
   - If your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), mount the CD or DVD manually.
     - AIX
       Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
       ```
       mount -v cdrfs -o ro /dev/cd0 /cdrom
       ```
     - Linux
       Mount the CD or DVD using a command like:
       ```
       mount /dev/cdrom /cdrom
       ```
     - Solaris
       Mount the CD/DVD using a command like:
       ```
       mount /dev/cdrom /cdrom
       ```

4. Complete these preparations:
   a. Ensure that `/bin/hostname` returns the fully qualified domain name for this system.
   b. Ensure that the fully qualified domain name resolves to the IP address of the system and not to localhost. Depending on how domain names are resolved, taking this step may require changes to the DNS, changes to the `/etc/hosts` file (`/etc/inet/hosts` on Solaris systems), or some other configuration step.

5. Change to the `/cdrom` directory and start the installation script using the following command:
   ```
   ./install
   ```

6. Follow the directions on each window of the script, making a note of the location you choose for the Domino executable directory and the Domino data directory. You need this information when you install the community server.

   To install Lotus Domino on partitioned servers:
   a. When prompted to install more than one Lotus Domino server on this computer, click Yes.
   b. When prompted for the location of the data directory and the Notes user account, be sure to specify a unique location for the data directory and the appropriate user name for each partitioned server.

7. For Lotus Domino 8.5 and 8.5.1 only: Create a file to modify XML transforms needed by Sametime:
   a. Navigate to the `Domino_program_directory/jvm/lib` directory.
   b. Create a file called `jaxp.properties`.
   c. Add the following line to the file:
      ```
      javax.xml.transform.TransformerFactory=
          org.apache.xalan.processor.TransformerFactoryImpl
      ```
   d. Save and close the file.
If the Lotus Domino server is running, restart it so that this change takes effect.

What to do next

Start and stop the Lotus Domino server at least once before installing the Sametime server. This action creates certain files that Sametime needs to install correctly.

Related tasks

“Starting and stopping servers in a Sametime deployment” on page 481
An IBM Sametime deployment is made of up several component servers that can be started and stopped independently.

Configuring partitioned Lotus Domino servers on AIX, Linux, or Solaris:

Prepare IBM Lotus Domino partitioned servers before installing the Sametime community server on AIX, Linux, or Solaris operating systems. Partitioned Lotus Domino servers are not supported on Microsoft Windows.

About this task

Follow these steps to configure each server. Use the appropriate Lotus Notes user account for each server you want to configure. For example, log in as notes and configure the first server. Then log out, log in as notes2 and configure the second server, and so on.

Procedure

1. Log in with the first Lotus Notes user account and enter the following command:
   /opt/lotus/bin/server

2. During configuration, make sure that any field referring to the server's name or IP address is set up correctly. By default, the IP address and server name fields for each configuration contain the IP address and server name of the first server. For each additional server, you must update these fields so that they are appropriate for that partition.

3. After configuration for each server is complete, provide the host name for each partitioned Lotus Domino server:
   a. Start the Lotus Domino server.
   b. Open a browser and go to the server's Lotus Domino directory, which is usually names.nsf.
   c. Open the server document for this particular Lotus Domino server.
   d. Select the Internet Protocols / HTTP tab and enter the host name with the fully qualified name of the server, and then enable Bind to host name. For multi-homed servers, do not enter the host name; instead enter all IP addresses into the Host name field.
   e. Save and close the server document.
   f. Open the notes.ini file and add the following field:
      TCPIP_TcpIpAddress=0,(server_ip):1352

4. Log out.

5. Access the Community Services Network settings from the Sametime administration tool by selecting Configuration > Connectivity > Networks and Ports. You must change the Event Server port and the Token Server port for
each additional partition that you install. Ensure that the values are unique and that they are not in use by another Sametime server or process. Use ports above 9098.

6. Repeat the process until you have configured all the partitioned Lotus Notes servers.

What to do next
1. Start each partitioned Lotus Domino server, one at a time.
2. Verify that each server has successfully started.
3. Verify that no errors are reported.
4. Stop each Lotus Domino server.

Installing the Lotus Notes client and Lotus Domino administrative client:

To administer the Lotus Domino server, you must install and configure at least one Microsoft Windows computer as the administration workstation.

Before you begin

Before you can install the Lotus Domino administrator and Lotus Notes clients, you must have installed and set up the Lotus Domino server.

About this task

Use the IBM Lotus Domino software that shipped with IBM Sametime to install and configure the Lotus Domino administrator and IBM Lotus Notes clients on the administration workstation.

Procedure
1. If you are installing from physical media, insert the Lotus Notes Client CD into the computer you plan to use as the administrator’s workstation.
2. Start the installation wizard.
3. Follow the instructions on each panel of the Lotus Notes installation wizard, selecting to install both the Lotus Domino administrator and Lotus Notes clients.
4. Copy the certifier ID and administrator ID files from the Lotus data directory of your Lotus Domino server to the Lotus Notes data directory of the administrator workstation. You can use File Transfer Protocol (FTP) or another method, or you can let the initial communications between the server and administration workstation copy the files for you automatically.
5. If necessary, start the Lotus Domino server.
6. Open Lotus Notes.
7. Follow the instructions in the setup wizard to configure the Lotus Notes client. If you have moved the certifier and administrator ID files to the computer that you have designated as your administration workstation, indicate the correct location when asked. If you have not copied the ID files, simply provide the user administrator name that you specified during HTTP setup. You are prompted for the password for this ID. The ID files are copied and stored on your administration workstation for you automatically.
What to do next

When you have set up the Lotus Domino administrator and Lotus Notes clients, you are ready to begin preparing the Lotus Domino server for Sametime installation.

Verifying your Lotus Domino environment:

Verify that your Lotus Domino server environment has the correct document settings and is accessible.

Verifying the Lotus Domino server document settings:

After installing the Lotus Domino server and before installing Sametime community server, you should edit the Lotus Domino server document to make sure that the fields are completed as described in this topic.

Procedure

Follow these steps to edit the server document.
1. Start the Lotus Domino server and wait until it is started.
2. Open the Lotus Domino administrator and click the Configuration tab.
3. Expand the Server section and then click All Server Documents.
4. Open the server document for the Lotus Domino server on which you are installing Sametime. Use the following table to verify the appropriate values for the fields in the server document. Change the document if necessary.

<table>
<thead>
<tr>
<th>Server document field</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basics tab</td>
<td></td>
</tr>
<tr>
<td>Fully qualified Internet host name</td>
<td>You complete this field during the Domino server installation. It contains the fully qualified host name as known by the DNS server. The value cannot be a numeric IP address.</td>
</tr>
<tr>
<td>Load Internet configurations from Server\Internet Sites documents</td>
<td>In a test environment, you can use DNS or the local hosts table.</td>
</tr>
<tr>
<td>Directory assistance database name</td>
<td>Disabled</td>
</tr>
<tr>
<td>Directory type</td>
<td>If a directory assistance database does not exist on the server, Sametime creates one during server installation and sets this field to da.nsf.</td>
</tr>
<tr>
<td>Security tab</td>
<td>This field must be Primary Domino Directory.</td>
</tr>
<tr>
<td></td>
<td>If this field contains Configuration Directory, shut down the Domino server and replicate names.nsf from a master server. Master servers use the Primary Domino Directory type.</td>
</tr>
<tr>
<td>Server document field</td>
<td>Description and values</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrators</td>
<td>You complete this field during the Lotus Domino server installation. It contains the</td>
</tr>
<tr>
<td></td>
<td>name of the Sametime administrator. If the name is incorrect, click the arrow to select</td>
</tr>
<tr>
<td></td>
<td>a name from an address book.</td>
</tr>
<tr>
<td>Internet authentication</td>
<td>The default value is Fewer name variations with higher security, which is better for</td>
</tr>
<tr>
<td></td>
<td>tighter security.</td>
</tr>
<tr>
<td></td>
<td>Select More name variations with lower security if you use Lotus Domino Directory</td>
</tr>
<tr>
<td></td>
<td>authentication and want users to be able to use short names.</td>
</tr>
<tr>
<td>Access server</td>
<td>Leave this field blank. If you do include entries, you must add the following entry to</td>
</tr>
<tr>
<td></td>
<td>the list of trusted directories:</td>
</tr>
<tr>
<td></td>
<td>Sametime Development/Lotus Notes</td>
</tr>
<tr>
<td></td>
<td>Companion Products</td>
</tr>
<tr>
<td>Sign or run unrestricted methods and operations</td>
<td>After you install the Sametime server, this field includes these entries:</td>
</tr>
<tr>
<td></td>
<td>• The name of the server</td>
</tr>
<tr>
<td></td>
<td>• The name of the administrator</td>
</tr>
<tr>
<td></td>
<td>• Sametime Development/Lotus Notes</td>
</tr>
<tr>
<td></td>
<td>Companion Products</td>
</tr>
<tr>
<td></td>
<td>If you have signed agents with an additional signature, include that name in this field</td>
</tr>
<tr>
<td>Ports - Notes Network Ports tab</td>
<td>This field must be TCPIP. Use uppercase letters.</td>
</tr>
<tr>
<td>Port</td>
<td>This field must be TCP.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The fully qualified host name for the Lotus Domino server as known by the DNS server.</td>
</tr>
<tr>
<td>Net address</td>
<td>The value of this field must be the same as the fully qualified Internet host name on</td>
</tr>
<tr>
<td></td>
<td>the Basics tab and the host name on the</td>
</tr>
<tr>
<td></td>
<td>Internet Protocols-HTTP tab. The value cannot be a numeric IP address.</td>
</tr>
<tr>
<td></td>
<td>For example, computername.domain_name.com or stdom1.example.com.</td>
</tr>
<tr>
<td>Ports - Internet Ports - Web tab</td>
<td>This field must be 80.</td>
</tr>
<tr>
<td>TCP/IP port number</td>
<td>Before you install the community server, the port number must be set to 80. The TCP/IP</td>
</tr>
<tr>
<td></td>
<td>port number changes after installation to 8088 automatically if you enable HTTP</td>
</tr>
<tr>
<td></td>
<td>tunneling.</td>
</tr>
<tr>
<td>TCP/IP port status</td>
<td>This field must be Enabled.</td>
</tr>
</tbody>
</table>
### Server document field

<table>
<thead>
<tr>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name &amp; password</td>
</tr>
<tr>
<td>This field must be Yes.</td>
</tr>
<tr>
<td>Anonymous</td>
</tr>
<tr>
<td>This field must be Yes.</td>
</tr>
</tbody>
</table>

### Internet Protocols - HTTP tab

<table>
<thead>
<tr>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>The fully qualified host name of the Lotus Domino server as known by the DNS server. The value of this field must be the same as the fully qualified Internet host name on the Basics tab and the net address on the Ports - Notes Network Ports tab. The value cannot be a numeric IP address. If the servers are running on AIX, Linux or Solaris operating systems and have multiple valid IP addresses, enter all of the IP addresses instead of the host name. For example, <code>computername.domain_name.com</code> or <code>stdom1.example.com</code>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bind to host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field must be set to Disable for Microsoft Windows servers and for IBM AIX, Linux, or Solaris servers that do not use partitioned Lotus Domino servers. This field must be set to Enable for IBM i servers and for IBM AIX, Linux, or Solaris servers that use partitioned Lotus Domino servers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow HTTP clients to browse databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field must be set to Yes for portals.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Home URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field is set to <code>stcenter.nsf</code> during Sametime installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSAPI filter file names</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this field is set to <code>NDOLEXTN</code> (Lotus Domino offline services), remove the value and leave this field blank.</td>
</tr>
</tbody>
</table>

### Internet Protocols - Domino Web Engine tab

<table>
<thead>
<tr>
<th>Session authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field is set to Multiple Servers (SSO) during Sametime installation. If single sign on (SSO) is not being used, you can change this field to <code>single-server</code>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web SSO configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field is set to <code>LtpaToken</code> during Sametime installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Java servlet support</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field must be Domino Servlet Manager.</td>
</tr>
</tbody>
</table>

5. Click **Save and Close**.

6. Stop and restart the Lotus Domino server for the changes to take effect.

7. Verify that the IBM Lotus Domino server is available from client workstations. Start a web browser on the workstation and attempt to access a database that clients can access, such as `names.nsf`. Enter `http://hostname.example.com/names.nsf` If you can sign on using the server administrator ID and Internet password to view the contents of `names.nsf`, the Lotus Domino server is available and ready for installation of Sametime.
Related tasks
“Starting and stopping servers in a Sametime deployment” on page 481
An IBM Sametime deployment is made up of several component servers that can be started and stopped independently.

Preparing to install a Sametime Community Server
Use the system console to create a deployment plan, which stores information needed for a server installation.

Before you begin
Start the system console if it is not already running. Start the Lotus Domino server to allow validation of the administrator during the installation.

Procedure
If you have not already opened the Install Sametime Community Server guided activity, follow these steps:
1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime system console server.
   http://serverhostname.domain:8700/ibm/console
   For example:http://sametime.example.com:8700/ibm/console
2. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.
3. On the left side of the navigation tree, click the Sametime System Console task to open it.
4. Click Sametime Guided Activities > Install Sametime community server.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install a Sametime Community Server:
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation fields.

Before you begin
If the system console uses only IPv6 addressing, do not use this procedure. Instead install the community server without a deployment plan, as described in the article, "Installing Sametime 8.5.x servers without using deployment plans” on the Sametime wiki:
http://www-10.lotus.com/ldd/stwiki.nsf

Make sure that you have installed and prepared the IBM Lotus Domino server environment on the server where you plan to install the community server and started the Lotus Domino server. If you plan to connect to a separate slide conversion server, you must have configured the server and know its name and port number.
About this task

Follow these steps to store a deployment plan on the system console to be used when you run the installation program for community server.

Procedure

1. Plan a product installation.
   In the Install Sametime community server guided activity, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.
   Specify a unique, recognizable deployment name that includes the installation and node type, such as stComm. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive. The name is shown only in the system console. Click Next.

   Select the product version that you want to install, and then click Next.

4. Connect to Domino Server.
   Provide the fully qualified host name for this community server. Do not use an IP address or the host's short name.
   Leave 80 as the default port unless you are using another port for the HTTP server.
   Enter the existing Lotus Domino administrator’s user ID and password, and then click Next.
   Use the common-name portion of the ID, not the hierarchical name that includes slashes. The system console validates the administrator credentials on the Lotus Domino server.

5. Slide Conversion.
   Do one of the following:
   Select Use the Sametime server to host the slide conversion feature on the current server, and then click Next.
   Select Use Sametime slide conversion server to host the slide conversion feature on a different community server. Provide the host name and port to connect to that server, and then click Next.

6. Connect to an LDAP Server.
   Click the LDAP directory that you configured with the system console guided activity, and then click Next.

7. HTTP Tunneling.
   To allow Sametime clients to make HTTP-tunneled connections on port 80 to a server with a single IP address, click Enable HTTP Tunneling, and then click Next.
   Selecting this feature increases the possibility that users in restrictive network environments can exchange data in chats on a community server that is extended to the Internet.

8. Deployment Summary.
   Review the summary page, and then click Finish.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click Modify an Existing Deployment Plan and update the plan. All changes must be made prior to running the installation.
What to do next

“Installing a Sametime Community Server and supporting software” on page 277

Mapping the system console's host name when IPv4 and IPv6 are enabled:

If you created a deployment plan for the community server and the system console supports both IPv4 and IPv6 addressing, you must map both addresses to the console's host name before installing the community server.

About this task

Mapping IPv4 and IPv6 addresses to the system console host name allows the installation program, which does not support IPv6 addressing, to retrieve the deployment plan by using the console's IPv4 address.

Procedure

1. Log on to the computer where you will install the community server as a user with root or administrator privileges.
2. Navigate to the directory containing the /etc/hosts file:
   - AIX, Linux: /etc/hosts
   - Solaris: /etc/inet/hosts
   - Windows: C:/WINDOWS/system32/drivers/etc/hosts
3. Add the following statements to the hosts file to map the system console's IPv4 address and its IPv6 address to the same host:
   
<table>
<thead>
<tr>
<th>Explicit_IPv6_address</th>
<th>Fully_qualified_host_name</th>
<th>Short_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit_IPv4_address</td>
<td>Fully_qualified_host_name</td>
<td>Short_name</td>
</tr>
</tbody>
</table>
   
   Where:

   - **Explicit_IPv6_address** specifies the IPv6-formatted address for the Sametime System Console.
   - **Explicit_IPv4_address** specifies the IPv4-formatted address for the Sametime System Console.
   - **Fully_qualified_host_name** specifies the fully qualified host name (server.domain) for the Sametime System Console. This value is the same for both statements.
   - **Short_name** specifies the short host name for the Sametime System Console. This value is the same for both statements.

   Example:

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Fully_qualified_host_name</th>
<th>Short_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8:1:2:3:4:5:6</td>
<td>stsyscon.example.com</td>
<td>stsyscon</td>
</tr>
<tr>
<td>192.0.2.10</td>
<td>stsyscon.example.com</td>
<td>stsyscon</td>
</tr>
</tbody>
</table>

4. Save and close the file.
5. Restart the server before attempting to run the community server installation program.

Installing a community server on AIX, Linux, Solaris, or Windows

By using the deployment plan that you created earlier, you have fewer selections to make when you run the installation program. The community server cannot be installed on a computer with any other IBM Sametime servers.
Before you begin

You should have a deployment plan for the community server. If the system console supports both IPv4 and IPv6 addressing, you must have mapped both addresses to the console's host name. Start the system console server and verify that the server deployment plan is in the Ready to Install state. Close any open Sametime clients.

Complete any pending restart actions you have from installing other applications. Make sure that all applications on the computer are closed, including the Lotus Domino server administrator and the web browser. All Lotus Domino services must be stopped. Otherwise, you might corrupt any shared files and the installation program might not run correctly.

On AIX, Linux, or Solaris operating systems, verify that:

- The /bin/hostname command returns the fully qualified domain name of this system.
- The fully qualified domain name resolves to the IP address of the system and not to the local host. Depending on how domain names are resolved, you may need to change the DNS, make changes to the /etc/hosts file for AIX or Linux or the /etc/inet/hosts file for Solaris.
- If you are installing using the GUI mode, you must use the full X11 desktop environment.

On Linux, library libstdc++-libc6.1-1.so.2 is required.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.
3. Prepare to use the Sametime Community Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files for Sametime and open the Server folder. Start the installation program by entering one of the following commands:

- AIX
  
  .setupaix.bin

- Linux
  
  .setuplinux.bin

- Solaris
  
  .setupsolaris.bin

- Windows
  
  demo32.exe runs if autorun is on; otherwise, enter this command:

  setupwin32.exe

5. Select the language and click OK.

6. Click Next.

7. Click the I accept the terms in the license agreements option and click Next.

8. Click Yes to install from the system console, and then click Next.

9. Supply the values for connecting to the system console, and then click Next.

   - Sametime System Console host name
     
     Use the host name and not a DNS alias.

   - Use SSL
     
     Keep this option selected to run the server over a secure connection.

   - Sametime System Console port
     
     9443 is the default value.

   - Sametime System Console administrator
     
     Provide the WebSphere Application Server user ID and password that you created when you installed the system console.

   - Fully qualified host name for this Sametime server
Provide the fully qualified host name of the computer that you are currently using. This name is the same name that you used when you created the deployment plan for this installation. Do not use an IP address or short host name.

10. Select the community server deployment plan that you created earlier with the system console guided activity, and then click **Next**.

11. Review the summary, then click **Install** to start the installation.

12. Click **Finish**.

13. If you are prompted, click **Finish** to restart the system.

14. On Windows 2008 only:
   After the installation, perform this required configuration step. In a text editor, open the `sametime.ini` file located in the community server installation directory. For example, the default directory in Windows is `C:\Program Files (x86)\IBM\Lotus\Domino`. Check for the following line to the `[Config]` section and add it if it is missing to ensure continuous connections for Sametime components:
   ```
   BREAK_CONN_ON_ZERO_BYTES_SENT=0
   ```
   Close and save the file.

Results

The `Domino_data_directory\stsetup_exit_status.txt` file contains a zero (0) if the installation is successful. If the installation was not successful, look at the installation logs for more information. Fix the problem, then try installing again. The installation logs are stored in the following locations.

**AIX, Linux, or Solaris**
The default Lotus Domino data directory is `/local/notesdata/`.

Lotus Domino data directory
- `SametimeInstall.log`
- `stsetup.log`
- `stsetup_exit_status.txt`

`SametimeIniParser.log`
This log can be in `/tmp` or in the Lotus Domino data directory.

Console connection log
- `/tmp/SSCLogs/ConsoleUtility0.log`

**Windows**
The default Lotus Domino data directory is `c:\program files\ibm\lotus\domino\data` and the Lotus Domino program directory is `c:\program files\ibm\lotus\domino`.

Lotus Domino data directory
- `SametimeInstall.log`
- `stsetup.log`
- `stsetup_exit_status.txt`

Lotus Domino program directory
- `stsetup_exit_code_windows.txt`

`SametimeIniParser.log`
This log can be in `%TEMP%` or in the Lotus Domino data directory.
Related tasks

“Mapping the system console's host name when IPv4 and IPv6 are enabled” on page 289
If you created a deployment plan for the community server and the system console supports both IPv4 and IPv6 addressing, you must map both addresses to the console's host name before installing the community server.

“Guided activity: Preparing to install a Sametime Community Server” on page 287
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation fields.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Enabling the administrator to manage the community server:

When you use a deployment plan to install the community server, you must add the Sametime Administrator listed in the LDAP directory to the Sametime Configuration database to enable the administrator to manage the community server. Skip this task if you installed the community server without using a deployment plan or if you upgraded the community server from an earlier release.

Procedure

Follow these steps to add the administrator to the server's access control list to ensure that the user account has the appropriate access.

1. The Lotus Domino server needs to be running to complete this task. If the community server is running, stop it now.
   a. Open a command window.
   b. Navigate to the Lotus Domino installation directory.
   c. Start the Lotus Domino server console by entering jconsole.
   d. In the Lotus Domino server console, stop the Sametime server by entering Tell STADDIN Quit.

2. Open the Lotus Notes client on this server.

3. Open the Sametime Configuration database:
   a. Click File > Open > Lotus Notes Application.
   b. In the Look in field, select the server where the community server is installed.
      If you are using a Lotus Notes client on the same server, the location is Local.
   c. In the Open Application window, click the Data folder and then click Open.
   d. In that folder, locate the Sametime Configuration database (stconfig.nsf) in the Sametime Configuration folder and click Open.

4. Add the Sametime administrator to the access control list for this database:
   a. Click File > Application > Access Control.
   b. In the Access Control List window, locate the following name:
      (%objectclass=groupOfNames)(member=%s)
      This user is included by default but is not needed. Rather than creating a user, you can change this user's name.
c. Click the name, and then click the Rename button. If this user does not appear in the list, use the Add option to add your Sametime Administrator to the ACL.

d. Provide the name of the person who is the Sametime administrator, as it is listed in your LDAP directory, and then click OK.

For example, if the LDAP content shows CN=John Smith,OU=East,0=Corp, enter the following text as the distinguished name:

CN=John Smith/OU=East/O=Corp

e. Click OK.

5. Close the Lotus Notes client.

Configuring partitioned Lotus Domino servers to avoid IP conflicts:

After installing a community server in an IBM Lotus Domino partitioned-server environment on AIX, Linux, or Oracle Solaris operating systems, configure the partitioned servers to avoid IP conflicts.

About this task

If your computer hosts multiple community servers (a "multi-homed" configuration), you must define settings to ensure that the IP addresses for each community server do not conflict.

Procedure

1. If your server has multiple IP addresses but they do not all translate to single DNS names, configure the community server to indicate which IP addresses to trust.
   a. Log in to the Integrated Solutions Console.
   b. Click Sametime System Console > Sametime Servers > Sametime community servers.
   c. In the Sametime community servers list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
   d. Click the Connectivity tab.
   e. Under Trusted Servers, enter the IP address of the server that must connect to the Sametime community server in the New IP Address field, and click Add.
   f. Click OK.

2. By default, the broadcast server binds to one IP address and port. If multiple IP addresses resolve to the same DNS name, you must bind all of them to the broadcast server.
   a. Start the community server.
   b. Log in as administrator, and open the administration tool by clicking Administer the Server.
   c. Click Configuration > Connectivity > Broadcast gateway address for client connections.
   d. Do one of the following:
      • Enter the specific IP address that you want to use for Broadcast connections.
      • Specify that the Broadcast Server should bind to all IP addresses on the server.
   e. Close the administration tool.
f. Open the meetingserver.ini file and make the following change before saving the file. Under the [SOFTWARE\Lotus\Sametime\BroadcastGateway\DBNL] section, locate the entry:
   IPBindAll=0
   and change it to
   IPBindAll=1

3. If you entered a DNS name as the host name address for client connections and HTTP-tunneled client connections, you must specify a dotted-decimal IPv4 address that the fully qualified domain name resolves to.
   a. Start the community server.
   b. Log in as administrator, and open the administration tool by clicking **Administer the Server**.
   c. Click **Configuration > Connectivity**.
   d. Enter the dotted-decimal IPv4 address in the following fields:
      - Address for client connections > Host name
      - Address for HTTP tunneled client connections > Host name

4. Restart the community server.

Verifying a community server installation on AIX, Linux, Solaris, or Windows:

After installing the community server on AIX, Linux, Solaris or Windows, start the server and verify that the installation was successful.

**Procedure**

Follow these steps to confirm that you can connect to the community server.

1. On the Lotus Domino server, start the Domino server and community server.
2. On the system console system, start the Sametime System Console.
3. Start the Deployment Manager for the cell.
4. From a browser, log in to the Integrated Solutions Console:
   a. Enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the system console server.
      
      http://serverhostname.domain:8700/ibm/console
      
      For example:
      
      http://sametime.example.com:8700/ibm/console
   b. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.
5. Click **Sametime System Console > Sametime Servers > Sametime community servers**.
6. In the **Sametime community servers** list, click the deployment name of the server that you installed.
7. Click any of the tabs to see the types of settings that you can change. You make most configuration changes from these tabs.
8. Log in to the Sametime administration tool.
   a. Using a browser, enter the URL `http://serverhostname.domain:port/stcenter.nsf`
Replace `serverhostname.domain` with your community server name and add the port number if you determined it is not the default port number 80. For example: `http://st85comm1.example.com/stcenter.nsf`

b. Log in with the Lotus Domino administrator's name and password.

c. On the Welcome page, under Administrator Tools, click **Administer the server** and verify that it opens.

**Related concepts**

“Starting and stopping servers running on Lotus Domino” on page 492

The IBM Sametime Community Server is configured as a set of services that start and stop automatically when the Domino server is stopped or started.

**Related tasks**

“Guided activity: Preparing to install a Sametime Community Server” on page 287

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation fields.

**Installing a community server in silent mode**

Use a silent server installation command to install a community server on AIX, Linux, Solaris, or Windows without any intervention during the installation process. An options file provides the information for the installation process.

**About this task**

Follow these steps to customize the default installation options file for your environment and then use it to run the silent installation command.

**Procedure**

1. Open the default options file, which is provided on the CD and the web download image.
   
   If you are using a CD, copy the options file to a local, writable directory before opening it.

   **AIX, Linux, or Solaris**
   
   options-unix.txt

   **Windows**
   
   options-windows.txt

2. Update the options file for your environment by using the instructions included in the file. Then save the updated file with a new name, such as `options-unix-update.txt` or `options-windows-update.txt`.

3. Open a command prompt window and change to the directory where the installation launch programs are located.

4. Enter the launch command, specifying the `-silent` and `-options` parameters and the name of the updated options file, including the full path to the file.

   Use the following format:
   
   `InstallLauncherCommand -silent -options optionsfilename`

   **Note:** UNIX commands are case-sensitive.

   - **AIX**
   
     `./setupaix.bin -silent -options options-unix-update.txt`

   - **Linux**
   
     `./setuplinux.bin -silent -options options-unix-update.txt`

   - **Solaris**
5. On Windows 2008 only:

After the installation, perform this configuration step. In a text editor, open the sametime.ini file located in the community server installation directory. For example, the default directory in Windows is C:\Program Files (x86)\IBM\Lotus\Domino. Add the following line to the [Config] section to ensure continuous connections for Sametime components:

```
BREAK_CONN_ON_ZERO_BYTES_SENT=0
```

Close and save the file.

Results

The program indicates whether the silent installation was successful by providing an exit status and logging errors. The stsetup.log and SametimeInstall.log files are located in the Sametime data directory. If the exit status of the program and the contents of stsetup_exit_status.txt are both 0, the installation was successful. If either of these values are anything other than 0, the installation was not successful. Check the stsetup.log and SametimeInstall.log files in the server data directory for information.

Enabling IPv6 support on a Sametime community server

Enabling support for IPv6 addressing on an IBM Sametime server involves configuring settings for both Lotus Domino and Sametime.

Before you begin

Install Lotus Domino and a Sametime Community Server as described earlier; these products must be installed before you can modify their configuration settings.

Important: Due to the way the Sametime community server functions, you must not disable IPv4 addressing in the server's operating system. Even if you will use IPv6-only addressing with the Sametime community server and with your network, internal server components use IPv4 addresses (for example, in loopback addresses) and will fail if the operating system does not support IPv4 addressing.

About this task

To enable support for IPv6 addressing on the Sametime Community Server, modify the configuration settings for Lotus Domino and for Sametime as explained in the following topics:

Configuring Lotus Domino to support IPv6 addressing:

The IBM Sametime Community Server is hosted on Lotus Domino. When you enable support for IPv6 addressing on the community server, you must additionally ensure that the underlying Lotus Domino server also supports IPv6.

Before you begin

Sametime supports IPv6 addressing only with Lotus Domino 8.0 or later. If you use an earlier release of Lotus Domino, you must upgrade it to release 8.x before you can configure it for IPv6 addressing.
About this task

The steps to enabling IPv6 support in Lotus Domino vary with the operating system:

**Configuring Lotus Domino for IPv6 addressing on AIX, Linux, or Solaris:**

Before an IBM Sametime server can support IPv6 addressing on IBM AIX, Linux, or Solaris, you must configure IPv6 support for the Lotus Domino server on which it is hosted.

**Before you begin**

Lotus Domino and the Sametime Community server must be installed; the Lotus Domino server must be running (it does not matter whether the community server is also running at this point).

**About this task**

In Lotus Domino, only IPv4 addressing is enabled by default. Configuring Lotus Domino to support IPv6 involves modifying the Sametime community server’s “Server” document within the Lotus Domino Administrator interface, as well as adding configuration settings to the notes.ini file used by Lotus Domino.

For information on supporting IPv6 with Lotus Domino, see "IPv6 and Lotus Domino" in the Lotus Domino Administration information center at:

Lotus Domino Administration information center

**Procedure**

1. To support both IPv4 and IPv6 addressing, update the “Server” document for the community server so that both formats will be accepted:

   **Note:** If you will only support IPv6 addressing, skip this step.


   b. In the Domino Administrator, navigate to the Server pane and double-click your community server’s name to select it. This opens the corresponding “Server” document.

   c. In the “Server” document, navigate to the Internet Protocols > HTTP tab.

   d. Update the HTTP hostname field by entering the community server’s fully qualified host name, followed by the explicit IPv4 and IPv6 IP addresses for this server.

      **Attention:** When you fill out this field, you must enter the values using the following format:

      - The first value in the field must a fully qualified host name (for example: commsvr1.example.com).
      - The second and third values must be the explicit IP addresses (using IPv4 dot notation or IPv6 colon notation) that correspond to that host name; the order of these two IP addresses does not matter.
      - Separate values with a carriage return by pressing the ENTER key before adding another value.

   e. Save and close the "Server" document.
f. Restart the HTTP service on the Lotus Domino server by running the following command in the console: `tell http restart`

2. Enable support for IPv6 addresses by adding the following setting to the `notes.ini` file, located in the Lotus Domino server data directory:

   `tcp_enableipv6=1`
   `DONT_USE_REMEMBERED_ADDRESSES=1`

   Leave this file open for the next step.

3. (AIX and Solaris only) Add the following setting to the `notes.ini` file to define the default zone for your server:

   `tcp_defaultzone=zone`

   In this statement, `zone` is the default zone; this information can be obtained by running the `ifconfig -a` command.

4. Restart the Lotus Domino server so your changes can take effect.

Configuring Lotus Domino for IPv6 on Windows:

Before an IBM Sametime community server can support IPv6 addressing on Microsoft Windows, you must configure IPv6 support for the IBM Lotus Domino server on which it is hosted.

Before you begin

Lotus Domino and the Sametime Community server must be installed; the Lotus Domino server must be running (it does not matter whether the community server is also running at this point).

About this task

In Lotus Domino, only IPv4 addressing is enabled by default. Configuring Lotus Domino to support IPv6 involves modifying the Sametime community server's "Server" document within the Lotus Domino Administrator interface, as well as adding configuration settings to the `notes.ini` file used by Lotus Domino.

For information on supporting IPv6 with Lotus Domino, see "IPv6 and Lotus Domino" in the Lotus Domino Administration information center at:

Lotus Domino Administration information center

Procedure

1. To support both IPv4 and IPv6 addressing, update the "Server" document for the community server so that both formats will be accepted:

   Note: If you will only support IPv6 addressing, skip this step.

   
   b. In the Domino Administrator, navigate to the Server pane and double-click your community server's name to select it.
   
   This opens the corresponding "Server" document.
   
   c. In the "Server" document, navigate to the Internet Protocols > HTTP tab.
   
   d. Update the HTTP hostname field by entering the fully qualified host name, followed by the explicit IPv4 and IPv6 IP addresses for this server.
Attention: When you fill out this field, you must enter the values using the following format:

- The first value in the field must a fully qualified DNS (for example: `commsvr1.example.com`).
- The second and third values must be the explicit IP addresses (using IPv4 dot notation or IPv6 colon notation) that correspond to that host name; the order of these two IP addresses does not matter.
- Separate values with a carriage return by pressing the ENTER key before adding another value.

e. Save and close the "Server" document.

f. Restart the HTTP service on the Lotus Domino server by running the following command in the console:

```
tell http restart
```

2. Enable support for IPv6 addresses by adding the following settings to the `notes.ini` file, located in the Lotus Domino server's data directory:

```
tcp_enableipv6=1
DONT_USE_REMEMBERED_ADDRESSES=1
```

In the next statement, `zone` is the default zone.

```
tcp_defaultzone=zone
```

This set of statements creates one port for IPv4 addressing (TCPIP) and another port for IPv6 addressing (TCPIPV6):

```
TCPIP=tcp,0,15,0
tcplib_tcpipaddress=0,Domino_server's_IPv4_address
ports=tcplib,tcipv6
```

```
TCPIPV6=tcp,0,15,0
tcipv6_tcpipv6address=0,Domino_server's_IPv6_address
ports=tcipv6
```

3. Restart the Lotus Domino server so your changes can take effect.

**Configuring the Sametime Community Server to support IPv6 addressing:**

Configure settings to establish connectivity and resolve addresses when using IPv6 addressing on the IBM Sametime community server.

**Before you begin**

Enable support for IPv6 addresses on the Lotus Domino server hosting this Sametime community server.

**Important:** Due to the way the Sametime community server functions, you must not disable IPv4 addressing in the server's operating system. Even if you will use IPv6-only addressing with the Sametime community server and with your network, internal server components use IPv4 addresses (for example, in loopback addresses) and will fail if the operating system does not support IPv4 addressing.

**About this task**

Follow the steps below to configure IPv6 support on the Sametime community server:

**Procedure**

1. Stop the Community Server.

2. Locate the `sametime.ini` file in the Sametime community server's data directory, and open the file so you can edit it.

3. In the [Connectivity] section, add (or modify) the following statements:
UCM_RESOLVE_PREFERRED_IP_VER=IPv4_or_IPv6_selection
VPS_HOST=Explicit_IP_address_of_this_server
UCM_LOCAL_IP=Explicit_IP_address_of_this_server
VPHMX_HTTP_SERVER_IP=IP_address_of_Domino_HTTP_server
VPHMX_HTTP_SERVER_PORT=Domino_HTTP_port

where:

- **UCM_RESOLVE_PREFERRED_IP_VER** specifies which type of addresses should be preferred when a domain name resolves to multiple addresses of both protocols:
  - If you support only IPv6 addressing, set this to "6" to disallow IPv4–formatted addresses.
  - If you support both IPv4 and IPv6 addressing, set this to "4" to allow both protocols but attempt to resolve addresses, using IPv4 protocol first.

- **VPS_HOST** specifies the explicit IP address of this Sametime community server. Use the IP address that matches the setting in **UCM_RESOLVE_PREFERRED_IP_VER**. For example, if you set that value to "4" then specify an IPv4–format address, but if you set that value to "6" then specify an IPv6–format address.

- **UCM_LOCAL_IP** specifies the explicit IP address of this Sametime community server. Use the IP address that matches the setting in **UCM_RESOLVE_PREFERRED_IP_VER**. For example, if you set that value to "4" then specify an IPv4–format address, but if you set that value to "6" then specify an IPv6–format address.

- **VPHMX_HTTP_SERVER_IP** specifies the IP address of the Lotus Domino HTTP server running on this computer.

- **VPHMX_HTTP_SERVER_PORT** specifies the port used by the Lotus Domino HTTP server running on this computer; normally this is port 80.

4. In the [Config] section, add (or modify) the following statement:

    STLINKS_HOST=Explicit_IP_address_of_this_server

    where **STLINKS_HOST** specifies the explicit IP address of this Sametime community server. Use the IP address that matches the setting in **UCM_RESOLVE_PREFERRED_IP_VER**. For example, if you set that value to "4" then specify an IPv4–format address, but if you set that value to "6" then specify an IPv6–format address.

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 explicit address (dot notation)</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:2e66</td>
</tr>
<tr>
<td>IPv6 explicit address using IPv4-suffix notation</td>
<td>3ef0::bee7:9.148.46.102</td>
</tr>
<tr>
<td>IPv4 &quot;any&quot; (four zeroes)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IPv6 &quot;any&quot; (a double colon)</td>
<td>::</td>
</tr>
</tbody>
</table>

5. Add (or modify) the following statements in the [Debug] section within the **sametime.ini** file:

    - If this Sametime community server will support both IPv4 and IPv6 addressing:
VPMX_DISABLE.Configuration.Update=1
VPMX_HOSTNAME=::,0.0.0.0
VPMX_PORT=1533
VPHMX_HOSTNAME=::,0.0.0.0
VPHMX_PORT=8082

Where:
- VPMX_DISABLE_CONFIGURATION_UPDATE=1 requires all four of the statements that follow it.
- VPMX_HOSTNAME specifies the addresses where the multiplexer residing on this server handles Sametime client communications. (The multiplexer was installed automatically as a part of the Sametime community server; if you will additionally install a stand-alone Community Mux, you will need to enable support for IPv6 addressing on that server as well).

Table 44. Accepted values for VPMX_HOSTNAME

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 explicit address (dot notation)</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:2e66</td>
</tr>
<tr>
<td>IPv6 explicit address using IPv4-suffix notation</td>
<td>3ef0::bee7:9.148.46.102</td>
</tr>
<tr>
<td>IPv4 &quot;any&quot; (four zeroes)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IPv6 &quot;any&quot; (a double colon)</td>
<td>::</td>
</tr>
</tbody>
</table>

For example, set this to ::,0.0.0.0 to accept "any" address using either IP protocol.
- VPMX_PORT specifies the port on which the multiplexer residing on this server listens for client connections, normally port 1533.
- VPHMX_HOSTNAME specifies the addresses where the multiplexer residing on this server handles HTTP client communications.

Table 45. Accepted values for VPHMX_HOSTNAME

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 explicit address (dot notation)</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:2e66</td>
</tr>
<tr>
<td>IPv6 explicit address using IPv4-suffix notation</td>
<td>3ef0::bee7:9.148.46.102</td>
</tr>
<tr>
<td>IPv4 &quot;any&quot; (four zeroes)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IPv6 &quot;any&quot; (a double colon)</td>
<td>::</td>
</tr>
</tbody>
</table>

For example, set this to ::,0.0.0.0 to accept "any" address using either IP protocol.
- VPHMX_PORT specifies the port on which the multiplexer residing on this server listens for HTTP client connections, normally port 8082.
- If this Sametime community server will support only IPv6 addressing:
6. **IBM i only:** If you will support both IPv4 and IPv6 addressing, replace all of the remaining Sametime community server host names in the `sametime.ini` file with the correct IPv4 or IPv6 address, based on your address preference as specified with the `UCM_RESOLVE_PREFERRED_IP_VER` setting.

   For example:
   - If the `UCM_RESOLVE_PREFERRED_IP_VER` setting is "6", change every occurrence of `stserver1.example.com` to `2001:DB8:1:2:3:4:5:6` (the corresponding IPv6 address).
   - If the `UCM_RESOLVE_PREFERRED_IP_VER` setting is "4", change every occurrence of `stserver1.example.com` to `192.0.2.10` (the corresponding IPv4 address).

7. Save and close the file.

8. Start the Community Server.

**What to do next**

If your Sametime community server is hosted on a Linux SuSE server, you will additionally need to edit the `ststart` script to enable support for IPv6 addressing in SuSE as described in the next topic.

*Enabling IPv6 addressing for a community server on Linux SuSE:*

By default, support for IPv6 addressing is disabled in the version of IBM Sametime that runs on Linux SuSE operating systems; you must enable IPv6 support in the "ststart" script used by Sametime on a Linux SuSE server.

**Before you begin**

Previous releases of Sametime did not support IPv6 addressing. Because the Linux SuSE operating system already supported IPv6 by default, it was necessary to specifically disable IPv6 for Sametime on those servers. If you want to support the use of IPv6 addresses with Sametime on a Linux SuSE server, you must re-enable support for IPv6 by modifying the `ststart` script.

**Note:** This task is needed only for Linux SuSE servers.

**Procedure**

1. On the community server, open a command window and navigate to the Sametime data directory (for example, `/local/notesdata`).
2. Open the `ststart` script so you can edit it.
3. Comment out the following statements by inserting the `#` character at the beginning of each line:
   ```
   if [ -f /etc/SuSE-release ]; then
     IBM_JAVA_OPTIONS=-Djava.net.preferIPv4Stack=true
     export IBM_JAVA_OPTIONS
   fi
   
   The statements should now look like this:
Installing and setting up a stand-alone Community Services multiplexer

Installing and setting up a stand-alone Community Services multiplexer involves the following procedures.

Consider the requirements of the community server multiplexer machine before installing it.

- Community server multiplexer installation files are available for Windows, AIX, Linux, and Solaris. A stand-alone community server multiplexer cannot be installed on IBM i. However, Sametime on IBM i supports the use of a stand-alone multiplexer installed on a Windows system.
- The minimum system requirements for the community server multiplexer machine are the same as the system requirements for the core Sametime community server.
- A machine that meets the minimum system requirements should be able to handle approximately 20,000 simultaneous client connections.
- Testing indicates that machines with dual 1133 MHz CPUs and 2 GB of RAM can handle approximately 30,000 simultaneous client connections.
- TCP/IP connectivity must be available between the community server multiplexer machine and the Sametime community server. Port 1516 is the default port for the connection from the community server multiplexer machine to the Sametime Community Server.

Related tasks

“Deploying a stand-alone Community Server Mux” on page 237
Optionally install an IBM Sametime Community Server Mux (multiplexer) on a separate computer to remove the connection-handling load from the Sametime Community Server. Configuring a stand-alone multiplexer enables the Community Server to handle a larger number of users and improves its stability.

Installing the Community Services multiplexer:

To deploy a stand-alone Community Services multiplexer, install it on a separate computer.

About this task

Follow these steps to install the Community Services multiplexer:

Procedure

1. Insert the Sametime CD into the Community Services multiplexer machine, start the installation program, and choose the option to install the Community Services Mux.
2. At the “Select a language” screen, select a language for the installer, and then click OK.
3. At the “Welcome” screen, click Next.
4. At the license agreement screen, click **I accept both the IBM and the non-IBM terms**, and then click **Next**.

5. At the "Directory name" screen, browse to a the directory where you want to install the Community Mux (or accept the default), and then click **Next**.

6. At the "Host name or IP address" screen, enter the **fully qualified host name** of the Sametime community server that this Community Mux will serve. For best results, do not use an IP address.

7. At the summary screen, click **Install**.

8. At the "successfully installed" screen, click **Finish**.

9. **Windows 2008 only**
   After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is C:\Program Files (x86)\IBM\Lotus\Domino. Check for the following line to the [Config] section and add it if it is missing to ensure continuous connections for Sametime components:
   
   BREAK_CONN_ON_ZERO_BYTES_SENT=0
   
   Close and save the file, then restart the server.

**Connecting to a Sametime Community Mux server:**

Use the IBM Sametime System Console to connect to a Sametime Community Mux and validate its settings.

**Before you begin**

Start the Sametime Community Mux if it is not already running.

**Procedure**

If you have not already opened the Connect to Sametime Community Mux Servers activity, follow these steps:

1. From a browser, enter the following URL, replacing **serverhostname.domain** with the fully qualified host name of the Sametime System Console server (for example stconsole.example.com).
   
   http://serverhostname.domain:8700/ibm/console
   
   For example: http://sametime.example.com:8700/ibm/console
   
   If you are prompted with a security exception, accept the certificate, and continue.

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Expand **Sametime Prerequisites**, and click **Connect to Sametime Community Mux Servers**.
Related concepts

“Planning for an LDAP directory” on page 232
The IBM Sametime 8.5 multiple-server environment requires an LDAP directory for user authentication. The LDAP server should be set up and running before deploying Sametime.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

*Sametime prerequisite: Connecting to a Sametime Community Mux Server:*

Validate the host name and ports specified for a new IBM Sametime Community Mux server.

**Before you begin**

Use this page to validate the host name of a new Community Mux, along with the ports on which it will listen for client connections. This ensures you have a working multiplexer before you attempt to connect it to a Sametime community server or cluster.

**Procedure**

1. **Connect to Sametime Community Mux Servers.**
   
   Click **Add** to begin the guided activity, which lets you validate your installed Sametime Community Mux servers before connecting them to community servers.
   
   You can optionally edit or delete connections to Community Mux servers. Click **Refresh** to view your most recent changes.

2. **Add Sametime Community Mux Servers.**
   
   a. In “Connect to Sametime Community Mux Servers”, click **Add**.
   
   b. In the **Host Name** field, type the fully qualified host name of the new Sametime Community Mux (for example: `mux1.example.com`).
   
   c. Accept the default settings for the **Client Port** and **Client HTTP Port** fields.
      
      These settings indicate the ports that the multiplexer will listen on for connections from Sametime Connect clients and from web clients, respectively.

   d. Click **Save**.
      
      The connection to the Sametime Community Mux is validated when you save the settings.

**Configuring security for the multiplexer:**

Update the CommunityConnectivity document in the stconfig.nsf database to enable the Sametime Community Server to accept connections from the community server multiplexer.

**About this task**

A Sametime Community Server only accepts connections from a Community Services multiplexer that is listed in the “CommunityTrustedIps” field of a “CommunityConnectivity” document to prevent an unauthorized machine from connecting to the Sametime community server.
Procedure
1. Use a Lotus Notes client to open the stconfig.nsf database on the Sametime community server.
2. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking on the date associated with the document.
   If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose Create > CommunityConnectivity from the menu bar in the stconfig.nsf database.
3. In the "CommunityTrustedIps" field, enter the IP addresses of the Community Services multiplexer machine(s). If you enter multiple addresses, separate each address with a comma.
   The IP addresses of SIP Connector machines associated with a Sametime community are also entered in this field.
4. Save and close the CommunityConnectivity document.

Configuring the sametime.ini file for a stand-alone multiplexer:

Review the sametime.ini settings on the stand-alone Community Server multiplexer to confirm that they are appropriate for your site.

About this task

Follow these steps to confirm or change the settings for VPS_HOST, VPS_PORT, and VPMX_CAPACITY. If you have Sametime Community Servers running releases earlier than Sametime 8.0.2, also add the VPMX_ASSUME_COMMUNITY_ISFUNC setting.

Procedure
1. Open a text editor on the community server multiplexer machine.
2. Open the Sametime.ini file located in the Sametime server installation directory (the default directory in Windows is C:\program files\lotus\domino).
3. In the [Connectivity] section, confirm the host name (VPS_HOST) of the Sametime server to which the Community Services multiplexer connects (specified during the Community Services multiplexer installation and in the stconfig.nsf database).
4. If you are not using the default port of 1516, add the port (VPS_PORT) the community server multiplexer uses to establish the connection with the Sametime server.
5. The Maximum user and server connections to the community server setting in the Sametime Administration Tool for the Sametime community server does not apply to a stand-alone multiplexer. Instead, the VPMX_CAPACITY= parameter in the multiplexer's sametime.ini file controls the maximum number of connections.
   In the [Config] section, confirm or change the maximum number of simultaneous connections allowed to the stand-alone multiplexer. The default value is 20,000 connections.
   VPMX_CAPACITY=20000
6. If the multiplexer connects to older Sametime community servers running releases earlier than Sametime 8.0.2, add the following setting with a value of 1 in the [Config] section. This setting enables the multiplexer to connect to the older server.
7. Save the sametime.ini file.

Enabling IPv6 on a multiplexer:

Configure settings to establish connectivity between an IBM Sametime server and a stand-alone Sametime Community Mux when using IPv6 addressing.

About this task

Each Sametime server contains a local Community Services multiplexer component. The multiplexer handles and maintain connections from Sametime clients to the Community Services on the Sametime server. If your multiplexer is hosted on the same server as Community Services, it was already enabled for IPv6 support when you configured the Community Services.

If you installed a stand-alone Community Mux (hosted on a separate server), you can enable IPv6 support as described below.

Procedure

1. Stop the multiplexer.
2. Locate the sametime.ini file in the Sametime Community Mux installation directory, and open the file so you can edit it.
3. Add (or modify) the following statements to the [Connectivity] section within the file:

   Note: The first three settings must match the values used for the Sametime server where Community Services are hosted; these values must use the same IP protocol as well.

   UCM_RESOLVE_PREFERRED_IP_VER=IPv4_or_IPv6_selection
   VPS_HOST=Explicit_IP_address_of_Sametime_server
   UCM_LOCAL_IP=Explicit_IP_address_of_Community_Mux
   VPMX_HTTP_SERVER_IP=IP_address_of_Domino_HTTP_server
   VPMX_HTTP_SERVER_PORT=Dominio_HTTP_port

   where:

   • **UCM_RESOLVE_PREFERRED_IP_VER** specifies which type of addresses should be preferred when a domain name resolves to multiple addresses of both protocols:
     - If you support both IPv4 and IPv6 addressing, set this to "4" to allow both protocols but attempt to resolve addresses using IPv4 protocol first.
     - If you support only IPv6 addressing, set this to "6" -- this will still allow both protocols, but will attempt to resolve addresses using IPv6 protocol first in case your operating system is enabled for both IP protocols.

   • **VPS_HOST** specifies the explicit IP address of the Sametime server to which this Community Services multiplexer connects. This value must use the format specified in UCM_RESOLVE_PREFERRED_IP_VER; for example if you entered a "4" for that setting, then you must provide an IPv4–format IP address here.

   • **UCM_LOCAL_IP** specifies the explicit IP address of the Community Mux machine (using dot notation for IPv4 protocol or colon notation for IPv6 protocol). This value must use the format specified in UCM_RESOLVE_PREFERRED_IP_VER; for example if you entered a "4" for that setting, then you must provide an IPv4–format IP address here.
• **VPHMX_HTTP_SERVER_IP** specifies the IP address of the Lotus Domino HTTP server where Sametime is running.

• **VPHMX_HTTP_SERVER_PORT** specifies the port used by the Lotus Domino HTTP server where Sametime is running; normally port 80.

4. Add (or modify) the following statements in the `[Debug]` section within the `sametime.ini` file:

   • If this Sametime server will support both IPv4 and IPv6 addressing:
     
     ```
     VPMX_DISABLE_CONFIGURATION_UPDATE=1
     VPMX_HOSTNAME=::,0.0.0.0
     VPMX_PORT=1533
     VPHMX_HOSTNAME=::,0.0.0.0
     VPHMX_PORT=8082
     ```

     Where:
     
     - **VPMX_DISABLE_CONFIGURATION_UPDATE=1** requires all four of the statements that follow it.
     - **VPMX_HOSTNAME** specifies the addresses where this multiplexer serves Sametime client communications.

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 explicit address (dot notation)</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IPv6 explicit address using colon notation</td>
<td>2001:0DB8:1:2:3:4:5:6</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:2e66</td>
</tr>
<tr>
<td>IPv6 explicit address using IPv4-suffix notation</td>
<td>3ef0::bee7:9.148.46.102</td>
</tr>
<tr>
<td>IPv4 &quot;any&quot; (four zeroes)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IPv6 &quot;any&quot; (a double colon)</td>
<td>::</td>
</tr>
</tbody>
</table>

     For example, set this to ::,0.0.0.0 to accept "any" address using either IP protocol.

     - **VPMX_PORT** specifies the port on which this multiplexer listens for client connections, normally port 1533.
     - **VPHMX_HOSTNAME** specifies the addresses where this multiplexer serves HTTP client communications.

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 explicit address (dot notation)</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IPv6 explicit address using colon notation</td>
<td>2001:0DB8:1:2:3:4:5:6</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:2e66</td>
</tr>
<tr>
<td>IPv6 explicit address using IPv4-suffix notation</td>
<td>3ef0::bee7:9.148.46.102</td>
</tr>
<tr>
<td>IPv4 &quot;any&quot; (four zeroes)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IPv6 &quot;any&quot; (a double colon)</td>
<td>::</td>
</tr>
</tbody>
</table>

     For example, set this to ::,0.0.0.0 to accept "any" address using either IP protocol.

     - **VPHMX_PORT** specifies the port on which the stand-alone Community Mux listens for HTTP client connections, normally port 8082.
• If this Sametime server will support only IPv6 addressing:
  
  [Debug]
  VPMX_DISABLE_CONFIGURATION_UPDATE=1
  VPMX_HOSTNAME=::
  VPMX_PORT=1533
  VPHMX_HOSTNAME=::
  VPHMX_PORT=8082

5. Save and close the file.
6. Restart the Community Mux so your changes can take effect.

Load-balancing client connections to multiplexers (optional):

Dynamically load-balancing connections to multiple Community Services multiplexers is an optional procedure.

Set up load balancing in one of these ways:

• Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Community Services multiplexer machines to a single DNS name.
  
  For example, associate the IP address of Community Services multiplexer machine 1 (192.0.2.10) and Community Server multiplexer machine 2 (192.0.2.11) to the DNS name cscluster.sametime.com.

• Set up an IBM WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server Network Dispatcher to distribute connections to the Community Services multiplexer machines. See the documentation for the IBM WebSphere Edge Server for more information.

Related concepts

“Setting up the load-balancing mechanism (rotating DNS or Network Dispatcher)” on page 316

The way in which you set up the load-balancing mechanism varies slightly depending on whether you have deployed Community Server multiplexers on separate machines.

“Rotating DNS Limitations with cached DNS resolve requests” on page 318

This section describes some of the limitations related to setting up a rotating DNS system to load balance connections to the IBM Sametime Community Services cluster.

Clustering Sametime Community Servers

IBM Sametime Community Server clusters provide load balancing and failover functionality for large communities and are part of an IBM Lotus Domino server cluster. Six Domino servers is the maximum number of servers in a cluster, which means the number of Sametime servers in a cluster is also six. Generally, the largest communities can be supported with fewer than six Sametime servers operating in a cluster.

Each Sametime server must belong to just one cluster. Two or more clusters pointing to the same Sametime Server is not supported.

This section explains how to cluster a group of Sametime Community servers, using the example of clustering two servers.
Related concepts
“Clustering Sametime servers for high enterprise availability” on page 227
In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

Setting up the Sametime Community Server cluster:
Create a Domino server cluster, then register Community Servers in the cluster.

Replicating the Domino Directory across all servers in the cluster:
Ensure that the Sametime Community servers in the cluster are part of the same Domino domain by registering them in the same Domino Directory and replicating the directory with all servers in the cluster.

About this task
The Domino Directory must replicate to all Sametime Community Servers to ensure proper functioning of the Domino servers on which Sametime is installed. This is a requirement even if you are maintaining the user community in an LDAP directory on a separate server that is not part of the cluster.

Procedure
Creating a Domino server cluster:
A Sametime Community Server cluster runs on Domino. If you are unfamiliar with the functioning of Domino clusters, see the Lotus Domino Administrator Help, available from the Documentation Library at www.lotus.com/ldd.

Before you begin
1. Install the Sametime Community Servers that will be part of the cluster, as described in Installing a Sametime Community Server and supporting software.
2. Replicate the Domino Directory across all servers in the cluster.
3. Verify that you have at least "Author" access and "Delete Documents" rights specified in the Domino Directory's ACL, and at least "Author" access in the Administration Requests database ACL.

About this task
Follow these basic steps to create a Sametime Community Server cluster running on Domino.

Procedure
1. On one of the Sametime servers, start the Domino administrator client.
   To start this client on a Microsoft Windows machine, click Start > Run and type nlnotes.exe adminonly.
2. When the administrator client starts, make sure the Sametime server is the current server.
3. Click the Configuration tab.
4. In the Tasks pane, expand Server and click All Server Documents.
5. In the Results pane, select the servers you want to add to the cluster. Select both Sametime servers that you installed in the previous step.
6. Click Add to Cluster.
7. In the Cluster Name dialog box, click Create New Cluster, and then click OK.
8. Type the name of the new cluster and then click OK.
9. Choose Yes to add the servers to the cluster immediately. The cluster information is immediately added to the Domino Directory of the server that you used to create the cluster.

Results

If the server you used to create the Domino cluster is part of the cluster, the server immediately starts the cluster processes and replicates its Domino Directory with another server in the cluster. This process informs other servers in the cluster that they are a part of the cluster. If you did not use a cluster member to create the cluster, this process starts when the Domino Directory of the server you used to create the cluster replicates with the Domino Directory of a server in the cluster.

Verifying that a cluster was created properly:

About this task

You can do the following to verify the cluster was created correctly:

<table>
<thead>
<tr>
<th>Action</th>
<th>What you should see</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Domino Administrator, expand Clusters in the Server pane.</td>
<td>The name of the cluster followed by the names of the cluster servers.</td>
</tr>
<tr>
<td>1. From the Domino Administrator, click the Configuration tab, expand Cluster, and then click Clusters.</td>
<td>1. The name of the cluster followed by the names of the cluster servers displayed in the Results pane.</td>
</tr>
<tr>
<td>2. In the Results pane, open the Server documents of the servers you added to the cluster.</td>
<td>2. The name of the cluster in the Cluster name field on the Basics tab.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the Server pane, and then click the Server - Status tab.</td>
<td>CLDBDIR (the Cluster Database Directory Manager) and CLREPL (the Cluster Replicator) in the Task list.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the Server pane, and then click the Files tab.</td>
<td>The title &quot;Cluster Directory&quot; and the file name &quot;cldbdir.nsf&quot; to show that Domino created the Cluster Database Directory.</td>
</tr>
<tr>
<td>Compare the replica IDs of the Cluster Database Directories on each cluster server.</td>
<td>The same replica ID on each server.</td>
</tr>
</tbody>
</table>

Creating a cluster document in the Configuration database (stconfig.nsf):

The cluster document enables the servers in a cluster to operate as part of the cluster, and enables servers outside of the cluster (but still within the community) to communicate with the cluster.
About this task

Creating a cluster document in the IBM Sametime Configuration database (stconfig.nsf) is one of the tasks associated with Setting up a Community Services cluster without clustering the Meeting Services.

The Sametime administrator must manually create a cluster document in the Sametime Configuration database (stconfig.nsf) on a Sametime server in the Community Services cluster. The cluster document defines the Community Services cluster.

The cluster document stores the following information:

- The Community Services cluster name.
- The DNS name assigned to the rotating DNS system or IBM WebSphere Edge Server that performs the load-balancing operations.
- A list of all servers in the Community Services cluster.

To create the cluster document in the Sametime Configuration database:

Procedure

1. Using an IBM Lotus Notes client, open the Sametime Configuration database (stconfig.nsf) that replicates between the Sametime servers in the cluster.
2. Click Create > Cluster Information.
3. In the Cluster Name field, type the cluster’s name.
   The cluster is named at your discretion. You can name the cluster after one of the servers in the cluster, but it is not mandatory. If you do name the cluster after one of the servers in the cluster, keep the following points in mind:
   - You might save time when you add the cluster name to the Sametime server field of each user’s Person document to configure client connectivity because users will already have that server name listed in their Person documents (or LDAP directory person entries).
   - Use the IBM Domino full canonical name of the server when entering the name in the Cluster Name field (for example, cn=servername/ou=organizational unit/o=organization).
   - The cluster name must not contain a comma.
4. In the DNS Name field, enter the fully qualified DNS name for the cluster. This name must be the DNS name of the rotating DNS system or the WebSphere Edge Server Network Dispatcher that performs the load balancing operations for the clustered Community Services.
5. In the List of Servers in Cluster field, type the names of all the servers that are part of the cluster. The names must be entered in the IBM Lotus Domino full canonical name format (do not use the fully qualified DNS names in this field). Separate the server names with a semicolon and a space, as in: cn=sametimeserver1/ou=west/o=acme; cn=sametimeserver2/ou=west/o=acme
6. Save and close the cluster document.
   Leave the Configuration database open. In the next procedure, you will copy the new Cluster Information document to all other Sametime servers within the Sametime community (because the stconfig.nsf database is not replicated).

Copying a cluster document to all Sametime Community servers:

Each Sametime Community server cluster has a Cluster Information document, which was created on one Sametime server in the cluster. Every server in the IBM
Sametime community must have a copy of this Cluster Information document, even if the server is not part of a cluster. The document allows users to share presence and instant messaging capabilities with all other users in the community, regardless of their home server assignment.

**About this task**

If you have multiple clusters in a single community, there are multiple Cluster Information documents and every server in the community must have a copy of all of them. Creating separate clusters for different locations is more efficient because you avoid replicating databases in real-time across a WAN connection. For example, you could have one cluster for your Dublin office users and another for your Paris office users.

Follow these steps to copy each Cluster Information document to all other Sametime Community servers in the community.

**Important:** Do not replicate the Configuration database. The Configuration database contains some fields that cannot be replicated to all Sametime servers in a community.

**Procedure**

1. If necessary, open the Sametime Configuration database (stconfig.nsf) in which you created the Cluster Information document that defines the cluster.
2. Copy the Cluster Information document:
   a. Locate "Cluster Information" in the **Form Name** column of the Configuration database.
   b. In the Cluster Information's **Last Modified Date** column, right-click on the date that represents the Cluster Information document you want to copy.
   c. Select **Copy**.
   d. Click **File > Close** to close the Configuration database.
3. Paste the Cluster Information document into the Configuration database on each Sametime server in the community:
   a. From the Lotus Notes client, click **File > Database > Open**.
   b. In the **Server** field, type the name of another Sametime server in the community.
   c. Click **Open**.
   d. In the **Database** list, select the Configuration database (stconfig.nsf).
   e. Click **Open**.
   f. Click **Edit > Paste** to paste the Cluster Information document into the Configuration database on this Sametime server. The document name and date will appear in the **Last Modified Date** column of **Form Name** section in the Configuration database.
   g. Save and close the Configuration database.
4. Repeat step 3 for every Sametime server in the Sametime community.
5. Repeat this set of steps until all Cluster Information documents have been copied to all servers in the community.

**What to do next**

Ensure that clients can access the Community Services cluster by configuring client connectivity for the Community Services cluster.
Registering a Community Server cluster on AIX, Linux, Solaris, and Windows:

After configuring a cluster of Sametime Community Servers on IBM AIX, Linux, Sun Solaris, or Microsoft Windows, register the cluster with the Sametime System Console, so you can manage all of the Sametime servers from a central location.

Before you begin

Make sure each of these servers is ready for the cluster registration task:
• Each of the Sametime Community Servers in the cluster must be registered with the Sametime System Console (which occurred when you used a deployment plan to install them)
• Each Community Server must be started.
• The Sametime System Console must be started.
• The LDAP server must be started, and must be connected to the Sametime System Console.

Procedure
1. If you just configured cluster settings for a group of Sametime Community Servers, restart all of the cluster members now so the cluster goes into effect before you continue.
2. Run the registration utility using the following command:
   AIX and Solaris
   registerSTCluster.sh
   Linux
   /your_path/notesdata/console/registerSTCluster.sh
   Windows
   registerSTCluster.bat
3. As the registration utility runs, you will be prompted to enter the following information:

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Type the name you created when you configured the cluster, and press Enter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of notes.ini file</td>
<td>This is the user name and password that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the full path to the directory containing the notes.ini file, and press Enter. For example, on Windows: C:\Lotus\Domino</td>
</tr>
<tr>
<td>Lotus Domino administrator user name</td>
<td>This is the account that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the Lotus Domino administrator's user name, and press Enter.</td>
</tr>
<tr>
<td>Lotus Domino administrator password</td>
<td>Type the password associated with the Lotus Domino administrator user account, and press Enter.</td>
</tr>
</tbody>
</table>

The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory.
4. Restart the Sametime Community Server where you ran the registration utility.
Creating a community ID for all nodes in a cluster:

To ensure that clients recognize all nodes in a cluster as belonging to a single community, you must add an ST_COMMUNITY_ID value to sametime.ini.

About this task

Follow these steps to add the same ST_COMMUNITY_ID parameter to each Community Server node in a cluster. Doing so prevents clients from creating redundant communities for servers that are in the same cluster.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server installation directory. The default directories are listed below:
   - AIX: /local/notesdata
   - Linux: /local/notesdata
   - Solaris: /local/notesdata
   - Windows: C:\Lotus\Domino
3. In the [Config] section, add the community ID. The value can be any descriptive string, not necessarily a domain name. Use this syntax:
   
   ST_COMMUNITY_ID=community_name

   For example, the following value names the community sametime.example.com:
   
   ST_COMMUNITY_ID=sametime.example.com

4. Save the sametime.ini file.
5. Repeat the procedure for every Community server in the cluster.

Setting up the load-balancing mechanism (rotating DNS or Network Dispatcher):

The way in which you set up the load-balancing mechanism varies slightly depending on whether you have deployed Community Server multiplexers on separate machines.

Setting up the load-balancing mechanism without separate multiplexers:

If you have not deployed Community Server multiplexers on separate machines, you have two choices for setting up the load balancing mechanism.

- Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Sametime server machines to a single DNS name.

  For example, associate the IP address of Sametime server 1 (11.22.33.66) and Sametime server 2 (11.22.33.77) to the DNS name ccluster.sametime.com.

- Set up an IBM WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server Network Dispatcher to distribute connections to the Sametime Community servers. For more information, see the WebSphere Edge Server documentation, available at the website www.redbooks.ibm.com (and also provided with the WebSphere Edge Server).

The diagram below shows the Sametime servers with the rotating DNS system in place. Note that the WebSphere Edge Server can be used in place of the rotating DNS system.
Setting up the load-balancing mechanism with stand-alone multiplexers:

If you have deployed stand-alone Community Server multiplexers, you have two choices for setting up the load balancing mechanism.

- Set up a rotating DNS system to accomplish load balancing. Use rotating DNS to associate the IP addresses of the Community Services multiplexer machines to a single DNS name.
  
  For example, associate the IP address of Multiplexer Machine 1 (11.22.33.44) and Multiplexer Machine 2 (11.22.33.55) to the DNS name cscluster.sametime.com.

- Set up a WebSphere Edge Server (Network Dispatcher) in front of the Sametime servers that you intend to cluster. Use the WebSphere Edge Server Network Dispatcher to distribute connections to the multiplexer machines. For more information, see the WebSphere Edge Server documentation, available at the website www.redbooks.ibm.com (and also provided with the WebSphere Edge Server).

The diagram below shows the Community Services multiplexers with the rotating DNS system in place. Note that the WebSphere Edge Server can be used in place of the rotating DNS system.
Rotating DNS Limitations with cached DNS resolve requests:

This section describes some of the limitations related to setting up a rotating DNS system to load balance connections to the IBM Sametime Community Services cluster.

Ideally, as users connect to the rotating DNS system, consecutive attempts to resolve a cluster name will result in an even distribution of connections to the servers in the cluster. In practice, the DNS caching mechanism can cause Sametime Connect to repeatedly attempt connections to the same server in the cluster. If a server fails, and the DNS resolve requests are cached, IBM Sametime Connect might attempt to reconnect to the server that is down instead of failing over to a different server.

The Sametime Connect client's **Sametime Connectivity** settings control whether the client attempts to connect to the Sametime server through a proxy server or attempts a direct connection to the Sametime server. These connectivity settings affect the failover behavior when DNS resolve requests are cached. This behavior varies for the IBM Sametime Connect for the desktop client and the IBM Sametime Connect for browsers client.

The failover behavior of the Sametime Connect clients when DNS resolve requests are cached is discussed below.

**Sametime Connect for the desktop**

When the DNS resolve requests are cached and a server fails, Sametime Connect for the desktop automatically attempts to connect to another server in the cluster.
When any of the following settings are selected on the **Sametime Connectivity** tab, a successful connection to the cluster depends on the client machine and its settings:

- Direct connection using standard Sametime protocol
- Use SOCKS4 proxy with "Resolve server name locally" checked
- Use SOCKS5 proxy with "Resolve server name locally" checked
- Direct connection using HTTP protocol

If Sametime Connect cannot reconnect to the cluster when these settings are selected, the user can try any of the following options:

- On Windows 2003 machines, change the registry key that controls the cache time for DNS requests so the DNS requests are cached for only one second:
  1. Start the registry editor and open `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters`
  2. Change the value of the registry key "MaxCacheEntryTtlLimit" to "1"
- In the Sametime Connect client's **Sametime Connectivity** settings, change the name in the **Host** setting from the cluster name to the name of a specific server within the cluster.

When any of the following settings are selected in the **Sametime Connectivity** tab, a proxy server resolves the cluster name. Resolving the cluster name depends on the settings of the proxy server. The proxy server might return a valid server name in the cluster, or it might return the address of the server that is already down.

- Use HTTP proxy
- Use HTTPS proxy
- Use SOCKS4 proxy with "Resolve server name locally" unchecked
- Use SOCKS5 proxy with "Resolve server name locally" unchecked

If Sametime Connect cannot reconnect to the cluster when these settings are selected, check the settings on the proxy server to verify the proxy is attempting to connect to the servers within the cluster in rotating order.

When **Use my Internet Explorer browser settings** is selected in the **Sametime Connectivity** tab, the behavior of the client depends on the proxy connectivity settings of the Microsoft Internet Explorer web browser.

- If the browser settings do not specify a proxy server, the client attempts a Direct connection using HTTP protocol. If the client is unable to reconnect following a server failure, the user can try any of the options listed for Direct connection using HTTP protocol above.
- If the browser settings specify an HTTP proxy server, the HTTP proxy server resolves the cluster name. If the client cannot reconnect, check the settings on the proxy server to verify the proxy is attempting to connect to the servers in the cluster.

**Sametime Connect for browsers**

With Sametime Connect for browsers, the client resolves the cluster name when any of the following options are selected:

- Direct connection using standard Sametime protocol
- Direct connection using HTTP protocol
- Use SOCKS4 proxy with "Resolve server name locally" checked
- Use SOCKS5 proxy with "Resolve server name locally" checked

If Sametime Connect for browsers cannot reconnect to the cluster when these settings are selected, the user should do the following:
- On Windows NT and Windows 98 machines, restart the Sametime Connect client or restart the web browser.
- On Windows 2000 machines, change the registry key that controls the cache time for DNS requests so that DNS requests are cached for only one second:
  1. Start the registry editor and open HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters
  2. Change the value of the registry key "MaxCacheEntryTtlLimit " to "1"
- In the Sametime Connect client's Sametime Connectivity settings, change the name in the Host field from the cluster name to the name of a specific server within the cluster.

When any of the following settings are selected in the Sametime Connect for browsers Sametime Connectivity tab, a proxy server resolves the cluster name. Resolving the cluster name depends on the settings of the proxy server. The proxy server might return a valid server name in the cluster, or it might return the address of the server that is already down.
- Use SOCKS4 proxy with "Resolve server name locally" unchecked
- Use SOCKS5 proxy with "Resolve server name locally" unchecked
- Use HTTP proxy
- Use HTTPS proxy

If Sametime Connect cannot reconnect to the cluster when these settings are selected, check the proxy settings to verify the proxy is attempting to connect to the servers in the cluster in rotating order.

When Use my browser settings is selected in the Sametime Connectivity tab, the behavior of the client depends on the proxy connectivity settings of the web browser.
- If the browser settings do not specify a proxy server, the client attempts a Direct connection using standard Sametime protocol or a Direct connection using HTTP protocol. If the client is unable to reconnect following a server failure, the user can try any of the options listed for Direct connection using standard Sametime protocol and Direct connection using HTTP protocol above.
- If the browser settings specify a SOCKS proxy server, and the client is unable to reconnect following a server failure, the user can try any of the options listed for the Use SOCKS4 and Use SOCKS5 proxy settings above.
- If the browser settings specify an HTTP or HTTPS proxy server, the proxy server resolves the cluster name. If the client cannot reconnect, check the settings on the proxy server to verify the proxy is attempting to connect to the servers in the cluster.

Adding a server to the Community Server cluster:

You can add IBM Sametime Community servers to an existing cluster.

Procedure
1. Follow these steps to ensure sure that all databases have the same replica ID.
a. Add the Sametime Community Server to the IBM Lotus Domino server cluster following the guidelines described in Creating a Domino server cluster.

2. Update the Cluster Information document and copy the updated document to all Sametime Community servers in the community:

   a. Add the name of the new Sametime server to the **List of Servers in Cluster** field in the Cluster Information document in the Configuration database (stconfig.nsf) on one Sametime server.

       Enter the server name in the Domino full canonical name format (for example, `cn=servername/ou=organizational unit/o=organization`). Do not use the fully qualified DNS name in this field.

       The list includes every Sametime server in the cluster; separate the server names with a semicolon and a space as shown in the example below:

       `cn=sametimeserver1/ou=west/o=mycompany; cn=sametimeserver2/ou=west/o=mycompany`

   b. Copy the updated Cluster Information document and paste it into the Configuration database on every Sametime server in the community (both clustered servers and non-clustered servers).

       **Note:** After pasting the new Cluster Information document in the Configuration database, you can delete the previous version of the Cluster Information document.

3. Optional: You can deploy a stand-alone Sametime Community Mux to ensure the connection load for your Community Services cluster is handled efficiently. However, if you do not deploy another Community Services multiplexer, the existing Community Services multiplexers can still make connections to the newly added Sametime server.

   If you deploy a stand-alone Sametime Community Mux, make sure to update the Community Connectivity configuration document on every Sametime server in the cluster and include the IP address of the new multiplexer.

### Configuring Sametime Community Server connectivity

Define the host names and ports for Community Services on the IBM Sametime Community Server.

#### About this task

Community Services supports all presence (or awareness) and text chat activity in a Sametime community. Any Sametime client that contains a presence list must connect to Community Services on the Sametime Community Server.

Community Services includes:

- Client login requests
- Connections from clients that access the Sametime server through a direct TCP/IP connection, or a HTTP, HTTPS, or SOCKS proxy server. Community Services clients connect to the Community Services multiplexer component, which is deployed on a separate machine from the Sametime Community Server.
- Directory access for user name search and display.
- Directory access to compile lists of all servers and users in the community.
- Dissemination of presence and chat data to all users connected to Community Services.
- Maintenance of privacy information for online users.
- Connections from the Community Services on other Sametime Community servers when multiple servers are installed.
- Logging of server community events to the Sametime log (stlog.nsf).

This must be completed separately for each server within a Sametime Community Server cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click *Sametime System Console > Sametime Servers > Sametime Community Servers*.
3. In the *Sametime Community Servers* list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the *Connectivity* tab.
5. Under *Server Connections*, type the fully qualified *Host Name* and *Port* for the internal Sametime processes to communicate with one another. Community Services listens for direct TCP/IP connections from Community Services of other Sametime Community Servers on this port. If you have installed multiple Sametime servers, this port must be open for presence, chat, and other data to pass between the servers.
6. Under *Client Connections*, type the fully qualified *Host Name* and *Port* from which Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients. A direct TCP/IP connection occurs when the Sametime client uses a unique Sametime protocol over TCP/IP to establish a connection with the Community Services.
7. Under *HTTP Tunneled Client Connections*, type the fully qualified *Host Name* and *Port* from which Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. Port 8082 ensures compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime server, the client might attempt this connection on port 8082.
8. If you will be using previous version of the Sametime Meeting Room client, click *Enable pre 8.5 releases of the Meeting Room client to try HTTP Tunneling to the Community Server after trying other options*.
9. Under *HTTPS Tunneled Client Connections*, type the fully qualified *Host Name* and *Port* from which the Community Services clients attempt HTTPS connections when accessing the Sametime Community Server through an HTTPS proxy server. If a Community Services client connects to the Sametime Community server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted.
10. Click *OK*.
11. Restart the Sametime Community Server for settings to take effect.

**Updating Sametime Community Server connection properties on the console:**

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Community Server.
About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Community Server. These settings are only used by the Sametime System Console to connect to the Sametime Community Server.

If you are configuring the Sametime Community Server to use SSL (Secure Socket Layer), make sure the server’s Domino CA certificate has been added to the Sametime System Console's trust store using the Integrated Solutions Console (Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates). See the WebSphere Application Server information center for more information on adding certificates to a trust store.

Follow these steps to update connection setting information.

Procedure
1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's User name and Password for connecting to the Sametime Community Server.
5. Enter the HTTP port (typically 80) and HTTPS port (typically 443).
6. By default, the Sametime Community Server trusts other Sametime components. If you want to change this setting, then select Do not auto-accept SSL certificate.
7. Click Save.
8. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Ports used by the Sametime Community Server:

IBM Sametime uses a number of ports on the server. This topic lists the default ports and their uses.

You can use the Sametime Administration Tool to configure the ports on which the Sametime services listen for connections from clients.

The port settings for all services can be accessed from the Configuration > Connectivity > Networks and Ports options of the Sametime Administration Tool.

HTTP Services, Domino Services, LDAP Services, and Sametime intraserver ports

The following ports are used by the Sametime HTTP Services, IBM Lotus Domino Application Services, and LDAP Services.
<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 80</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Community Services multiplexer on the Sametime Community Server listens for HTTP connections from web browsers, Sametime Connect clients, Sametime Meeting Room clients, and Sametime Recorded Meeting clients on port 80. If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server listens for HTTP connections on this port.</td>
</tr>
<tr>
<td>Alternate HTTP port (8088)</td>
<td>If the administrator allows HTTP tunneling on port 80 during the Sametime installation (or afterward), the Domino HTTP server on which Sametime is installed must listen for HTTP connections on a port other than port 80. The Sametime installation changes the Domino HTTP port from port 80 to port 8088 if the administrator allows HTTP tunneling on port 80 during a Sametime Community Server installation. <strong>Note:</strong> If the administrator allows HTTP tunneling on port 80 during the Sametime installation, web browsers make HTTP connections to the Community Services multiplexer on port 80, and the Community Services multiplexer makes an intraserver connection to the Sametime HTTP server on port 8088 on behalf of the web browser. This configuration enables the Sametime Community Server to support HTTP tunneling on port 80 by default following the server installation.</td>
</tr>
<tr>
<td>Port 389</td>
<td>If you configure the Sametime Community Server to connect to an LDAP server, the Sametime Community Server connects to the LDAP server on this port.</td>
</tr>
<tr>
<td>Port 443</td>
<td>The Domino HTTP server listens for HTTPS connections on this port by default. This port is used only if you have set up the Domino HTTP server to use Secure Sockets Layer (SSL) for web browser connections. To configure the Sametime HTTP server to use SSL for Web browser connections, see About SSL and Sametime.</td>
</tr>
<tr>
<td>Port 1352</td>
<td>The Domino server on which Sametime is installed listens for connections from Notes clients and Domino servers on this port.</td>
</tr>
<tr>
<td>Port 9092</td>
<td>The Event Server port on the Sametime Community Server is used for intraserver connections between Sametime components. Make sure that this port is not used by other applications on the server.</td>
</tr>
</tbody>
</table>
### Default Port

**Port 9094**

**Purpose**

The Token Server port on the Sametime Community Server is used for intraserver connections between Sametime components.

If this port is used by multiple applications, refer to the topic “Token server port” on page 329 for a discussion on resolving access to this port.

### Community Services ports

The following ports are used by the Sametime Community Services. Most of these ports are configurable.

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1516</td>
<td>Community Services listens for direct TCP/IP connections from the Community Services of other Sametime Community Servers on this port. If you have installed multiple Sametime Community servers, this port must be open for presence, chat, and other Community Services data to pass between the servers. The communications that occur on port 1516 also enable one Sametime Community Server to start a meeting on another server (or “invite” the other server to the meeting).</td>
</tr>
<tr>
<td>Default Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Port 1533    | The Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients (such as Sametime Connect and Sametime Meeting Room clients) on this port.  
*Note:* The term “direct” TCP/IP connection means that the Sametime client uses a unique Sametime protocol over TCP/IP to establish a connection with the Community Services.  
The Community Services also listen for HTTPS connections from the Community Services clients on this port by default. The Community Services clients attempt HTTPS connections when accessing the Sametime Community Server through an HTTPS proxy server. If a Sametime client connects to the Sametime Community Server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted.  
If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Community Services clients attempt HTTP-tunneled connections to the Community Services on port 1533 by default. |
| Port 80      | If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 80.  
*Note:* When HTTP tunneling on port 80 is allowed during the Sametime installation, the Community Services multiplexer listens for HTTP-tunneled connections on both port 80 and port 1533. The Community Services multiplexer simultaneously listens for direct TCP/IP connections on port 1533. |
Default Port
Port 8082

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>When HTTP tunneling support is enabled, the Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer on port 8082 by default. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. Port 8082 ensures backward compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime Community Server, the client might attempt this connection on port 8082.</td>
</tr>
</tbody>
</table>

*Changing the HTTP port of a Domino HTTP server:*

IBM Sametime installs on an IBM Lotus Domino server and uses the HTTP server provided with Domino.

**About this task**

During a Sametime installation, the administrator can allow HTTP tunneling on port 80. To support the HTTP tunneling on port 80 functionality, the Community Services multiplexer on the server listens for HTTP connections from clients (including web browsers) on port 80. A web browser connects to the Community Services multiplexer on port 80, and the Community Services multiplexer makes an intraserver connection to the Domino HTTP server on behalf of the web browser.

If the administrator allows HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server must listen for HTTP connections on a port other than port 80. In this scenario, the Sametime server installation programmatically changes the HTTP port of the Domino HTTP server to port 8088 during the Sametime installation process. It is not necessary to manually change the setting.

If the administrator does not allow HTTP tunneling on port 80 during the Sametime installation, the Domino HTTP server listens for HTTP connections on port 80 by default.

On some platforms, you can configure Sametime to operate using a Microsoft IIS HTTP server or IBM WebSphere HTTP server. For information on setting up Sametime to use a different HTTP Web server, see "Sametime Server Installation."

Follow these instructions if you need to change the HTTP port of the Domino HTTP server:

**Procedure**

1. Open the Sametime Administration Tool.
2. Select **Configuration > Connectivity > Networks and Ports**.
3. Select **Configure HTTP Services on a web page in its own window**.

4. Select **Ports**.

5. Select **Internet Ports**.
   
   If the Domino server is set up for HTTP connections from web browsers, you can change the **TCP/IP port number** setting, located under the **Web (HTTP/HTTPS)** column of the settings. To change the port used by the HTTP server, change the port associated with the **TCP/IP port number** field. (For example, if you are enabling HTTP tunneling on port 80 on a Sametime server that includes a single IP address, you may want to change the HTTP port from port 80 to 8088.)

6. Select **Internet Protocols**.

7. Select **Domino Web Engine**.

8. Under the **Generating References to this server** section, make the following changes:
   
   If the HTTP server uses HTTP for web browser connections:
   
   - In the **Protocol** setting, select **http**.
   - In the **Port number** field, enter the same port entered in the **TCP/IP port number** setting in Step 5.

9. Click **Save and Close** to save the Server document.

10. Change the port number in the stconvservices.properties file to match, as the HTTP port is pulled from this setting.

11. Restart the Domino server for the change to take effect.

**Event server port:**

The "Event server" port (default 9092) is used for intraserver connections between components of the IBM Sametime server.

Generally, it is only necessary to change this port if you have installed multiple Sametime servers on a single server machine or if another application on the server uses port 9092.

**Note:** If you run Sametime on an IBM i, Linux, Sun Solaris, or IBM AIX machine, you can install multiple Sametime servers on a single machine, within the same logical partition. Each Sametime server instance runs on a separate partitioned IBM Lotus Domino server. If you run Sametime on Microsoft Windows, you can only install one server on each Windows machine.

If multiple Sametime servers are running on the same machine, you must ensure that each Sametime server specifies a different port as the "Event server" port. For example, if Sametime server 1 and Sametime server 2 are running in separate partitions of an IBM i machine, you can specify port 9092 as the "Event server" port for Sametime server 1 and port 9095 as the "Event server" port for Sametime server 2. Sametime for IBM i provides an option to specify the "Event server" port at the time you configure your Sametime server.

**Assigning IP addresses to multiple servers installed on a single computer:**

If you install multiple IBM Sametime servers on a single computer, you must assign a distinct IP address to each server.
If you are operating Sametime on an IBM i, IBM AIX, Linux, or Sun Solaris server, you can install multiple Sametime servers on a single computer, within the same logical partition. In this scenario, each Sametime server instance runs on a separate partitioned IBM Lotus Domino server.

**Note:** Do not install multiple Sametime servers on a Microsoft Windows server as that configuration is not supported.

When multiple Sametime servers are running on separate Domino partitions within the same logical partition of an IBM i server, it is important for each Sametime server to be assigned a separate IP address. If you are also running any other Domino servers or HTTP servers within the same logical partition, you must also be certain that those servers are assigned separate IP addresses to avoid port conflicts.

*Token server port:*

The “Token server” port (default 9094) is used for intraserver connections between components of the IBM Sametime server.

Generally, it is only necessary to change this port if you have installed multiple Sametime servers on a single server machine or if another application on the server uses port 9094.

**Note:** If you run Sametime on an IBM i, Linux, Sun Solaris, or IBM AIX machine, you can install multiple Sametime servers on a single machine within the same logical partition. Each Sametime server instance runs on a separate partition of the IBM Lotus Domino server. If you run Sametime on Microsoft Windows, you can only install one server on each Windows machine.

If multiple Sametime servers are running on the same machine, you must ensure that each Sametime server specifies a different port as the “Token server” port. For example, if Sametime server 1 and Sametime server 2 are running in separate partitions of an IBM i machine, you might want to specify port 9094 as the “Token server” port for Sametime server 1 and port 9096 as the “Token server” port for Sametime server 2. Sametime for IBM i provides an option to specify the Token server port at the time you configure your Sametime server.

For more information, see Assigning IP addresses to multiple Sametime servers installed on a single server machine.

### Configuring LDAP and Domino connections

Configure the IBM Sametime Community Server to work with LDAP and Domino directories.

#### Excluding certain domains from user and group directory lookups:

When you use Inbox awareness, you can prevent redundant requests to the LDAP or Domino directory by defining which domains are allowed to accept resolve requests. Previous releases allowed this filtering through the use of custom code and was available only for LDAP directories.

**About this task**

Use either `ST_RESOLVE_BLACKLIST` or `ST_RESOLVE_WHITELIST` parameters to define domains to be excluded or included in resolve requests. The default
setting is blank for each list, which results in all requests being accepted.

**Procedure**

1. Open the `sametime.ini` file in a text editor. By default the file is located in the Sametime Community Server installation folder.
2. In the [Config] section of the `sametime.ini` file, decide if you want to exclude domains with the `ST_RESOLVE_BLACKLIST` parameter or include domains with the `ST_RESOLVE_WHITELIST` parameter.
3. Enter a comma-delimited list of domains to exclude or include in resolve requests. You can use wildcard characters. The limit for the list is 64,000 characters.
   For example, this list excludes requests with email addresses from the `external.org` domain and its sub-domains:
   ```plaintext
   ST_RESOLVE_BLACKLIST=*.external.org
   ```
4. Save and close the file.
5. Restart the Sametime Community Server.

**Example**

**Resolve requests from internal domains and sub-domains**

The following example resolves requests with email addresses from the `domain1.org` or `domain2.org` domains and their sub-domains:

```plaintext
[Config]
ST_RESOLVE_WHITELIST=*.domain1.org,*.domain2.org
```

**Resolve requests from internal domains without including sub-domains**

The following example resolves requests with email addresses from the `domain1.org` or `domain2.org` domains without their sub-domains:

```plaintext
[Config]
ST_RESOLVE_WHITELIST=domain1.org,domain2.org
```

**Specifying a user's login ID:**

Specify an LDAP attribute that is appropriate for logging in to IBM Sametime. If you do not perform these steps, the default LDAP attribute, `DN`, is used.

**About this task**

Determine the value of the LDAP attribute of the person entry that defines the internal ID of a Sametime user that is appropriate for logging in to Sametime. The Sametime user ID attribute must be identical on all the Community servers in the community. This task must be completed separately for each server within a Sametime Community Server cluster.

To avoid running the name change tool in the future, you can select an LDAP attribute that is not likely to change when users change their name or relocate. Here are examples of stable attributes in some well-known LDAP servers:

- **IBM Directory Server:** `ibm-entryUUID`
- **Domino LDAP:** `dominounid`
- **Novell Directory Server (NDS):** `guid`
- **SunOne:** `nsuniqueid`
• Active Directory: objectGUID

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. Under LDAP Attributes, enter the name of the field within the LDAP person entries that contains the ID used for logging in the Attribute used for determining the internal user ID field.
6. Click OK.
7. Restart the Sametime Community Server for settings to take effect.

Defining the ID attribute for Active Directory:

If your Sametime servers connect to an Active Directory (LDAP) server and you prefer to use the DN attribute rather than the objectGUID attribute for the Sametime internal user ID, you must assign the DN attribute as the internal ID for Sametime users. Doing so guarantees that Active Directory returns the DN attribute in the same case-sensitive and space-sensitive format. Forcing Sametime to use a consistent attribute for the internal user ID prevents awareness problems caused by ambiguous internal user IDs. Do not use the DN attribute with other LDAP server types.

About this task

If you choose the DN attribute for the Sametime internal user ID, but do not assign the DN attribute as the internal ID, you may see the following problems:
• Awareness for some users does not work.
• A user's name appears multiple times in the same Contact list.
Note that you can assign the objectGUID attribute as the internal user ID to eliminate the need to run the name change tool in the future.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Server.
3. In the Sametime Community Servers list, click the deployment name of the Sametime Community Server.
4. Click the Configuration tab.
5. Under LDAP Attributes for The attribute used for determining the internal user ID, enter the value DistinguishedName.
6. Click OK.
7. Restart the Sametime Community Server so the change can take effect.
Related tasks

“Migrating older user IDs to a unique directory attribute” on page 777

If you are using an older release, you can migrate user IDs to a unique ID, so you do not need to run the name change utility when a person’s name changes in the directory. Having a constant user ID attribute eliminates the need to change a user ID when a name changes.

Creating custom Java classes for searching the LDAP:

Create custom Java classes that provide greater control over how the Sametime Community server conducts name searches of an LDAP directory and how results are formatted.

About this task

Creating a custom Java class can be especially effective with complex LDAP directory schemas. The Java code that you write must be compatible with the Java Run-Time Environment (JRE 1.5.0). In addition to the following topics, the Sametime wiki contains an article on writing Java classes that includes sample search filters.

New and existing custom Java classes for searching the Community Server’s LDAP directory must include the appropriate UUID attribute for the LDAP directory if UUID is used with policy assignments or Sametime user login IDs:

- Lotus Domino LDAP: dominounid
- IBM Tivoli Directory Server: ibm-entryuuid
- Microsoft Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

Example: Writing a Java class to filter searches for people and groups:

If a single search filter is not adequate to resolve user or group name searches, you can write a Java class containing a method that specifies exactly how directory searches are conducted. The class can invoke different LDAP search filters depending on search criteria entered by users.

About this task

The Search filter for resolving person names and the Search filter for resolving group names settings in the LDAP directory settings of the Sametime Administration Tool define the LDAP directory search filters responsible for selecting user and group names from the LDAP directory.

Note: You do not have to write Java classes to control the search behavior for both users and groups. You can use a Java class to control the search behavior for users while using a single LDAP search filter to control the search behavior for groups, or vice versa.

The specific source code that you write to support customized LDAP searches is entirely dependent on your environment. This section provides a code sample to help you understand how to write the Java class appropriate for your environment.
Note: The searched name must be escaped according to LDAP RFC2254 before adding it to the created LDAP filter. Use the escape and the isHex methods as is from the following example.

Example

The following example invokes different LDAP directory search filters based on the text string that is entered into the Sametime user interface by a user. The search filters invoked by the method are dependent on the directory schema and the search behavior needed for the environment. Assume that three different users want to add the user Victor Lazlow to their Sametime Connect buddy lists. Each of the three users searches for Victor Lazlow in a different way. The logic of the Java class dictates the results of these three user searches:

- **User 1**
  
  **Input:** User 1 enters "Victor L*" into the Sametime client user interface to add Victor Lazlow to the buddy list.
  
  **Results:** This search attempt returns an error because the Java class is programmed to return an error when the user enters a text string that includes an asterisk.

- **User 2**
  
  **Input:** User 2 enters "Victor_Lazlow@acme.com" into the Sametime client interface.
  
  **Results:** This search attempt succeeds and returns the value "Victor_Lazlow@acme.com" (Victor Lazlow's email address) from the LDAP directory. The search attempt succeeds in this way because the Java class is programmed to return an LDAP search filter that can resolve an LDAP directory search to a user's email address. The Java class returns this email address search filter if the search text string entered by the end user includes the "at" character (@).

- **User 3**
  
  **Input:** User 3 enters "Victor L" into the Sametime client interface. This search attempt succeeds and returns the common name (cn) directory attribute of "Victor Lazlow."
  
  **Results:** The search attempt succeeds in this way because the Java class is programmed to return an LDAP search filter that can resolve an LDAP directory search to a user's common name (cn). The Java class returns this common name search filter if the search text string entered by the end user does not include either an asterisk or "at" (@) character.

Sample code

The code sample below shows the Java source code that produces the search behavior described above. This code creates a Java class named "StLdapCustomized" that includes the "peopleResolveFilter" method. The if statements in the peopleResolveFilter method examine the text string entered by the user in the Sametime client user interface and return the appropriate LDAP search filter based on this text string. The comments in the source code explain the purpose of each if statement.

```java
public class StLdapCustomized {

  /**
   * String representing an escaped forward slash sign '/'
   */
  private final static String SLASH_SIGN_CONVERTED = "\5c";
```
/**
 * String representing an escaped 'sign '*'
 */
private final static String STAR_SIGN_CONVERTED = "\\2a";

/**
 * String representing an escaped opening bracket sign '('
 */
private final static String OPENING_BRACKET_SIGN_CONVERTED = "\\28";

/**
 * String representing an escaped closing bracket sign ')'
 */
private final static String CLOSING_BRACKET_SIGN_CONVERTED = "\\29";

/**
 * Escape problematic characters in the name to match the LDAP filter escaping
 * criteria according to RFC2254
 * rfc2254 - The String Representation of LDAP Search
 * @param name the name to escape
 * @return an escaped string
 */
private static String escape(String name)
{
    StringBuffer escapedName = new StringBuffer();
    for (int i=0; i< name.length(); ){
        switch(name.charAt(i)){
            case '\':
            // if the next 2 chars are hex we don't need to escape
            if((i< name.length()-2) && isHex(name.charAt(i+1)) &&
                isHex(name.charAt(i+2))){
                escapedName.append('\');
                escapedName.append(name.charAt(++i));
                escapedName.append(name.charAt(++i));
            } else{
                escapedName.append(SLASH_SIGN_CONVERTED);
                i++;  
                break;
            }
            case '*':
                escapedName.append(STAR_SIGN_CONVERTED);
                i++;
                break;
            case '(':
                escapedName.append(OPENING_BRACKET_SIGN_CONVERTED);
                i++;
                break;
            case ')':
                escapedName.append(CLOSING_BRACKET_SIGN_CONVERTED);
                i++;
                break;
            default:
                escapedName.append(name.charAt(i));   
                i++;
                break;
        }
    }
    return escapedName.toString();
}
Verifies whether this char is a hex char
* @param c
* @return
*/
private static boolean isHex(char c){
    boolean hex = true;
    hex = !(Character.digit(c, 16) == -1);
    return hex;
}

/**
* Generates a search filter for finding a user, given the user's
* name.
* The searched name is escaped according to LDAP filters escaping rules.
* The checks on the searched name format should be done before escaping the value.
* @param name The user's name as provided by the Sametime client.
* @return The search filter, or null if the name is invalid.
* */

public static String peopleResolveFilter (String name)
{
    String escapedName;
    // prevent users from adding their own wildcards
    if (name.indexOf('*') != -1)
        return null;
    // if name looks like email, do not search with wildcards, and only search in mail attribute
    if (name.indexOf('@') != -1)
    {
        escapedName = escape(name);
        return "(&(objectclass=person)(mail=" + escapedName + ")");
    }
    // otherwise, search as CN with wildcard
    escapedName = escape(name);
    return "(&(objectclass=person) (cn=" + escapedName + ")");
}

What to do next

After writing your Java class, complete the tasks in this section to integrate the class into the Sametime Community server.

Example: Writing a Java class to format names returned in a search:

To return a user name in a format that is not available in an LDAP directory entry attribute, you can write a Java class that manipulates existing information in the LDAP directory to produce the user name in the desired format.

About this task

In most environments, the value of the **The attribute of the person entry that defines the user's name** setting can specify a common LDAP directory attribute, such as **cn** (common name) or **mail** (email address). When configured in this way, the search returns the value assigned to a user’s cn or mail directory attribute and displays this value in the Sametime client user interface.

To return names in a format different from the LDAP directory attributes, create a custom Java class. For example, you might create a Java class that does the following:
• Combines the values of two LDAP directory attributes to produce the user name in a desired format.
• Edits the information in a single LDAP directory attribute to produce the user name in a format that is different than the value specified by the attribute.

Example

The sample code below shows how to combines the values of the sn and givenName attributes to return a user name with the Last Name shown first, assuming the following requirements:
• LDAP searches must return a user name in the format LastName, FirstName (for example: Smith, John)
• None of the LDAP directory attributes specify the user name in the LastName, FirstName format.
• The LDAP directory attribute sn specifies each user's last name.
• The LDAP directory attribute givenName specifies each user's first name.

Sample code

This example takes values from the sn and givenName directory attributes and combines these values into a single display name in the format of LastName, FirstName.

```java
public class StLdapCustomizedAttributes {

    public static String displayName (String givenName, String sn) {
        String result = sn + ", " + givenName;
        return result;
    }

}
```

What to do next

After writing your Java class, complete the tasks in this section to integrate it into the Sametime Community server.

Adding the new class to the Sametime Community Server:

Add a new Java class to the IBM Sametime Community server by compiling the source code and then copying the class to its new location.

About this task

Follow these steps to add the class to the Sametime Community Server.

Note:

When you use this feature on IBM AIX, Linux, or Solaris, you must compile your class using Java 1.5 or later. This requires you to use IBM Lotus Domino 8.0 or later because earlier versions do not include the right version of Java.
Procedure
1. Compile the Java source code file to produce the Java class file.
2. Copy the compiled class file (StLdapCustomized.class) to the "java"
   subdirectory of the Sametime server installation directory.
   
   The default path for the class file is: c:\Lotus\Domino\java

Adding paths for the new class to the sametime.ini file:

Add the path for your new custom Java class to the sametime.ini file so that the
IBM Sametime Community Server can locate the new class.

About this task

Edit the sametime.ini file on the Sametime Community Server and add the paths
for the new custom class.

Procedure
1. Use a text editor to open the sametime.ini file, which is stored in the Domino
   installation directory.

   In Microsoft Windows, the default location for this file is: C:\Lotus\Domino

2. Add or modify the following statements to the [Config] section of the file:

   Make sure your file contains all three statements when you finish:

   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\StConfig.jar;
   C:\Lotus\Domino\StConfigXml.jar;C:\Lotus\Domino\xerces.jar;custom_class_directory

   ST_JAVA_JVM_PATH=java_jvm_install_path
   ST_JAVA_CUSTOM_PATH=custom_class_directory

   where:

   • java_jvm_install_path indicates the path where the Java JVM is installed
     (the default path on Windows is: C:\Lotus\Domino\ibm-jre\jre\bin\classic\jvm.dll; on Solaris use this path: ibm-jre/lib/sparc/server/libjvm.so.

     Make sure to use the JVM installed under the ibm-jre folder and not the one
     under the jvm folder.

   • custom_class_directory indicates the path to the new custom Java class. Since
     the jar file is loaded by both C++ and Java-based components, the value
     must be provided in two ways, with the double backslash (\) signs, and
     with single backslash (\) signs. The default path on Windows is
     C:\Lotus\Domino\java;C:\Lotus\Domino\java.

3. Save and close the file.

Adding the custom Java class name and method to the Sametime LDAP settings:

Use the IBM Sametime Administration Tool to add the class name and method of
your new custom Java class to the LDAP settings used by the Sametime
Community Server.

About this task

Use the Sametime Administration Tool to add the new custom Java class to the
LDAP directory settings.
Procedure

1. Log on to the Sametime Community Server as the Sametime administrator.
2. Open the Sametime Administration Tool by clicking Administer the Server.
3. Click LDAP Directory > Basics.
4. In the Search settings for server list, select the LDAP server that contains the LDAP directory you are modifying with your custom Java class.
5. If you are adding a custom Java class that defines a search filter, click Searching and do the following:
   a. In the Search filter for resolving person names settings, enter the class name and method name for a Person filter, using this format: 
      `Classname.methodname()`  
      Following the earlier code example for a Person filter, you would enter `StLdapCustomized.peopleResolveFilter()` for the new class.
   b. In the Search filter for resolving group names settings, enter the class name and method name for a Group filter, using this format: 
      `Classname.methodname()`  
      For example, you might have named your class like this: `StLdapCustomized.groupsResolveFilter()`.
6. If you are adding a custom Java class that formats search results, locate The attribute of the person entry that defines the user's name settings, and enter the class name and method name, using this format: `Classname.methodname()`  
   Following the earlier code example for formatting search results, you would enter `StLdapCustomizedAttributes.displayName(givenName, sn)` for the new class.
7. If you are adding a custom Java class that defines an authentication, policy or business card filter, do the following:
   In the Search filter to use when resolving a user name to a distinguished name settings, enter the class name and method name for this filter, using this format: `Classname.methodname()`  
   Following the earlier code example for this filter, you would enter `StLdapCustomized.authenticationFilter()` for the new class.
8. If you are adding a custom Java class that defines a Policy filter, do the following:
   In the GroupMembership settings, enter the class name and method name for a group membership filter, using this format: `Classname.methodname()`  
   Following the earlier code example for a this filter, you would enter `StLdapCustomized.groupMembershipFilter()` for the new class.
9. After you have added all of your custom Java classes, click Update.
10. Restart the Sametime Community Server for the changes to take effect.

Related tasks
“Creating a customized class for your Sametime Community Server Novell LDAP filters” on page 783
The resolve and the authentication filters need to be customized Java filters.

Preparing the Sametime Community server for users

Before deploying clients, set up the login and licensing requirements that suit your environment.

Assigning users to a home Sametime Community Server:
A user's home Sametime Community Server saves the user's preferences and data. Each user connects to the home server for online presence (or awareness) and chat functionality.

**About this task**

After installing a new Sametime server, you can assign specific users to the new server by entering the name of the new Sametime server in the **Sametime server** field in each user’s Person document. If you install multiple Sametime servers, you can assign different "home" Sametime servers for users in the community. Server-to-server connections among the Community Services of the multiple Sametime servers ensure that all users in the community have presence and chat capabilities with all other users.

Each user's person entry in an LDAP directory must contain a field in which a user's home Sametime Community Server can be specified. You can either:

- Add a new field to the LDAP directory to hold the name of each user's home Sametime Community server. This added field must appear in the person entry of every Sametime user in the LDAP directory.
- Use a field that already exists in the person entries of each Sametime user (such as the email address) for this purpose.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the **Community Services** tab.
5. Under LDAP Attributes, enter the name of the field within the LDAP person entries that contains the name of each user's home Sametime Community server in the **Attribute used for determining the home server** field.

   **Note:** The server name cannot have a comma.
6. Click OK.
7. Restart the Sametime Community Server for settings to take effect.

**Connecting clients to a Community Server cluster:**

After you have created and named a Community Server cluster, ensure that the clients can connect to the cluster by adding the cluster name to a field in each user's Person entry in the LDAP directory.

The configuration fields that affect client connectivity are:

- The "Sametime server" field of the user's Person document in the Domino Directory, or a Sametime cluster field you have added to an LDAP directory.

   **Note:** Sametime uses this field to ensure that a user connects to one of the Sametime servers in the Community Server cluster. This field serves the same purpose as the "home Sametime server" field in the single-server approach to Community Server deployment that was used in previous Sametime releases.
When the Sametime servers are configured to connect to an LDAP directory on an LDAP server (as in this example), the administrator can do one of the following:

- Manually add a field to the LDAP directory to contain the name of the Community Server cluster. The added field must exist in the Person record of every Sametime user in the LDAP directory.
- Use an existing field in the LDAP directory to hold the name of the Community Server cluster. This field must exist in the Person record of every Sametime user in the LDAP directory. In this case, you must specify the cluster name in this field in the LDAP directory.

Note: This example uses the "Sametime server" field of each user's Person document in the Domino Directory as the field that holds the Sametime cluster name. The field you select to hold the name of the Community Server cluster must be specified in the LDAP Directory-Authentication-Name of the Home Server attribute setting in the Sametime Administration Tool. In this example, the "Sametime server" field was specified when you configured the connection to the LDAP server when installing the Sametime servers.

To complete the example, you can enter the cluster name in the "Sametime server" field of each user's Person document in the Domino Directory on the Domino LDAP server. Note that you defined the cluster name when creating a cluster document in the Configuration database.

If you used a server name as the cluster name, you can enter the server name in the Domino hierarchical name format (sametimeserver1/west/acme) when entering the name in the Sametime server field of the Person document.

Forcing users to connect to a home server:

When you are deploying security applications such as FaceTime, you want to ensure that your users connect to their home IBM Sametime Community servers or home clusters. Preventing users from connecting to remote servers is done by specifying trusted IP addresses and rejecting forwarded logins during the login process.

About this task

For users that must log in through FaceTime or similar proxies, the Sametime Community Server should allow them to connect through the home server only. The Sametime Community Mux Server should accept connections that come from Facetime IP addresses only. You must dedicate a specific Mux to a specific server, and limit users to connecting to that Mux through FaceTime only. This applies to local Muxes, as well as standalone Muxes. The following settings should be set on all Muxes in your deployment.

Procedure

1. Use a text editor to open the sametime.ini file located in the Sametime Community server installation directory (for example, root/lotus/domino).
2. In the Connectivity section, add or create a comma-separated list of trusted IP addresses of proxies.
   
   VPMX_TRUSTED_CLIENT_IPS=IPaddress1, IPaddress2
   
   This setting controls which clients are allowed to connect by assigning a comma separated list of IP addresses. An empty list of trusted addresses (default) means the feature is turned off, and that clients from all IP addresses can connect.
3. Create or edit the `VP_REJECT_FORWARDED_LOGINS` setting so that forwarded logins are rejected.
   
   `VP_REJECT_FORWARDED_LOGINS=1` When that setting is set to 1, users must connect to their assigned home servers. This is essential when users must connect through FaceTime.

4. Save the `sametime.ini` file.

Managing client types and logins:

You can manage the manner and order of client logins to IBM Sametime.

Related concepts

“Supporting older Sametime clients during migration” on page 771

Maintaining a flexible login policy during a migration to a new release of IBM Sametime is especially important in environments that include a large number of older Sametime clients. Immediately enforcing a minimum client version can result in a high volume of users experiencing login problems.

Configuring allowed client types:

You can define the types of clients that can connect to the IBM Sametime Community Server.

About this task

Follow these steps to specify the list of client types that are allowed to connect to the Sametime Community Server.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the `sametime.ini` file located in the Sametime Community Server installation directory. For example, the default directory in Windows is `C:\program files\lotus\domino`.
3. In the `Config` section, enter the client type IDs for the allowed client types in the `VPS_ALLOWED_LOGIN_TYPES` flag. If the flag is not specified or its value is empty, then all client types are allowed to connect to the server. Its a comma-separated list.

   Note: Once the `VPS_ALLOWED_LOGIN_TYPES` flag is used, you must update the values whenever you add new client types; otherwise the new client type cannot log in.

   `[Config]
   VPS_ALLOWED_LOGIN_TYPES=130B,130A

   For a list of client types, see Technote 1114318 on the IBM Lotus Support website at http://www.ibm.com/support/docview.wss?uid=swg21114318. For information on adding new client names to match application types and handle unknown type entries that are displayed in Community Logins, see http://www.ibm.com/support/docview.wss?uid=swg21291894.

4. Save the `sametime.ini` file.

Configuring the single login type:

The `single login type` mode means that only one login per user is allowed. When a client attempts to log in to the IBM Sametime Community Server, the server
checks to see if there are any existing logins of the same user, and disconnects
them. Any client on the exclusion list is not disconnected, which is useful for users
who want to run multiple clients simultaneously.

About this task

To configure the single login function and exclude certain client types from
qualifying as logins, edit the sametime.ini file.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server
   installation directory. For example, the default directory in Windows is
   C:\program files\lotus\domino.
3. In the Config section, set the following flag to activate single client login mode:
   VP_ONLY_SINGLE_LOGIN_ALLOWED=1
   If the flag is set to 1 than the server works in the single login allowed mode.
   When a new client login request is received, all the previous logins are
disconnected. Only one client type connection per machine is allowed at one
time (related to client types, not users).
4. Specify which client types are not considered logins when the server checks
   whether to accept or disconnect clients. Separate the client types with commas.
   VPS_EXCLUDED_LOGIN_TYPES=clienttype1, clienttype2
   For a list of client types, see Technote 1114318 on the IBM Lotus Support
   In the following configuration, even though single client login mode is
   activated, logins originating from C++ clients and Unified instant messaging
   clients will not be disconnected if they have logged in from the Sametime client
too.VPS_EXCLUDED>Login_TYPES=1002, 1304
5. Save the sametime.ini file.

Configuring the preferred login list:

If a user is already connected to the IBM Sametime Community Server through
several different clients, and another user attempts to initiate an instant messaging
session with the logged-in user, Sametime uses a default login order to determine
which client type should receive the instant messaging session. A preferred login
list allows you to override the default order.

About this task

The Sametime Community Server depends upon the default list of client types,
each of which has a predefined weight. Login order for each user depends upon
the login-type weight. The first login type, having minimal weight, is the one
provided for the incoming instant messaging session.

Default order of login types on Sametime:

1. Sametime Connect clients
2. Sametime Mobile clients
3. Sametime Proxy clients

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime server installation directory (the default directory in Windows is C:\program files\lotus\domino).

3. In the [Config] section, specify the order of the login types that overrides the default order:

   VPS_PREFERRED_LOGIN_TYPES=login_type1,login_type2

   For example:

   VPS_PREFERRED_LOGIN_TYPES=130C,130B,130A,1308,1306,1304,1436,1435,1434,1433,1432,
   1431,1430,14A3,14A2,14A1,14A0


4. Save the sametime.ini file.

Configuring a mixed-license environment with clients that connect to Sametime Entry servers:

To comply with licensing limitations involving Sametime Entry servers, take steps to configure the mixed environment for two types of clients – those who are licensed to use instant messaging and meetings and those who are licensed only for instant messaging.

Related concepts
“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 248

A mixed-license environment includes a combination of IBM Sametime Entry servers, along with Sametime Standard servers and possibly Sametime Advanced. When you deploy IBM Sametime Entry servers with other types of servers, plan for additional steps to meet the licensing requirements for Sametime Entry, which offers only instant messaging features and does not offer meetings. Sametime Entry users are licensed for instant messaging features only and not Web conferencing. Fully-licensed users for Sametime Standard or Sametime Advanced have access to instant messaging and Web conferencing.

Configuring users in a mixed-license environment with Sametime Entry servers:

In a mixed-license environment that includes IBM Sametime Entry servers, the servers must be configured for the different licensed users.

An instant messaging-only user should have the Sametime Entry server listed as his or her home Sametime server. A fully licensed user should have the Sametime Standard server listed as his or her home Sametime server. To configure the server support of the mixed environment, follow these steps:

1. Create a group for your fully-licensed Sametime Standard users (Web conferencing users). (See the guidelines below.)
2. Change the access control list (ACL) of stsrc.nsf to give anonymous users “no access,” and then add the Web conferencing users group to the ACL with Author access.
3. Change the ACL of stcenter.nsf to give anonymous users “no access,” and then add the web conferencing users group to the access control list with Author access.
4. Change the ACL of stconf.nsf to give anonymous users “no access,” and then add the web conferencing users group to the ACL with Author access.
5. Set the Embedded_client_full_access policy to numeral 1 for the web conferencing users group in stpolicy.nsf.
This configuration prevents the instant messaging-only user from being invited to meetings and from joining meetings, but it also forces all users to authenticate when they create or join a meeting; therefore, Web conferencing users will authenticate twice. It is the policy that will determine if user can invite others. Users will authenticate with their Sametime Connect client and with the Domino server when they join a meeting and launch their web browser.

If the instant messaging-only user tries to attend a meeting, the user receives a message saying he or she is not authorized to join the meeting. If a Web conferencing user tries to invite an instant messaging-only user to an instant meeting, both the Web conferencing user and the instant messaging-only user receive an invitation, but the instant messaging-only user cannot join, receiving a message that he or she is not authorized. The Web conferencing user who initiated the meeting receives no indication that the instant messaging-only user is unable to attend.

Using the Sametime policy service, the groups can be added to a policy that determines whether a user can create instant meetings. If the user does not have this enabled in their policy, they cannot initiate an instant meeting.

Guidelines for creating groups

Use the following guidelines when creating these groups:

- If you want all users licensed to use the standard Sametime servers to have the ability to both create and attend meetings, you can include all standard Sametime server users in a single group.
  If you have a large Sametime community, you can create multiple groups for this purpose. For example, you might create groups named "Meeting Creator Group 1" and "Meeting Creator Group 2."

- If you want some standard Sametime users to have the ability to both create and attend meetings while limiting other standard Sametime servers to attender-only privileges, you must create a minimum of two groups.
  One group must contain the users who can both create and attend meetings and the other group must contain users who can attend meetings but not create them. For example, you might create two groups: one named "Meeting Creators" and one named "Meeting Attenders."
  If you have a large Sametime community, you can create multiple groups for each purpose. For example, you can create two separate groups that contain users who can create and attend meetings and two separate groups that contain users who can only attend meetings. These groups might be named as follows:
  - Meeting Creator Group 1
  - Meeting Creator Group 2
  - Meeting Attender Group 1
  - Meeting Attender Group 2
Related tasks
“Configuring a mixed-license environment with clients that connect to Sametime Entry servers” on page 343
To comply with licensing limitations involving Sametime Entry servers, take steps to configure the mixed environment for two types of clients – those who are licensed to use instant messaging and meetings and those who are licensed only for instant messaging.

“Creating meeting user groups in a mixed-license environment”
Add groups for users who have Sametime Standard or Sametime Advanced home servers and therefore are entitled to access meeting features. Users who are not members of these groups are prevented from using meetings.

Related reference
“Sametime offering features by client type” on page 164
The features available to users depend on the type of client they use and the Sametime offering installed on their home servers.

Creating meeting user groups in a mixed-license environment:
Add groups for users who have Sametime Standard or Sametime Advanced home servers and therefore are entitled to access meeting features. Users who are not members of these groups are prevented from using meetings.

Before you begin
Plan how many groups you need for your organization. Make sure that you have Editor access or Author access with the GroupCreator role in the IBM Lotus Domino Directory.

About this task
Follow these steps for each group you want to create.

Procedure
1. From the Domino Administrator or Web Administrator, click the People & Groups tab.
2. Select Domino Directories, and then select Groups > Add Group.
3. On the Basics tab, enter a name for the group in the Group name field (for example, Meeting Creator Group 1 or Meeting Attender Group 1).
4. Select a Group type.
5. List the members of the group in the Members field. Make sure to enter a name exactly as it is entered in the top line of the User name field of the user’s Person document.
6. Click the Administration tab.
7. Enter the names of the group owners in the Owners field. Generally, the group owner is the administrator creating the group.
8. Click Save and Close.

Related concepts
“Configuring users in a mixed-license environment with Sametime Entry servers” on page 343
In a mixed-license environment that includes IBM Sametime Entry servers, the servers must be configured for the different licensed users.

Turning off case sensitivity on the Sametime Community Server:
You must turn off case sensitivity on the IBM Sametime Community Server to allow awareness in IBM Lotus iNotes and WebSphere applications.

Procedure
1. Open a text editor on the Sametime Community server.
2. Open the sametime.ini file located in the Sametime Community server installation directory. The default directory is C:\program files\lotus\domino.
3. In the Config section, add AWARENESS_CASE_SENSITIVE=0.
   Starting in Sametime 8.5, by default, the Sametime Community server is not case-sensitive. This is the suggested configuration. This setting controls whether it is possible to add a user ID to the contact list, using different case, than the case used in the Directory. When you add this setting and give it a value of 0, the Sametime server is no longer case-sensitive.
4. You must restart the Sametime Community server for the change to take effect.

What to do next
Also turn off case sensitivity in the Sametime Connect client by changing the isCaseInsensitive attribute to true. The attribute is one of the People preferences.

Related concepts
“People preferences” on page 996
The following table lists the people preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Installing a Sametime Proxy Server
The IBM Sametime Proxy Server enables browser-based clients to participate in Sametime instant messaging and online meetings. In addition, the Sametime Proxy Server works with Sametime Community Server or Connections to enable the business card feature in Sametime, and with Sametime Unified Telephony or other TCSPUI-enabled products to enable the Sametime click-to-call feature. The Sametime Proxy Server also provides live names awareness, and can replace the Links Toolkit used in earlier releases of Sametime.

About this task
Important: If you will be supporting the use of LiveNames in your Sametime deployment, you should deploy all Sametime Meeting Servers and Sametime Proxy Servers within the same subnet. It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Related concepts
“Configuring a Sametime Proxy Server” on page 1021
Configure connection settings to enable the IBM Sametime Proxy Server to communicate with other servers in the deployment.

Preparing to install a Sametime Proxy Server
Use the Sametime System Console to prepare to install an IBM Sametime Proxy Server by pre-populating values required for installation.
Before you begin

Start the Sametime System Console if it is not already running.

Procedure

If you have not already opened the Install Sametime Proxy Server guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   
   http://serverhostname.domain:8700/ibm/console
   
   For example:
   
   http://sametime.example.com:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Sametime Guided Activities > Install Sametime Proxy Server.

Related tasks

“Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine” on page 371

When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server on the same machine using the same server host name, conflicts with cookies that are used by each server can occur. If you install both servers on the same machine, then configure the Sametime Proxy Server with a host alias as a different host name.

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install a Sametime Proxy Server:

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

Before you begin

The following servers must be installed and running:

- LDAP server
- Sametime System Console
- Sametime Community Server, installed using a deployment plan created on the System Console

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Proxy Server.

Procedure

1. Plan a product installation.
   
   In the Install Sametime Proxy Server portlet, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.
Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click **Next**.

The name should include the installation and node type, such as stProxy_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.

3. **Deployment Product Version Selection.**
   Select the product version you want to install, and then click **Next**.

4. **Choose the configuration type.**
   Select **Primary Node** if this is the first server of its type. Select **Secondary Node** for additional servers. Then click **Next**.
   
   The **Cell** option is reserved for special-use cases in which the server must be self-contained. If you select **Cell**, you must provide a host name, user ID, and password when prompted to do so.

5. **Node Federation at Install Time.**
   This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click **Next**.

   **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

6. **WebSphere Profile Settings.**
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server.
      Supply a password, and then click **Next**.
      If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

      **Important:** This must be a unique user ID that does not exist in the LDAP directory.

7. **Connect to Community Server.**
   Select the deployment plan that represents the Community Server to which this Proxy server connects, and then click **Next**.

8. **Deployment Summary.**
   Review the summary screen, and then click **Finish**.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click **Modify an Existing Deployment Plan** and update the plan. All changes must be made prior to running installation.

**What to do next**

“Installing a Sametime Proxy Server on AIX, Linux, Solaris, or Windows” on page 349
Installing a Sametime Proxy Server on AIX, Linux, Solaris, or Windows

Run the installation program on the machine where you plan to install a Sametime Proxy Server.

Before you begin

You should have already created a deployment plan for the Sametime Proxy Server. Verify that the deployment plan is in the "Ready to Install" state and start the Sametime System Console server.

Linux

The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

AIX, Linux, and Solaris:

If you are installing using the GUI mode, the full X11 desktop environment is required.

Attention: Check the hosts file and remove any lines that start with the following:

- 127.0.0.1 fully_qualified_domain_name short_name
- ::1 fully_qualified_domain_name short_name

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

About this task

By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.

3. Prepare to use the Proxy Server installation package.
a. To download installation packages:
   1) To download installation packages, you must have an IBM Passport
      Advantage account. For information on using Passport Advantage, see
      the topic Using Passport Advantage to download IBM products.
   2) Open this release's Download document at the following web address:
      &uid=swg24029128
      Locate the components that you need in the document's listing, then
      download the packages labelled with the corresponding part numbers
      to the system on which you are installing.

      **Tip:** When extracting downloads on Windows operating systems, use a
      short path location such as C:\ and not a long path location such as
      the user's desktop or Temp directories. When extracting to long path
      locations or deeply nested directories and using the built-in Windows
      extract utility, corruption is sometimes seen without any warning. This
      corruption occurs when maximum path lengths on some Windows
      versions are exceeded.

b. If you are installing from physical media and your operating system
   mounts CDs or DVDs automatically with execution privileges turned off,
   mount the CD or DVD manually instead.

   **AIX**
   Mount the CD or DVD using the SMIT utility or the appropriate version of
   the following command:
   ```bash
   mount -v cdrfs -o ro /dev/cd0 /cdrom
   ```

   **Linux**
   Mount the CD or DVD using a command similar to the following
   command:
   ```bash
   mount /dev/cdrom /cdrom
   ```

   **Solaris**
   Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the
   installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**
     ```bash
     ./launchpad.sh
     ```
   - **Windows**
     ```bash
     launchpad.exe
     ```

   **Note:** If you do not have a web browser, go to the Installation Manager
   package directory and run the installation program (**install** for Linux or
   **install.exe** for Windows). Find the Installation Manager package directory
   here:
   ```bash
   sametime_server_package/IM/platform
   ```
   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language**
   list.

6. Click **Install IBM Sametime Proxy Server** and click **Launch IBM Sametime
   Proxy Server 8.5.2 installation**.
7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.
8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.
9. Click Install.
10. Select the packages that you want to install and click Next.
11. Click the I accept the terms in the license agreements option and click Next.
12. Select a package group option and accept the installation directory. Then click Next.
   Select Create a new package group if you have not installed any other Sametime software on this machine.
   Leave Use the existing package group selected if you are installing several Sametime servers on the same machine.
13. Select IBM Sametime Proxy Server as the feature to install and select Use Sametime System Console to install. Click Next.
14. At the Common Configurations screen, supply values for connecting to the Sametime System Console.
   • Host Name: Provide the Host Name for the Sametime System Console. The Host Name was determined when you installed the Sametime System Console. The host name must be the actual host name and not a DNS alias.
   • Use SSL: Leave this option selected to run the server over a secure connection.
   • HTTPS Port: Leave 9443 as the default value.
   • User ID and password: Provide the WebSphere Application Server User ID and password that you created when you installed the Sametime System Console.
15. Provide the host name for the machine you are currently using, which is the same name you used when you created the deployment plan for this installation.
   Do not use an IP address or short host name.
16. Click Validate to log in to the Sametime System Console. The button name changes to Validated after you log in.
17. When you are logged in, click Next.
18. Select the Sametime Proxy Server deployment plan you created earlier with the Sametime System Console guided activity. Then click Next.
19. Review the deployment settings, then click Next.
20. Review the summary, then click Install to start the installation.
21. When installation is complete, click Exit to close the Installation Manager.
22. If the Sametime Proxy server is installed on a system with multiple active IP addresses, follow these steps for each Proxy Server in the cell. Otherwise the Community Server may reject connections from the Proxy Server.
   a. Add the Proxy Server’s IP address to the stproxyconfig.xml file used by the Proxy Server's deployment manager. Complete this step for each Proxy Server in the cell.
1) Find the stproxyconfig.xml file in the Proxy Server's deployment manager profile configuration in this location:
   
   $dm_server_root/profiles/STPDMgrProfile/config/cells/ProxyCell_Name/nodes/ProxyNode_Name/servers/STProxyServer/

2) Add a localip setting with the IP address that corresponds to the host name of the Proxy Server specified during Proxy Server installation. Save the file.
   
   For example:
   
   ```
   <?xml version="1.0" encoding="UTF-8" ?>
   - <configuration>
     - <server>
       <host>stcommunityserver.example.com</host>
       <port>1516</port>
       <clusterlist />  
       <maxconnections>-1</maxconnections>
       <localip>192.0.2.0</localip>
     </server>
   </configuration>
   ```

b. Synchronize the Proxy Server deployment manager with each Proxy Server application server node.

1) Log in to the Proxy Server deployment manager's Integrated Solutions Console.

2) Choose System Administration > Nodes.

3) For each Proxy Server application node, select the node and click Full Resynchronize.

c. Restart the Proxy Server.

Results

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs

   Console connection log: /tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

   Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

   Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.
What to do next

“Managing trusted IP addresses” on page 1081

Related tasks

“Guided activity: Preparing to install a Sametime Proxy Server” on page 347
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Verifying a Sametime Proxy Server installation on AIX, Linux, Solaris, or Windows:

Open the IBM Sametime browser-based client to verify that the installation of a primary node was successful.

About this task

Follow these steps to verify the installation on a primary node. These instructions do not apply to verifying the installation on a secondary node because it does not have installed applications. To verify installation on a secondary node, verify that the installation completed successfully.

Procedure

1. Using a browser, log in to the Sametime Proxy Server application with the following URL:
   http://serverhostname.domain:port/stwebclient/index.jsp
   Replace serverhostname.domain with your server name and add the port number.
   For example:
   http://stproxy1.example.com:9080/stwebclient/index.jsp

   Tip: To verify the port number being used by the application, log in to the console on the Sametime Proxy Server:
   a. Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
      http://serverhostname.domain:8600/ibm/console
      8600 is the default port when the Proxy Server is installed as a Cell Profile.
      For example:
http://stproxy1.example.com:8600/ibm/console

b. Enter the WebSphere Application Server User ID and password that you created when you installed the server.

c. Click **Servers > WebSphere application servers > STProxyServer > ports > WC_defaulthost** to find the port number.

You can also verify the HTTP port number being used by the Sametime Proxy Server by opening the `AboutThisProfile.txt` file for the Sametime Proxy Application Server Profile and use the setting specified for the **HTTP transport port**. The default profile name is `short_host_nameSTPPNProfile1` when you use a deployment plan to install the server.

2. Verify that you can create or view contacts.

**Related tasks**

“Logging in to the console” on page 483

Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

**Installing a Sametime Proxy Server in silent mode**

If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

**Before you begin**

Information about downloading packages for Sametime is located at the following web address:

&uid=swg24029128

&uid=swg24027364

Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

**About this task**

Follow these steps to install the IBM Installation Manager in silent mode.

Customize each product’s response file, then install the product in silent mode using the customized response file.

**Important:** For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.
Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.

2. Navigate to the directory where you copied and extracted the installation files: \TMP\server_offering

3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.

4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows.

For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.

5. The SSCPassword value should be encoded. To generate an encoded password, use the generateEncodedPassword utility packaged with the installer.

The utility is on the installation media in the same directory as launchpad.exe or launchpad.sh.


7. Open a command window.

8. Enter the following command to install the IBM Installation Manager in silent mode.

   - AIX, Linux, or Solaris: \IBMIM\IM\windows\install
     --launcher.ini silent-install.ini

   - Windows: \IBMIMc --launcher.ini silent-install.ini

9. Navigate to the Installation Manager installation directory. The default directories are shown below.

   - AIX, Linux, or Solaris
     /opt/ibm/InstallationManager/eclipse

   - Windows
     C:\Program Files\IBM\Installation Manager\eclipse

10. For all installations except DB2, start the Sametime System Console.

11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.

    AIX, Linux, or Solaris: ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense

    Windows: IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense

**Tip: Generating a response file automatically**

The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation: ./install --launcher.ini your .ini file -record response_file path -skipInstall agentDataLocation
The response file is stored in the agentDataLocation directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same agentDataLocation in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using -skipInstall are not stored.

Adding a Sametime Proxy Server to the Sametime Community Server’s trusted IP addresses
Whenever you install a server that communicates with a community server, you must add the new server’s IP address to the community server’s settings.

About this task
The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server’s IP address to the community server.

If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).

You do not need to add the system console’s IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the Connectivity tab.
5. Under Trusted Servers, enter the IP address of the server that must connect to the Sametime Community Server in the New IP Address field, and click Add.

Note:
• If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.
• For the media manager, enter the Conference Manager server IP address.

To delete an IP address from the list, select it and click Delete Selected.
6. Click OK.
7. Restart the community server for the change to take effect.
Clustering Sametime Proxy Servers
Configuring a cluster of IBM Sametime Proxy Servers involves several tasks, including synchronizing system clocks, configuring the cluster settings, and optionally deploying an IBM Load Balancer in front of the cluster.

Before you begin
You can create two types of clusters:
• A Vertical cluster resides on the Primary node and includes two or more cluster members, which run the same application.
• A Horizontal cluster includes a Primary node plus one or more Secondary nodes, all running the same application. Each node contains one cluster member.

Important: It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Before you can configure a cluster of Sametime Proxy Servers, you must have installed the following servers:
1. Sametime System Console
This server will function as the cluster's Deployment Manager; the console can function as the Deployment Manager for multiple clusters.

**Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

2. Sametime Community Server
   At least one Sametime Community Server must be deployed to provide presence and awareness for users attending online meetings.

3. One Sametime Proxy Server installed with the **Primary Node** option.
   Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster's application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node's application server. The Primary node's application server can only belong to one cluster. The Primary Node can be used as a container for additional cluster members when creating a vertical cluster (multiple cluster members on the same physical system). The Primary Node must already be registered with the Sametime System Console. Registration happens automatically on AIX Linux, Solaris, and Windows, but on IBM i, you run the registration utility to register servers.

4. (Horizontal cluster only) One or more Sametime Proxy Servers installed with the **Secondary Node** option.
   Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as a container for additional cluster members, which are can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a horizontal cluster. Secondary Nodes must already be registered with the Sametime System Console. Registration happens automatically on AIX Linux, Solaris, and Windows, but on IBM i, you run the registration utility to register servers.

**About this task**

There are several tasks involved in creating a cluster; complete them in the sequence shown here:

**Related concepts**

“Clustering Sametime servers for high enterprise availability” on page 227
In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

**Setting clocks on the Sametime Proxy Servers to be clustered:**

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.
About this task

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.

Procedure

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager's (the Sametime System Console) system clock.

Clustering two or more Sametime Proxy Servers:

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

Start the Sametime System Console and the servers you intend to cluster.

Note: This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Guided Activities > Cluster WebSphere Application Servers.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Clustering Sametime Proxy Servers:
This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.

   This guided activity applies to the following Sametime servers if they are installed in your deployment.
   • Sametime Proxy Server
   • Sametime Meeting Server
   • Sametime Media Manager

   Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.
   • Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster’s Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.
If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager's SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

Procedure
1. Cluster WebSphere Application Servers.
   - Click Next to begin the clustering activity.
2. Select Product to Cluster.
   - Select the product server to cluster, and then click Next.
   - The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).
3. Select or Create a Cluster.
   - To create a cluster:
     a. Click Create Cluster if you are setting up a new cluster.
     b. Type a descriptive name for the cluster in the Cluster Name field.
        - For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.
     c. Click Next.
   - To modify an existing cluster; for example, to add a new cluster member:
     a. Click Select Existing Cluster.
     b. Select a cluster in the Cluster Name list.
        - If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.
     c. Click Next.
4. Select the Deployment Manager.
   - In the Select Deployment Manager list, select the Sametime System Console as the cluster's deployment manager, and then click Next.
   - Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.
5. Create the Cluster with the Primary Node.
You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node’s application server is running. Click Create cluster to configure the cluster settings, and then click Next.

Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. Select One or More Secondary Nodes.

If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the Secondary Node Name list, click the node you want to add to the cluster and click Next.

7. Add Cluster Members.

If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more “cluster members” to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.

The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be “Clustered” if the cluster member has been completely configured on the node. If the status is “Ready to Cluster”, select the Cluster Member and use the “Add to Cluster” button to finish configuring the cluster member.

**Vertical cluster:**

a. To add new cluster member, click New.

b. Select the default name generated for the cluster member or enter your own cluster member server name.

c. Select the Primary Node to create the cluster member on.

d. Click Add to Cluster.

   The status will change from “Ready to cluster” to “Clustered”.

e. Click Next.

**Horizontal cluster:**

For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.

a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.

b. One at a time, select each cluster member and click Add to Cluster.

   Do not proceed until the current cluster member’s status changes from “Ready to cluster” to “Clustered”; then you can add the next cluster member.

c. If you want to add more cluster members, click New to add another row to the table, and then fill out the information accordingly.

d. Click Next.

8. Deployment Summary.

Click Finish to save the cluster configuration.

Continue with the cluster configuration tasks described in the Sametime information center.

*Restarting and synchronizing nodes in the Sametime Proxy Server cluster:*
Synchronize the nodes in an IBM WebSphere Application Server network deployment.

About this task

Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node's configuration.

Procedure

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Stop the Deployment Manager:
   a. Click System Administration > Deployment manager.
   b. Click the "Configuration" tab.
   c. On the Configuration tab of the deployment manager settings, click Stop.
3. Now start the Deployment Manager:
   a. Open a command window and navigate to the app_server_root/profiles/DeploymentManagerName/bin directory.
   b. Run the following command:
      IBM AIX, Linux, or Solaris
      ./startManager.sh
      Microsoft Windows
      startManager.bat
      IBM i
      1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.
      2) At the Qshell prompt, run the following commands:
         cd app_server_root/profiles/DeploymentManagerName/bin
         startManager dmgr
4. Log in to the Integrated Solutions Console.
5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.
6. Restart all nodes in the cluster:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Node agents.
   b. Click a node agent, and then click Restart (the node agent should already be running).

Restarting the application servers in the Sametime Proxy Server cluster:

During cluster configuration, each node's application server was stopped so that the node could be federated. Start all of the application servers now.
About this task

Use the IBM Sametime System Console to start each of the application servers in the cluster.

Procedure

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Clusters > WebSphere application server clusters in the navigation tree.
3. Select the cluster's check box and click Start to start all cluster member servers.

Installing IBM Load Balancer for a Sametime Proxy Server cluster:

Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.

Before you begin

Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Note: The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.

IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure

1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
      Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
   For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.
3. After you have installed IBM Load Balancer, configure two static IP addresses for it:
   • Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:

Table 48. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer: loadbal.example.com</td>
<td>Load balancer (Cluster address)</td>
<td>Load balancer (NFA): 192.0.2.15</td>
</tr>
<tr>
<td>Cluster: st-cluster.example.com</td>
<td></td>
<td>Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>Deployment Manager (Sametime System Console)</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>svr1.example.com</td>
<td>Primary Node (a Sametime server)</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td>svr2.example.com</td>
<td>Secondary Node (a Sametime server)</td>
<td>192.0.2.5</td>
</tr>
</tbody>
</table>

Configuring IBM Load Balancer for a Sametime Proxy Server cluster:

Configure IBM Load Balancer for a cluster of IBM Sametime servers.

About this task

The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

Configuring IBM Load Balancer for a Sametime Proxy Server cluster (AIX, Linux, Solaris):

Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.
As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.

**Procedure**

1. Configure the nodes of the cluster.
   - **For cluster nodes running on AIX, Linux, and Solaris**
     Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   - **For cluster nodes running on IBM i**
     Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.
     For example:
     ```
     ADDTCPIFC INETADDR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)
     ```
     When the virtual TCP/IP interface is started, the server accepts packets for that address.

     **Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   **Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process with the following command:
      ```
      dsserver
      ```
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).

      **AIX**
      1) Run the following command:
         ```
         autoconf6
         ```
      2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
         ```
         start /usr/bin/autoconf6 * -A
         ```

      **Linux**
      Run the following command (you must be logged in as root):
      ```
      modprobe ipv6
      ```
**Solaris** Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:
```
ifconfig device inet6 plumb
ifconfig device inet6 address/prefix up
```
d. Start the executor function of the dispatcher:
dscontrol executor start
e. Add the cluster to the service:
dscontrol cluster add cluster's_fully_qualified_host_name
where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
stms-cluster.example.com
f. Add the cluster port:
dscontrol port add cluster's_fully_qualified_host_name@port
where `cluster's_fully_qualified_host_name@port` is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
stms-cluster.example.com@80
g. Add the nodes for which this server will balance workload:
dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node
where:
- `cluster_host@port@primary_node` indicates the cluster's fully qualified host name with the port appended as in the previous step, plus now with the primary node's fully qualified host name appended; for example:
stms-cluster.example.com@80@meetsvr1.example.com
- `cluster_host@port@secondary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
stms-cluster.example.com@80@meetsvr2.example.com
h. Now start the Load Balancer administration interface with the following command:
`. /lbadmin`

**Note:** If you have difficulty starting the administration interface, try stopping and then starting the executor and dsserver services before running the command again:
dsserver stop
dscontrol executor stop
dscontrol executor start
dsserver start
`. /lbadmin`

4. Continue configuring Load Balancer as follows:
a. Add the cluster to the executor:
dscontrol executor add cluster's_fully_qualified_host_name
where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
stms-cluster.example.com
b. Start the manager:
   `dscontrol manager start`

c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
   `dscontrol advisor start http 80`

5. Define server affinity with a "sticky time":
   By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

   The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

   a. Open a command window on the load balancer server.
   b. Stop the service with the following command:
      `dsserver stop`
   c. Set the sticky time with the following command:
      `dscontrol port set fully_qualified_host_name@port_number stickytime number_of_seconds`

      Where:
      - `fully_qualified_host_name` is the fully qualified host name of the server where IBM Load Balancer runs.
      - `port_number` is the port that will be affected by the new sticky time setting.
      - `number_of_seconds` is the duration, in seconds, of the time that a client should "stick to" the specified port.

      For example:
      `dscontrol port set myserver.com@80 stickytime 60`

6. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
   b. Click **Save Configuration File as** and accept the default name (default.cfg).

      The configuration settings stored in default.cfg are restored every time the server is restarted.
   c. Click **OK**.

   **Configuring IBM Load Balancer for a Sametime Proxy Server cluster (Windows):**

   Configure IBM Load Balancer on a server running Microsoft Windows.
Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

Procedure

1. Configure the nodes of the cluster.
   a. **For cluster nodes running on Windows**
      Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   b. **For cluster nodes running on IBM i**
      Use the `Add TCP/IP Interface` command to create a virtual IP address with the "cluster" IP address you want to use.
      For example:
      ```
      ADDTCPIFC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
      ```
      When the virtual TCP/IP interface is started, the server accepts packets for that address.
      Note: Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.
   Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process by clicking Start > Control Panel > Administrative Tools > Services. right-click IBM Dispatcher (ULB), and then click Start.
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Run the following command while logged in as the Windows administrator:
netsh interface ipv6 install

This command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.

d. Start the executor function of the dispatcher:
   dscontrol executor start

e. Add the cluster to the service:
   dscontrol cluster add cluster's_fully_qualified_host_name
   where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
   stms-cluster.example.com

f. Add the cluster port:
   dscontrol port add cluster's_fully_qualified_host_name@port
   where cluster's_fully_qualified_host_name@port is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
   stms-cluster.example.com@80

g. Add the nodes for which this server will balance workload:
   dscontrol server add cluster_host@port@primary_node
   dscontrol server add cluster_host@port@secondary_node
   where:
   * cluster_host@port@primary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:
     stms-cluster.example.com@80@meetsvr1.example.com
   * cluster_host@port@secondary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
     stms-cluster.example.com@80@meetsvr2.example.com

h. Add the cluster to the executor:
   dscontrol executor add cluster's_fully_qualified_host_name
   where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
   stms-cluster.example.com

i. Start the manager:
   dscontrol manager start

j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
   dscontrol advisor start http 80

k. Now you can stop the service:
   dsserver stop

l. Close the command window.
4. Define server affinity with a "sticky time":
   By default the Load Balancer will round-robin HTTP requests between the
   cluster members, so that a single client may be routed to different cluster
   members for subsequent requests rather than continuing to be routed to the
   same cluster member. Since a client typically accesses an online meeting every
   30-40 seconds during the session, you may want to enable server affinity for a
   Sametime cluster so that the client continues to access the same server during a
   single meeting.

   The dispatcher component of IBM Load Balancer supports a configurable
   "sticky time". This means that the load balancer will remember which cluster
   member a client was routed to; subsequent requests will "stick to" the same
   server until the preset time expires. IBM recommends a "sticky" time
   configuration of 60 seconds for a Sametime cluster.

   **Windows**
   a. Start IBM Load Balancer.
   b. In the navigation tree, select the **Executor** (the load balancer's
      non-forwarding IP address, which appears under its host name).
   c. Click **Configuration Settings**.
   d. In "Port-Specific Settings", change the **Default sticky-time settings** from 0 to
      60 seconds, and click **Update Configuration**.
   e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the
      host name of the load balancer you just configured (for example,
      loadbal.example.com).
   b. Click **Save Configuration File as** and accept the default name
      (**default.cfg**).

      The configuration settings stored in **default.cfg** are restored every time the
      server is restarted.
   c. Click **OK**.

**Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine**

When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server
on the same machine using the same server host name, conflicts with cookies that
are used by each server can occur. If you install both servers on the same machine,
then configure the Sametime Proxy Server with a host alias as a different host
name.

**About this task**

If you deploy the Sametime Proxy Server and the Sametime Meeting Server on one
machine, and both servers have the same host name, users cannot stay connected
to instant meetings initiated by the Sametime Proxy web client. Users can start
instant meetings, but eventually they are disconnected. This error occurs because
WebSphere sets the JSESSIONID cookie whenever an application is started, and the
JSESSIONID cookie is being overwritten because the Sametime Proxy Server and
the Sametime Meeting Server share a hostname. Due to the matching host names,
the WebSphere JSESSIONID is not recognizing them as separate applications. You
can work around this by providing the Sametime Proxy Server with a host alias
with a hostname different from the Sametime Meeting Server host name.
An example of a host alias is `stproxy`. For more information on host alias settings, see “Host alias settings” in the WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

**Procedure**

1. Install the Sametime Meeting Server and the Sametime Proxy Server on the same server.
2. Change the host name of the Sametime Proxy Server using a host alias:
   a. Log in to the Integrated Solutions Console on the Sametime Proxy Server.
   b. Click `Environment > Virtual Hosts > default_host > Host Aliases`.
   c. Configure the host aliases of the Virtual Host, `default_host`, of the Sametime Proxy Server so that their host names do not match either the host name of the Sametime Meeting Server or the wild card character, `*` (asterisk).
      
      The new host name alias must refer to the IP address at the DNS level, so that the machines will be able to ping the Web server by using the host name. Update the host name of all of the host alias entries to the host name that the Sametime Proxy Server or Sametime Meeting Server will use. Use the same host name for all aliases.
      
      1) Click the host name link associated with each port.
      2) Enter the fully qualified host name for the Sametime Proxy Server. It must not be the same host name assigned to the Sametime Meeting Server.
      3) Click Apply, and then click Save.
   d. Restart the Sametime Proxy Server.
3. On the Sametime System Console, go to the configuration page for Sametime Advanced and update the host name to match the host name alias you created for the Proxy Server or Meeting Server.
   a. Log in to the Integrated Solutions Console.
   b. Click `Sametime System Console > Sametime Servers > Sametime Proxy Servers`.
   c. In the `Sametime Proxy Servers` list, click the deployment name of the server with the information that you want to add or change.
   d. Click the `Administrative Settings` tab.
   e. In the Sametime Meeting Server section, modify the host name to reflect the new host alias you created.

**Installing a Sametime Media Manager on Linux or Windows**

The Sametime Media Manager is available for installing on the Linux or Windows platforms only. Follow the instructions for your operating system to install a Sametime Media Manager on those platforms.

**Related tasks**

“Configuring a Sametime Media Manager” on page 1025
This section describes how to configure the components of the Sametime Media Manager.

**Preparing to install a Sametime Media Manager on Linux or Windows**

Use the Sametime System Console to prepare to install a Sametime Media Manager by pre-populating values required for installation. The media manager runs on Linux or Microsoft Windows only.
Before you begin

Start the Sametime System Console if it is not already running.

Procedure

If you have not already opened the Install Sametime Media Manager guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   
   http://serverhostname.domain:8700/ibm/console
   
   For example:http://sametime.example.com:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Sametime Guided Activities > Install Sametime Media Manager.

Related tasks

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install a Sametime Media Manager:

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens. The IBM Sametime Media Manager runs on Linux and Microsoft Windows only. The media manager is comprised of three components: Proxy/Registrar, Conference Manager, and Packet Switcher. In an enterprise deployment, you should install these Media Manager components on separate machines for better performance.

Before you begin

The instructions below assume you have decided what type of deployment plan you are setting up for the Media Manager. A small deployment uses one machine and one deployment plan. An enterprise deployment typically distributes each Media Manager component on a separate machine and therefore uses multiple deployment plans. In addition, you can cluster the Proxy/Registrar and Conference Manager components, which requires a deployment plan for the component's primary node and another deployment plan for secondary nodes. Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher.

- **Small deployment prerequisite**
  
  You must have installed a Sametime Community server using a deployment plan.

- **Enterprise deployment prerequisites**
  
  The SIP Proxy and Registrar requires that you have installed a Sametime Community server using a deployment plan.
  
  The Conference Manager requires that you have installed a Sametime Community server and a SIP Proxy and Registrar using deployment plans.
  
  The Packet Switcher requires that you have installed a Sametime Community server and a Conference Manager using deployment plans.
Create deployment plans and install each component in this order to meet prerequisites:
1. SIP Proxy and Registrar
2. Conference Manager
3. Packet Switcher

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Media Manager or one of its components.

Procedure

1. Plan a product installation.
   In the Install Sametime Media Manager portlet, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.
   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.
   The name should include the installation and node type, such as stMedia_primary or stMediaProxReg_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.

   Select the product version you want to install, and then click Next.

4. Media Manager Feature Installation.
   Select which components to install, and then click Next:
   - Small deployment: Click Install All Components to install all media manager components on the same computer.
   - Enterprise deployment: Select the component to install on the current computer.
     - Install Proxy/Registrar
     - Install Conference Manager
     - Install Packet Switcher

   Attention: The Packet Switcher can only be deployed with Conference Managers that have already been installed and registered with the Sametime System Console. You can deploy multiple Packet Switchers for a single Conference Manager; the Packet Switchers cannot be clustered but the Conference Manager distributes the workload among them.

5. Choose the configuration type.
   Select Primary Node if this is the first server of its type or if you are installing a Packet Switcher. Select Secondary Node for additional Proxy/Registrar or Conference Manager servers. Then click Next.
   The Cell option is reserved for special-use cases in which the server must be self-contained. If you select Cell, you must provide a host name, user ID, and password when prompted to do so.

This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click Next.

**Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

7. WebSphere Profile Settings.
   a. Type the fully qualified host name of the server where you will be installing the media manager component.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click Next.
      If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.
      **Important:** This must be a unique user ID that does not exist in the LDAP directory.

8. Connect to Community Server.
   Select the deployment plan that represents the Community Server to which this Media Manager component (or components) connect, and then click Next.
   For a Conference Manager deployment plan, also select the existing Proxy/Registrar deployment plan. For a Packet Switcher deployment plan, also select the existing Conference Manager deployment plan.

   Review the summary screen, and then click Finish.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click Modify an Existing Deployment Plan and update the plan. All changes must be made prior to running installation.
   Repeat this guided activity for each media manager component you plan to install on a separate computer.

What to do next

“Installing a media manager on Linux or Windows”

**Installing a media manager on Linux or Windows**
Run the installation program on the machine where you plan to install Sametime Media Manager. The media manager runs only on Linux or Windows.

**Before you begin**

You should have already created a deployment plan for the Sametime Media Manager. Verify that the deployment plan is in the "Ready to Install" state and start the Sametime System Console server. Be sure there are no firewalls or connectivity problems to the LDAP server or the installation will fail.

**Linux** The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed.
and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**
If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:** Check the `hosts` file and remove any lines that start with the following:
- `127.0.0.1 fully_qualified_domain_name short_name`
- `::1 fully_qualified_domain_name short_name`

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

**About this task**
By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

**Procedure**
1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the `SELINUX` setting. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
3. Prepare to use the Sametime Media Manager installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

      **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**Linux**

Mount the CD or DVD using a command similar to the following command:

```bash
mount /dev/cdrom /cdrom
```

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX, Linux, and Solaris**
  ```bash
  ./launchpad.sh
  ```

- **Windows**
  ```bash
  launchpad.exe
  ```

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

*platform* is the installation package name for this server.

5. If necessary, select a language other than English from the Select a language list.

6. Click **Install IBM Lotus Sametime Media Manager** and click Launch IBM Sametime Media Manager 8.5.2 installation.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose File > Preferences.

   b. Uncheck Search service repositories during installation and updates and click OK.

9. Click Install.

10. Select the packages that you want to install and click Next.

11. Click the I accept the terms in the license agreements option and click Next.

12. Select a package group option and accept the installation directory. Then click Next.

   Select Create a new package group if you have not installed any other Sametime software on this machine.

   Leave Use the existing package group selected if you are installing several Sametime servers on the same machine.

13. Select IBM Sametime Media Manager as the feature to install and select Use Sametime System Console to install. Click Next.
At the Common Configurations screen, supply values for connecting to the Sametime System Console.

- **Host name**: Provide the fully qualified domain name in the Host Name field for the Sametime System Console. The host name was determined when you installed the Sametime System Console. The host name must be the actual host name and not a DNS alias.
- **Use SSL**: Leave this option selected to run the server over a secure connection.
- **HTTPs port**: Leave 9443 as the default value.
- **User ID and password**: Provide the WebSphere Application Server User ID and password that you created when you installed the Sametime System Console.

Provide the host name for the machine you are currently using, which is the same name you used when you created the deployment plan for this installation.

Do not use an IP address or short host name.

15. Click **Validate** to log in to the Sametime System Console. The button name changes to **Validated** after you log in.
16. When you are logged in, click **Next**.
18. Select the Sametime Media Manager deployment plan you created earlier with the Sametime System Console guided activity. Then click **Next**.
19. Review the deployment settings, then click **Next**.
20. Review the summary, then click **Install** to start the installation.
21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var.ibm/InstallationManager/logs

`Console connection log`: /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

`Console connection log`: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

`Console connection log`: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.
Related tasks

“Guided activity: Preparing to install a Sametime Media Manager” on page 373
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens. The IBM Sametime Media Manager runs on Linux and Microsoft Windows only. The media manager is comprised of three components: Proxy/Registrar, Conference Manager, and Packet Switcher. In an enterprise deployment, you should install these Media Manager components on separate machines for better performance.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

“Managing multiple Packet Switcher nodes in a cluster with the Sametime System Console” on page 433
In a clustered environment, if you have installed an additional Packet Switcher node, you must manually map the application modules to manage them with the Sametime System Console.

Installing a Sametime Media Manager in silent mode:

If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

Before you begin

Information about downloading packages for Sametime is located at the following web address:

Standard: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128


Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

About this task

Follow these steps to install the IBM Installation Manager in silent mode. Customize each product’s response file, then install the product in silent mode using the customized response file.
Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.

2. Navigate to the directory where you copied and extracted the installation files:
   \TMP\server_offering

3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.

4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows.
   For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.

5. The SSCPassword value should be encoded. To generate an encoded password, use the generateEncodedPassword utility packaged with the installer.
   The utility is on the installation media in the same directory as launchpad.exe or launchpad.sh.


7. Open a command window.

8. Enter the following command to install the IBM Installation Manager in silent mode.
   - **AIX, Linux, or Solaris**
     SametimeOffering/IM/windows/install
     --launcher.ini silent-install.ini
   - **Windows**
     SametimeOffering\IM\windows\installc --launcher.ini silent-install.ini

9. Navigate to the Installation Manager installation directory. The default directories are shown below.
   - **AIX, Linux, or Solaris**
     /opt/ibm/InstallationManager/eclipse
   - **Windows**
     C:\Program Files\IBM\Installation Manager\eclipse

10. For all installations except DB2, start the Sametime System Console.

11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.
    - **AIX, Linux, or Solaris**
      ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
    - **Windows**
      IBMIMc --launcher.ini silent-install.ini -input response_file
    
    Tip: Generating a response file automatically
The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation.

```
./install --launcher.ini your .ini file -record response file path -skipInstall agentDataLocation
```

The response file is stored in the `agentDataLocation` directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same `agentDataLocation` in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using `-skipInstall` are not stored.

**Verifying a media manager installation on Linux or Windows:**

After installing the Sametime Media Manager, verify that you can use audio-visual services.

**About this task**

Follow these steps to verify that the server started automatically after installation and that you can use audio-visual services from the Sametime Connect client.

**Procedure**

1. Check the WebSphere Application Server `systemout.log` and `systemerr.log` for any exceptions.
2. From a browser, log in to the console on the Sametime Media Manager:
   a. Enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the server.
      
      ![URL](http://serverhostname.domain:8800/ibm/console)
      
      8800 is the default port when the Media Manager is installed as a Cell Profile.
      
      For example:
      
      ![URL](http://sametime.example.com:8800/ibm/console)
   b. Enter the WebSphere Application Server User ID and password that you created when you installed the server.
   c. Click the Sametime System Console task to open it in the navigation tree.
3. Click **Servers > Server types > WebSphere application servers**.
4. Find the Media Manager server in the list and verify that the status column shows that the server is running.
5. Log in to the Sametime Client and verify that you can use audio-visual services in a meeting or a chat.

**Adding the Sametime Media Manager to the Sametime Community Server’s trusted IP addresses**

Whenever you install a server that communicates with a community server, you must add the new server's IP address to the community server's settings.

**About this task**

The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services
page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server’s IP address to the community server.

If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to complete include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).

You do not need to add the system console’s IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the Connectivity tab.
5. Under Trusted Servers, enter the IP address of the server that must connect to the Sametime Community Server in the New IP Address field, and click Add.
   
   **Note:**
   - If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.
   - For the media manager, enter the Conference Manager server IP address.
   
   To delete an IP address from the list, select it and click Delete Selected.
6. Click OK.
7. Restart the community server for the change to take effect.

Disabling IPv6 addressing on the Media Manager
If you installed the IBM Sametime Media Manager or any of its components on Microsoft Windows 2008 or later, disable IPv6 addressing on that server.

About this task
This task is only needed for Media Manager components installed on Windows 2008 or later servers. The Media Manager does not support IPv6 addressing, even when IPv4 addressing is enabled at the same time. Windows 2008 or later servers enable IPv6 addressing by default, so you must disable it now to ensure the Media Manager functions properly. If Media Manager components are installed on separate computers, disable IPv6 addressing on all components.

Disable IPv6 support by setting the java.net.preferIPv4Stack custom property to true in IBM WebSphere Application Server.

**Note:** This disables IPv6 addressing support for the IBM WebSphere Application Server on which the Media Manager components are hosted – it does not disable IPv6 addressing in Windows.
Procedure
1. On the computer hosting the Media Manager or one of its components, log in to the Integrated Solutions Console as the WebSphere administrator.
   If the Media Manager component is clustered, complete this task on the cluster’s Deployment Manager.
2. Click Servers > Application Servers.
3. In the list of application servers, click the server hosting the Media Manager or component.
4. On the Configuration page, locate the "Server Infrastructure" section, and click Java and process management > Process definition > Java virtual machine > Custom Properties.
5. Do one of the following:
   • If the java.net.preferIPv4Stack custom property is listed, edit it and set its Value to true.
   • If the java.net.preferIPv4Stack custom property is not listed, create it now by clicking New and assigning it the following values before clicking OK:
     – Name: java.net.preferIPv4Stack
     – Value: true
6. Do one of the following:
   • For a stand-alone Media Manager or component, restart the server.
   • For a clustered Media Manager component, synchronize nodes and restart the cluster as follows:
     a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
     b. Select all nodes in the cluster
     c. Click Full Resynchronize.
     d. Back in the navigator, click System Administration > Node agents.
     e. Click a node agent, and then click Restart; repeat for each node agent.

Clustering Sametime Media Manager components
The IBM Sametime Media Manager includes several components. You can install the components separately and optionally cluster some of them.

About this task
The Sametime Media Manager comprises three components:
• Packet Switcher
  Based on voice-activated switching, the Packet Switcher routes audio and video data to participant endpoints. There can be one or more Packet Switchers in a deployment; it cannot be clustered. A Packet Switcher can only be registered with one Conference Manager. If you have a Conference Manager cluster then the Packet Switcher is registered with the cluster and each cluster member uses the same Packet Switcher.
• Conference Manager
  Manages multipoint conferences by maintaining a dialog with each participant, and ensuring that all media flows between those participants. You can install multiple Conference Manager components and cluster them for high availability and failover.
• SIP Proxy/Registrar
Directs conference participants to Conference Manager servers and provides high availability and failover functionality. You can install multiple SIP Proxy/Registrar components and cluster them for high availability and failover.

Complete the clustering tasks in the sequence shown:

**Related concepts**

“Clustering Sametime servers for high enterprise availability” on page 227

In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

**Clustering SIP Proxy and Registrar components:**

Configuring a cluster of IBM Sametime Media Manager “SIP Proxy and Registrar” components involves several tasks, including synchronizing system clocks, configuring one or more IBM WebSphere proxy server to operate with the cluster.

**Before you begin**

You can create two types of clusters:

- A **Vertical cluster** resides on the Primary node and includes two or more cluster members, which run the same application.
- A **Horizontal cluster** includes a Primary node plus one or more Secondary nodes, all running the same application. Each node contains one cluster member.
Important: It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Before you can configure a cluster of Sametime Media Manager "SIP Proxy and Registrar" components, you must have installed the following servers:

1. Sametime System Console
   This server will function as the cluster's Deployment Manager; the console can function as the Deployment Manager for multiple clusters.
   
   **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

2. Sametime Community Server
   At least one Sametime Community Server must be deployed to provide presence and awareness for users.

3. One Sametime Media Manager "SIP Proxy and Registrar" component, installed with the **Primary Node** option.
Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster's application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node's application server. The Primary node's application server can only belong to one cluster. The Primary Node can be used as a container for additional cluster members when creating a vertical cluster (multiple cluster members on the same physical system).

4. (Horizontal cluster only) One or more Sametime Media Manager "SIP Proxy and Registrar" components, installed with the **Secondary Node** option. Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as a container for additional cluster members, which are can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a horizontal cluster.

To cluster SIP Proxy and Registrar components, complete the following tasks in the sequence shown:

*Setting clocks on the SIP Proxy and Registrars to be clustered:*

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.

**About this task**

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.

**Procedure**

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager's (the Sametime System Console) system clock.

*Clustering SIP Proxy and Registrars:*

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

**Before you begin**

Start the Sametime System Console and the servers you intend to cluster.

**Note:** This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

**About this task**

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is...
defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   
   http://serverhostname.domain:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Guided Activities > Cluster WebSphere Application Servers**.

Related tasks

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Guided activity: Clustering SIP Proxy and Registrars:**

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

**Before you begin**

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.

   This guided activity applies to the following Sametime servers if they are installed in your deployment.

   • Sametime Proxy Server
   • Sametime Meeting Server
   • Sametime Media Manager

   Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.

   • Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.
About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster's Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager's SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

Procedure

1. Cluster WebSphere Application Servers.
   Click Next to begin the clustering activity.

2. Select Product to Cluster.
   Select the product server to cluster, and then click Next.
   The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).

3. Select or Create a Cluster.
   To create a cluster:
   a. Click Create Cluster if you are setting up a new cluster.
   b. Type a descriptive name for the cluster in the Cluster Name field.
For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.

c. Click Next.

To modify an existing cluster; for example, to add a new cluster member:

a. Click Select Existing Cluster.

b. Select a cluster in the Cluster Name list.

If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.

c. Click Next.

4. Select the Deployment Manager.

In the Select Deployment Manager list, select the Sametime System Console as the cluster's deployment manager, and then click Next.

Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.

5. Create the Cluster with the Primary Node.

You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node's application server is running. Click Create cluster to configure the cluster settings, and then click Next.

Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. Select One or More Secondary Nodes.

If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the Secondary Node Name list, click the node you want to add to the cluster and click Next.

7. Add Cluster Members.

If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more "cluster members" to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.

The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be "Clustered" if the cluster member has been completely configured on the node. If the status is "Ready to Cluster", select the Cluster Member and use the "Add to Cluster" button to finish configuring the cluster member.

**Vertical cluster:**

a. To add new cluster member, click New.

b. Select the default name generated for the cluster member or enter your own cluster member server name.

c. Select the Primary Node to create the cluster member on.

d. Click Add to Cluster.
The status will change from "Ready to cluster" to "Clustered".

e. Click Next.

**Horizontal cluster:**

For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.

a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.

b. One at a time, select each cluster member and click **Add to Cluster**.

Do not proceed until the current cluster member's status changes from "Ready to cluster" to "Clustered"; then you can add the next cluster member.

c. If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.

d. Click Next.

8. Deployment Summary.

   Click **Finish** to save the cluster configuration.

   Continue with the cluster configuration tasks described in the Sametime information center.

**Restarting and synchronizing the SIP Proxy and Registrar cluster:**

Complete the configuration for clustering IBM Sametime Media Manager SIP Proxy and Registrar components using an IBM WebSphere Application Server network deployment by restarting and synchronizing nodes in the cluster and restarting the application servers in the cluster.

**Before you begin**

Create a cluster of SIP Proxy and Registrar components using the guided activity.

**About this task**

Completing the cluster's configuration requires the following tasks:

**Restarting and synchronizing nodes in the SIP Proxy and Registrar cluster:**

Synchronize the nodes in an IBM WebSphere Application Server network deployment.

**About this task**

Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node's configuration.

**Procedure**

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.

2. Stop the Deployment Manager:
   a. Click **System Administration > Deployment manager**.
   b. Click the "Configuration" tab.
   c. On the Configuration tab of the deployment manager settings, click **Stop**.

3. Now start the Deployment Manager:
a. Open a command window and navigate to the app_server_root/profiles/DeploymentManagerName/bin directory.

b. Run the following command:

**IBM AIX, Linux, or Solaris**

```
./startManager.sh
```

**Microsoft Windows**

```
startManager.bat
```

**IBM i**

1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.

2) At the Qshell prompt, run the following commands:

```
cd app_server_root/profiles/DeploymentManagerName/bin
startManager dmgr
```

4. Log in to the Integrated Solutions Console.

5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:

   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes in the cluster.
   c. Click **Full Resynchronize**.

6. Restart all nodes in the cluster:

   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Node agents**.
   b. Click a node agent, and then click **Restart** (the node agent should already be running).

**Restarting the application servers in the SIP Proxy and Registrar cluster:**

During cluster configuration, each node’s application server was stopped so that the node could be federated. Start all of the application servers now.

**About this task**

Use the IBM Sametime System Console to start each of the application servers in the cluster.

**Procedure**

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.

2. Click **Servers > Clusters > WebSphere application server clusters** in the navigation tree.

3. Select the cluster’s check box and click **Start** to start all cluster member servers.

**Setting up a WebSphere proxy server for the SIP Proxy and Registrar cluster:**

Set up an IBM WebSphere proxy server for use with a cluster of IBM Sametime servers. The proxy server can be hosted on a product node, or on a separate computer; it performs routing and caching tasks for the servers in the cluster.
About this task
If you deployed the cluster using a standalone Deployment Manager, you must deploy a WebSphere proxy server to operate with the cluster. If the cluster uses the Sametime System Console as its Deployment Manager, the WebSphere proxy server was automatically deployed on the console but may need to be configured.

If the cluster experiences a high level of demand, you may want to deploy an additional, stand-alone, WebSphere proxy server to distribute the load and mitigate the single point-of-failure.

(Optional) Adding a stand-alone WebSphere proxy server to the SIP Proxy and Registrar cluster:
Install a stand-alone IBM WebSphere proxy server for use with a cluster of IBM Sametime servers.

Before you begin
This topic explains how to install a stand-alone WebSphere proxy server by installing an extra node into the Sametime cluster, removing the Sametime application, and then configuring the WebSphere proxy server that remains. If you just want to configure the WebSphere proxy server that was automatically installed with WebSphere Application Server on one of existing nodes in your Sametime cluster, skip this task and proceed directly to Configuring a WebSphere proxy server.

About this task
A cluster of Sametime servers requires at least one WebSphere proxy server to handle routing and caching tasks. When you install Sametime on a node in the cluster, WebSphere Application Server and WebSphere proxy server are also installed. The WebSphere proxy server merely needs to be configured for use.

To reduce the resource load on product nodes and avoid port conflicts, you may choose to install a stand-alone WebSphere proxy server on a separate computer instead of using the instance that was installed on a Sametime node. Or, you may configure the instance on the Sametime node and then install an additional instance on a separate computer, and use a load balancer to share the load between them.

Note: If you previously installed a WebSphere proxy server on one of the Sametime nodes in the cluster and are now seeing excessive CPU usage on that node, you should install and configure an additional proxy server now.

To install a stand-alone WebSphere proxy server, you will install an extra Sametime node using the "Secondary Node" option, and then federate the new node into the cluster. You will then remove the Sametime application from the new node while leaving WebSphere proxy server intact. Finally, you will configure the WebSphere proxy server for use with the cluster.

Installing an additional Sametime server as a Secondary Node in the SIP Proxy and Registrar cluster:
Install an IBM Sametime product server as a Secondary Node, and then federate it into a cluster.
About this task

The first stage in deploying a stand-alone IBM WebSphere proxy server is to create a deployment plan, and then use the Sametime System Console to install the new Sametime server. Because you will later federate the new product node into the cluster, you must install the same product now.

Important: Install the new node using the "Secondary Node" option to ensure you can federate it to the cluster later.

Federating the new Secondary Node to the SIP Proxy and Registrar cluster:

Federate the newly installed Secondary Node into a cluster of IBM Sametime servers.

About this task

The next stage in deploying a stand-alone IBM WebSphere proxy server is to federate the new Sametime node into the existing cluster. For this task, you will use the Clustering guided activity, selecting the "Select Existing Cluster" option (in Step 3) and then choosing the appropriate cluster.

When you run the cluster guided activity there are phases: first, the proxy server is federated to the cluster’s Deployment Manager; then the proxy server is added into the cluster as a new member. Be sure to complete all steps in the guided activity to properly add the proxy server to the cluster.

Removing the Sametime product from the new node in the SIP Proxy and Registrar cluster:

After you have federated a new IBM Sametime node to a cluster, remove the Sametime application but leave the IBM WebSphere proxy server intact.

About this task

After the new node has been federated to the cluster, it can be managed by the cluster’s Deployment Manager. Since the purpose of this new node is to provide a WebSphere proxy server, the Sametime product application is no longer needed on that node, and can be removed.

Procedure

1. On the cluster’s Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > WebSphere application servers.
3. In the list of servers, click the name of the new Sametime node.
4. At the top of the list, click the Delete button.
5. When prompted for confirmation, click OK.
6. Save the change by clicking the Save link the "Messages" box at the top of the page.
7. Verify that the server has been deleted by making sure it no longer appears in the list of servers.

Configuring a WebSphere proxy server for the SIP Proxy and Registrar cluster:
Configure an IBM WebSphere proxy server to perform routing and caching tasks for a cluster of IBM Sametime servers running on WebSphere Application Server.

**Before you begin**

Create a cluster of Sametime servers running on WebSphere Application Server; start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Use these instructions to configure a WebSphere proxy server that operates with the following Sametime server clusters:

- Meeting Server
- Conference Manager
- SIP Proxy and Registrar

**About this task**

A cluster of Sametime servers that run on WebSphere Application Server can use a WebSphere proxy server to manage routing and caching tasks. To ensure redundancy in the case of a proxy server failure, you may want to configure multiple proxy servers for the cluster. Use a Load Balancer in that case to divide the incoming load between the proxy servers. You can host a WebSphere proxy server on any node in the cluster (except the Sametime System Console) but because it uses a lot of system resources, you may want to host it on its own computer.

**Note:** If you install multiple WebSphere proxy servers, you will need a Load Balancer to divide the incoming load among the proxy servers. Installing IBM Load Balancer is discussed later in this section.

**Procedure**

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click **Servers > Server Types > WebSphere proxy servers**.
3. In the proxy servers table, click the **New** button at the top of the table.
4. In the "Create a new proxy server entry" dialog box, do the following:
   a. In the "Select a node" box, select the node that will host the WebSphere proxy server. Be sure to select a node that belongs to the appropriate cluster.
   b. Type a name for the new proxy server; for example "was_proxy1", and then click **Next**.
   c. In the "Specify server specific properties" box, select the appropriate "Support protocol" settings for your cluster, select **Generate unique ports**, and then click **Next**.
      - If you are configuring this WebSphere proxy server for a Meeting Server cluster: deselect the SIP protocol.
      - If you are configuring this WebSphere proxy server for a SIP Proxy and Registrar cluster: accept both HTTP and SIP protocols.
      - If you are configuring this WebSphere proxy server for a Conference Manager cluster: accept both HTTP and SIP protocols.
In the "Select a server template" box, select **proxy_server_foundation** (the WebSphere Default Proxy Server Template), and then click **Next**.

In the "Confirm new server" box, click **Finish**.

5. Save the changes by clicking the **Save** link in the "Messages" box at the top of the page.

6. Resynchronize the nodes:
   a. On the Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
   b. Click **System Administration > Nodes**.
   c. Select all of the nodes in the cluster.
   d. Click **Full Resynchronize**.

7. (Conference Manager cluster, SIP Proxy and Registrar cluster) Assign the new proxy server to the cluster:
   a. Click **Servers > Server Types > WebSphere proxy servers > proxy_server_name > SIP Proxy Server Settings > SIP proxy settings**.
   b. In the "Default cluster" field, select the cluster that you are configuring this WebSphere proxy server to work with.
   c. Click **Apply**.
   d. Save the changes by clicking the **Save** link in the "Messages" box at the top of the page.

8. Now start the new WebSphere proxy server:
   a. Again in the Integrated Solutions Console's navigation tree, click **Servers > Server Types > WebSphere proxy servers**.
   b. In the "WebSphere proxy servers" page, select the new proxy server from the list.
   c. Click the **Start** button above the list of proxy servers.

---

Adding ports to the virtual host alias for the SIP Proxy and Registrar cluster:

After creating an IBM Sametime Media Manager SIP Proxy and Registrar cluster, add the SIP ports of each cluster member to the virtual host alias. This step is required.

**Before you begin**

Create a cluster of SIP Proxy and Registrar components. Adding the SIP ports of each cluster member to the virtual host alias is required to ensure that the cluster operates properly.

**About this task**

On the cluster's Deployment Manager (the Sametime System Console), update the sip_proxyreg_host virtual host with a unique set of web access ports. Such a configuration lets a single host machine resemble multiple host machines.

**Tip:** Print this page and use the table to record the port settings as you look them up in steps 1 and 2:

**Table 49. Write down the port numbers used for these settings in every cluster member**

<table>
<thead>
<tr>
<th>Cluster member 1</th>
<th>SIP_DEFAULTHOST</th>
<th>SIP_DEFAULTHOST_SECURE</th>
<th>PROXY_SIP_ADDRESS</th>
<th>PROXY_SIPS_ADDRESS</th>
</tr>
</thead>
</table>

Chapter 11. Installing 395
Table 49. Write down the port numbers used for these settings in every cluster member (continued)

<table>
<thead>
<tr>
<th>Cluster member 2</th>
<th>SIP_DEFAULTHOST</th>
<th>SIP_DEFAULTHOST_SECURE</th>
<th>PROXY_SIP_ADDRESS</th>
<th>PROXY_SIPS_ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster member 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Procedure**

1. Determine the ports used by every cluster member:
   a. In the Deployment Manager's (the Sametime System Console) Integrated Solutions Console, click **Servers > Server Types > WebSphere application servers**.
   b. In the table listing the servers, click the name of the cluster member. This displays the cluster member's "Configuration" page.
   c. On the "Configuration" page, look under "Communication", and expand **Ports**.
   d. Look in the Ports table and write down the following port settings for use in the next step:
      - SIP_DEFAULTHOST
      - SIP_DEFAULTHOST_SECURE
   e. Repeat this process for every cluster member.

2. Next, determine the ports used by every WebSphere proxy server that operates with this cluster.
   a. In the Deployment Manager's (the Sametime System Console) Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers**.
   b. In the table listing the servers, click the name of the WebSphere proxy server. This displays the cluster member's "Configuration" page.
   c. On the "Configuration" page, look under "Communication", and expand **Ports**.
   d. Look in the Ports table and write down the following port settings for use in the next step:
      - PROXY_SIP_ADDRESS
      - PROXY_SIPS_ADDRESS
   e. Repeat this process for every WebSphere proxy server used by the cluster.

3. Now add the ports used by all the cluster members and all of the WebSphere proxy servers to the Deployment Manager's Virtual Hosts table.
   a. Now return to the Integrated Solutions Console navigation tree and click **Environment > Virtual Hosts**.
   b. In the Virtual Hosts table, click the host called **sip_proxyreg_host**. This displays the "Configuration" page for the sip_proxyreg_host.
   c. Under "Additional Properties", click **Host Aliases**.
   d. In the "Host Aliases" table, add the ports used by all of the cluster members (the information you collected in Step 1): Remember that you have information on the two ports for each cluster member; however if a port is already listed in the table, you do not need to add it again.
To add a port:
1) Click the New button at the top of the table.
2) In the Host Name field, type *.
3) In the Port field, type a port from your list.
4) Click OK.
5) Repeat this for the two ports for every cluster member (unless a port is already listed in this table).

e. Now delete all of the table entries that do not use * as the Host Name.
   To delete an entry, click on the check box next to it, and then click the Delete button at the top of the table.

f. Save the new port settings to the master configuration and synchronize the nodes in the cluster:
   WebSphere Application Server displays a message prompting you to save changes to the master configuration. Click Preference > Synchronize nodes option before clicking the Save button.

Reconfiguring ports for a WebSphere proxy server hosted on a product node in the SIP Proxy and Registrar cluster:

If the IBM WebSphere proxy server is hosted on the same computer as an IBM Sametime product, reconfigure ports to avoid a conflict.

Checking for port conflicts between the SIP Proxy and Registrar and the WebSphere proxy server:

If the IBM Sametime Media Manager’s SIP Proxy and Registrar server and the WebSphere Application Server SIP Proxy server are running on the same computer, avoid problems by verifying that the IBM WebSphere Application Server SIP Proxy Server is listening on the correct ports and is not in conflict with the IBM Sametime SIP Proxy and Registrar server running on the same computer.

About this task

Follow these steps to compare the SIP ports used by the WebSphere Application Server SIP Proxy with those used by the Sametime SIP Proxy and Registrar Server cluster member running on the same machine. If your cluster has both Sametime and WebSphere proxy server running on multiple nodes, be sure to check the ports on each node.

Procedure
1. On the node being checked, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Check the ports used by the WebSphere Application Server SIP Proxy server:
   a. Click Servers > Server Types > WebSphere proxy servers.
   b. In the list of proxy servers, click the node’s WebSphere Application Server SIP Proxy server to open its Configuration page.
   c. Under “Communications” click Ports.
   d. Write down the values assigned to the following ports:
      • PROXY_SIP_ADDRESS
      • PROXY_SIPS_ADDRESS
3. Check the ports used by the Sametime SIP Proxy and Registrar Server cluster member running on the same computer.
a. Click **Servers > Server Types > WebSphere application servers**.
b. In the list of application servers, click the name of the Sametime SIP Proxy and Registrar Server to open its Configuration page.
c. Under "Communications" click **Ports**.
d. Write down the values assigned to the following ports:
   - SIP_DEFAULTHOST
   - SIP_DEFAULTHOST_SECURE

**Results**

The ports are in conflict if the WebSphere Application Server SIP Proxy server is listening on the same ports as the Sametime SIP Proxy and Registrar server.

**What to do next**

Your next task depends on whether there is a port conflict to resolve:
- If the ports are in conflict, proceed to Changing a WebSphere proxy server's port settings.
- If the ports are not in conflict, then the WebSphere proxy server configuration is complete. Skip to Installing IBM Load Balancer.

*Changing a WebSphere proxy server’s port settings for the SIP Proxy and Registrar cluster:*

Change the defined port settings on an IBM WebSphere proxy server used by an IBM Sametime cluster.

**About this task**

If any of the WebSphere proxy server's port settings is incorrect, change it to the correct value.

**Procedure**

1. On the node where WebSphere proxy server is running, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click **Servers > Server Types > WebSphere proxy servers**.
3. In the list of proxy servers, click the node's WebSphere proxy server to open its Configuration page.
4. Under "Communications" click **Ports**.
5. Use the Ports table to change the SIP ports as follows:
   a. Click on the **PROXY_SIP_ADDRESS** link, change its setting (for example, to 5060), and then click **OK**.
   b. Click on the **PROXY_SIPS_ADDRESS** link, change its setting (for example, to 5061), and then click **OK**.
6. Save the changes by clicking the **Save** link in the "Messages" box at the top of the page.

*Changing the SIP Proxy and Registrar’s port settings:*

Change the defined port settings on an IBM Sametime node to avoid a conflict with the IBM WebSphere proxy server running on the same computer.
About this task

If any of the Sametime server’s port settings conflicts with a port used by the WebSphere proxy server running on the same node, enter new port settings now.

Procedure

1. On the node where the Sametime server is running, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Server Types > Application Servers.
3. In the list of application servers, click the Sametime server to open its Configuration page.
5. Use the Ports table to change the SIP ports as follows:
   a. Click on the PROXY_SIP_ADDRESS link, change its setting (for example, to 5062), and then click OK.
   b. Click on the PROXY_SIPS_ADDRESS link, change its setting to (for example, to 5063), and then click OK.
6. Save the changes by clicking the Save link in the “Messages” box at the top of the page.

Verifying ports for the virtual host:

After resolving a ports conflict, you should verify that all required ports are listed in the virtual host.

About this task

For instructions, see Adding ports to the virtual host alias.

Synchronizing nodes in the SIP Proxy and Registrar cluster:

Synchronize all nodes in the IBM Sametime cluster.

Procedure

1. On the cluster’s Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click System administration > Nodes.
3. Select all of the nodes in the cluster.
4. Click Full Resynchronize.

Verifying that the port collision has been resolved in the SIP Proxy and Registrar cluster:

After resolving port collisions between IBM WebSphere proxy server and IBM Sametime, verify that the port settings are now correct.

About this task

Start the servers in the cluster; clear the WebSphere proxy server’s logs before starting that server, and then check the logs for errors that may indicate a port collision.
Procedure
1. Start all of the servers and processes in the cluster except for the WebSphere proxy server where you just resolved the ports conflict.
2. Clear all of the WebSphere proxy server logs.
3. Start the WebSphere proxy server.
4. Check the WebSphere proxy server log for any errors indicating a possible port collision; for example:
   - ADMU3028I
   - TCPC0003E
   - The port may already be in use

What to do next
If other nodes in the cluster have both Sametime and WebSphere proxy server, be sure to check those nodes for possible port conflicts as well before continuing proceeding to the next task.

Installing IBM Load Balancer for the SIP Proxy and Registrar cluster:
Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.

Before you begin
Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Note: The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.

IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure
1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
      &uid=swg24029128
      &uid=swg24027364
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.

3. After you have installed IBM Load Balancer, configure two static IP addresses for it:

   - Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
   - Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

   For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:

   Table 50. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer:</td>
<td>Load balancer</td>
<td>192.0.2.15</td>
</tr>
<tr>
<td>loadbal.example.com</td>
<td>(Cluster address)</td>
<td></td>
</tr>
<tr>
<td>Cluster:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>st-cluster.example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>Deployment Manager</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td></td>
<td>(Sametime System Console)</td>
<td></td>
</tr>
<tr>
<td>svr1.example.com</td>
<td>Primary Node</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td></td>
<td>(a Sametime server)</td>
<td></td>
</tr>
<tr>
<td>svr2.example.com</td>
<td>Secondary Node</td>
<td>192.0.2.5</td>
</tr>
<tr>
<td></td>
<td>(a Sametime server)</td>
<td></td>
</tr>
</tbody>
</table>

Configure IBM Load Balancer for the SIP Proxy and Registrar cluster:

Configure IBM Load Balancer for a cluster of IBM Sametime servers.

About this task

The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

Configuring IBM Load Balancer for the SIP Proxy and Registrar cluster (Linux):

Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the
cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node’s MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.

Procedure

1. Configure the nodes of the cluster.
   
   **For cluster nodes running on AIX, Linux, and Solaris**
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   **For cluster nodes running on IBM i**
   Use the Add TCP/IP Interface command to create a virtual IP address with the “cluster” IP address you want to use.
   
   For example:
   
   ```bash
   ADDTCPIPFC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
   ```
   
   When the virtual TCP/IP interface is started, the server accepts packets for that address.

   **Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same “cluster” IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:

   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   **Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer’s Dispatcher process with the following command:
      ```bash
dserver
   ```
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).

      **AIX**
      1) Run the following command:
         ```bash
         autoconf6
         ```
      2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
Run the following command (you must be logged in as root):

```
modprobe ipv6
```

**Solaris** Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:

```
ifconfig device inet6 plumb
ifconfig device inet6 address/prefix up
```

d. Start the executor function of the dispatcher:

```
dscontrol executor start
```

e. Add the cluster to the service:

```
dscontrol cluster add cluster's_fully_qualified_host_name
```

where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

```
stms-cluster.example.com
```

f. Add the cluster port:

```
dscontrol port add cluster's_fully_qualified_host_name@port
```

where `cluster's_fully_qualified_host_name@port` is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:

```
stms-cluster.example.com@80
```

g. Add the nodes for which this server will balance workload:

```
dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node
```

where:

- `cluster_host@port@primary_node` indicates the cluster's fully qualified host name with the port appended as in the previous step, plus now with the primary node's fully qualified host name appended; for example:
  
  ```
stms-cluster.example.com@80@meetsvr1.example.com
  ```

- `cluster_host@port@secondary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
  
  ```
stms-cluster.example.com@80@meetsvr2.example.com
  ```

h. Now start the Load Balancer administration interface with the following command:

```
./lbadmin
```

**Note:** If you have difficulty starting the administration interface, try stopping and then starting the executor and dsserver services before running the command again:

```
dsserver stop
dscontrol executor stop
dscontrol executor start
dsserver start
./lbadmin
```

4. Continue configuring Load Balancer as follows:

a. Add the cluster to the executor:

```
dscontrol executor add cluster's_fully_qualified_host_name
```
where cluster’s_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

stms-cluster.example.com

b. Start the manager:
   dscontrol manager start

c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
   dscontrol advisor start http 80

5. Define server affinity with a "sticky time":
By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

a. Open a command window on the load balancer server.
b. Stop the service with the following command:
   dsserver stop
c. Set the sticky time with the following command:
   dscontrol port set fully_qualified_host_name@port_number stickytime number_of_seconds

Where:

- fully_qualified_host_name is the fully qualified host name of the server where IBM Load Balancer runs.
- port_number is the port that will be affected by the new sticky time setting.
- number_of_seconds is the duration, in seconds, of the time that a client should "stick to" the specified port.

For example:
   dscontrol port set myserver.com@80 stickytime 60

6. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).

   b. Click Save Configuration File as and accept the default name (default.cfg). The configuration settings stored in default.cfg are restored every time the server is restarted.

   c. Click OK.

Configuring IBM Load Balancer for the SIP Proxy and Registrar cluster (Windows):

Configure IBM Load Balancer on a server running Microsoft Windows.
Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

Procedure

1. Configure the nodes of the cluster.
   For cluster nodes running on Windows
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   For cluster nodes running on IBM i
   Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.

   For example:
   ADDTCPIFC INTNETADR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)

   When the virtual TCP/IP interface is started, the server accepts packets for that address.

   Note: Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:

   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process by clicking Start > Control Panel > Administrative Tools > Services. right-click IBM Dispatcher (ULB), and then click Start.
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Run the following command while logged in as the Windows administrator:
netsh interface ipv6 install
Theis command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.

d. Start the executor function of the dispatcher:
dsonruct executor start
e. Add the cluster to the service:
dsonruct cluster add cluster's_fully_qualified_host_name
where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
stms-cluster.example.com

f. Add the cluster port:
dsonruct port add cluster's_fully_qualified_host_name@port
where cluster's_fully_qualified_host_name@port is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
stms-cluster.example.com@80

g. Add the nodes for which this server will balance workload:
dsonruct server add cluster_host@port@primary_node
dsonruct server add cluster_host@port@secondary_node
where:
• cluster_host@port@primary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:
stms-cluster.example.com@80@meetsvr1.example.com

• cluster_host@port@secondary_node indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
stms-cluster.example.com@80@meetsvr2.example.com

h. Add the cluster to the executor:
dsonruct executor add cluster's_fully_qualified_host_name
where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
stms-cluster.example.com

i. Start the manager:
dsonruct manager start

j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
dsonruct advisor start http 80

k. Now you can stop the service:
dsserver stop

l. Close the command window.
4. Define server affinity with a "sticky time":

By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

**Windows**

a. Start IBM Load Balancer.

b. In the navigation tree, select the **Executor** (the load balancer's non-forwarding IP address, which appears under its host name).

c. Click **Configuration Settings**.

d. In "Port-Specific Settings", change the **Default sticky-time settings** from 0 to 60 seconds, and click **Update Configuration**.

e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:

a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).

b. Click **Save Configuration File as** and accept the default name (default.cfg).

   The configuration settings stored in default.cfg are restored every time the server is restarted.

c. Click **OK**.

**Clustering Conference Manager components:**

Configuring a cluster of IBM Sametime Media Manager "Conference Manager" components involves several tasks, including synchronizing system clocks, configuring one or more IBM WebSphere proxy servers to operate with the cluster.

**Before you begin**

You can create two types of clusters:

- A **Vertical cluster** resides on the Primary node and includes two or more cluster members, which run the same application.

- A **Horizontal cluster** includes a Primary node plus one or mode Secondary nodes, all running the same application. Each node contains one cluster member.
**Important:** It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Before you can configure a cluster of Sametime Media Manager "Conference Manager" components, you must have installed the following servers:

1. **Sametime System Console**
   This server will function as the cluster's Deployment Manager; the console can function as the Deployment Manager for multiple clusters.

   **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

2. **Sametime Community Server**
   At least one Sametime Community Server must be deployed to provide presence and awareness for users attending online meetings.

3. **Sametime Meeting Server**
At least one Sametime Meeting Server must be deployed to host online meetings where the audio and video features will be used.

4. Sametime Media Manager "Packet Switcher" component
   At least one Packet Switcher component must be deployed to route audio and video data to participant endpoints. You can deploy multiple Packet Switchers, but they cannot be clustered (the Conference Managers will balance the load among multiple Packet Switchers).

5. One Sametime Media Manager "Conference Manager" component, installed with the Primary Node option.
   Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster's application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node's application server. The Primary node's application server can only belong to one cluster. The Primary Node can be used as a container for additional cluster members when creating a vertical cluster (multiple cluster members on the same physical system).

6. (Horizontal cluster only) One or more Sametime Media Manager "Conference Manager" components, installed with the Secondary Node option.
   Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as a container for additional cluster members, which are can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a horizontal cluster.

To cluster Conference Manager components, complete the following tasks in the sequence shown:

**Attention:** You must complete all of the tasks to ensure your cluster operates properly.

**Related concepts**

“Clustering Sametime servers for high enterprise availability” on page 227

In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

*Setting clocks on the Conference Managers to be clustered:*

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.

**About this task**

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.
Procedure

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager’s (the Sametime System Console) system clock.

*Clustering Conference Managers:*

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

**Before you begin**

Start the Sametime System Console and the servers you intend to cluster.

**Note:** This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

**About this task**

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

**Procedure**

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing `servername.domain` with the fully qualified domain name of the Sametime System Console server.  
   http://servername.domain:8700/ibm/console  
2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.  
3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.  
4. Click **Guided Activities > Cluster WebSphere Application Servers**.

**Related tasks**

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Guided activity: Clustering Conference Managers:**

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.
Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.

   This guided activity applies to the following Sametime servers if they are installed in your deployment.
   - Sametime Proxy Server
   - Sametime Meeting Server
   - Sametime Media Manager

   Clustering is not available for the Packet Switcher; it is also not available for an "All Components” installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.
   - Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the sever after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster’s Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager’s SOAP port. The port
assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

Procedure

1. Cluster WebSphere Application Servers.
   Click Next to begin the clustering activity.

2. Select Product to Cluster.
   Select the product server to cluster, and then click Next.
   The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).

3. Select or Create a Cluster.
   To create a cluster:
   a. Click Create Cluster if you are setting up a new cluster.
   b. Type a descriptive name for the cluster in the Cluster Name field.
      For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.
   c. Click Next.
   To modify an existing cluster; for example, to add a new cluster member:
   a. Click Select Existing Cluster.
   b. Select a cluster in the Cluster Name list.
      If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.
   c. Click Next.

4. Select the Deployment Manager.
   In the Select Deployment Manager list, select the Sametime System Console as the cluster’s deployment manager, and then click Next.
   Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.

5. Create the Cluster with the Primary Node.
   You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node’s application server is running. Click Create cluster to configure the cluster settings, and then click Next.
Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. **Select One or More Secondary Nodes.**

   If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the **Secondary Node Name** list, click the node you want to add to the cluster and click **Next**.

7. **Add Cluster Members.**

   If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more "cluster members" to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.

   The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be "Clustered" if the cluster member has been completely configured on the node. If the status is "Ready to Cluster", select the Cluster Member and use the "Add to Cluster" button to finish configuring the cluster member.

   **Vertical cluster:**
   
   a. To add new cluster member, click **New**.
   
   b. Select the default name generated for the cluster member or enter your own cluster member server name.
   
   c. Select the Primary Node to create the cluster member on.
   
   d. Click **Add to Cluster**.
   
   The status will change from "Ready to cluster" to "Clustered".
   
   e. Click **Next**.

   **Horizontal cluster:**

   For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.

   a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.
   
   b. One at a time, select each cluster member and click **Add to Cluster**.
   
   Do not proceed until the current cluster member's status changes from "Ready to cluster" to "Clustered"; then you can add the next cluster member.
   
   c. If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.
   
   d. Click **Next**.

8. **Deployment Summary.**

   Click **Finish** to save the cluster configuration.

   Continue with the cluster configuration tasks described in the Sametime information center.

   **Configuring the Conference Manager cluster:**

   Complete the configuration for clustering IBM Sametime Media Manager Conference Manager components using an IBM WebSphere Application Server network deployment.
Before you begin

Create a cluster of Conference Manager components using the guided activity.

About this task

Completing the cluster's configuration requires the following tasks:

**Configuring the Conference Manager cluster to use the SIP Proxy and Registrar cluster:**

After you create clusters of IBM Sametime Media Manager Conference Manager components and SIP Proxy and Registrar components, configure the Conference Manager cluster to work with the IBM WebSphere proxy server that is used by the SIP Proxy and Registrar cluster (so that the two clusters share the proxy server).

Before you begin

Create and configure the Conference Manager and SIP Proxy and Registrar clusters.

About this task

By default, a Conference Manager is configured to access the SIP Proxy and Registrar component directly, and must be reconfigured to communicate with a cluster. Modify the Conference Manager's stavconfig.xml file to access the WebSphere proxy server used by the SIP Proxy Registrar cluster. The WebSphere proxy server will direct SIP requests to available nodes in the cluster. Complete this task for every Conference Manager in the cluster.

Procedure

1. On the server that is being used as the Deployment Manager, open the stavconfig.xml file for editing.

   The stavconfig.xml is located at:

   \dm_install_root\config\cells\cell_name\nodes\node_name\servers\server_name

   For example:

   \config\cells\bassMediaCell1\nodes\bassMediaNode1\servers\STMediaServer

2. Modify the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPProxyServerHost</td>
<td>Use the host name of the computer where the WebSphere proxy server is installed for the SIP Proxy and Registrar cluster.</td>
</tr>
<tr>
<td>SIPProxyServerPort</td>
<td>Use the PROXY_SIPS_ADDRESS port value of the same WebSphere proxy server (used by the SIP Proxy and Registrar cluster).</td>
</tr>
</tbody>
</table>

   For example:

   `<configuration lastUpdated="1226425838277" name="SIPProxyServerHost" value="waspProxy_pr.acme.com"/>
   <configuration lastUpdated="1226425838277" name="SIPProxyServerPort" value="5080"/>

3. Save and close the file.
4. Repeat for every Conference Manager in the cluster.

   5.
**Restarting and synchronizing nodes in the Conference Manager cluster:**

Synchronize the nodes in an IBM WebSphere Application Server network deployment.

**About this task**

Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node’s configuration.

**Procedure**

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Stop the Deployment Manager:
   a. Click **System Administration > Deployment manager**.
   b. Click the “Configuration” tab.
   c. On the Configuration tab of the deployment manager settings, click **Stop**.
3. Now start the Deployment Manager:
   a. Open a command window and navigate to the
      `app_server_root/profiles/DeploymentManagerName/bin` directory.
   b. Run the following command:
      
      **IBM AIX, Linux, or Solaris**
      ```
      ./startManager.sh
      ```
      **Microsoft Windows**
      ```
      startManager.bat
      ```
      **IBM i**
      1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.
      2) At the Qshell prompt, run the following commands:
         ```
         cd app_server_root/profiles/DeploymentManagerName/bin
         startManager dmgr
         ```
        
4. Log in to the Integrated Solutions Console.
5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:
   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes in the cluster.
   c. Click **Full Resynchronize**.
6. Restart all nodes in the cluster:
   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Node agents**.
   b. Click a node agent, and then click **Restart** (the node agent should already be running).

**Restarting the application servers in the Conference Manager cluster:**

During cluster configuration, each node’s application server was stopped so that the node could be federated. Start all of the application servers now.
About this task

Use the IBM Sametime System Console to start each of the application servers in the cluster.

Procedure

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Clusters > WebSphere application server clusters in the navigation tree.
3. Select the cluster’s check box and click Start to start all cluster member servers.

Setting up a WebSphere proxy server for the Conference Manager cluster:

Set up an IBM WebSphere proxy server for use with a cluster of IBM Sametime servers. The proxy server can be hosted on a product node, or on a separate computer; it performs routing and caching tasks for the servers in the cluster.

About this task

If you deployed the cluster using a standalone Deployment Manager, you must deploy a WebSphere proxy server to operate with the cluster. If the cluster uses the Sametime System Console as its Deployment Manager, the WebSphere proxy server was automatically deployed on the console but may need to be configured.

If the cluster experiences a high level of demand, you may want to deploy an additional, stand-alone, WebSphere proxy server to distribute the load and mitigate the single point-of-failure.

(Optional) Adding a stand-alone WebSphere proxy server to the Conference Manager cluster:

Install a stand-alone IBM WebSphere proxy server for use with a cluster of IBM Sametime servers.

Before you begin

This topic explains how to install a stand-alone WebSphere proxy server by installing an extra node into the Sametime cluster, removing the Sametime application, and then configuring the WebSphere proxy server that remains. If you just want to configure the WebSphere proxy server that was automatically installed with WebSphere Application Server on one of existing nodes in your Sametime cluster, skip this task and proceed directly to Configuring a WebSphere proxy server.

About this task

A cluster of Sametime servers requires at least one WebSphere proxy server to handle routing and caching tasks. When you install Sametime on a node in the cluster, WebSphere Application Server and WebSphere proxy server are also installed. The WebSphere proxy server merely needs to be configured for use.

To reduce the resource load on product nodes and avoid port conflicts, you may choose to install a stand-alone WebSphere proxy server on a separate computer instead of using the instance that was installed on a Sametime node. Or, you may
configure the instance on the Sametime node and then install an additional instance on a separate computer, and use a load balancer to share the load between them.

**Note:** If you previously installed a WebSphere proxy server on one of the Sametime nodes in the cluster and are now seeing excessive CPU usage on that node, you should install and configure an additional proxy server now.

To install a stand-alone WebSphere proxy server, you will install an extra Sametime node using the "Secondary Node" option, and then federate the new node into the cluster. You will then remove the Sametime application from the new node while leaving WebSphere proxy server intact. Finally, you will configure the WebSphere proxy server for use with the cluster.

*Installing an additional Sametime Conference Manager server as a Secondary Node in the Conference Manager cluster:*

Install an IBM Sametime product server as a Secondary Node, and then federate it into a cluster.

**About this task**

The first stage in deploying a stand-alone IBM WebSphere proxy server is to create a deployment plan, and then use the Sametime System Console to install the new Sametime server. Because you will later federate the new product node into the cluster, you must install the *same* product now.

**Important:** Install the new node using the "Secondary Node" option to ensure you can federate it to the cluster later.

*Federating the new Secondary Node to the Conference Manager cluster:*

Federate the newly installed Secondary Node into a cluster of IBM Sametime servers.

**About this task**

The next stage in deploying a stand-alone IBM WebSphere proxy server is to federate the new Sametime node into the existing cluster. For this task, you will use the Clustering guided activity, selecting the "Select Existing Cluster" option (in Step 3) and then choosing the appropriate cluster.

When you run the cluster guided activity there are phases: first, the proxy server is federated to the cluster's Deployment Manager; then the proxy server is added into the cluster as a new member. Be sure to complete all steps in the guided activity to properly add the proxy server to the cluster.

*Removing the Sametime product from the new node in the Conference Manager cluster:*

After you have federated a new IBM Sametime node to a cluster, remove the Sametime application but leave the IBM WebSphere proxy server intact.

**About this task**

After the new node has been federated to the cluster, it can be managed by the cluster's Deployment Manager. Since the purpose of this new node is to provide a
WebSphere proxy server, the Sametime product application is no longer needed on that node, and can be removed.

Procedure
1. On the cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > WebSphere application servers.
3. In the list of servers, click the name of the new Sametime node.
4. At the top of the list, click the Delete button.
5. When prompted for confirmation, click OK.
6. Save the change by clicking the Save link the "Messages" box at the top of the page.
7. Verify that the server has been deleted by making sure it no longer appears in the list of servers.

Configuring a WebSphere proxy server for the Conference Manager cluster:

Configure an IBM WebSphere proxy server to perform routing and caching tasks for a cluster of IBM Sametime servers running on WebSphere Application Server.

Before you begin

Create a cluster of Sametime servers running on WebSphere Application Server; start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Use these instructions to configure a WebSphere proxy server that operates with the following Sametime server clusters:

• Meeting Server
• Conference Manager
• SIP Proxy and Registrar

About this task

A cluster of Sametime servers that run on WebSphere Application Server can use a WebSphere proxy server to manage routing and caching tasks. To ensure redundancy in the case of a proxy server failure, you may want to configure multiple proxy servers for the cluster. Use a Load Balancer in that case to divide the incoming load between the proxy servers. You can host a WebSphere proxy server on any node in the cluster (except the Sametime System Console) but because it uses a lot of system resources, you may want to host it on its own computer.

Note: If you install multiple WebSphere proxy servers, you will need a Load Balancer to divide the incoming load among the proxy servers. Installing IBM Load Balancer is discussed later in this section.

Procedure
1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. In the navigation tree, click Servers > Server Types > WebSphere proxy servers.
3. In the proxy servers table, click the New button at the top of the table.
4. In the "Create a new proxy server entry" dialog box, do the following:
   a. In the "Select a node" box, select the node that will host the WebSphere proxy server.
      Be sure to select a node that belongs to the appropriate cluster.
   b. Type a name for the new proxy server; for example "was_proxy1", and then click Next.
   c. In the "Specify server specific properties" box, select the appropriate "Support protocol" settings for your cluster, select Generate unique ports, and then click Next.
      • If you are configuring this WebSphere proxy server for a Meeting Server cluster: deselect the SIP protocol.
      • If you are configuring this WebSphere proxy server for a SIP Proxy and Registrar cluster: accept both HTTP and SIP protocols.
      • If you are configuring this WebSphere proxy server for a Conference Manager cluster: accept both HTTP and SIP protocols.
   d. In the "Select a server template" box, select proxy_server_foundation (the WebSphere Default Proxy Server Template), and then click Next.
   e. In the "Confirm new server" box, click Finish.
5. Save the changes by clicking the Save link in the "Messages" box at the top of the page.
6. Resynchronize the nodes:
   a. On the Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
   b. Click System Administration > Nodes.
   c. Select all of the nodes in the cluster.
   d. Click Full Resynchronize.
7. (Conference Manager cluster, SIP Proxy and Registrar cluster) Assign the new proxy server to the cluster:
   a. Click Servers > Server Types > Websphere proxy servers > proxy_server_name > SIP Proxy Server Settings > SIP proxy settings.
   b. In the "Default cluster" field, select the cluster that you are configuring this WebSphere proxy server to work with.
   c. Click Apply.
   d. Save the changes by clicking the Save link in the "Messages" box at the top of the page.
8. Now start the new WebSphere proxy server:
   a. Again in the Integrated Solutions Console's navigation tree, click Servers > Server Types > WebSphere proxy servers.
   b. In the "WebSphere proxy servers" page, select the new proxy server from the list.
   c. Click the Start button above the list of proxy servers.

Adding ports to the Deployment Manager's virtual host alias:

After creating an IBM Sametime Media Manager Conference Manager cluster, add the SIP ports of each cluster member to the virtual host alias.
Before you begin

Create a cluster of IBM Sametime Media Manager "Conference Manager" components. Adding the SIP ports of each cluster member to the virtual host alias is required to ensure that the cluster operates properly.

About this task

On the cluster's Deployment Manager (the Sametime System Console), update the default_host virtual host with a unique set of web access ports. Such a configuration lets a single host machine resemble multiple host machines.

Tip: Print this page and use the table to record the port settings as you look them up in steps 1 and 2:

Table 51. Write down the port numbers used for these settings in every cluster member

<table>
<thead>
<tr>
<th>Cluster member</th>
<th>SIP_DEFAULTHOST</th>
<th>SIP_DEFAULTHOST_SECURE</th>
<th>PROXY_SIP_ADDRESS</th>
<th>PROXY_SIPS_ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster member 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster member 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Procedure

1. Determine the ports used by every cluster member:
   a. In the Deployment Manager's (the Sametime System Console) Integrated Solutions Console, click Servers > Server Types > WebSphere application servers.
   b. In the table listing the servers, click the name of the cluster member. This displays the cluster member's "Configuration" page.
   d. Look in the Ports table and write down the following port settings for use in the next step:
      • SIP_DEFAULTHOST
      • SIP_DEFAULTHOST_SECURE
   e. Repeat this process for every cluster member.
2. Next, determine the ports used by every WebSphere proxy server that operates with this cluster.
   a. In the Deployment Manager's (the Sametime System Console) Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers.
   b. In the table listing the servers, click the name of the WebSphere proxy server. This displays the cluster member's "Configuration" page.
   d. Look in the Ports table and write down the following port settings for use in the next step:
      • PROXY_SIP_ADDRESS
      • PROXY_SIPS_ADDRESS
e. Repeat this process for every WebSphere proxy server used by the cluster.

3. Now add the ports used by all the cluster members and all of the WebSphere proxy servers to the Deployment Manager’s Virtual Hosts table.
   a. Now return to the Integrated Solutions Console navigation tree and click Environment > Virtual Hosts.
   b. In the Virtual Hosts table, click the host called default_host.
      This displays the “Configuration” page for the default_host.
   d. In the “Host Aliases” table, add the ports used by all of the cluster members (the information you collected in Step 1):
      Remember that you have information on two ports for each cluster member; however if a port is already listed in the table, you do not need to add it again.
      To add a port:
      1) Click the New button at the top of the table.
      2) In the Host Name field, type *.
      3) In the Port field, type a port from your list.
      4) Click OK.
      5) Repeat this for the two ports for every cluster member (unless a port is already listed in this table).
   e. Now delete all of the table entries that do not use * as the Host Name.
      To delete an entry, click on the check box next to it, and then click the Delete button at the top of the table.
   f. Save the changes by clicking the Save link in the "Messages" box at the top of the page.

4. Synchronize all of the nodes:
   a. Still working on the Deployment Manager, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.

Reconfiguring ports for a WebSphere proxy server hosted on a product node in the Conference Manager cluster:

If the IBM WebSphere proxy server is hosted on the same computer as an IBM Sametime product, reconfigure ports to avoid a conflict.

Checking for port conflicts between the Conference Manager and WebSphere proxy server:

If the IBM Sametime Media Manager’s SIP Proxy and Registrar server and the WebSphere Application Server SIP Proxy server are running on the same computer, avoid problems by verifying that the IBM WebSphere Application Server SIP Proxy Server is listening on the correct ports and is not in conflict with the IBM Sametime SIP Proxy and Registrar server running on the same computer.

About this task

Follow these steps to compare the SIP ports used by the WebSphere Application Server SIP Proxy with those used by the Sametime SIP Proxy and Registrar Server cluster member running on the same machine. If your cluster has both Sametime
and WebSphere proxy server running on multiple nodes, be sure to check the ports on each node.

Procedure
1. On the node being checked, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Check the ports used by the WebSphere Application Server SIP Proxy server:
   a. Click Servers > Server Types > WebSphere proxy servers.
   b. In the list of proxy servers, click the node's WebSphere Application Server SIP Proxy server to open its Configuration page.
   c. Under "Communications" click Ports.
   d. Write down the values assigned to the following ports:
      • PROXY_SIP_ADDRESS
      • PROXY_SIPS_ADDRESS
3. Check the ports used by the Sametime SIP Proxy and Registrar Server cluster member running on the same computer.
   a. Click Servers > Server Types > WebSphere application servers.
   b. In the list of application servers, click the name of the Sametime SIP Proxy and Registrar Server to open its Configuration page.
   c. Under "Communications" click Ports.
   d. Write down the values assigned to the following ports:
      • SIP_DEFAULTHOST
      • SIP_DEFAULTHOST_SECURE

Results
The ports are in conflict if the WebSphere Application Server SIP Proxy server is listening on the same ports as the Sametime SIP Proxy and Registrar server.

What to do next
Your next task depends on whether there is a port conflict to resolve:
• If the ports are in conflict, proceed to Changing a WebSphere proxy server's port settings.
• If the ports are not in conflict, then the WebSphere proxy server configuration is complete. Skip to Installing IBM Load Balancer.

Changing a WebSphere proxy server’s port settings for the Conference Manager cluster:

Change the defined port settings on an IBM WebSphere proxy server used by an IBM Sametime cluster.

About this task
If any of the WebSphere proxy server’s port settings is incorrect, change it to the correct value.

Procedure
1. On the node where WebSphere proxy server is running, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the list of proxy servers, click the node's WebSphere proxy server to open its Configuration page.
4. Under "Communications" click Ports.
5. Use the Ports table to change the SIP ports as follows:
   a. Click on the PROXY_SIP_ADDRESS link, change its setting (for example, to 5060), and then click OK.
   b. Click on the PROXY_SIPS_ADDRESS link, change its setting (for example, to 5061), and then click OK.
6. Save the changes by clicking the Save link in the "Messages" box at the top of the page.

Changing the Conference Manager’s port settings:

Change the defined port settings on an IBM Sametime node to avoid a conflict with the IBM WebSphere proxy server running on the same computer.

About this task

If any of the Sametime server’s port settings conflicts with a port used by the WebSphere proxy server running on the same node, enter new port settings now.

Procedure

1. On the node where the Sametime server is running, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Server Types > Application Servers.
3. In the list of application servers, click the Sametime server to open its Configuration page.
4. Under "Communications" click Ports.
5. Use the Ports table to change the SIP ports as follows:
   a. Click on the PROXY_SIP_ADDRESS link, change its setting (for example, to 5062), and then click OK.
   b. Click on the PROXY_SIPS_ADDRESS link, change its setting to (for example, to 5063), and then click OK.
6. Save the changes by clicking the Save link in the "Messages" box at the top of the page.

Synchronizing nodes in the Conference Manager cluster:

Synchronize all nodes in the IBM Sametime cluster.

Procedure

1. On the cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click System administration > Nodes.
3. Select all of the nodes in the cluster.
4. Click Full Resynchronize.

Verifying that the port collision has been resolved in the Conference Manager cluster:

After resolving port collisions between IBM WebSphere proxy server and IBM Sametime, verify that the port settings are now correct.
About this task

Start the servers in the cluster; clear the WebSphere proxy server's logs before starting that server, and then check the logs for errors that may indicate a port collision.

Procedure

1. Start all of the servers and processes in the cluster except for the WebSphere proxy server where you just resolved the ports conflict.
2. Clear all of the WebSphere proxy server logs.
3. Start the WebSphere proxy server.
4. Check the WebSphere proxy server log for any errors indicating a possible port collision; for example:
   - ADMU3028I
   - TCP0003E
   - The port may already be in use

What to do next

If other nodes in the cluster have both Sametime and WebSphere proxy server, be sure to check those nodes for possible port conflicts as well before continuing proceeding to the next task.

Configuring the Packet Switchers to access the cluster’s WebSphere proxy server:

After you create clusters of IBM Sametime Media Manager Conference Manager and SIP Proxy and Registrar components, configure the Packet Switcher components to communicate with the cluster through the IBM WebSphere proxy server.

Before you begin

Install at least one Lotus Media Manager Packet Switcher component and start the server. Create and configure the Conference Manager and SIP Proxy and Registrar clusters.

About this task

By default, a Packet Switcher is configured to access the Conference Manager and the SIP Proxy and Registrar components directly, and must be reconfigured to communicate with clusters. Modify the Packet Switcher's stavconfig.xml file to access the WebSphere proxy servers used by the Conference Manager cluster and the SIP Proxy and Registrar cluster. The WebSphere proxy server will direct SIP requests to available nodes in the cluster.

You will need to complete this task for every Packet Switcher.

Procedure

1. On the server hosting the Packet Switcher, open the stavconfig.xml file for editing.
   - The stavconfig.xml is located at:
     dm_install_root/config/cells/cell_name/nodes/node_name/servers/server_name
   - For example:
2. Modify the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConferenceServerHost</td>
<td>Use the host name of the computer where the WebSphere proxy server is installed for the Conference Manager cluster.</td>
</tr>
<tr>
<td>ConferenceServerPort</td>
<td>Use the PROXY_SIPS_ADDRESS port value of the same WebSphere proxy server (used by the Conference Manager cluster).</td>
</tr>
<tr>
<td>SIPProxyServerHost</td>
<td>Use the host name of the computer where the WebSphere proxy server is installed for the SIP Proxy and Registrar cluster.</td>
</tr>
<tr>
<td>SIPProxyServerPort</td>
<td>Use the PROXY_SIPS_ADDRESS port value of the same WebSphere proxy server (used by the SIP Proxy and Registrar cluster).</td>
</tr>
</tbody>
</table>

For example:

```xml
<configuration lastUpdated="1226425838277" name="ConferenceServerHost" value="wasproxy_cf.acme.com"/>
<configuration lastUpdated="1226425838277" name="ConferenceServerPort" value="5062"/>
<configuration lastUpdated="1226425838277" name="SIPProxyServerHost" value="wasproxy_pr.acme.com"/>
<configuration lastUpdated="1226425838277" name="SIPProxyServerPort" value="5080"/>
```

3. Save and close the file.

4. Repeat steps 1 through 3 for each additional Packet Switcher in the deployment.

5. (Optional) Synchronize all nodes in the Deployment Manager that manages the Packet Switcher:
   - This step is not needed if the Packet Switcher was installed using the Network Deployment > Primary Node option.
   - a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
   - b. Click Full Resynchronize.

6. Restart the Packet Switchers.

**Installing IBM Load Balancer for the Conference Manager cluster:**

Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.

**Before you begin**

Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

**Note:** The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.
IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure

1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
        &uid=swg24029128
        &uid=swg24027364
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
   For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.

3. After you have installed IBM Load Balancer, configure two static IP addresses for it:
   - Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
   - Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

   For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:

   **Table 52. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer**

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer:</td>
<td>Load balancer</td>
<td>Load balancer (NFA):192.0.2.15</td>
</tr>
<tr>
<td>loadbal.example.com</td>
<td>(Cluster address)</td>
<td>Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>Cluster:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>st-cluster.example.com</td>
<td>Deployment Manager</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td></td>
<td>(Sametime System Console)</td>
<td></td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>Primary Node (a Sametime server)</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td>svr1.example.com</td>
<td>Secondary Node (a Sametime server)</td>
<td>192.0.2.5</td>
</tr>
<tr>
<td>svr2.example.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   **Configuring IBM Load Balancer for the Conference Manager cluster:**

   Configure IBM Load Balancer for a cluster of IBM Sametime servers.
About this task

The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

*Configuring IBM Load Balancer for the Conference Manager cluster (Linux):*

Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

**Before you begin**

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load Balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node’s MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.

**Procedure**

1. Configure the nodes of the cluster.
   - **For cluster nodes running on AIX, Linux, and Solaris**
     Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   - **For cluster nodes running on IBM i**
     Use the `ADDTCPIFC INTNETADR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)` command to create a virtual IP address with the “cluster” IP address you want to use.

     For example:
     ```plaintext
     ADDTCPIFC INTNETADR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)
     ```
     When the virtual TCP/IP interface is started, the server accepts packets for that address.

     **Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the `PREFIFC` parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same “cluster” IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   - IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.
Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process with the following command:
      `dsserver`
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).
      **AIX**
      1) Run the following command:
         `autoconf6`
      2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
         `start/usr/bin/autoconf6 * -A`
      **Linux** Run the following command (you must be logged in as root):
         `modprobe ipv6`
      **Solaris** Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:
         `ifconfig device inet6 plumb`
         `ifconfig device inet6 address/prefix up`
   d. Start the executor function of the dispatcher:
      `dscontrol executor start`
   e. Add the cluster to the service:
      `dscontrol cluster add cluster's_fully_qualified_host_name`
      where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
      `stms-cluster.example.com`
   f. Add the cluster port:
      `dscontrol port add cluster's_fully_qualified_host_name@port`
      where `cluster's_fully_qualified_host_name@port` is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
      `stms-cluster.example.com@80`
   g. Add the nodes for which this server will balance workload:
      `dscontrol server add cluster_host@port@primary_node`
      `dscontrol server add cluster_host@port@secondary_node`
      where:
      * `cluster_host@port@primary_node` indicates the cluster's fully qualified host name with the port appended as in the previous step, plus now with the primary node's fully qualified host name appended; for example:
        `stms-cluster.example.com@00meetsvr1.example.com`
      * `cluster_host@port@secondary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the
secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:

stms-cluster.example.com@80@meetsvr2.example.com

h. Now start the Load Balancer administration interface with the following command:

./lbadmin

**Note:** If you have difficulty starting the administration interface, try stopping and then starting the executor and dsserver services before running the command again:

dsserver stop
dsserver stop
dsserver executor start
dsserver start

4. Continue configuring Load Balancer as follows:

a. Add the cluster to the executor:

dscntrol executor add cluster's_fully_qualified_host_name

where *cluster's_fully_qualified_host_name* is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

stms-cluster.example.com

b. Start the manager:

dscntrol manager start

c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):

dscntrol advisor start http 80

5. Define server affinity with a "sticky time":

By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

a. Open a command window on the load balancer server.

b. Stop the service with the following command:

dsserver stop
c. Set the sticky time with the following command:

```
dscntrol port set fully_qualified_host_name@port_number stickytime number_of_seconds
```

Where:

- *fully_qualified_host_name* is the fully qualified host name of the server where IBM Load Balancer runs.
• `port_number` is the port that will be affected by the new sticky time setting.
• `number_of_seconds` is the duration, in seconds, of the time that a client should "stick to" the specified port.

For example:

dsmcontrol port set myserver.com@80 stickytime 60

6. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
   b. Click Save Configuration File as and accept the default name (default.cfg).
      The configuration settings stored in default.cfg are restored every time the server is restarted.
   c. Click OK.

Configuring IBM Load Balancer for the Conference Manager cluster (Windows):

Configure IBM Load Balancer on a server running Microsoft Windows.

Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

Procedure

1. Configure the nodes of the cluster.
   a. **For cluster nodes running on Windows**
      Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   b. **For cluster nodes running on IBM i**
      Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.
      For example:
      
```
ADDTCP1FC INTNETADR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)
```
      When the virtual TCP/IP interface is started, the server accepts packets for that address.
Note: Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
   IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

   Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer's Dispatcher process by clicking Start > Control Panel > Administrative Tools > Services. right-click IBM Dispatcher (ULB), and then click Start.
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Run the following command while logged in as the Windows administrator:
      ```
      netsh interface ipv6 install
      ```
      This command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.
   d. Start the executor function of the dispatcher:
      ```
      dscontrol executor start
      ```
   e. Add the cluster to the service:
      ```
      dscontrol cluster add cluster's_fully_qualified_host_name
      ```
      where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
      ```
      stms-cluster.example.com
      ```
   f. Add the cluster port:
      ```
      dscontrol port add cluster's_fully_qualified_host_name@port
      ```
      where `cluster's_fully_qualified_host_name@port` is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
      ```
      stms-cluster.example.com@80
      ```
   g. Add the nodes for which this server will balance workload:
      ```
      dscontrol server add cluster_host@port@primary_node
      dscontrol server add cluster_host@port@secondary_node
      ```
      where:
      - `cluster_host@port@primary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:
        ```
        stms-cluster.example.com@80@meetsvr1.example.com
        ```
      - `cluster_host@port@secondary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the
secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:

    stms-cluster.example.com@80@meetsvr2.example.com

h. Add the cluster to the executor:

d control executor add cluster's_fully_qualified_host_name

where cluster's_fully_qualified_host_name is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

    stms-cluster.example.com


i. Start the manager:

d control manager start

j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):

d control advisor start http 80

k. Now you can stop the service:

dsserver stop

l. Close the command window.

4. Define server affinity with a "sticky time":

By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

**Windows**

a. Start IBM Load Balancer.

b. In the navigation tree, select the **Executor** (the load balancer's non-forwarding IP address, which appears under its host name).

c. Click **Configuration Settings**.

d. In "Port-Specific Settings", change the **Default sticky-time settings** from 0 to 60 seconds, and click **Update Configuration**.

e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:

a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).

b. Click **Save Configuration File as** and accept the default name (default.cfg).

   The configuration settings stored in default.cfg are restored every time the server is restarted.

c. Click **OK**.
Managing multiple Packet Switcher nodes in a cluster with the Sametime System Console:

In a clustered environment, if you have installed an additional Packet Switcher node, you must manually map the application modules to manage them with the Sametime System Console.

Procedure
1. Log in to the Sametime System Console on the Deployment Manager.
2. Click Applications > Application Types > WebSphere enterprise applications.
3. Click the link for the Packet Switcher .ear file.
4. Under Modules, click Manage Modules.
5. Select all the application modules listed.
6. Under Clusters and servers, select the two Packet Switcher server instances.
   Click Apply.
7. Click OK and save the changes.
8. Synchronize the changes with the nodes.
9. Restart the application servers.

Installing a Sametime Meeting Server

Follow the instructions for your operating system to install an IBM Sametime Meeting Server.

About this task

Important: If you will be supporting the use of LiveNames in your Sametime deployment, you should deploy all Sametime Meeting Servers and Sametime Proxy Servers within the same subnet. It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Related tasks
“Configuring a Sametime Meeting Server” on page 1031
This section describes how to configure a Sametime Meeting Server.

Creating a database for the Sametime Meeting Server

Before installing the IBM Sametime Meeting Server on AIX, Linux, Solaris, or Windows, create a database to store its data.

About this task

Run the scripts that come with the Sametime Meeting Server package. They are also included with Sametime in the DB2 installation package.

Procedure
1. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation.
2. Open a command prompt and navigate to the folder where you extracted the SametimeMeetingServer installation package.
3. Create the database by entering one of the following commands from the SametimeDB2 folder. Wait until you see confirmation that the database has been created and the command has finished.

- **AIX, Linux, or Solaris.** `/createMeetingDb.sh STMS dbadmin`
- **Windows.** `createMeetingDb.bat STMS dbadmin`

Replace STMS in the command if you want to choose a different database name. Names can be from 1 - 8 characters, but cannot contain special or multibyte characters.

Replace `dbadmin` with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.

When naming DB2 objects, follow the rules for your operating system.

4. Close the command window.

5. Open the DB2 control center.

- **AIX, Linux, or Solaris**
  
  Open the IBM DB2 folder on the desktop and click **Control Center**.

- **Windows**
  
  Click **Start > Programs > IBM DB2 > General Administration Tools > Control Center**.

6. Find the database name to verify that the new database was created.

**Related tasks**

“Installing DB2 on Linux or Windows” on page 251

Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store information about servers, users, bandwidth configuration, and meetings.

Sametime Advanced uses DB2 to store information about persistent chats and broadcast communities.

**Connecting Sametime Meeting Server to a DB2 database**

Use the Sametime System Console to connect to the Sametime Meeting Server, Sametime Gateway, or Sametime Advanced database before installing the server from the System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

**Before you begin**

Start the Sametime System Console if it is not already running.

**Procedure**

If you have not already opened the Connect to DB2 Databases activity, follow these steps:

1. From a browser, enter the following URL, replacing `servername.domain` with the fully qualified domain name of the Sametime System Console server.

   `http://servername.domain:8700/ibm/console`

   For example:

   `http://sametime.example.com:8700/ibm/console`

   **IBM i**: The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary or use the setting...
specified for the Administrative console secure port in the AboutThisProfile.txt file. For the Sametime System Console Deployment Manager Profile (STSCDmgrProfile), the file is located in the following path:
/QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/
STSCDmgrProfile/logs/AboutThisProfile.txt

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Sametime Prerequisites > Connect to DB2 Databases.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Sametime prerequisite: Connecting to a DB2 database:

This activity takes you through the steps for connecting to the Meeting Server, Gateway, or Advanced Server database you created.

Before you begin

AIX, Linux, Solaris, Windows: Ensure that IBM DB2 has been installed and that you have created the Sametime Meeting Server, Gateway, or Sametime Advanced database.

IBM i: Ensure that you have created the required database schemas and tables.

In the Connect to DB2 Databases portlet, verify that the Sametime System Console database you created earlier is already displayed in the list of databases.

About this task

Follow these steps to connect to the Meeting Server, Gateway, or Advanced Server database. You must do this before you can install the Meeting Server or the Advanced Server using the Sametime System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

Procedure
1. DB2 Configuration Guided Activity.
   Click Add to begin the guided activity that will connect your server to the DB2 database. If a connection already exists, you can optionally edit or delete it.

2. Add a new database:
   a. In the Connect to DB2 Databases portlet, click Add.
      If you want to edit or delete a database instead, then select one, and click the appropriate button.
   b. Enter the fully qualified host name of the DB2 server in the Host name field.
      Do not enter an IP address or a short host name.
c. The Port field shows the default port of 50000. Accept the default unless you specified a different port during DB2 installation or your server is using a different port.
   Linux: Check the /etc/services file on the DB2 server to verify the port number being used.

d. In the Database name, field, enter the name of the database you want to connect to.

e. In the Application user ID field, supply the DB2 application’s administrative user name that you created when you installed DB2, such as db2admin. This user has database administration authority and you will use this user ID and password whenever you work with DB2 databases for Sametime. On IBM i, this is the user profile you specified as the owner of the Meeting Server database schemas in your copy of the stms.default.response.properties file or the user profile you logged in with when you created the Gateway database schemas.

f. In the Application password field, enter the password for the DB2 administrative user ID.

g. (Meeting Server or Gateway databases) If you are connecting to a database on an IBM i server, click Hosted on IBM i.

h. Click Finish.

Preparing to install a Sametime Meeting Server

Use the Sametime System Console to prepare to install a Sametime Meeting Server by pre-populating values required for installation.

Before you begin

Start the Sametime System Console if it is not already running.

Procedure

If you have not already opened the Install Sametime Meeting Server guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
   For example:http://sametime.example.com:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Sametime Guided Activities > Install Sametime Meeting Server.
Related tasks

“Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine” on page 371
When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server on the same machine using the same server host name, conflicts with cookies that are used by each server can occur. If you install both servers on the same machine, then configure the Sametime Proxy Server with a host alias as a different host name.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install a Sametime Meeting Server:

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

Before you begin

You have set up an IBM DB2 database and an LDAP server, and have run the guided activities for connecting to the DB2 database and to the LDAP server.

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Meeting Server.

Procedure

1. Plan a product installation.
   In the Install Sametime Meeting Server portlet, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.
   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.
   The name should include the installation and node type, such as stMeeting_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.

   Select the product version you want to install, and then click Next.

4. Choose the configuration type.
   Select Primary Node if this is the first server of its type. Select Secondary Node for additional servers. Then click Next.
   The Cell option is reserved for special-use cases in which the server must be self-contained. If you select Cell, you must provide a host name, user ID, and password when prompted to do so.

5. Node Federation at Install Time.
   This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click Next.
Attention: Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

6. WebSphere Profile Settings.
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click Next.
   If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

   Important: This must be a unique user ID that does not exist in the LDAP directory.

7. Choose a database for this deployment. This panel appears if you selected Primary node or Cell as the configuration type.
   Select the Sametime Meeting Server database that you configured with the Sametime System Console activity, and then click Next.

8. Connect to an LDAP Server. This panel appears if you selected Cell as the configuration type.
   Select the LDAP directory that you configured with the Sametime System Console guided activity, and then click Next.

   Review the summary screen, and then click Finish.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click Modify an Existing Deployment Plan and update the plan. All changes must be made prior to running installation.

What to do next

“Installing a meeting server on AIX, Linux, Solaris, or Windows”

Installing a meeting server on AIX, Linux, Solaris, or Windows
Run the installation program on the machine where you plan to install a Sametime Meeting Server.

Before you begin

You should have already created a deployment plan for the Sametime Meeting Server. Verify that the deployment plan is in the “Ready to Install” state and start the Sametime System Console server. Be sure there are no firewalls or connectivity problems to the LDAP server or the installation will fail.

Linux The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the
Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**
If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:** Check the hosts file and remove any lines that start with the following:
- 127.0.0.1 *fully_qualified_domain_name short_name*
- ::1 *fully_qualified_domain_name short_name*

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

**About this task**

By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

**Important:** For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server deployments.

**Procedure**

1. **Red Hat Enterprise Linux only:** Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the `SELINUX` setting. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.
3. Prepare to use the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
      Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following command:
```bash
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - AIX, Linux, and Solaris: ./launchpad.sh
   - Windows: launchpad.exe

Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

sametime_server_package is the installation package name for this server.

platform is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM Sametime Meeting Server and click Launch IBM Sametime Meeting Server 8.5.2 installation.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.

9. Click Install.

10. Select the packages that you want to install and click Next.
11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Select a package group option and accept the installation directory. Then click **Next**.
   - Select **Create a new package group** if you have not installed any other Sametime software on this machine.
   - Leave **Use the existing package group** selected if you are installing several Sametime servers on the same machine.

13. Select **IBM Sametime Meeting Server 8.5.2** as the feature to install and select **Use Sametime System Console to install**. Click **Next**.

14. At the Common Configurations screen, supply values for connecting to the Sametime System Console.
   - **Host Name**: Provide the fully qualified domain name in the Host Name field for the Sametime System Console. The host name was determined when you installed the Sametime System Console. The host name must be the actual host name and not a DNS alias.
   - **Use SSL**: Leave this option selected to run the server over a secure connection.
   - **HTTPS Port**: Leave 9443 as the default value.
   - **User ID and password**: Provide the WebSphere Application Server User ID and password that you created when you installed the Sametime System Console.

15. Provide the host name for the machine you are currently using, which is the same name you used when you created the deployment plan for this installation.
   - Do not use an IP address or short host name.

16. Click **Validate** to log in to the Sametime System Console.
   - The button name changes to **Validated** after you log in.

17. When you are logged in, click **Next**.

18. Select the Sametime Meeting Server deployment plan you created earlier with the Sametime System Console guided activity. Then click **Next**.

19. Review the deployment settings, then click **Next**.

20. Review the summary, then click **Install** to start the installation.

21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the **ant** and **native** subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var.ibm/InstallationManager/logs

   Console connection log: /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs
Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Windows 2003
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.

Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 481
Starting and stopping IBM Sametime servers that run on WebSphere Application Server involves other server components such as the Deployment Manager and the node agent.

“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Verifying a Sametime Meeting Server installation:

Log in to the Sametime Meeting Server to verify that the installation was successful.

About this task
Verify the installation by logging in to the server. Then try creating a new meeting room.

Procedure
1. From a web browser, navigate to the Meeting Room Center by entering the following URL:
   http://servername.domain/stmeetings
   Replace serverhostname.domain with your server name. For example:
   http://stmeet1.example.com/stmeetings

   Tip: To verify the port number being used by the application, log in to the console on the Sametime Meeting Server:
   a. Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
      http://servername.domain:8600/ibm/console
8600 is the default port when the Meeting Server is installed as a Cell Profile.
For example:
http://stmeet1.example.com:8600/ibm/console

b. Enter the WebSphere Application Server User ID and password that you created when you installed the server.

c. Click Servers > WebSphere application servers > STMeetingServer > ports > WC_defaulthost to find the port number.

You can also verify the HTTP port number being used by the Sametime Meeting Server by opening the AboutThisProfile.txt file for the Sametime Meeting Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is short_host_nameSTMPNProfile1 when you use a deployment plan to install the server. On IBM i, look for the AboutThisProfile.txt file in the following location:
/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs/AboutThisProfile.txt

2. Click Log In and then enter your User name and Password to log in to the Meeting Center. Use the name and password that is in the LDAP directory connected to the Sametime System Console.

3. Click New Meeting Room, then fill in the fields and click Save.

4. The new meeting appears in the list of meetings that you own. Click Enter Meeting Room below the name of the new meeting to join the meeting.

Installing a Sametime Meeting Server in silent mode

If the system to be installed does not have a graphical user interface, you can perform a silent installation using a customized response file. The results are the same as if you had installed using the IBM Installation Manager and deployment plans. This procedure applies to installing IBM DB2 for Linux or Windows, the Sametime System Console, the Sametime Proxy Server, the Sametime Media Manager, the Sametime Meeting Server, and Sametime Advanced. This procedure does not apply to IBM Sametime Community Server, Sametime Gateway, or Sametime Bandwidth Manager.

Before you begin

Information about downloading packages for Sametime is located at the following web address:

&uid=swg24029128

&uid=swg24027364

Use the Sametime system console to create a deployment plan that contains installation values for the server that you are installing.

About this task

Follow these steps to install the IBM Installation Manager in silent mode. Customize each product’s response file, then install the product in silent mode using the customized response file.
Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server and Advanced Server deployments.

Procedure

1. From the installation media, copy and extract the files from the installation image to a temporary directory \TMP on the computer where you will be installing the server offering.

2. Navigate to the directory where you copied and extracted the installation files:
   \TMP\server_offering

3. Fully documented sample response files are contained in the responseFiles directory on the installation DVD. The response file to use in this procedure is the one that you use with an existing deployment plan and includes _ssc.rsp in its file name. Make a copy of the file and use that copy for the rest of this procedure. The other response files in the directory are used for installing without a deployment plan and uninstalling, respectively.

4. In a text editor, open the response file and edit the values to correspond to values that you would normally supply in the installation windows.
   For all installations except DB2, include the Sametime System Console host name, port, and user credentials and the name of the deployment plan that you created.

5. The SSCPassword value should be encoded. To generate an encoded password, use the generateEncodedPassword utility packaged with the installer.
   The utility is on the installation media in the same directory as launchpad.exe or launchpad.sh.


7. Open a command window.

8. Enter the following command to install the IBM Installation Manager in silent mode.
   - AIX, Linux, or Solaris
     SametimeOffering/IM/windows/install
     --launcher.ini silent-install.ini
   - Windows
     SametimeOffering\IM\windows\installc --launcher.ini silent-install.ini

9. Navigate to the Installation Manager installation directory. The default directories are shown below.
   - AIX, Linux, or Solaris
     /opt/ibm/InstallationManager/eclipse
   - Windows
     C:\Program Files\IBM\Installation Manager\eclipse

10. For all installations except DB2, start the Sametime System Console.

11. Enter the following command to install the product in silent mode, specifying the edited response file name and path and a log file name.
    - AIX, Linux, or Solaris
      ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
    - Windows
      IBMIMc --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense

Tip: Generating a response file automatically
The following command runs the graphical installation program without installing software. You can use the resulting response file in a silent installation.

```
./install --launcher.ini your .ini file -record response file path -skipInstall agentDataLocation
```

The response file is stored in the `agentDataLocation` directory, which must be a writable directory. You can use the new file as the response file in a silent installation. You can use the same `agentDataLocation` in the next recording session to record updating or modifying the product. The products that you installed, and the preferences, including repository settings that you use in the graphical user installation interface or the record mode without using `-skipInstall` are not stored.

**Clustering Sametime Meeting Servers**

Configuring a cluster of IBM Sametime Meeting Servers involves several tasks, including synchronizing system clocks, configuring the cluster settings, and configuring an IBM WebSphere proxy server for the cluster, as well as optionally deploying an IBM Load Balancer in front of the cluster.

**Before you begin**

You can create two types of clusters:

- A **Vertical cluster** resides on the Primary node and includes two or more cluster members, which run the same application.
- A **Horizontal cluster** includes a Primary node plus one or more Secondary nodes, all running the same application. Each node contains one cluster member.
Important: It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Before you can configure a cluster of Sametime Meeting Servers, you must have installed the following servers:

- The Sametime System Console
  This server can function as the Deployment Manager for the vertical or horizontal cluster scenarios described in this procedure.

  Attention: Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

- (Optional) Sametime Community Servers
  At least one Sametime Community Server must be deployed if you want to provide presence and awareness for users attending online meetings.

- One Sametime Meeting Server installed with the Primary Node option.
Every cluster requires exactly one Primary Node. The application server on the Primary Node will function as the cluster’s application template. All other application servers in the cluster (nodes and cluster members) will be duplicated from the Primary Node’s application server. The Primary node’s application server can only belong to one cluster. The Primary Node can be used as a container for additional cluster members when creating a vertical cluster (multiple cluster members on the same physical system). The Primary Node must already be registered with the Sametime System Console. Registration happens automatically on AIX Linux, Solaris, and Windows, but on IBM i, you run the registration utility to register servers.

• (Horizontal cluster only) One or more Sametime Meeting Servers installed with the Secondary Node option.

Secondary nodes are used to horizontally scale your cluster across multiple physical systems. These additional nodes act as containers for additional cluster members, which can be used to balance loads and provide failover within the cluster. During the clustering process, you can deploy additional product application servers on any Secondary Nodes within the cluster, creating a horizontal cluster (one cluster member on each Secondary Node, plus one cluster member or one vertical cluster on the Primary Node). Secondary Nodes must already be registered with the Sametime System Console. Registration happens automatically on AIX Linux, Solaris, and Windows, but on IBM i, you run the registration utility to register servers.

About this task

There are several tasks involved in creating a cluster; complete them in the sequence shown here:

Attention: Complete all of the tasks to ensure your cluster operates properly.

Related concepts

“In Clustering Sametime servers for high enterprise availability” on page 227

In an enterprise deployment, use clustering to provide failover and load balancing by creating a cluster of multiple Sametime servers of the same type. Each cluster of servers can be managed by the Sametime System Console. Most clustered Sametime deployments have several clusters – one for each type of Sametime server. All Sametime servers can be clustered except for the Sametime System Console and the Packet Switcher component of the Media Manager.

Setting clocks on the servers to be clustered:

Synchronize the system clocks on the servers to be clustered with an IBM WebSphere Application Server network deployment.

About this task

This task is required to ensure that the servers can be federated to the Deployment Manager during creation of the cluster. Working on the Sametime System Console, complete this task for every server that you will add to the cluster.

Procedure

For each server that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager’s (the Sametime System Console) system clock.
Clustering Sametime servers running on WebSphere Application Server:

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

Start the Sametime System Console and the servers you intend to cluster.

Note: This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.
3. On the left side of the navigation tree, click the Sametime System Console task to open it.
4. Click Guided Activities > Cluster WebSphere Application Servers.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Clustering Sametime servers running on WebSphere Application Server:

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.
This guided activity applies to the following Sametime servers if they are installed in your deployment.

- Sametime Proxy Server
- Sametime Meeting Server
- Sametime Media Manager

Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.

- Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster's Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell – this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager’s SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions.
Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

Procedure
1. Cluster WebSphere Application Servers.
   Click Next to begin the clustering activity.
2. Select Product to Cluster.
   Select the product server to cluster, and then click Next.
   The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).
3. Select or Create a Cluster.
   To create a cluster:
   a. Click Create Cluster if you are setting up a new cluster.
   b. Type a descriptive name for the cluster in the Cluster Name field.
      For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.
   c. Click Next.
   To modify an existing cluster; for example, to add a new cluster member:
   a. Click Select Existing Cluster.
   b. Select a cluster in the Cluster Name list.
      If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.
   c. Click Next.
4. Select the Deployment Manager.
   In the Select Deployment Manager list, select the Sametime System Console as the cluster’s deployment manager, and then click Next.
   Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.
5. Create the Cluster with the Primary Node.
   You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node’s application server is running. Click Create cluster to configure the cluster settings, and then click Next.
   Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.
6. Select One or More Secondary Nodes.
   If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and
federated the secondary nodes when you installed them. In the **Secondary Node Name** list, click the node you want to add to the cluster and click **Next**.

7. **Add Cluster Members.**

If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more "cluster members" to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.

The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be "Clustered" if the cluster member has been completely configured on the node. If the status is "Ready to Cluster", select the Cluster Member and use the "Add to Cluster" button to finish configuring the cluster member.

**Vertical cluster:**

a. To add new cluster member, click **New**.

b. Select the default name generated for the cluster member or enter your own cluster member server name.

c. Select the Primary Node to create the cluster member on.

d. Click **Add to Cluster**.

   The status will change from "Ready to cluster" to "Clustered".

e. Click **Next**.

**Horizontal cluster:**

For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.

a. Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.

b. One at a time, select each cluster member and click **Add to Cluster**.

   Do not proceed until the current cluster member's status changes from "Ready to cluster" to "Clustered"; then you can add the next cluster member.

c. If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.

d. Click **Next**.

8. **Deployment Summary.**

   Click **Finish** to save the cluster configuration.

   Continue with the cluster configuration tasks described in the Sametime information center.

**Configuring the cluster:**

Complete the configuration for clustering IBM Sametime Meeting Servers using an IBM WebSphere Application Server network deployment.

**Before you begin**

Create a cluster of Sametime Meeting Servers using the guided activity, synchronize the nodes in the cluster, and start all of the application servers.
About this task

Completing the cluster's configuration requires the following tasks:

*Restarting and synchronizing nodes in the cluster:*

Synchronize the nodes in an IBM WebSphere Application Server network deployment.

About this task

Synchronizing nodes in a cluster ensures that the Deployment Manager has an up-to-date copy of each node's configuration.

Procedure

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Stop the Deployment Manager:
   a. Click System Administration > Deployment manager.
   b. Click the "Configuration" tab.
   c. On the Configuration tab of the deployment manager settings, click Stop.
3. Now start the Deployment Manager:
   a. Open a command window and navigate to the app_server_root/profiles/DeploymentManagerName/bin directory.
   b. Run the following command:
      - IBM AIX, Linux, or Solaris:
        ```
        ./startManager.sh
        ```
      - Microsoft Windows:
        ```
        startManager.bat
        ```
      - IBM i:
        1) On the Control Language (CL) command line, run the Start Qshell (STRQSH) command.
        2) At the Qshell prompt, run the following commands:
           ```
           cd app_server_root/profiles/DeploymentManagerName/bin
           startManager dmgr
           ```
4. Log in to the Integrated Solutions Console.
5. Wait until the nodes have all started. Then follow these steps to synchronize all the nodes:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.
6. Restart all nodes in the cluster:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Node agents.
   b. Click a node agent, and then click Restart (the node agent should already be running).

*Restarting the application servers in the cluster:*
During cluster configuration, each node's application server was stopped so that the node could be federated. Start all of the application servers now.

**About this task**

Use the IBM Sametime System Console to start each of the application servers in the cluster.

**Procedure**

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Servers > Clusters > WebSphere application server clusters** in the navigation tree.
3. Select the cluster's check box and click **Start** to start all cluster member servers.

**Setting up a WebSphere proxy server for the cluster:**

Set up an IBM WebSphere proxy server for use with a cluster of IBM Sametime servers. The proxy server can be hosted on a product node, or on a separate computer; it performs routing and caching tasks for the servers in the cluster.

**About this task**

If you deployed the cluster using a standalone Deployment Manager, you must deploy a WebSphere proxy server to operate with the cluster. If the cluster uses the Sametime System Console as its Deployment Manager, the WebSphere proxy server was automatically deployed on the console but may need to be configured.

If the cluster experiences a high level of demand, you may want to deploy an additional, stand-alone, WebSphere proxy server to distribute the load and mitigate the single point-of-failure.

**(Optional) Adding a stand-alone WebSphere proxy server to the cluster:**

Install a stand-alone IBM WebSphere proxy server for use with a cluster of IBM Sametime servers.

**Before you begin**

This topic explains how to install a stand-alone WebSphere proxy server by installing an extra node into the Sametime cluster, removing the Sametime application, and then configuring the WebSphere proxy server that remains. If you just want to configure the WebSphere proxy server that was automatically installed with WebSphere Application Server on one of existing nodes in your Sametime cluster, skip this task and proceed directly to Configuring a WebSphere proxy server.

**About this task**

A cluster of Sametime servers requires at least one WebSphere proxy server to handle routing and caching tasks. When you install Sametime on a node in the cluster, WebSphere Application Server and WebSphere proxy server are also installed. The WebSphere proxy server merely needs to be configured for use.
To reduce the resource load on product nodes and avoid port conflicts, you may choose to install a stand-alone WebSphere proxy server on a separate computer instead of using the instance that was installed on a Sametime node. Or, you may configure the instance on the Sametime node and then install an additional instance on a separate computer, and use a load balancer to share the load between them.

**Note:** If you previously installed a WebSphere proxy server on one of the Sametime nodes in the cluster and are now seeing excessive CPU usage on that node, you should install and configure an additional proxy server now.

To install a stand-alone WebSphere proxy server, you will install an extra Sametime node using the "Secondary Node" option, and then federate the new node into the cluster. You will then remove the Sametime application from the new node while leaving WebSphere proxy server intact. Finally, you will configure the WebSphere proxy server for use with the cluster.

*Installing an additional Sametime server as a Secondary Node:*

Install an IBM Sametime product server as a Secondary Node, and then federate it into a cluster.

**About this task**

The first stage in deploying a stand-alone IBM WebSphere proxy server is to create a deployment plan, and then use the Sametime System Console to install the new Sametime server. Because you will later federate the new product node into the cluster, you must install the *same* product now.

**Important:** Install the new node using the "Secondary Node" option to ensure you can federate it to the cluster later.

*Federating the new Secondary Node to the cluster:*

Federate the newly installed Secondary Node into a cluster of IBM Sametime servers.

**About this task**

The next stage in deploying a stand-alone IBM WebSphere proxy server is to federate the new Sametime node into the existing cluster. For this task, you will use the Clustering guided activity, selecting the "Select Existing Cluster" option (in Step 3) and then choosing the appropriate cluster.

When you run the cluster guided activity there are phases: first, the proxy server is federated to the cluster’s Deployment Manager; then the proxy server is added into the cluster as a new member. Be sure to complete all steps in the guided activity to properly add the proxy server to the cluster.

*Adding the additional WebSphere proxy server to the Meeting Server cluster:*

Use the IBM Sametime System Console to create a cluster of Sametime Servers hosted on IBM WebSphere Application Server. The Sametime servers must all be running the same type of server; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.
Before you begin

Start the Sametime System Console and the servers you intend to cluster.

**Note:** This guided activity is only for Sametime servers hosted on IBM WebSphere Application Server, and does not apply to the Sametime Community Server.

About this task

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Procedure

If you have not already opened the Cluster WebSphere Application Servers guided activity, follow these steps:

1. From a browser, enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the Sametime System Console server.
   
   `http://serverhostname.domain:8700/ibm/console`

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Guided Activities > Cluster WebSphere Application Servers**.

Related tasks

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Adding the additional WebSphere proxy server to the Meeting Server cluster:

This guided activity takes you through the steps for clustering new IBM Sametime servers hosted on IBM WebSphere Application Server. The servers you add to the cluster must all be running the same Sametime product application; for example, Sametime Meeting Server, Sametime Proxy Server, Sametime Media Manager Conference Manager, Sametime Media Manager SIP Proxy and Registrar, or Sametime Advanced.

Before you begin

1. Install the Sametime System Console and two or more Sametime servers of the same product type; then start the Sametime System Console and all of the servers you plan to cluster.

   This guided activity applies to the following Sametime servers if they are installed in your deployment.
   - Sametime Proxy Server
   - Sametime Meeting Server
   - Sametime Media Manager

   Clustering is not available for the Packet Switcher; it is also not available for an "All Components" installation of the Media Manager, which includes the
Packet Switcher. The Conference Manager components and the SIP Proxy and Registrar components must be installed and clustered on dedicated computers.

- Sametime Advanced

2. Run the backupConfig utility for the Deployment Manager, the Primary Node, and any Secondary Nodes before beginning the cluster guided activity. The utility is located in the bin folder under the profile of each server. The utility automatically shuts down any running servers in the profile, so you must restart the servers after running the utility. Use the restoreConfig utility to restore the configuration if the changes need to be undone. For more information on backupConfig and restoreConfig, see the WebSphere Application Server Information Center.

**About this task**

Multiple product clusters are not supported on a single computer; however, vertical clusters (all cluster members installed on the Primary Node) are supported when each product cluster is on a dedicated computer. A horizontal cluster is defined as a cluster with each cluster member having a dedicated computer (one on the Primary Node and one on each Secondary Node).

Note that you cannot use this activity to cluster Sametime Community Servers (see "Clustering Sametime Community Servers") or Sametime Gateway servers (see "Installing Sametime Gateway servers in a cluster").

Configure a cluster of one type of product server to improve performance with high availability, and to provide failover. You can create a horizontal cluster in which each node is hosted on a separate computer, as well as a vertical cluster with multiple cluster members hosted on the Primary Node.

These instructions generally assume that you will use the Sametime System Console as the cluster's Deployment Manager, which provides a single Integrated Solutions Console for all WebSphere administrative functions for all servers participating in the cell—this simplifies the administrative experience. If you deploy clusters for both Sametime Proxy Server and Sametime Meeting Server, then at least one of those clusters require a dedicated Deployment Manager.

If you are creating or updating a cluster that does not use the Sametime System Console as the Deployment Manager, it is necessary to ensure that the Deployment Managers are able to create SOAP connections to each other. A firewall should not be blocking the SOAP port and the host names should be resolvable. Also the System Console needs to access any standalone primary node’s application port and a primary node needs to access its Deployment Manager’s SOAP port. The port assignments may be different so it is important to verify them in the Integrated Solutions Console. The Deployment Manager ports are under the System Administration -> Deployment Manager -> Ports section. A server’s ports can be checked by selecting the server in the Servers view of Integrated Solutions Console. The SOAP ports are called SOAP_CONNECTOR_ADDRESS and the application ports are WC_defaulthost and WC_defaulthost_secure.

**Procedure**

1. Cluster WebSphere Application Servers.
   
   Click **Next** to begin the clustering activity.

2. Select Product to Cluster.
Select the product server to cluster, and then click Next.

The list only displays Sametime products for which one or more servers have been installed and registered with the Sametime System Console. If you installed servers using deployment plans, they are registered with the console automatically. If you did not use a deployment plan, you must manually register the servers with the console before proceeding as you would if installation failed (see "Registering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows" in the Troubleshooting section).

3. Select or Create a Cluster.

To create a cluster:

a. Click Create Cluster if you are setting up a new cluster.

b. Type a descriptive name for the cluster in the Cluster Name field.
   For example, if you are creating a cluster of Sametime Meeting Servers, you will probably want to indicate that in the cluster name so you can easily identify it later.

c. Click Next.

To modify an existing cluster; for example, to add a new cluster member:

a. Click Select Existing Cluster.

b. Select a cluster in the Cluster Name list.
   If you are going to add a node or cluster member to the cluster, you must use the same Sametime product. For example, you cannot add a Sametime Meeting Server cluster member to a cluster of Sametime Proxy Servers.

c. Click Next.

4. Select the Deployment Manager.

In the Select Deployment Manager list, select the Sametime System Console as the cluster’s deployment manager, and then click Next.

Every cluster must have exactly one Deployment Manager; the Sametime System Console can function as the Deployment Manager for multiple clusters. Remember that if you will create clusters for both Sametime Proxy Server and Sametime Meeting Server, at least one of those clusters requires a dedicated Deployment Manager; this is only true when your deployment will include both types of cluster.

5. Create the Cluster with the Primary Node.

You created and federated a primary node when you installed the first server for this product. Make sure that the Primary Node’s application server is running. Click Create cluster to configure the cluster settings, and then click Next.

Do not click anywhere on the browser until the operation completes or it may interrupt the clustering process.

6. Select One or More Secondary Nodes.

If you are creating a horizontal cluster where each node is hosted on a separate computer, add one or more secondary nodes to the cluster. You created and federated the secondary nodes when you installed them. In the Secondary Node Name list, click the node you want to add to the cluster and click Next.

7. Add Cluster Members.

If you are creating a vertical cluster where multiple copies of the application are hosted on a single computer, add one or more “cluster members” to the Primary Node. If you are creating a horizontal cluster, add one cluster member to each of the secondary nodes you federated in the previous step.
The table lists Cluster Members, the Node that the cluster resides on, and the Status of each cluster member. Each node in the cluster needs to have at least one cluster member created on it for the node to be used in the cluster. The status of a Cluster Member will be “Clustered” if the cluster member has been completely configured on the node. If the status is “Ready to Cluster”, select the Cluster Member and use the "Add to Cluster" button to finish configuring the cluster member.

**Vertical cluster:**
- To add new cluster member, click **New**.
- Select the default name generated for the cluster member or enter your own cluster member server name.
- Select the Primary Node to create the cluster member on.
- Click **Add to Cluster**.

  The status will change from "Ready to cluster" to "Clustered".
- Click **Next**.

**Horizontal cluster:**
For each Secondary Node you added in the previous step, a cluster member is prepopulated into the table for you, one on each of the Secondary Nodes.
- Select the default cluster member name for each server or update with your own name, and verify that the nodes the cluster member servers will be created on are correct for your topology.
- One at a time, select each cluster member and click **Add to Cluster**.

  Do not proceed until the current cluster member’s status changes from "Ready to cluster" to "Clustered"; then you can add the next cluster member.
- If you want to add more cluster members, click **New** to add another row to the table, and then fill out the information accordingly.
- Click **Next**.

8. Deployment Summary.
- Click **Finish** to save the cluster configuration.
- Continue with the cluster configuration tasks described in the Sametime information center.

**Removing the Sametime product from the new node:**

After you have federated a new IBM Sametime node to a cluster, remove the Sametime application but leave the IBM WebSphere proxy server intact.

**About this task**

After the new node has been federated to the cluster, it can be managed by the cluster’s Deployment Manager. Since the purpose of this new node is to provide a WebSphere proxy server, the Sametime product application is no longer needed on that node, and can be removed.

**Procedure**
1. On the cluster’s Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click **Servers > WebSphere application servers**.
3. In the list of servers, click the name of the new Sametime node.
4. At the top of the list, click the **Delete** button.
5. When prompted for confirmation, click **OK**.
6. Save the change by clicking the Save link the “Messages” box at the top of the page.

7. Verify that the server has been deleted by making sure it no longer appears in the list of servers.

*Configuring a WebSphere proxy server:*

Configure an IBM WebSphere proxy server to perform routing and caching tasks for a cluster of IBM Sametime servers running on WebSphere Application Server.

*Before you begin*

Create a cluster of Sametime servers running on WebSphere Application Server; start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.

Use these instructions to configure a WebSphere proxy server that operates with the following Sametime server clusters:

- Meeting Server
- Conference Manager
- SIP Proxy and Registrar

*About this task*

A cluster of Sametime servers that run on WebSphere Application Server can use a WebSphere proxy server to manage routing and caching tasks. To ensure redundancy in the case of a proxy server failure, you may want to configure multiple proxy servers for the cluster. Use a Load Balancer in that case to divide the incoming load between the proxy servers. You can host a WebSphere proxy server on any node in the cluster (except the Sametime System Console) but because it uses a lot of system resources, you may want to host it on its own computer.

*Note:* If you install multiple WebSphere proxy servers, you will need a Load Balancer to divide the incoming load among the proxy servers. Installing IBM Load Balancer is discussed later in this section.

*Procedure*

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.

2. In the navigation tree, click **Servers > Server Types > WebSphere proxy servers**.

3. In the proxy servers table, click the **New** button at the top of the table.

4. In the ”Create a new proxy server entry” dialog box, do the following:
   
   a. In the ”Select a node” box, select the node that will host the WebSphere proxy server.
      
      Be sure to select a node that belongs to the appropriate cluster.
   
   b. Type a name for the new proxy server; for example "was_proxy1", and then click **Next**.
   
   c. In the ”Specify server specific properties” box, select the appropriate “Support protocol” settings for your cluster, select **Generate unique ports**, and then click **Next**.
If you are configuring this WebSphere proxy server for a Meeting Server cluster: deselect the SIP protocol.

If you are configuring this WebSphere proxy server for a SIP Proxy and Registrar cluster: accept both HTTP and SIP protocols.

If you are configuring this WebSphere proxy server for a Conference Manager cluster: accept both HTTP and SIP protocols.

d. In the "Select a server template" box, select **proxy_server_foundation** (the WebSphere Default Proxy Server Template), and then click **Next**.

e. In the "Confirm new server" box, click **Finish**.

5. Save the changes by clicking the **Save** link in the "Messages" box at the top of the page.

6. Resynchronize the nodes:
   a. On the Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
   b. Click **System Administration** > **Nodes**.
   c. Select all of the nodes in the cluster.
   d. Click **Full Resynchronize**.

7. (Conference Manager cluster, SIP Proxy and Registrar cluster) Assign the new proxy server to the cluster:
   a. Click **Servers** > **Server Types** > **Websphere proxy servers** > **proxy_server_name** > **SIP Proxy Server Settings** > **SIP proxy settings**.
   b. In the "Default cluster" field, select the cluster that you are configuring this WebSphere proxy server to work with.
   c. Click **Apply**.
   d. Save the changes by clicking the **Save** link in the "Messages" box at the top of the page.

8. Now start the new WebSphere proxy server:
   a. Again in the Integrated Solutions Console’s navigation tree, click **Servers** > **Server Types** > **WebSphere proxy servers**.
   b. In the "WebSphere proxy servers" page, select the new proxy server from the list.
   c. Click the **Start** button above the list of proxy servers.

---

### Enabling the WebSphere proxy server to cache dynamic content:

Optionally configure an IBM WebSphere proxy server to cache dynamic content.

**Before you begin**

Configure a WebSphere proxy server for use with a cluster of Sametime Meeting Servers, and then start the WebSphere proxy server.

**About this task**

The WebSphere proxy server does not cache application server dynamic content by default; you can optionally enable caching by completing these steps.

**Procedure**

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Server Types** > **WebSphere Proxy Servers**.
3. In the "WebSphere Proxy Servers" dialog box, select the proxy you would like to enable dynamic caching on.

4. On the "Configuration" page, expand **HTTP Proxy Server Settings** and under it, click **Proxy Settings**.

5. On the "Proxy Settings" page, locate the "Caching section" and do the following:
   - a. Go to the "Enable Caching" section.
   - b. Select a cache from the "Cache instance name" list.
   - c. Click **Cache Dynamic Content**.
   - d. Accept the default "Cache update URI" value.
   - e. Click **OK**.
   - f. Click **Save**.

6. Synchronize all nodes in the cluster:
   - a. Back in the Integrated Solution Console’s navigation tree, click **System Administration > Nodes**.
   - b. Select all of the nodes in the cluster.
   - c. Click **Full Resynchronize**.

---

**Creating object cache instances for the WebSphere proxy server:**

Create an object cache for the IBM WebSphere proxy server so it can track which server hosts each online meeting.

**Before you begin**

Add one or more WebSphere proxy servers that will operate with a cluster of IBM Sametime Meeting Servers.

**About this task**

The WebSphere proxy server requires an object cache in which to store information tracking which online meetings are hosted on which Sametime Meeting Servers.

**Procedure**

1. Log in to the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.

2. Click **Resources > Cache Instances > Object Cache Instances**.

3. Click in the **Scope** field and select a WebSphere proxy server that will be used by the cluster of Sametime Meeting Servers.

4. Click **New**.
   - This launches a wizard to create the new object cache.

5. In the "New Object Cache" dialog box, click in the **Name** field and type a descriptive name for the new cache; for example "Wasproxy1_Id_Cache".

6. In the **JNDI Name** field, type **proxy/rtc4web_id_cache** exactly as shown.

7. Click **OK** to complete the wizard.

8. Save your changes to the master configuration by clicking the **Save** button when prompted.

9. Repeat this process for each WebSphere proxy server used by the cluster.

**Adding a path for routing filters on the WebSphere proxy server:**
Add a path to the IBM WebSphere proxy server's class path loader to enable the IBM Sametime routing filters to be loaded correctly for a cluster.

**Before you begin**

Configure one or more WebSphere proxy servers to operate with the cluster of Sametime servers.

**About this task**

Defining a path for "ws.ext.dirs" enables the Sametime routing filters to be properly loaded by the root class path loader.

**Procedure**

1. Log in to the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Servers > Server Types > WebSphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify. This displays the Configuration tab for the selected proxy server.
5. Under "Additional Properties", click **Java Virtual Machine**.
6. Under "Additional Properties", click **Custom Properties**.
7. In the table listing the custom properties, click the **New** button.
8. Create a new entry named **ws.ext.dirs** with the value `${USER_INSTALL_ROOT}/optionalLibraries/rtc` (spell it exactly as shown here).
9. Click **OK** to save the new custom property.
10. Click **Save**.
11. Repeat this process for every WebSphere proxy server that is operating with the cluster.
12. Synchronize the nodes and restart the cluster of Sametime servers:
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes in the cluster.
   c. Back in the navigator, click **System Administration > Node agents**.
   d. Click a node agent, and then click **Restart**; repeat for each node agent.

**Installing IBM Load Balancer in a Meeting Server cluster:**

Install and configure IBM Load Balancer to distribute workload among a cluster of these type of servers: Sametime Proxy Server, Sametime Meeting Server, Media Manager Conference Manager, or Media Manager SIP Proxy and Registrar, and Sametime Advanced.

**Before you begin**

Create the cluster of servers first. Then configure the cluster and then start the Deployment Manager (the Sametime System Console) as well as all node agents and application servers in the cluster.
Note: The IBM Load Balancer is not available on IBM i, but you can deploy it on a server running a different operating system for use with a Sametime deployment hosted on IBM i.

IBM Load Balancer is not required for a Sametime clustered deployment; you can use any load-balancing mechanism that supports HTTP session affinity so that a user is repeatedly routed to the same server during a single session. IBM Load Balancer is included in the Sametime package with the other IBM WebSphere components.

Procedure
1. Download IBM Load Balancer onto the server where you will install it:
   a. Open this release's Download document at the following web address:
         &uid=swg24029128
         &uid=swg24027364
   b. Locate the appropriate IBM WebSphere Edge server component in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
2. Navigate to the folder where you stored the downloaded files, locate the folder for IBM Load Balancer, and start the installation program.
   For instructions on installing IBM Load Balancer, see the Load Balancer for IPv4 and IPv6 configuration guide.
3. After you have installed IBM Load Balancer, configure two static IP addresses for it:
   • Non-Forwarding Address: The NFA is the address of the server itself. It is used for logging in and administering the load balancer.
   • Cluster Address: This is the address by which clients and other servers will access the cluster. It must be DNS-resolvable.

   For example, suppose your cluster contains two nodes, and you configure an IBM Load Balancer for the cluster. Your IP addresses will look like this:

   Table 53. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer

<table>
<thead>
<tr>
<th>Fully qualified host name</th>
<th>Server's role in deployment</th>
<th>Server's IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer: loadbal.example.com</td>
<td>Load balancer (Cluster address)</td>
<td>Load balancer (NFA): 192.0.2.15</td>
</tr>
<tr>
<td>Cluster: st-cluster.example.com</td>
<td></td>
<td>Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>stconsole.example.com</td>
<td>Deployment Manager (Sametime System Console)</td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>svr1.example.com</td>
<td>Primary Node (a Sametime server)</td>
<td>192.0.2.4</td>
</tr>
<tr>
<td>svr2.example.com</td>
<td>Secondary Node (a Sametime server)</td>
<td>192.0.2.5</td>
</tr>
</tbody>
</table>
Configuring IBM Load Balancer in a Meeting Server cluster:

Configure IBM Load Balancer for a cluster of IBM Sametime servers.

About this task

The steps to configure IBM Load Balancer are different for the various operating systems; choose the appropriate topic:

Configuring IBM Load Balancer on AIX, Linux, or Solaris in a Sametime Advanced cluster:

Configure IBM Load Balancer on a server running IBM AIX, Linux, or Sun Solaris.

Before you begin

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

About this task

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address. Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

As you work through the procedure, you will switch back and forth between the Load Balancer interface and a command window.

Procedure

1. Configure the nodes of the cluster.
   
   For cluster nodes running on AIX, Linux, and Solaris
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.

   For cluster nodes running on IBM i
   Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.
   For example:
   ADDTCP1FC INTNETADR('192.0.2.0') LIND(+VIRTUALIP) SUBNETMASK(+HOST)
   When the virtual TCP/IP interface is started, the server accepts packets for that address.

   Note: Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:
IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

Tip: When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. Configure load balancing for the cluster:
   a. Open a command window on the load balancer server.
   b. Start the load balancer’s Dispatcher process with the following command:
      
   c. If you are using IPv6 addresses, enable the processing of IPv6 packets:
      Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start (on Solaris, the executor will start, but no IPv6 packets can be viewed).

   AIX
   1) Run the following command:
      ```
      autoconf6
      ```
   2) To enable uninterrupted processing of IPv6 packets, even after a system reboot, edit the etc/rc.tcpip file and uncomment the following line, and add the -A flag:
      ```
      startusr/bin/autoconf6 " " -A
      ```

   Linux Run the following command (you must be logged in as root):
   ```
   modprobe ipv6
   ```
   Solaris Run the following command (you must be logged in as su) to change the device to your device name, and change the IPv6 IP address and prefix to your address and prefix values:
   ```
   ifconfig device inet6 plumb
   ifconfig device inet6 address/prefix up
   ```
   d. Start the executor function of the dispatcher:
   ```
   dscontrol executor start
   ```
   e. Add the cluster to the service:
   ```
   dscontrol cluster add cluster's_fully_qualified_host_name
   ```
   where `cluster's_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
   ```
   stms-cluster.example.com
   ```
   f. Add the cluster port:
   ```
   dscontrol port add cluster's_fully_qualified_host_name@port
   ```
   where `cluster's_fully_qualified_host_name@port` is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:
   ```
   stms-cluster.example.com@80
   ```
   g. Add the nodes for which this server will balance workload:
   ```
   dscontrol server add cluster_host@port@primary_node
   dscontrol server add cluster_host@port@secondary_node
   ```
   where:
• *cluster_host@port@primary_node* indicates the cluster's fully qualified host name with the port appended as in the previous step, plus now with the primary node's fully qualified host name appended; for example:
  stms-cluster.example.com@80@meetsvr1.example.com

• *cluster_host@port@secondary_node* indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
  stms-cluster.example.com@80@meetsvr2.example.com

h. Now start the Load Balancer administration interface with the following command:
   
   ```
   ./lbadmin
   ```

   **Note:** If you have difficulty starting the administration interface, try stopping and then starting the executor and dsserver services before running the command again:
   ```
   dsserver stop
   dscontrol executor stop
   dscontrol executor start
   dsserver start
   ./lbadmin
   ```

4. Continue configuring Load Balancer as follows:

   a. Add the cluster to the executor:
      ```
      dscontrol executor add cluster's_fully_qualified_host_name
      ```
      where *cluster's_fully_qualified_host_name* is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
      ```
      stms-cluster.example.com
      ```

   b. Start the manager:
      ```
      dscontrol manager start
      ```

   c. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
      ```
      dscontrol advisor start http 80
      ```

5. Define server affinity with a "sticky time":

   By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

   The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

   a. Open a command window on the load balancer server.
   b. Stop the service with the following command:
      ```
      dsserver stop
      ```
   c. Set the sticky time with the following command:
dscontrol port set fully_qualified_host_name@port_number stickytime number_of_seconds

Where:
- `fully_qualified_host_name` is the fully qualified host name of the server where IBM Load Balancer runs.
- `port_number` is the port that will be affected by the new sticky time setting.
- `number_of_seconds` is the duration, in seconds, of the time that a client should "stick to" the specified port.

For example:
    dscontrol port set myserver.com@80 stickytime 60

6. Save the load balancer settings:
   a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
   b. Click Save Configuration File as and accept the default name (default.cfg).
      The configuration settings stored in default.cfg are restored every time the server is restarted.
   c. Click OK.

Configuring IBM Load Balancer in a Meeting Server cluster (Windows):

Configure IBM Load Balancer on a server running Microsoft Windows.

**Before you begin**

Install IBM Load Balancer and assign two static IP addresses to it. The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.

**About this task**

Configure IBM Load balancer to support your cluster using MAC Address rewriting. With this method, the load balancer receives a packet intended for the cluster. It uses configured metrics to determine which node in the cluster should process the message, and then sends the message back out to the network, routing it to the appropriate node's MAC address.

Each of the nodes in the cluster is configured with a loopback adapter; when the packet is rewritten to the network, the appropriate node will receive and process the packet.

**Procedure**

1. Configure the nodes of the cluster.
   **For cluster nodes running on Windows**
   Add a loopback adapter with the IP address of the cluster on each of the nodes of the cluster. For instructions, see the Load Balancer for IPv4 and IPv6 administration guide.
   **For cluster nodes running on IBM i**
   Use the Add TCP/IP Interface command to create a virtual IP address with the "cluster" IP address you want to use.
   For example:
ADDTCPFIC INNATDAR('192.0.2.0') LIND(*VIRTUALIP) SUBNETMASK(*HOST)

When the virtual TCP/IP interface is started, the server accepts packets for that address.

**Note:** Do not enable proxy ARP for the Virtual IP Address. In other words, do not specify the PREFIFC parameter on the command or enable proxy through the graphical user interface configuration. Doing so prevents multiple systems from using the same "cluster" IP address simultaneously.

2. Configure port settings on the cluster nodes so that IBM Load Balancer can route the packets properly:

IBM Load Balancer requires every node in the cluster to use same port number for both HTTP and HTTPS service (typically, port 80). If you have configured your nodes to use unique port numbers, change them to the same port now.

**Tip:** When configuring the ports, you can use the wildcard * when specifying the host name for the HTTP and HTTPS. This will listen on all interfaces configured in the system, including the loopback adapter set up for the cluster.

3. On the load balancer server, configure load balancing for the cluster:

a. Open a command window on the load balancer server.

b. Start the load balancer's Dispatcher process by clicking **Start > Control Panel > Administrative Tools > Services.** right-click **IBM Dispatcher (ULB),** and then click **Start.**

c. If you are using IPv6 addresses, enable the processing of IPv6 packets:

   Run the following command while logged in as the Windows administrator:

   ```
   netsh interface ipv6 install
   ```

   This command enables processing of IPv6 packets. Issue this command only once; thereafter, you can start and stop the executor as often as you need. If you do not issue the command to enable processing of IPv6 packets on these systems, the executor will not start.

d. Start the executor function of the dispatcher:

   ```
   dscontrol executor start
   ```

e. Add the cluster to the service:

   ```
   dscontrol cluster add cluster's_fully_qualified_host_name
   ```

   where **cluster's_fully_qualified_host_name** is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

   ```
   stms-cluster.example.com
   ```

g. Add the cluster port:

   ```
   dscontrol port add cluster's_fully_qualified_host_name@port
   ```

   where **cluster's_fully_qualified_host_name@port** is the fully qualified host name that you assigned to the cluster when you installed the load balancer, with the HTTP/HTTPS port appended to it (typically port 80); for example:

   ```
   stms-cluster.example.com@80
   ```

   f. Add the nodes for which this server will balance workload:

   ```
   dscontrol server add cluster_host@port@primary_node
dscontrol server add cluster_host@port@secondary_node
   ```

   where:
• `cluster_host@port@primary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the primary node's fully qualified host name appended; for example:
  stms-cluster.example.com@80@meetsvr1.example.com

• `cluster_host@port@secondary_node` indicates the cluster's fully qualified host name with the port appended (as in the previous step) plus now with the secondary node's fully qualified host name appended (include an additional line for each additional secondary node); for example:
  stms-cluster.example.com@80@meetsvr2.example.com

h. Add the cluster to the executor:
  
  `dscontrol executor add cluster’s_fully_qualified_host_name`

  where `cluster’s_fully_qualified_host_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
  stms-cluster.example.com

  ...

  i. Start the manager:
  
  `dscontrol manager start`

  j. Start the HTTP advisor for the port you are using (the port you specified in the previous steps, typically port 80):
  
  `dscontrol advisor start http 80`

  k. Now you can stop the service:
  
  `dsserver stop`

  l. Close the command window.

4. Define server affinity with a "sticky time":

By default the Load Balancer will round-robin HTTP requests between the cluster members, so that a single client may be routed to different cluster members for subsequent requests rather than continuing to be routed to the same cluster member. Since a client typically accesses an online meeting every 30-40 seconds during the session, you may want to enable server affinity for a Sametime cluster so that the client continues to access the same server during a single meeting.

The dispatcher component of IBM Load Balancer supports a configurable "sticky time". This means that the load balancer will remember which cluster member a client was routed to; subsequent requests will "stick to" the same server until the preset time expires. IBM recommends a "sticky" time configuration of 60 seconds for a Sametime cluster.

Windows

a. Start IBM Load Balancer.

b. In the navigation tree, select the **Executor** (the load balancer's non-forwarding IP address, which appears under its host name).

c. Click **Configuration Settings**.

d. In "Port-Specific Settings", change the **Default sticky-time settings** from 0 to 60 seconds, and click **Update Configuration**.

e. Leave IBM Load Balancer open for the next step.

5. Save the load balancer settings:

a. In IBM Load Balancer, return to the navigation tree and right-click on the host name of the load balancer you just configured (for example, loadbal.example.com).
b. Click **Save Configuration File as** and accept the default name (default.cfg).

The configuration settings stored in default.cfg are restored every time the server is restarted.

c. Click **OK**.

**Deploying Sametime Meeting Server and Sametime Proxy Server on the same computer**

When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server on the same machine using the same server host name, conflicts with cookies that are used by each server can occur. If you install both servers on the same machine, then configure the Sametime Proxy Server with a host alias as a different host name.

**About this task**

If you deploy the Sametime Proxy Server and the Sametime Meeting Server on one machine, and both servers have the same host name, users cannot stay connected to instant meetings initiated by the Sametime Proxy web client. Users can start instant meetings, but eventually they are disconnected. This error occurs because Websphere sets the JSESSIONID cookie whenever an application is started, and the JSESSIONID cookie is being overwritten because the Sametime Proxy Server and the Sametime Meeting Server share a hostname. Due to the matching host names, the WebSphere JSESSIONID is not recognizing them as separate applications. You can work around this by providing the Sametime Proxy Server with a host alias with a hostname different from the Sametime Meeting Server host name.

An example of a host alias is *stproxy*. For more information on host alias settings, see "Host alias settings" in the WebSphere Application Server information center:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

**Procedure**

1. Install the Sametime Meeting Server and the Sametime Proxy Server on the same server.

2. Change the host name of the Sametime Proxy Server using a host alias:
   
a. Log in to the Integrated Solutions Console on the Sametime Proxy Server.

   b. Click **Environment > Virtual Hosts > default_host > Host Aliases**.

   c. Configure the host aliases of the Virtual Host, default_host, of the Sametime Proxy Server so that their host names do not match either the host name of the Sametime Meeting Server or the wild card character, ‘*’ (asterisk).

   The new host name alias must refer to the IP address at the DNS level, so that the machines will be able to ping the Web server by using the host name. Update the host name of all of the host alias entries to the host name that the Sametime Proxy Server or Sametime Meeting Server will use. Use the same host name for all aliases.

   1) Click the host name link associated with each port.

   2) Enter the fully qualified host name for the Sametime Proxy Server. It must not be the same host name assigned to the Sametime Meeting Server.

   3) Click **Apply**, and then click **Save**.

   d. Restart the Sametime Proxy Server.
3. On the Sametime System Console, go to the configuration page for Sametime Advanced and update the host name to match the host name alias you created for the Proxy Server or Meeting Server.
   a. Log in to the Integrated Solutions Console.
   b. Click Sametime System Console > Sametime Servers > Sametime Proxy Servers.
   c. In the Sametime Proxy Servers list, click the deployment name of the server with the information that you want to add or change.
   d. Click the Administrative Settings tab.
   e. In the Sametime Meeting Server section, modify the host name to reflect the new host alias you created.

Preparing the Sametime Meeting server for users
Before deploying clients, set up the preferences and login requirements that suit your environment.

Preconfiguring a Sametime Meeting Server using managed preferences:
One or more IBM Sametime meeting servers can be dynamically configured in the Connect Client using the Expeditor managed settings framework. There is a minimum number of entries required to correctly configure a server but in all a completely configured server can be introduced, including support for proxy and reverse proxy configuration.

About this task
The Expeditor managed settings framework is at its core a set of key/value pairs. If using the Sametime framework then these key/value pairs will be inputted into a managed-settings.xml file and pushed to clients through a special update site. If using the Notes system for managing preferences, the same key/value pairs will apply but they will be entered into the Managed Settings page in the Notes configuration document as custom entries.

Preconfiguring a single Sametime Meeting Server using managed preferences:
Many Meeting preferences can be set automatically using the Expeditor managed settings framework. This topic describes what you must set up in advance to preconfigure client preferences for a single Sametime Meeting Server.

About this task
Add these required client preferences to automatically update client preferences with the Expeditor managed settings framework.

Procedure
Follow these steps to add the required entries for configuring managed preferences. You can set the preferences from the Notes configuration documents or in a managed-settings.xml file.
1. Add these required entries:
   • com.ibm.rtc.meetings.shelf/serverName
     Use the fully qualified domain name of the meeting server.
   • com.ibm.rtc.meetings.shelf/connectionType
The default of 0 uses a direct connection. Specify 1 to use a reverse proxy server.

- `com.ibm.rtc.meetings.shelf/serverPort`
  Specify the port used to connect to the meeting server.

- `com.ibm.rtc.meetings.shelf/useHTTP` or `com.ibm.rtc.meetings.shelf/useHTTPS`
  Set the value to `true` for one of these entries. If you set the first entry to `true`, the client uses HTTP to connect to the meeting server. If you set the second entry to `true`, the client uses an HTTPS connection.

2. Specify whether users can re-use the credentials used to log into a community server or if they must use custom credentials.
   a. To set up single sign-on, where the client re-uses the credentials from a community server to log in to a meeting server, set these keys:
      - `com.ibm.rtc.meetings.shelf/useCommunityCredentials=true`
      - `com.ibm.rtc.meetings.shelf/communityServerName=server_name`
      where `server_name` matches the community server name that is configured in the client.
      - `com.ibm.rtc.meetings.shelf/loginByToken=true`
      If the community server and meeting server are configured in the same single sign-on domain, this key, when set to true, forces the meeting client to log in with the LTPA token from the community server. If the meeting server is configured to re-use the community server credentials, the client automatically attempts to log in with a user name and LTPA token before falling back to a user name and password. Note that clients running releases earlier than 8.5.1 can also use an LTPA token but do not attempt to do so automatically and have no fallback mechanism. This value cannot be applied to specific meeting servers. Because it is a global setting for all servers, do not use this value if you have these older clients and some community servers and meetings servers that are not configured for single sign-on.
      For more information, see Preparing servers running on WebSphere Application Server for single sign-on.
   b. To set the client to use custom credentials to log in to a meeting server, set:
      - `com.ibm.rtc.meetings.shelf/useCustomCredentials=true`

3. (Optional) Prevent users from modifying their meeting server lists:
   - `com.ibm.rtc.meetings.shelf/canRemoveServer`
     Setting this key to `false` prevents user from removing meeting servers.
   - `com.ibm.rtc.meetings.shelf/canAddOtherServers`
     Setting this key to `false` prevents users from adding meeting servers.
Related concepts

“Meeting preferences” on page 988

The following tables list the meeting preferences that can be managed for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Related tasks

“Automatically updating client preferences with the managed-settings.xml file” on page 951

When you use the Expeditor managed settings framework to create a managed-settings.xml file and post it to an update site, clients receive new or updated preferences automatically. The managed-settings.xml file is policy-based, so you can define different sets of preferences for different users. This method applies only to Sametime Connect clients. Settings for Sametime embedded clients for Lotus Notes are managed through the Domino desktop policy settings document instead.

Preconfiguring multiple Sametime Meeting Servers using managed preferences:

Many Meeting preferences can be set automatically using the Expeditor managed settings framework. This topic describes what you must set up in advance to preconfigure client preferences for multiple Sametime Meeting Servers.

About this task

Add these required client preferences to automatically update client preferences with the Expeditor managed settings framework.

Procedure

Follow these steps to add the required entries for configuring managed preferences. You can set the preferences from the Notes configuration documents or in a managed-settings.xml file.

1. Decide on a unique identifier, a GUID, for the server. It must be of the form, "stmsNNNNNNNNNNNNNN", where the Ns are a unique number made of 13 digits, such as the current system time when the meeting server was defined.
   For example:
   stms1938847293723

2. Open the Managed Settings page in the Notes configuration document.

3. Add these required entries, inserting the predefined GUID and a semi-colon (;) before the key. For example:
   com.ibm.rtc.meetings.shelf/stms1938847293723;meetings.serverName=meetings.example.com
   • com.ibm.rtc.meetings.shelf/GUID;meetings.serverName=
     Use the fully qualified domain name of the meeting server.
   • com.ibm.rtc.meetings.shelf/GUID;serverId=
     Use the predefined GUID for the meeting server.
   • com.ibm.rtc.meetings.shelf/GUID;serverConnectionType=
     The default of 0 uses a direct connection. Specify 1 to use a reverse proxy server.
   • com.ibm.rtc.meetings.shelf/GUID;meetings.serverPort=
     Specify the port used to connect to the meeting server.
   • com.ibm.rtc.meetings.shelf/GUID;meetings.HTTP or
     com.ibm.rtc.meetings.shelf/GUID;meetings.useSSLforLogin
Set the value to **true** for one of these entries. If you set the first entry to **true**, the client uses HTTP to connect to the meeting server. If you set the second entry to **true**, the client uses an HTTPS connection.

4. Add an entry to identify the available meeting servers by their GUIDs. Use the key that matches the types of clients that are deployed. Use semi-colons to separate the server GUIDs.
   - Clients running releases 8.5.1 and later:
     com.ibm.rtc.meetings.shelf/preconfiguredServerIds=GUID1;GUID2;GUID3
   - Clients running releases 8.5 and earlier:
     com.ibm.rtc.meetings.shelf/MeetingServerIds=GUID1;GUID2;GUID3

   **Note:** You must set this key before a client has been configured to any meeting server; otherwise the key will not be recognized.

5. Specify whether users can re-use the credentials used to log into a community server or if they must use custom credentials.
   a. To set up single sign-on, where the client re-uses the credentials from a community server to log in to a meeting server, set these keys:
      - com.ibm.rtc.meetings.shelf/useCommunityServer=true
      - com.ibm.rtc.meetings.shelf/communityServerName=server_name
      - server_name matches the community server name that is configured in the client.
      - com.ibm.rtc.meetings.shelf/loginByToken=true

      If the community server and meeting server are configured in the same single sign-on domain, this key, when set to true, forces the meeting client to log in with the LTPA token from the community server. If the meeting server is configured to re-use the community server credentials, the client automatically attempts to log in with a user name and LTPA token before falling back to a user name and password. Note that clients running releases earlier than 8.5.1 can also use an LTPA token but do not attempt to do so automatically and have no fallback mechanism. This value cannot be applied to specific meeting servers. Because it is a global setting for all servers, do not use this value if you have these older clients and some community servers and meetings servers that are not configured for single sign-on.

      For more information, see Preparing servers running on WebSphere Application Server for single sign-on.

   b. To set the client to use custom credentials to log in to a meeting server, set:
      - com.ibm.rtc.meetings.shelf/useCustomCredentials=true

6. (Optional) Prevent users from modifying their meeting server lists:
   - com.ibm.rtc.meetings.shelf/canRemoveServer
     - Setting this key to **false** prevents user from removing meeting servers.
   - com.ibm.rtc.meetings.shelf/canAddOtherServers
     - Setting this key to **false** prevents users from adding meeting servers.
Related concepts
“Meeting preferences” on page 988
The following tables list the meeting preferences that can be managed for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Related tasks
“Automatically updating client preferences with the managed-settings.xml file” on page 951
When you use the Expeditor managed settings framework to create a managed-settings.xml file and post it to an update site, clients receive new or updated preferences automatically. The managed-settings.xml file is policy-based, so you can define different sets of preferences for different users. This method applies only to Sametime Connect clients. Settings for Sametime embedded clients for Lotus Notes are managed through the Domino desktop policy settings document instead.

Installing the WebSphere Application Server Update Installer
Use the WebSphere Application Server Update Installer to add required software updates.

About this task
Follow these steps to download the update package and install the IBM Update Installer, which is needed for installed software updates for WebSphere Application Server.

Procedure
1. Log in with the same user account used to install the Sametime software.
2. On the local system, create a directory to store the update files, such as stwas Fixes.
3. Download the IBM Update Installer package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

- **Linux**
  Mount the CD or DVD using a command similar to the following command:
  ```bash
  mount /dev/cdrom /cdrom
  ```

- **Solaris**
  Mount the CD or DVD.

4. Extract the package to the local fixes directory you created.

5. In the UpdateInstallers subdirectory of the package you extracted, extract the updateInstaller package for your platform.

6. Navigate to the directory where you extracted the Update Installer and run the install program.

   - **AIX, Linux, or Solaris**
     ```bash
     ./install
     ```
   - **Windows**
     ```bash
     install.exe
     ```

7. The installation wizard initializes and displays the Welcome screen.
   
   a. If you are running on Linux Red Hat and you select the documentation links in the installation program for the Update Installer, your Web browser might not launch. The path to the web browser is not included in your PATH environment variable. To resolve this problem, you can add the web browser path to your PATH environment variable, and rerun the installation program.

   b. Click **Next** to continue.

8. The License agreement screen is displayed. Read the license agreement and accept its terms. After you accept the licensing terms, the installation wizard checks for a supported operating system and prerequisite patches. If you encounter a problem such as not having the right prerequisite updates on your system, cancel the installation, make the required changes, and restart the installation.

9. The Installation directory screen is displayed. Specify the destination of the installation root directory.

10. Select the **Create a start menu** icon to create a shortcut for the Update Installer. Deselect this checkbox if you do not need a shortcut for the Update Installer in your start menu. Click **Next** to continue.

11. The Installation summary panel appears. Review the summary. Click **Next** to begin the installation or click **Back** to make changes to previous panels.

12. The Installation results panel is displayed. Verify the success of the installer program by examining the completion panel.
   
   a. If you want to launch the Update Installer upon completion of the installation, select **Launch Update Installer for WebSphere Software** on exit.

   b. Click **Finish** to exit the installer.

**Installing WebSphere Application Server updates**

If you must install additional WebSphere Application Server software updates, perform this step on each of the servers in your deployment running on WebSphere Application Server.
**Before you begin**

To perform these steps, you must have already installed the WebSphere Application Server Update Installer.

**About this task**

Follow these steps to install the WebSphere Application Server software updates required for Sametime 8.5 servers as outlined in the Technote on the IBM Support Site.

http://www.ibm.com/support/docview.wss?rs=477&uid=swg21415822

System requirements for this release of the Sametime family of products is maintained as an IBM Technote at the following web address:


**Procedure**

1. Download the WebSphere Application Server updates package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      ```bash
      mount -v cdrfs -o ro /dev/cd0 /cdrom
      ```
      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      ```bash
      mount /dev/cdrom /cdrom
      ```
      **Solaris**
      Mount the CD or DVD.
2. Extract the updates to a local directory such as stwas_fixes.
3. Ensure that you stop all running processes as described in “Command reference for starting and stopping servers” on page 487.
4. If you have not already launched the WebSphere Application Server Update Installer, log in with the same user account used to install the Sametime software, then navigate to the directory where you installed the Update Installer and run the update program.
   AIX, Linux, and Solaris
   ./update.sh
   Windows
   update.bat
5. The Welcome screen is displayed. Click Next.
6. Specify the location of the product that you want updated.
7. Accept the default to Install maintenance. Click Next.
8. At the prompt, enter the directory name containing the Sametime update packages (for example, stwas_fixes). Click Next.
9. The system will automatically determine the appropriate maintenance packages based on the version of the product that is installed. Click Next.
10. Before the installation, the Confirmation panel confirms which packages will be installed. Click Next.
11. After you install the update package, check the installation log to verify that the install is successful. The log can be found at was_install_root/logs/update/maintenance_package.install.
12. Start the servers as described in “Command reference for starting and stopping servers” on page 487.

Results

To verify which updates have been installed, run the versionInfo command from the was_install_root/bin directory.

Linux

./versionInfo.sh -maintenancePackages > version.txt

Windows

versionInfo -maintenancePackages > version.txt

The command creates a text file that lists all the WebSphere Application Server updates that have been installed on the system.

Related tasks

“Installing the WebSphere Application Server Update Installer” on page 475
Use the WebSphere Application Server Update Installer to add required software updates.

Preparing to install Sametime Advanced using a deployment plan

Use the Sametime System Console to prepare to install Sametime Advanced by pre-populating values required for installation.
Before you begin

Start the Sametime System Console if it is not already running.

Procedure

If you have not already opened the Install Sametime Advanced guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   
   http://serverhostname.domain:8700/ibm/console

   For example: http://sametime.example.com:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Click Sametime Guided Activities &gt; Install Sametime Advanced Server.

Related tasks

“Deploying Sametime Proxy Server, Sametime Meeting Server, or Sametime Advanced on one machine” on page 51

If you deploy the Sametime Proxy Server or Sametime Meeting Server with Sametime Advanced on one machine, configure the servers to have the same host name, then configure Sametime Advanced to use that Sametime Proxy Server for awareness because users cannot get awareness on the Sametime Advanced pages.

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install Sametime Advanced using a deployment plan

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

Before you begin

You have set up an IBM DB2 database and an LDAP server, and have run the guided activities for connecting to the DB2 database and to the LDAP server.

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Advanced.

Procedure

1. Plan a product installation.
   
   In the Install Sametime Advanced Server portlet, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.

   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.

   The name should include the installation and node type, such as stAdv_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.
3. Choose the configuration type.
   Select **Primary Node** if this is the first server of its type. Select **Secondary Node** for additional servers. Then click **Next**.

   The **Cell** option is reserved for special-use cases in which the server must be self-contained. If you select **Cell**, you must provide a host name, user ID, and password when prompted to do so.

   This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click **Next**.

   **Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

5. WebSphere Profile Settings.
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click **Next**.

   If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

   **Important:** This must be a unique user ID that does not exist in the LDAP directory.

6. Chat room admin user settings
   Enter the credentials for the Sametime Advanced chat room administrator, and then click **Next**. Select **Use the WebSphere Administrator to use the user name and password you entered in the previous screen.** You can also supply a new user name and password specifically for chat room administration.

7. Choose a database for this deployment. This panel appears if you selected Primary Node or Cell as the configuration type.
   Select the Sametime Advanced database that you configured with the Sametime System Console activity, and then click **Next**.

8. Connect to an LDAP Server. This panel appears if you selected Cell as the configuration type.
   Select the LDAP directory that you configured with the Sametime System Console guided activity, and then click **Next**.

   Review the summary screen, and then click **Finish**.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click **Modify an Existing Deployment Plan** and update the plan. All changes must be made prior to running installation.
What to do next

Installing Sametime Advanced

Starting and stopping servers in a Sametime deployment

An IBM Sametime deployment is made of up several component servers that can be started and stopped independently.

Starting and stopping servers running on WebSphere Application Server

Starting and stopping IBM Sametime servers that run on WebSphere Application Server involves other server components such as the Deployment Manager and the node agent.

How installing cell profiles affects starting and stopping servers:

If you chose the configuration type “Cell Profile” when you installed a Sametime Proxy Server, Sametime Media Manager components, or a Sametime Meeting Server, you installed a self-contained set of WebSphere Application Server components for each server. You have this configuration type if you installed different Sametime servers on the same machine or on multiple machines that are not clustered.

A cell profile installs a Deployment Manager, node agent, and one Sametime server. You can manage the Sametime application through the deployment's central Sametime System Console. However, any WebSphere Application Server administration (such as starting and stopping servers) occurs directly on each server, using its own Integrated Solutions Console. For example, if you want to start a Sametime Proxy Server installed with its own Cell Profile, you must start all the components of the Sametime Proxy Server cell: its Deployment Manager, its node agent, and the Sametime Proxy Server. Even if you have multiple servers installed on the same machine, you start and stop components for each cell profile installed on the machine, starting with the Deployment Manager.

Starting and stopping the Deployment Manager:

The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

About this task

Before starting Sametime Servers, the Deployment Manager must be running for each cell.

Windows only: You can also use the Start - Programs menu to use the Start and Stop menu commands.

Procedure

1. Open a command window (on IBM i, start QSH).
2. Navigate to the app_server_root/profiles/DeploymentManagerName/bin directory for the Deployment Manager you want to start.
3. Run the following command to start and stop the Deployment Manager:
   AIX, Linux, or Solaris
   ./startManager.sh
Related tasks

“Starting and stopping WebSphere Application Servers on Windows” on page 486

Use the Start Programs menu in Microsoft Windows to start or stop any Sametime
servers running on WebSphere Application Server.

Related reference

“Command reference for starting and stopping servers” on page 487

You may use a command window to start and stop Sametime components running
on WebSphere Application Server. To stop servers, you will supply the WebSphere
Application Server administrator password that was established when you
installed the server.

Starting the Sametime System Console:

When started, the Sametime System Console runs as a task in the WebSphere
Application Server administrative console.

Before you begin

Verify that the Deployment Manager is running for the cell.

Procedure

1. Open a command window (on IBM i, run QSH command).
2. Navigate to the local app_server_root/profiles/STSCAppProfile profile directory
   and change to the bin directory.
3. Run the following command. Note that the name of the server is case sensitive:

   AIX, Linux, or Solaris
   ./startNode.sh
   ./startServer.sh STConsoleServer

   Windows
   startNode.bat
   startServer.bat STConsoleServer

   IBM i
   startNode
   startServer STConsoleServer
Related tasks

“Logging in to the console”
Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

“Starting and stopping the Deployment Manager” on page 481
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Adding trust for certificate authorities used by external communities” on page 834
External communities certificates are signed by a specific certificate authority - probably a different authority from the CA used to sign your Sametime Gateway certificate. In order for the Sametime Gateway to trust a certificate presented by an external community, the CA that issued this certificate would have to be configured to be trusted in advance.

“Requesting a certificate signed by a Certificate Authority” on page 835
To ensure Secure Sockets Layer (SSL) communication, servers require a personal certificate that is signed by a certificate authority (CA). You must first create a personal certificate request to obtain a certificate that is signed by a CA.

“Importing any intermediate CA certificates into the keystore” on page 836
If your server certificate is issued by an intermediary CA, then complete the steps that follow.

“Importing a signed certificate issued into the keystore” on page 839
“Setting up Sametime Gateway to use a new certificate” on page 840
Set up IBM Sametime Gateway server to use the new certificates.

Related reference

“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Logging in to the console:

Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

About this task

Log in to the Sametime System Console on the system where you installed the cell profile. If you deployed a cluster using a dedicated Deployment Manager, the cell is managed on a system other than the one where you installed the Sametime System Console.

Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Logging in to the console after starting the server:
Use the IBM Sametime system console to use guided activities to perform configuration tasks and administer any Sametime servers that are managed by the console.

**Procedure**

With the Sametime system console started, follow these steps to log in.

1. From a browser, enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the Sametime System Console server. For AIX, Linux, Solaris, or Windows, specify port 8700 for HTTP and 8701 for HTTP over SSL.

   During the installation process, WebSphere Application Server security is enabled. SSL is enabled as part of the security process and you are directed to another port that listens for HTTPS connections.

   \[ http://serverhostname.domain:port/ibm/console \]

   For example:

   \[ http://sametime.example.com:8700/ibm/console \]

   \[ https://sametime.example.com:8701/ibm/console \]

   **Note:** On IBM i, the port number cannot be 8700. Use the port that was listed in the system console installation results summary. To check the port, open the `AboutThisProfile.txt` file for the system console deployment manager profile and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:

   `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt`

2. The WebSphere Application Server Integrated Solutions Console opens. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.

   The default name is wasadmin.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

   **Logging in to the console for a cell profile:**

   If you chose the configuration type "Cell Profile" when you installed Sametime servers, you installed a self-contained set of WebSphere Application Server components for each server. This configuration type installs a WebSphere Application Server Integrated Solutions Console as part of the server's cell profile.

   **Before you begin**

   The Deployment Manager of the Sametime server must be started.

   **About this task**

   With the Deployment Manager of the Sametime server started, follow these steps to log in to the WebSphere Application Server Integrated Solutions Console.

   **Procedure**

   1. From a browser, enter the following URL to log into the console. Replace `serverhostname.domain` with the fully qualified domain name and port for the server.
Note: During the install process, WebSphere security is enabled. SSL is enabled as part of the WebSphere security process and you will be directed to another port which listens for https connections.

**• Sametime Proxy Server**
Enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the server.

http://serverhostname.domain:8600/ibm/console

8600 is the default port when the Proxy Server is installed as a Cell Profile.

For example:

http://sametime.example.com:8600/ibm/console

Note: (IBM i) The port number may not be the default listed above. Use the port that was listed in the Sametime Proxy Server installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime Proxy Deployment Manager Profile on the server and use the setting specified for the “Administrative console port.” For the default profile name (STPDMgrProfile), the file is located here:

/QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STPDMgrProfile/logs/AboutThisProfile.txt

**• Sametime Media Manager (Linux and Windows)**
Enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the server.

http://serverhostname.domain:8800/ibm/console

8800 is the default port when the Media Manager is installed as a Cell Profile.

For example: http://sametime.example.com:8800/ibm/console

**• Sametime Meeting Server**
Enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the server.

http://serverhostname.domain:8500/ibm/console

8500 is the default port when the Meeting Server is installed as a Cell Profile.

For example: http://sametime.example.com:8500/ibm/console

Note: (IBM i) The port number may not be the default listed above. Use the port that was listed in the Sametime Meeting Server installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime Meeting Deployment Manager Profile on the server and use the setting specified for the “Administrative console port.” For the default profile name (STMDMgrProfile), the file is located here:

/QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/profiles/STMDMgrProfile/logs/AboutThisProfile.txt

The WebSphere Application Server Integrated Solutions Console opens.

2. Enter the WebSphere Application Server User ID and password that you created when you installed the Sametime server.

The default name is wasadmin.
IBM Sametime uses a number of ports on the servers in your deployment. This topic lists the default ports and their uses; a range of ports means that the application can select any port in that range, in case one or more of those ports are already in use by other applications.

Running Sametime as services on Linux or Windows:

Newly installed Sametime servers running on WebSphere Application Server on Linux or Microsoft Windows can be started from the Services panel. When install completes, verify that services are created properly and for Windows, that dependencies are set to avoid problems when the system restarts.

About this task

Keep these guidelines in mind regarding Sametime server services.

Linux

Linux services will be turned off by default.

In Windows, dependency will be set by installer itself

During uninstall, these services will be removed by installer.

If Install or Uninstall fails, and the services are not removed or if you are creating a cluster, manually clean up the services with this command:

  chkconfig --del service_name

In a clustered environment, you should remove the original installed services and add the service for each cluster member.

Windows

Startup Type for Windows services will be in "Manual."

If Install or Uninstall fails, and the services are not removed or if you are creating a cluster, manually clean up the services with this command:

  sc delete service_name

In a clustered environment, you should remove the original installed services and add the service for each cluster member.

Starting and stopping WebSphere Application Servers on Windows:

Use the Start Programs menu in Microsoft Windows to start or stop any Sametime servers running on WebSphere Application Server.

About this task

From the IBM WebSphere menu off the Start Programs menu, you can navigate to the Start and Stop menu choices for a server.
Procedure
1. Working on the server you want to start or stop, click Start > All Programs.
2. Click IBM WebSphere Application Server > Network Deployment V7.0 > Profiles.
3. Select the profile for the server and click the appropriate Start or Stop menu command.

Related concepts
“How installing cell profiles affects starting and stopping servers” on page 481
If you chose the configuration type “Cell Profile” when you installed a Sametime Proxy Server, Sametime Media Manager components, or a Sametime Meeting Server, you installed a self-contained set of WebSphere Application Server components for each server. You have this configuration type if you installed different Sametime servers on the same machine or on multiple machines that are not clustered.

Related tasks
“Running Sametime as services on Linux or Windows” on page 486
Newly installed Sametime servers running on WebSphere Application Server on Linux or Microsoft Windows can be started from the Services panel. When install completes, verify that services are created properly and for Windows, that dependencies are set to avoid problems when the system restarts.

“Automating Sametime Community Server shutdown on Windows” on page 497
Follow these instructions for the proper sequence of events for an automated shutdown of a IBM Sametime Community Server on Windows.

Related reference
“Command reference for starting and stopping servers”
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Command reference for starting and stopping servers:
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Sequence for starting and stopping servers
Follow the sequence below when starting or stopping servers associated with a Sametime server.

Start server sequence
1. Start the Deployment Manager.
   If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.
2. Start the node agent.
3. Start the Sametime server.

Stop server sequence
1. Stop the Sametime server.
2. Stop the node agent.
3. Stop the Deployment Manager.

   If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.

**Note:** Before uninstalling WebSphere Application Server, you must stop the application server. If the server belongs to a cluster, you will also need to stop all node agents in the cluster, and then stop the Deployment Manager. Finally, close all browsers and command windows that may have been accessing the WebSphere Application Server.

### Server command directories

Run the commands from a command window on the machine where the server is installed and navigate to the appropriate **bin** directory shown in the following table.

**Table 54. Server command directories**

<table>
<thead>
<tr>
<th>Type</th>
<th>Profile /bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stSSC_profile_root/bin</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stM_profile_root/bin</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stP_profile_root/bin</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stMS_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stgw_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stAdv_profile_root/bin</td>
</tr>
</tbody>
</table>

**AIX, Linux, or Solaris**

**Note:** The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

**Table 55. Start server commands for AIX, Linux, or Solaris**

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Sametime System Console | ./startNode.sh  
|                     | ./startServer.sh STConsoleServer                  |
| Meeting Server     | ./startNode.sh  
|                     | ./startServer.sh STMeetingHttpProxy               |
|                     | ./startServer.sh STMeetingServer                  |
| Proxy Server       | ./startNode.sh  
|                     | ./startServer.sh STProxyServer                    |
| Media Manager      | Linux only:  
|                     | ./startNode.sh  
|                     | ./startServer.sh STMediaServer                    |
### Table 55. Start server commands for AIX, Linux, or Solaris (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Gateway</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STAdvancedServer</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

### Table 56. Stop server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>./stopServer.sh STConsoleServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>./stopServer.sh STMeetingServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>./stopServer.sh STProxyServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>./stopServer.sh STMediaServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>./stopserver.sh RTCGWServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>./stopServer.sh STAdvancedServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
</tbody>
</table>

**Windows**

The Start Programs menu is also a convenient way to start and stop Sametime servers running on WebSphere Application Server.
**Note:** The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

**Table 57. Start server commands for Windows**

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode.bat startServer.bat STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode.bat startServer.bat STMeetingHttpProxy startServer.bat STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>startNode.bat startServer.bat STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>startNode.bat startServer.bat STMediaServer</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>startNode.bat startServer.bat RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>startNode.bat startServer.bat STAdvancedServer</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

**Table 58. Stop server commands for Windows**

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer.bat STConsoleServer -username username -password password stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stopServer.bat STMeetingServer -username username -password password stopServer.bat STMeetingHttpProxy -username username -password password stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer.bat STProxyServer -username username -password password stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stopServer.bat STMediaServer -username username -password password stopNode.bat -username username -password password</td>
</tr>
</tbody>
</table>
Table 58. Stop server commands for Windows (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Gateway</td>
<td>stopserver.bat RTCGWServer</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stopServer.bat STAdvancedServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
</tbody>
</table>

IBM i

Note: The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

Table 59. Start server commands for IBM i

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>startServer STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>startNode</td>
</tr>
<tr>
<td></td>
<td>startServer RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>Not supported on IBM i</td>
</tr>
</tbody>
</table>

Note: Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

Table 60. Stop server commands for IBM i

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer STConsoleServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
</tbody>
</table>
Table 60. Stop server commands for IBM i (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Server</td>
<td>stopServer STMeetingServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopServer STMeetingHttpProxy -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer STProxyServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stopServer RTCGWServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>Not supported on IBM i</td>
</tr>
</tbody>
</table>

Related concepts
“How installing cell profiles affects starting and stopping servers” on page 481
If you chose the configuration type “Cell Profile” when you installed a Sametime
Proxy Server, Sametime Media Manager components, or a Sametime Meeting
Server, you installed a self-contained set of WebSphere Application Server
components for each server. You have this configuration type if you installed
different Sametime servers on the same machine or on multiple machines that are
not clustered.

Related tasks
“Starting and stopping the Deployment Manager” on page 481
The Deployment Manager manages the Sametime System Console and all
Sametime Server cells.
“Starting and stopping WebSphere Application Servers on Windows” on page 486
Use the Start Programs menu in Microsoft Windows to start or stop any Sametime
servers running on WebSphere Application Server.
“Determining Sametime server status using the Integrated Solutions Console” on
page 1196
You can use the Integrated Solutions Console to determine if an IBM Sametime
Meeting Server, Proxy Server, or Media Manager is running.

Starting and stopping servers running on Lotus Domino
The IBM Sametime Community Server is configured as a set of services that start
and stop automatically when the Domino server is stopped or started.
Related tasks

“Reconfiguring the UserInfo servlet after switching from Domino to LDAP” on page 715

The UserInfo servlet must be reconfigured after switching from Domino to LDAP to enable the Business Card to work.

Starting and stopping a Sametime server on AIX, Linux, or Solaris while Domino is running:

IBM Sametime on AIX, Linux, or Solaris is installed on an IBM Lotus Domino server. You can start and stop a Sametime server without starting and stopping the Domino server from running.

About this task

There are times when you will need to keep the Domino server running while doing Sametime maintenance tasks. For example, you might need to shut down Sametime services while you make configuration changes on the Sametime server, but you need to leave the Domino server running so you can access Domino databases on the server.

Procedure

1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, choose one of the following actions:
   - To start the Sametime server from a Domino server that is already running, type this command:
     `Load STADDIN`
   - To stop the Sametime server without stopping the Domino server, type this command:
     `Tell STADDIN Quit`

Related concepts

“Considerations for AIX, Linux, and Solaris” on page 496

If you install IBM Sametime on an IBM AIX, Linux, or Sun Solaris server, you should be aware of some special behaviors.

Starting and stopping a Sametime server on Windows while Domino is running:

IBM Sametime on Windows is installed on an IBM Lotus Domino server. You can start and stop a Sametime server without starting and stopping the Domino server from running.

About this task

There are times when you will need to keep the Domino server running while doing Sametime maintenance tasks. For example, you might need to shut down Sametime services while you make configuration changes on the Sametime server, but you need to leave the Domino server running so you can access Domino databases on the server.

Procedure

1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, choose one of the following actions:
To start the Sametime server from a Domino server that is already running, type this command:
Load STADDIN
To stop the Sametime server without stopping the Domino server, type this command:
Tell STADDIN Quit

Starting and stopping Domino and a Sametime Community Server on AIX, Linux, or Solaris:

Starting Domino and a Sametime Community Server on AIX, Linux, or Solaris:

Learn how to start and stop a Sametime Community Server running on AIX, Linux, or Solaris.

About this task
IBM Sametime is installed on an IBM Lotus Domino server. Once you set up the Lotus Domino server to launch Sametime automatically, then whenever you start or stop the Domino server, you are starting and stopping the Sametime server as well.

Procedure
1. Log in to the system as the default Domino user. Make sure the default path and environment are set correctly.
2. Start the Sametime server by issuing the following server command. Note that starting the Sametime server might take a few minutes.
   ./ststart
3. The "ststart" script file sets some important environment variables before launching the server executable (/opt/ibm/lotus/bin/server).

What to do next
Starting and stopping the Sametime server without starting and stopping Domino

You can start and stop the Sametime server and keep the Domino server running. For example, you might need to shut down Sametime services while you make configuration changes on the Sametime server, but you need to leave the Domino server running so you can access Domino databases on the server.
1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, choose one of the following actions:
   a. To start the Sametime server from a Domino server that is already running type this command:
      Load STADDIN
   b. To stop the Sametime server without stopping the Domino server type this command:
      Tell STADDIN Quit
You can run Sametime as a background process on an IBM AIX server.

Before you begin

The operating system’s IBM Lotus Domino user actually runs the background process, and must have permission to run the script and write files to the Domino Data Directory.

About this task

To run the Sametime server as a background process, complete the following steps:

Procedure

1. Open the ststart script located in the data directory, and copy the two sections below into the .profile of the Domino user that will run Sametime as a background process:

   ```
   # Define variables
   BINDIR=/opt/lotus/notes/latest/ibmpow/
   LOTUSDIR=/opt/lotus/bin
   
   # Export paths for notes user
   LIBPATH=${LIBPATH}:$BINDIR
   export LIBPATH
   PATH=${PATH}:$BINDIR
   export PATH
   
   Note: The PATH environment variable cannot contain the /lotus/bin directory, which defaults to /opt/lotus/bin.
   ```

2. Set up the Virtual Frame Buffer, and verify that it is running.

3. Set the DISPLAY environment variable to the host name:

   ```
   DISPLAY=example:1
   export DISPLAY
   ```

4. From the command prompt, run the following command, which enables you to manage the server only through the IBM Lotus Notes Administration Client:

   ```
   nohup /opt/lotus/bin/server < /dev/null > /dev/null 2>&1 &
   ```

5. If you want to use text files for stin and stout, use the following:

   a. Create the following script on the server:

      ```
      #!/usr/bin/sh
      DOMINO_PROGRAM_DIR=/opt/lotus
      DOMINO_DATA_DIR=/local/notesdata
      export DOMINO_PROGRAM_DIR
      export DOMINO_DATA_DIR
      cd $DOMINO_DATA_DIR
      if [ -f st.in ]; then
        rm st.in
      fi
      if [ -f st.out ]; then
        mv st.out st.out.bak
      ```
touch st.in
$DOMINO_PROGRAM_DIR/bin/server <st.in >st.out 2>&1 &
cd -

Note:
If /usr/bin/sh does not exist, change the path for sh at the top of the script.
If the default installation settings are not used, modify the
DOMINO_DATA_DIR and DOMINO_PROGRAM_DIR environment
variables at the top of the script.

b. Save the script on the AIX server.
c. Use the cd command to navigate to the folder where the script was saved.
d. Launch the script by typing:
   ./script_name
   where script_name is the file name of the script.

Results

Once the server is running, you can interact with the server console by using the
Administrator Client Server console. Alternatively, you can view the console in a
telnet session by issuing the following commands:
> cd DOMINO_DATA_DIR
> tail -f st.out

To enter commands at the server console, do the following:
> cd DOMINO_DATA_DIR
> echo {command} >>st.in

where

DOMINO_DATA_DIR is be the value for the Domino Data directory; for example,
/local/notesdata,

and

{command} is a Domino Server console command such as "Show Tasks"; for example:
> echo show tasks >>st.in

Stopping Domino and a Sametime Community Server on AIX, Linux, or Solaris:

Follow these instructions to stop a Sametime Community Server on AIX, Linux, or Solaris.

Procedure
1. Return to the terminal session where Domino was started.
2. If the prompt character > is not present, press the Enter key once to be
   presented with a prompt character. Then type either exit or quit and press the
   Enter key.

Considerations for AIX, Linux, and Solaris:

If you install IBM Sametime on an IBM AIX, Linux, or Sun Solaris server, you
should be aware of some special behaviors.
You must not have /opt.ibm/lotus/bin in your PATH, otherwise Sametime will not function correctly.

If you do not start Sametime from an XWindows environment, Save Annotations will not function unless you set up a Virtual frame buffer.

If you start Sametime from a telnet session, exiting the telnet session also terminates the Domino Console and Sametime.

Starting and stopping Domino and a Sametime Community Server on Windows:

Learn how to start and stop a Sametime Community Server on Windows.

Starting Domino and a Sametime server on Windows:

Follow these instructions to start a Sametime server on Windows.

Procedure
2. In the Services dialog box, select Services (Local).
3. Right-click “Sametime server” and select Start.

Stopping Domino and a Sametime Community Server on Windows:

Follow these instructions to stop a Sametime Community Server on Windows.

Procedure
2. In the Services dialog box, select Services (Local).
3. Right-click “Sametime server” and select Stop.

Automating Sametime Community Server shutdown on Windows:

Follow these instructions for the proper sequence of events for an automated shutdown of a IBM Sametime Community Server on Windows.

About this task

If you try to automate the shutdown of Sametime Community Servers in batch files by using the Windows net stop command against Lotus Domino without first shutting down Sametime services, then crash-on-shutdown events and long restart times can result. This sort of shutdown can also trigger crashes of other servers within a Community Services Cluster. These problems occur because the ST Community Launch service relaunches Sametime applications as needed. If Domino is stopped, then ST Community Launch works as designed and tries to relaunch the now-failing applications, with unpredictable results.

You can prevent these problems by creating your batch file with the proper sequence of events for an automated shutdown of the Lotus Community Sametime Server.

Procedure

Follow this order when you create your batch file:
net stop "ST Community Launch"
<wait for service shutdown>
net stop "Sametime Server"
<wait for service shutdown>
net stop "Lotus Domino Server"
<wait for service shutdown>

Note: If your site has changed the service names then adjust the commands accordingly. These individual services might require several minutes to shut down properly; this time is longer for high-volume servers. IBM recommends performing these steps manually first to observe the time required for each shutdown. Insert the appropriate wait sleep commands between the net stop commands when you create your batch files.

Starting and stopping a Sametime TURN Server
Starting and stopping IBM Sametime TURN Server requires you to start and stop the IBM Java program that runs the service.

Procedure
1. Start the TURN Server:
   a. On the computer where the TURN Server is running, open a command window.
   b. Navigate to the directory where the TURN Server is installed (for example in Microsoft Windows, C:\TURN).
   c. Run the batch file to start the TURN Server:
      Linux
      run.sh
      Windows
      run.bat
2. Stop the TURN Server:
   a. On the computer where the TURN Server was started, find the (already opened) command window from step 1 and press Ctrl+C.
   b. If the TURN server was started using a background task, find the Java process that runs the TURN server and simply kill it.

Running Sametime components as Windows services
Follow these instructions to configure IBM Sametime components as Windows services and start them automatically at system startup.

Before you begin
To set up this function on a Microsoft Windows operating system, you must belong to the Administrator group and have the following advanced user rights:
- Act as part of the operating system
- Log on as a service

Procedure
1. Use a text editor to create a file named createservices.bat with the following contents.
When you install a cell profile instead of a network deployment cluster, the name of the profile itself will be different, usually by appending the host name of the machine. For example, your Sametime Meeting Server's host name might be zeta-stmeet. Also, your path name might be different. For example, you might not have Program Files in your path. In this case the batch file would look like this:

```bash
PROFILE_PATH=C:\ibm\WebSphere\AppServer\profiles
wasservice.exe -add MediaServerDM -serverName dmgr -profilePath
"%PROFILE_PATH%\STMSDMgrProfile" -logRoot "%PROFILE_PATH%\STMSDMgrProfile\logs\dmgr"
  -username wasadmin -password password
wasservice.exe -add MediaServerNodeAgent -serverName nodeagent -profilePath
"%PROFILE_PATH%\STMSAppProfile" -logRoot "%PROFILE_PATH%\STMSAppProfile\logs\nodeagent"
  -username wasadmin -password password
wasservice.exe -add MediaServerPrimaryNode -serverName STMediaServer -profilePath
"%PROFILE_PATH%\STMSAppProfile" -logRoot "%PROFILE_PATH%\STMSAppProfile\logs\STMediaServer"
  -username wasadmin -password password
```

Note: STMDMgrProfile has been changed to zeta-stmeetMeetingDMProfile1. You must update the script to reflect the unique path to each component.

2. Run the file from the C drive to automate creation of the WebSphere Application Server services.

Note: If you’ve installed to a different drive letter, modify the file.
3. (Optional) To remotely create and start a service from the command line, you can use the SC tool (Sc.exe) included in the Resource Kit as described on the Microsoft Support site.

Results

To stop the services, WebSphere Application Server credentials are needed. Put the credentials in this file:

```
/profiles/profilename/properties/soap.client.props
```

```com.ibm.SOAP.loginUserId=wasadmin
com.ibm.SOAP.loginPassword=waspassword```

You also have the option of putting an encoded password in this property file. For instructions, see the WebSphere Application Server topic about manually encoding passwords here:


Related tasks

“Running Sametime as services on Linux or Windows” on page 486

Newly installed Sametime servers running on WebSphere Application Server on Linux or Microsoft Windows can be started from the Services panel. When install completes, verify that services are created properly and for Windows, that dependencies are set to avoid problems when the system restarts.

Uninstalling

Before you can install a newer version of IBM Sametime, you must uninstall the currently deployed version.

About this task

Complete these tasks to uninstall Sametime components.

Related tasks

“Troubleshooting installation or uninstallation” on page 1219

Use the following topics to troubleshoot problems that occur after installing and uninstalling IBM Sametime servers.

Uninstalling a non-clustered server on AIX, Linux, Solaris, or Windows

Uninstall a non-clustered server running any IBM Lotus Sametime component running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

The procedure for uninstalling Sametime vary according to the component you are uninstalling:

Uninstalling Sametime Community Server:

Follow the instructions for your operating system to uninstall IBM Sametime Community Server.

Unregistering a Community Server:
To remove an IBM Sametime Community Server from the list of the Sametime System Console's managed servers, run the unregister utility on the server. This step is required before uninstalling a Community Server that you installed without a deployment plan and then registered with the Sametime System Console later using the registration utility. If you installed the server with a deployment plan, unregistering is only needed if you are performing some other activity that requires removal of the product from the console.

Before you begin

The Sametime System Console must be started.

About this task

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server’s Sametime console directory:
      - **AIX, Linux, Solaris:** The console directory is under the Community Server data directory; for example: /opt/IBM/domino85/notesdata/console
      - **Windows:** The console directory is under the Domino directory; for example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

<table>
<thead>
<tr>
<th>Table 61. console.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCHostName</strong></td>
</tr>
<tr>
<td><strong>SSCHTTPPort</strong></td>
</tr>
<tr>
<td><strong>SSCUserName</strong></td>
</tr>
<tr>
<td><strong>SSCPassword</strong></td>
</tr>
<tr>
<td><strong>SSCSSLEnabled</strong></td>
</tr>
</tbody>
</table>
3. Verify that the settings in the `productConfig.properties` file are correct, modifying them as needed before saving and closing the file.
   Only the required values in this file are listed here:

   **Table 62. productConfig.properties settings**
   | **DepName** | The Dep Name must be the name that was used when you installed: the unique name for this deployment as known by the Sametime System Console. |
   | **NodeHostName** | Provide the fully qualified host name for the Community Server that is being unregistered. |

4. Start the Sametime Community Server.
5. Now unregister the server:
   a. Run the unregister utility with the following command:
      - **AIX, Linux, Solaris**: `unregisterProductNode.sh`
      - **Windows**: `unregisterProductNode.bat`
   b. As the unregister utility runs, you will be prompted enter the Location of the `notes.ini` file. You are only prompted for the `notes.ini` file location when unregistering the server. Type the full path to the directory containing the `notes.ini` file (for example, `/stserver/data`), and press **Enter**.

   The utility unregisters the server, generating a log file called `ConsoleUtility.log` and storing it in the `console/logs` directory. If the unregistration is successful, the `console.pid` will be removed.

   **Related tasks**
   “Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233
   If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

   **Related reference**
   “Command reference for starting and stopping servers” on page 487
   You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

   **Uninstalling a Sametime Community Server:**
   Follow the instructions for your operating system to uninstall IBM Sametime Community Server.

   **Uninstalling Sametime Community Server on Windows:**
   When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime.
Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

Before you begin

Before you uninstall the Sametime Community Server, it is always a good practice to back up any important files.

About this task

To completely remove Sametime Community Server, you must uninstall Lotus Domino as well, and also both the Lotus directory and the Notes data directories.

Procedure

1. Stop the Domino (Sametime) server.
2. From the Microsoft Windows Start menu, select Settings > Control Panel > Add/Remove Programs.
3. Select IBM Sametime 8.x from the list and click Add/Remove. Click Yes when prompted to remove the Sametime server.
4. When the Windows uninstall program completes, click OK to exit the uninstall program.

Uninstalling Sametime Community Server on AIX, Linux, or Solaris:

When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

Procedure

1. Stop the Domino (Sametime) server.
2. Switch to the root user.
3. Change to the following directory:
   
   `datadir/_uninstst`

4. Start the uninstall using the following command:

   `./uninstaller.bin`

Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, and Windows:

Uninstalling an IBM Sametime Meeting Server, Sametime Proxy Server, Sametime System Console, or Sametime Advanced uses a different procedure from Sametime Gateway.

About this task

Follow these steps to uninstall a Sametime Meeting Server, Sametime Proxy Server, Sametime System Console, or Sametime Advanced:

Unregistering Sametime Gateway on AIX, Linux, Solaris, or Windows:
Before you uninstall an IBM Sametime Gateway server on IBM AIX, Linux, Solaris, or Microsoft Windows, remove it from the list of the Sametime System Console’s managed servers by running the unregister utility. You should only unregister Sametime Gateway when you will uninstall the server or perform some other activity that requires removal of the product from the console.

About this task

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. On the Sametime Gateway server, navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

<table>
<thead>
<tr>
<th>Table 63. console.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCHostName</strong></td>
</tr>
<tr>
<td><strong>SSCHTTPPort</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>SSCUserName</strong></td>
</tr>
<tr>
<td><strong>SSCPASSWORD</strong></td>
</tr>
</tbody>
</table>

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.

<table>
<thead>
<tr>
<th>Table 64. productConfig.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DepName</strong></td>
</tr>
<tr>
<td><strong>NodeHostName</strong></td>
</tr>
</tbody>
</table>
4. Now unregister the server:
   a. Open a command window and run the unregistration utility with the following command:

      AIX, Linux, Solaris: unregisterWASProduct.sh -uninstall
      Windows: unregisterWASProduct.bat -uninstall

   The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, a console.pid will also be generated.

Related tasks

“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Removing a node from a Deployment Manager on AIX, Linux, Solaris, or Windows:

Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.

About this task

Note: For additional information on removing a node from the Deployment Manager, see the removeNode command in the WebSphere Application Server 7 information center. See Deleting specific cluster members for information on removing a cluster member.

Procedure

1. In the Deployment Manager's Integrated Solutions Console, click System administration > Nodes.
2. On the "Nodes" page, select the check box beside each node that you want to remove.
3. At the topic of the table, click the Remove Node button.
   If you cannot remove the node by clicking Remove Node, remove the node from the configuration by clicking Force Delete.
4. Click OK.
5. Save your change by clicking the Save link in the "Messages" box at the top of the page.

Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows:

Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

Before you begin

Remove the node from the Deployment Manager.
About this task

Running the install program on the Sametime server allows you to see the Uninstall option. You can uninstall any of these servers:

- Sametime System Console
- Sametime Proxy Server
- Sametime Meeting Server
- Sametime Media Manager
- Sametime Advanced

About uninstalling separate Media Manager components

The Media Manager is comprised of three components that work together: Packet Switcher, Conference Manager, and SIP Proxy and Registrar. When components are installed as non-clustered servers, you cannot uninstall a single component, but must uninstall them in sets of three, even if they are hosted on separate computers. Uninstall the components in this order: first Packet Switcher, then Conference Manager, and finally the SIP Proxy/Registrar.

If you configured clusters for the components, you can uninstall a single component from a cluster, provided you maintain at least one Packet Switcher, a SIP Proxy and Registrar cluster with at least one node, and a Conference Manager cluster with at least one node.

Procedure

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Working on the server you want to uninstall, run the Installation Manager.
   AIX, Linux, and Solaris
   /opt/IBM/InstallationManagerInstallationDirectory/eclipse/IBMIM
   Windows
   Select Start > Programs > IBM Installation Manager > IBM Installation Manager.
4. Choose the components to remove from the server. Click Next.
5. Click Uninstall.
   The Uninstall command removes the profile. The Repository Information section that appears after uninstalling the software will not have any files listed.
6. On the Deployment Manager, remove the Sametime application from the server by
   a. Start the Deployment Manager.
b. Start WebSphere Application Server.
c. Log in to the Integrated Solutions Console.
d. Follow the steps for Uninstalling enterprise applications in the WebSphere Application Server information center.
e.

7. If you uninstalled a Meeting server, you must also remove this node from the meeting_service_bus topology.
   a. On the Deployment Manager computer, start the Sametime server on the Deployment Manager if it is not already started.
   b. Log in to the Integrated Solutions Console.
   c. Click Service integration > Buses and click meeting_service_bus.
   d. In the content pane, under Topology, click Bus members.
   e. Select the node you uninstalled and click Remove
   f. Save your changes to the master configuration.
   g. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.

8. If you uninstalled an Advanced server, you must also remove this node from the bus topology.
   a. Start the Deployment Manager.
   b. Start WebSphere Application Server.
   c. Start the Sametime server.
   d. Log into the Integrated Solutions Console.
   e. Click Service integration > Buses.
   f. Click orgcollab_service_bus.
   g. In the content pane, under Topology, click Bus members.
   h. Select the node you uninstalled and click Remove
   i. Repeat the previous three steps to remove the bus member from the following buses:
      • rtc4web_cluster_service_bus
      • rtc4web_node_service_bus
      • MQTT_Bus
   j. Save your changes to the master configuration.
   k. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.

9. If you are uninstalling a Media Manager that was installed on separate systems, repeat these steps on each remaining server that is connected to the Media Manager component you just uninstalled.

10. If you uninstalled only some nodes in a cluster, synchronize the remaining nodes:
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Back in the navigator, click System Administration > Node agents.
   d. Click a node agent, and then click Restart; repeat for each node agent.
What to do next

During uninstallation, the server is unregistered from the Sametime System Console and the WebSphere Application Server profile removed. If you receive an error during the uninstallation process, refer to the following troubleshooting topics for instructions on manually completing the uninstallation process:

• Manually removing WebSphere Application Server
• “Unregistering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced” on page 1230
• Updating the Sametime System Console when server unregistration fails

Related tasks

“Removing a node from a Deployment Manager on AIX, Linux, Solaris, or Windows” on page 505

Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.

Uninstalling WebSphere and Sametime Gateway on AIX, Linux, Solaris, or Windows:

Uninstall the IBM WebSphere Application Server and IBM Sametime Gateway server applications on a computer running IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

The procedure for uninstalling the WebSphere Application Server and Sametime Gateway products vary with the operating system:

Uninstalling Sametime Gateway on AIX, Linux, or Solaris:

Uninstall IBM Sametime Gateway on a server running IBM AIX, Linux, or Solaris.

Before you begin

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there’s no need to uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

Note: WebSphere Application Server, the Sametime Gateway Profile, and Sametime Gateway must be uninstalled before installing anew. If all components are not removed, the VPD registry may determine that Sametime Gateway is still installed and believe that you are trying to install a second instance of Sametime Gateway.

Procedure

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Open a command window and navigate to the following directory:
   `sgw_server_root/_uninst`
4. Execute the appropriate command:
   - For **GUI mode** type `.\uninstaller.bin`
   - For **Console mode** type `.\uninstaller.bin -console`
5. Select the language you wish to use for the uninstall procedure and click **OK**. The Welcome screen is displayed.
6. Click **Next** to proceed. The Sametime Gateway features screen is displayed.
7. Select the check box for all available components/features and click **Next**. The Uninstall summary screen is displayed.
8. Click **Uninstall** to begin the procedure. The progress is displayed on the screen.
9. When the uninstall is complete, read the summary information and click **Finish** to exit the wizard.
10. Remove all Sametime Gateway install folders from your computer.

**What to do next**

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

*Uninstalling Sametime Gateway on Windows:*

Uninstall IBM Sametime Gateway on a server running Microsoft Windows.

**Before you begin**

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there’s no need to uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp.

**Procedure**

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Open a command window and navigate to the following directory:
   `slgw_server_root/_uninst`
4. Type the appropriate command to start the uninstall program:
   • For GUI mode, type `uninstaller.exe`
   • For console mode, type `uninstaller.exe -console`
5. Select the language you wish to use for the uninstall procedure and click **OK**.
   The Welcome screen is displayed.
6. Click **Next** to proceed. The Sametime Gateway features screen is displayed.
7. Select the check box for all available components/features and click **Next**. The Uninstall summary screen is displayed.
8. Click **Uninstall** to begin the procedure. The progress is displayed on the screen.
9. When the uninstall is complete, read the summary information and click **Finish** to exit the wizard.
10. Remove all Sametime Gateway install folders from your computer.

**What to do next**

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

**Uninstalling a Sametime Bandwidth Manager server on Linux or Windows:**

Uninstall IBM Sametime Bandwidth Manager on a server running Linux or Windows. This server runs on IBM WebSphere Application Server, similar to other Sametime servers, but requires a different process for uninstallation.

**Before you begin**

On the server node where you will uninstall the Bandwidth Manager, make sure the appropriate IBM WebSphere Application Server instance is running.

**Procedure**

1. On the server where you will uninstall the Bandwidth Manager, use a command line terminal or prompt, navigate to the `\TMP\BWM` folder containing the extracted uninstallation files.
2. Run the following command to uninstall the Bandwidth Manager:
   • **Linux**
     ```bash
     WAS_install_root/profiles/Profile_name/bin/ws_ant.sh uninstall
     ```
     where:
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application is installed, typically "AppServerProfile".
     - `WAS_install_root` is the root directory where WebSphere Application Server is installed. In Linux it is typically `/opt/IBM/WebSphere/AppServer`. 

510  Sametime Advanced: Installation and Administration Guide
For example:
```
/opt/IBM/WebSphere/AppServer/profiles/AppServerProfile/bin/ws_ant.sh uninstall
```
- **Microsoft Windows**
```
WAS_install_root\profiles\Profile_name\bin\ws_ant.bat uninstall
```
where:
- `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application is installed, typically "AppServerProfile".
- `WAS_install_root` is the root directory where WebSphere Application Server is installed. In Microsoft Windows this is typically `C:\Program Files\WebSphere\AppServer` and in Linux it is typically `/opt/IBM/WebSphere/AppServer`.

**Attention:** In Windows, you must use the DOS-shortened versions of the directory names; for example: `C:\PROGRA~1/IBM/WebSphere/AppServer`.

For example:
```
C:\PROGRA~1\IBM\WebSphere\AppServer\profiles\AppServerProfile\bin\ws_ant.bat uninstall
```

**Note:** Do not copy and paste the paths and parameters above because control characters may inadvertently be included in the command. For best results, type the command manually.

**Results**

The script makes the following changes:
- It removes the datasource `DS_BWM` created when you installed Bandwidth Manager.
- It removes these WebSphere Application Server applications: BandwidthManagerSIPFrontend, BW_Pool_Application, and BandwidthManager.
- It removes the Bandwidth Manager node from the Sametime Servers portlet node.

**What to do next**

If you performed any manual steps during the original installation (such as LDAP federated repository configurations), you must now undo or reverse those steps manually.

**Uninstalling a Sametime TURN Server**

Uninstall an IBM Sametime TURN Server by removing the product files from the computer.

**Procedure**

1. Stop the TURN Server:
   a. On the computer where the TURN Server was started, find the (already opened) command window from step 1 and press **Ctrl+C**.
   b. If the TURN server was started using a background task, find the Java process that runs the TURN server and simply kill it.

2. Delete the TURN Server files:
   a. Navigate to the directory where the TURN Server is installed (for example in Microsoft Windows, `C:\TURN`).
   b. Do one of the following:
• If you will not be re-installing the TURN Server, you can delete the entire folder.
• If you plan to re-install the TURN Server later, retain the folder but delete all files within it.

3. Disable the TURN service from the Sametime Media Manager's Conference Manager component:
   a. On the server hosting the Conference Manager, open the stayconfig.xml file for editing.
      
      \[Install_root/config/cells/Cell_name/nodes/Node_name/servers/Server_name\]
      
      For example:
      
      config/cells/bassMediaCell1/nodes/bassMediaNode1/servers/STMediaServer
      
      **Note:** If the Conference Manager is clustered, use the cluster's Deployment Manager profile.
   
   b. Set the value for NATTraversalEnabled to false.
      
      For example:
      
      `<configuration lastUpdated="1226425838277" name="NATTraversalEnabled" value="false"/>
      
   c. Save and close the file.
   
   d. If the Conference Manager is clustered, synchronize all nodes in the cluster:
      1) In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes.**
      
      2) Click **Full Resynchronize.**
   
4. Remove the TURN Server name from the Sametime Media Manager's Configuration page:
   a. On the server hosting the Sametime System Console, log in to the Integrated Solutions Console.
   
   b. Click **Sametime System Console > Sametime Servers > Sametime Media Manager.**
   
   c. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
   
   d. Click the **Configuration** tab.
   
   e. Locate the "NAT Traversal" section at the bottom of the page.
   
   f. Under "TURN server" replace the TURN Server's host name with "0.0.0.0" in the host name field that you configured when you installed the TURN Server.
   
   g. Click **OK.**
   
   h. Restart the Sametime Media Manager (not the Sametime System Console) so this change can take effect.

   **Note:** For added security, close the TURN server ports in the firewall (port 3478 by default). Also, uninstalling load balancer is not mandatory since it can be used for other tasks such as HTTP.

**Uninstalling one clustered server on AIX, Linux, Solaris, or Windows**

Use the instructions in this section to uninstall one clustered Sametime server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

**About this task**

Follow the procedure for the clustered Sametime server you want to uninstall:
Uninstalling one clustered Sametime Community Server on AIX, Linux, Solaris, or Windows:

You can uninstall one clustered IBM Sametime Community Server running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

Follow these steps to remove one clustered Sametime Community Server from the cluster before uninstalling it.

Related tasks

“Removing a cluster of Sametime Community servers on AIX, Linux, Solaris, or Windows” on page 525

To remove a cluster of Sametime Community servers on AIX, Linux, Solaris, or Windows, remove the nodes and the cluster first, then uninstall the individual servers.

Removing a Sametime Community Server from a cluster on AIX, Linux, Solaris, or Windows:

Before uninstalling an IBM Sametime Community Server that is part of a cluster administered by the Sametime System Console, remove the server from the cluster.

About this task

Follow these steps to remove the Sametime Community Server from the cluster administered with the Sametime System Console.

Procedure

1. Working on the server you want to remove from the cluster, navigate to the InstallLocation/console directory for the Deployment Manager profile.
2. If this is the first time you have run a utility on this server, open console.properties file and provide the System Console Host name, port, User Name and Password. Also, you can specify the log level, which is not mandatory.
3. Verify that the values in the productConfig.properties file are correct.
4. Run the utility from the console directory you used in Step 1.
   - AIX, Linux, Solaris: updateSTCluster.sh -remove
   - Windows: updateSTCluster.bat -remove
5. When you are prompted, enter the name of the cluster you are updating.

   The utility removes the Sametime Community Server from the cluster and generates the ConsoleUtility.log file in the console directory. It also deletes the console.pid file from the console directory.

Unregistering a Sametime Community Server node:

To remove an IBM Sametime Community Server from the list of the Sametime System Console's managed servers, run the unregister utility on the server. This step is required before uninstalling a Community Server that you installed without a deployment plan and then registered with the Sametime System Console later using the registration utility. If you installed the server with a deployment plan, unregistering is only needed if you are performing some other activity that requires removal of the product from the console.
Before you begin

The Sametime System Console must be started.

About this task

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's Sametime console directory:
      - **AIX, Linux, Solaris**: The console directory is under the Community Server data directory; for example: /opt/IBM/domino85/notesdata/console
      - **Windows**: The console directory is under the Domino directory; for example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

   **Table 65. console.properties settings**

   | SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
   | SSCHTTPPort | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false." |
   | SSCUserName | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin. |
   | SSCPassword | Enter the WebSphere Application Server password associated with the SSCUserName. |
   | SSCSSLEnabled | Change this value to "true" to connect to the Sametime System Console using a secure connection. |
   | SSCHTTPSPort | Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to "true." |

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.
   Only the required values in this file are listed here:
Table 66. productConfig.properties settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The Dep Name must be the name that was used when you installed: the unique name for this deployment as known by the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the Community Server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Start the Sametime Community Server.

5. Now unregister the server:
   a. Run the unregister utility with the following command:
      - **AIX, Linux, Solaris**: unregisterProductNode.sh
      - **Windows**: unregisterProductNode.bat
   b. As the unregister utility runs, you will be prompted enter the Location of the notes.ini file. You are only prompted for the notes.ini file location when unregistering the server. Type the full path to the directory containing the notes.ini file (for example, /stserver/data), and press Enter.

      The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.

Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233
If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Uninstalling a Sametime Community Server node:

Follow the instructions for your operating system to uninstall IBM Sametime Community Server.

Uninstalling a Sametime Community Server node on Windows:

When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

Before you begin

Before you uninstall the Sametime Community Server, it is always a good practice to back up any important files.
About this task

To completely remove Sametime Community Server, you must uninstall Lotus Domino as well, and also both the Lotus directory and the Notes data directories.

Procedure
1. Stop the Domino (Sametime) server.
2. From the Microsoft Windows Start menu, select Settings > Control Panel > Add/Remove Programs.
3. Select IBM Sametime 8.x from the list and click Add/Remove. Click Yes when prompted to remove the Sametime server.
4. When the Windows uninstall program completes, click OK to exit the uninstall program.

Uninstalling a Sametime Community Server node on AIX, Linux, or Solaris:

When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

Procedure
1. Stop the Domino (Sametime) server.
2. Switch to the root user.
3. Change to the following directory:
   datadir/_uninstst
4. Start the uninstall using the following command:
   ./uninstaller.bin

Uninstalling one clustered WebSphere-based server on AIX, Linux, Solaris, or Windows:

Uninstall a clustered IBM Sametime Proxy Server, Sametime Media Manager, or Sametime Meeting Server, or Sametime Advanced running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

Uninstalling a clustered Sametime server requires you to first remove that server from the cluster.

Related tasks
“Removing a cluster of WebSphere-based Sametime servers on AIX, Linux, Solaris, or Windows” on page 529
To remove a cluster of Sametime servers running on WebSphere Application Server on AIX, Linux, Solaris, or Windows, remove the nodes and the cluster first, then uninstall the individual servers.

Removing one clustered node from a Deployment Manager on AIX, Linux, Solaris, or Windows:
Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.

About this task

Note: For additional information on removing a node from the Deployment Manager, see the removeNode command in the WebSphere Application Server 7 information center. See Deleting specific cluster members for information on removing a cluster member.

Procedure
1. In the Deployment Manager's Integrated Solutions Console, click System administration > Nodes.
2. On the "Nodes" page, select the check box beside each node that you want to remove.
3. At the topic of the table, click the Remove Node button.
   If you cannot remove the node by clicking Remove Node, remove the node from the configuration by clicking Force Delete.
4. Click OK.
5. Save your change by clicking the Save link in the "Messages" box at the top of the page.

Removing a WebSphere Application Server node from a cluster on AIX, Linux, Solaris, or Windows:

Before uninstalling an IBM Sametime server that was clustered with an IBM WebSphere Application Server network deployment, use the updateWASCluster -remove command to remove the node from the cluster.

About this task

Removing a node from a cluster involves verifying configuration settings for the cluster and then running a utility to remove the node from the cluster. If you are uninstalling a cluster, run the utility on every node in the cluster.

These instructions apply to the following Sametime servers:
• Sametime Proxy Server
• Sametime Media Manager
• Sametime Meeting Server
• Sametime Gateway
• Sametime Advanced

Procedure
1. Update the console.properties file on the Deployment Manager:
   a. On the Deployment Manager server, navigate to the install_root/IBM/WebSphere/component/console folder for the Deployment Manager profile. The component varies depending on whether you are working with the Sametime Meeting, Media Manager, or Proxy server.
      Attention: The cluster's Primary Node is installed on the same computer, so be sure to use the Deployment Manager profile.
   b. Open the console.properties file for editing;
   c. Fill in values for the following settings:
<table>
<thead>
<tr>
<th><strong>SSCHostName</strong></th>
<th>Type the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCHTTPPort</strong></td>
<td>Type the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot; To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td><strong>SSCUserName</strong></td>
<td>Type the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td><strong>SSCPASSWORD</strong></td>
<td>Type the IBM WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

1. Back up the console.properties and productConfig.properties files:

2. Now open the productConfig.properties file (in the same folder) and verify that all of the settings are correct, changing settings as needed before you save and close the file.

3. Verify that the Sametime System Console has been started.

4. Open a command window and run the following command:
   - **Attention:** You must specify the -remove parameter. Otherwise, you will unregister the entire cluster rather than remove the one node.
   - IBM AIX, Linux, or Solaris: updateWASCluster.sh -remove
   - Microsoft Windows: updateWASCluster.bat -remove

5. When prompted by the utility, enter the name of the cluster from which you are removing the node, and press Enter.

**Results**

This utility removes the node from the specified cluster’s settings and generates a log file called ConsoleUtility.log, which it stores in the console/log directory.

**Unregistering a Sametime Gateway server:**

Before you uninstall an IBM Sametime Gateway server on IBM AIX, Linux, Solaris, or Microsoft Windows, remove it from the list of the Sametime System Console’s managed servers by running the unregister utility. You should only unregister Sametime Gateway when you will uninstall the server or perform some other activity that requires removal of the product from the console.

**About this task**

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

**Procedure**

1. Back up the console.properties and productConfig.properties files:
a. On the Sametime Gateway server, navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.

b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

   **Table 67. console.properties settings**

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.

   Only the required values in this file are listed here:

   **Table 68. productConfig.properties settings**

<table>
<thead>
<tr>
<th>DepName</th>
<th>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Now unregister the server:

   a. Open a command window and run the unregistration utility with the following command:
      - AIX, Linux, Solaris: unregisterWASProduct.sh -uninstall
      - Windows: unregisterWASProduct.bat -uninstall

   The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, a console.pid will also be generated.
Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233
If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Uninstalling a WebSphere-based node in a Sametime cluster:

Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

Before you begin
Remove the node from the Deployment Manager.

About this task
Running the install program on the Sametime server allows you to see the Uninstall option. You can uninstall any of these servers:
- Sametime System Console
- Sametime Proxy Server
- Sametime Meeting Server
- Sametime Media Manager
- Sametime Advanced

About uninstalling separate Media Manager components
The Media Manager is comprised of three components that work together: Packet Switcher, Conference Manager, and SIP Proxy and Registrar. When components are installed as non-clustered servers, you cannot uninstall a single component, but must uninstall them in sets of three, even if they are hosted on separate computers. Uninstall the components in this order: first Packet Switcher, then Conference Manager, and finally the SIP Proxy/Registrar.

If you configured clusters for the components, you can uninstall a single component from a cluster, provided you maintain at least one Packet Switcher, a SIP Proxy and Registrar cluster with at least one node, and a Conference Manager cluster with at least one node.

Procedure
1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
d. Stop the Deployment Manager.

2. Close all browsers and command windows that are accessing the server you plan to uninstall.

3. Working on the server you want to uninstall, run the Installation Manager.
   AIX, Linux, and Solaris
   /opt/IBM/InstallationManagerInstallationDirectory/eclipse/IBMIM
   Windows
   Select Start > Programs > IBM Installation Manager > IBM Installation Manager.

4. Choose the components to remove from the server. Click Next.

5. Click Uninstall.
   The Uninstall command removes the profile. The Repository Information section that appears after uninstalling the software will not have any files listed.

6. On the Deployment Manager, remove the Sametime application from the server by
   a. Start the Deployment Manager.
   b. Start WebSphere Application Server.
   c. Log in to the Integrated Solutions Console.
   d. Follow the steps for Uninstalling enterprise applications in the WebSphere Application Server information center.
   e.

7. If you uninstalled a Meeting server, you must also remove this node from the meeting_service_bus topology.
   a. On the Deployment Manager computer, start the Sametime server on the Deployment Manager if it is not already started.
   b. Log in to the Integrated Solutions Console.
   c. Click Service integration > Buses and click meeting_service_bus.
   d. In the content pane, under Topology, click Bus members.
   e. Select the node you uninstalled and click Remove
   f. Save your changes to the master configuration.
   g. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.

8. If you uninstalled an Advanced server, you must also remove this node from the bus topology.
   a. Start the Deployment Manager.
   b. Start WebSphere Application Server.
   c. Start the Sametime server.
   d. Log into the Integrated Solutions Console.
   e. Click Service integration > Buses.
   f. Click orgcollab_service_bus.
   g. In the content pane, under Topology, click Bus members.
   h. Select the node you uninstalled and click Remove
   i. Repeat the previous three steps to remove the bus member from the following buses:
      • rtc4web_cluster_service_bus
      • rtc4web_node_service_bus
MQTT_Bus
j. Save your changes to the master configuration.
k. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.

9. If you are uninstalling a Media Manager that was installed on separate systems, repeat these steps on each remaining server that is connected to the Media Manager component you just uninstalled.

10. If you uninstalled only some nodes in a cluster, synchronize the remaining nodes:
   a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Back in the navigator, click System Administration > Node agents.
   d. Click a node agent, and then click Restart; repeat for each node agent.

What to do next

During uninstallation, the server is unregistered from the Sametime System Console and the WebSphere Application Server profile removed. If you receive an error during the uninstallation process, refer to the following troubleshooting topics for instructions on manually completing the uninstallation process:

• Manually removing WebSphere Application Server
• “Unregistering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced” on page 1230
• Updating the Sametime System Console when server unregistration fails

Related tasks
“Removing a node from a Deployment Manager on AIX, Linux, Solaris, or Windows” on page 505

Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.

Uninstalling both WebSphere and Sametime Gateway from a node:

Uninstall the IBM WebSphere Application Server and IBM Sametime Gateway server applications on a computer running IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

The procedure for uninstalling the WebSphere Application Server and Sametime Gateway products vary with the operating system:

Uninstalling both WebSphere and Sametime Gateway from a node on AIX, Linux, or Solaris:

Uninstall IBM Sametime Gateway on a server running IBM AIX, Linux, or Solaris.

Before you begin

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there’s no need to
uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according to instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

**Note:** WebSphere Application Server, the Sametime Gateway Profile, and Sametime Gateway must be uninstalled before installing anew. If all components are not removed, the VPD registry may determine that Sametime Gateway is still installed and believe that you are trying to install a second instance of Sametime Gateway.

**Procedure**

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.

2. Close all browsers and command windows that are accessing the server you plan to uninstall.

3. Open a command window and navigate to the following directory: `stgw_server_root/_uninst`

4. Execute the appropriate command:
   - For **GUI mode** type `./uninstaller.bin`
   - For **Console mode** type `./uninstaller.bin -console`

5. Select the language you wish to use for the uninstall procedure and click **OK**. The Welcome screen is displayed.

6. Click **Next** to proceed. The Sametime Gateway features screen is displayed.

7. Select the check box for all available components/features and click **Next**. The Uninstall summary screen is displayed.

8. Click **Uninstall** to begin the procedure. The progress is displayed on the screen.

9. When the uninstall is complete, read the summary information and click **Finish** to exit the wizard.

10. Remove all Sametime Gateway install folders from your computer.

**What to do next**

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

*Uninstalling both WebSphere and Sametime Gateway from a node on Windows:*

Uninstall IBM Sametime Gateway on a server running Microsoft Windows.
Before you begin

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there’s no need to uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp.

Procedure

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Open a command window and navigate to the following directory:
   stgw_server_root/_uninst
4. Type the appropriate command to start the uninstall program:
   - For GUI mode, type uninstaller.exe
   - For console mode, type uninstaller.exe -console
5. Select the language you wish to use for the uninstall procedure and click OK. The Welcome screen is displayed.
6. Click Next to proceed. The Sametime Gateway features screen is displayed.
7. Select the check box for all available components/features and click Next. The Uninstall summary screen is displayed.
8. Click Uninstall to begin the procedure. The progress is displayed on the screen.
9. When the uninstall is complete, read the summary information and click Finish to exit the wizard.
10. Remove all Sametime Gateway install folders from your computer.

What to do next

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

Uninstalling all Sametime servers in a cluster on AIX, Linux, Solaris, or Windows

Use the instructions in this section to remove and uninstall a cluster of Sametime server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.
About this task

The procedure for uninstalling a cluster of Sametime server varies according to the component you are uninstalling:

Removing a cluster of Sametime Community servers on AIX, Linux, Solaris, or Windows:

To remove a cluster of Sametime Community servers on AIX, Linux, Solaris, or Windows, remove the nodes and the cluster first, then uninstall the individual servers.

About this task

Follow these steps to remove all servers in a cluster and to remove the cluster itself.

Unregistering a Sametime Community Server cluster on AIX, Linux, Solaris, or Windows:

If you will uninstall an entire cluster of IBM Sametime Community Servers, you must unregister the cluster from the Sametime System Console before you uninstall Sametime on the individual servers.

Before you begin

Start the Sametime System Console. Also start the Sametime Community Server on which you plan to run the utility. You can run the cluster unregistration utility from any server in the cluster.

About this task

Complete this task only if you want to remove the entire cluster of Sametime Community Servers from the Sametime System Console.

Procedure

1. Navigate to the Community Server's Install_location/console directory.
2. Update the following values in the console.properties file before saving and closing the file:

   | SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
   | SSCHTTPPort | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false." To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the "HTTP transport port." The default profile name is STSCAppProfile. |

3. Run the removeClusterRegistration registration utility:
   a. Run the following command to start the utility:
      - AIX, Linux, Solaris: removeClusterRegistration.sh
Windows: removeClusterRegistration.bat
b. When you are prompted for the cluster name, provide the same name that you used to create or register the cluster.

The utility unregisters the cluster from the console, and then registers each of the individual servers instead, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the cluster unregistration is successful, the console.pid will be removed.

Related tasks
“Starting and stopping servers in a Sametime deployment” on page 481
An IBM Sametime deployment is made of up several component servers that can be started and stopped independently.

Removing a Sametime Community Server from a cluster:

Before uninstalling an IBM Sametime Community Server that is part of a cluster administered by the Sametime System Console, remove the server from the cluster.

About this task

Follow these steps to remove the Sametime Community Server from the cluster administered with the Sametime System Console.

Procedure
1. Working on the server you want to remove from the cluster, navigate to the InstallLocation/console directory for the Deployment Manager profile.
2. If this is the first time you have run a utility on this server, open console.properties file and provide the System Console Host name, port, User Name and Password. Also, you can specify the log level, which is not mandatory.
3. Verify that the values in the productConfig.properties file are correct.
4. Run the utility from the console directory you used in Step 1.
   - AIX, Linux, Solaris: updateSTCluster.sh -remove
   - Windows: updateSTCluster.bat -remove
5. When you are prompted, enter the name of the cluster you are updating.
   The utility removes the Sametime Community Server from the cluster and generates the ConsoleUtility.log file in the console directory. It also deletes the console.pid file from the console directory.

Unregistering a clustered Community Server:

To remove an IBM Sametime Community Server from the list of the Sametime System Console’s managed servers, run the unregister utility on the server. This step is required before uninstalling a Community Server that you installed without a deployment plan and then registered with the Sametime System Console later using the registration utility. If you installed the server with a deployment plan, unregistering is only needed if you are performing some other activity that requires removal of the product from the console.

Before you begin

The Sametime System Console must be started.
About this task

During this task you will edit the following files; click the topic titles below to see
details on each file. You may want to open each topic in a new browser tab or
window so you can keep it open for reference:
• console.properties
• productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server’s Sametime console directory:
      • AIX, Linux, Solaris: The console directory is under the Community
          Server data directory; for example: /opt/IBM/domino85/notesdata/console
      • Windows: The console directory is under the Domino directory; for
          example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and
      productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

   Table 70. console.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
<td>Provide the fully qualified host name of the Sametime System Console server.</td>
</tr>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot; To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile. For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

3. Verify that the settings in the productConfig.properties file are correct,
   modifying them as needed before saving and closing the file.

   Only the required values in this file are listed here:

   Table 71. productConfig.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The Dep Name must be the name that was used when you installed: the unique name for this deployment as known by the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 71. productConfig.properties settings (continued)

| NodeHostName | Provide the fully qualified host name for the Community Server that is being unregistered. |

4. Start the Sametime Community Server.
5. Now unregister the server:
   a. Run the unregister utility with the following command:
      - AIX, Linux, Solaris: unregisterProductNode.sh
      - Windows: unregisterProductNode.bat
   b. As the unregister utility runs, you will be prompted enter the Location of the notes.ini file. You are only prompted for the notes.ini file location when unregistering the server. Type the full path to the directory containing the notes.ini file (for example, /stserver/data), and press Enter.

   The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.

Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233
If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

**Uninstalling a clustered Sametime Community Server:**

Follow the instructions for your operating system to uninstall IBM Sametime Community Server.

**Uninstalling a clustered Sametime Community Server on Windows:**

When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

**Before you begin**

Before you uninstall the Sametime Community Server, it is always a good practice to back up any important files.
About this task

To completely remove Sametime Community Server, you must uninstall Lotus Domino as well, and also both the Lotus directory and the Notes data directories.

Procedure
1. Stop the Domino (Sametime) server.
2. From the Microsoft Windows Start menu, select Settings > Control Panel > Add/Remove Programs.
3. Select IBM Sametime 8.x from the list and click Add/Remove. Click Yes when prompted to remove the Sametime server.
4. When the Windows uninstall program completes, click OK to exit the uninstall program.

Uninstalling a clustered Sametime Community Server on AIX, Linux, or Solaris:

When you uninstall IBM Sametime Community Server from an IBM Lotus Domino server using the Sametime Community Server uninstall program, all Sametime Community Server files that were added to the Lotus Domino installation are removed with the exception of files that were created while running Sametime Community Server. Updates that were made to the address books (including person documents, server documents, and changes to the Access Control List) are not removed.

Procedure
1. Stop the Domino (Sametime) server.
2. Switch to the root user.
3. Change to the following directory:
   
   datadir/_uninstst

4. Start the uninstall using the following command:
   
   ./uninstaller.bin

Removing a cluster of WebSphere-based Sametime servers on AIX, Linux, Solaris, or Windows:

To remove a cluster of Sametime servers running on WebSphere Application Server on AIX, Linux, Solaris, or Windows, remove the nodes and the cluster first, then uninstall the individual servers.

About this task

Follow these steps to remove all servers in a cluster and to remove the cluster itself.

Removing a node from a Deployment Manager before removing it from a cluster:

Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.
About this task

Note: For additional information on removing a node from the Deployment Manager, see the removeNode command in the WebSphere Application Server 7 information center. See Deleting specific cluster members for information on removing a cluster member.

Procedure
1. In the Deployment Manager’s Integrated Solutions Console, click System administration > Nodes.
2. On the "Nodes" page, select the check box beside each node that you want to remove.
3. At the topic of the table, click the Remove Node button.
   If you cannot remove the node by clicking Remove Node, remove the node from the configuration by clicking Force Delete.
4. Click OK.
5. Save your change by clicking the Save link in the "Messages" box at the top of the page.

Removing a WebSphere Application Server node from a cluster:

Before uninstalling an IBM Sametime server that was clustered with an IBM WebSphere Application Server network deployment, use the updateWASCluster -remove command to remove the node from the cluster.

About this task

Removing a node from a cluster involves verifying configuration settings for the cluster and then running a utility to remove the node from the cluster. If you are uninstalling a cluster, run the utility on every node in the cluster.

These instructions apply to the following Sametime servers:
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Gateway
- Sametime Advanced

Procedure
1. Update the console.properties file on the Deployment Manager:
   a. On the Deployment Manager server, navigate to the install_root/IBM/WebSphere/component/console folder for the Deployment Manager profile. The component varies depending on whether you are working with the Sametime Meeting, Media Manager, or Proxy server.
      Attention: The cluster’s Primary Node is installed on the same computer, so be sure to use the Deployment Manager profile.
   b. Open the console.properties file for editing.
   c. Fill in values for the following settings:

| SSCHostName | Type the fully qualified host name of the Sametime System Console server. |
SSCHTTPPort | Type the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false."
--- | ---
To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the "HTTP transport port." The default profile name is STSCAppProfile.

SSCUserName | Type the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.

SSCPASSWORD | Type the IBM WebSphere Application Server password associated with the SSCUserName.

d. Save and close the file.

2. Now open the productConfig.properties file (in the same folder) and verify that all of the settings are correct, changing settings as needed before you save and close the file.

3. Verify that the Sametime System Console has been started.

4. Open a command window and run the following command:
   **Attention:** You must specify the `-remove` parameter. Otherwise, you will unregister the entire cluster rather than remove the one node.
   - IBM AIX, Linux, or Solaris: updateWASCluster.sh -remove
   - Microsoft Windows: updateWASCluster.bat -remove

5. When prompted by the utility, enter the name of the cluster from which you are removing the node, and press Enter.

**Results**

This utility removes the node from the specified cluster's settings and generates a log file called ConsoleUtility.log, which it stores in the console/log directory.

**Unregistering a cluster of WebSphere-based servers on AIX, Linux, Solaris, or Windows:**

With the node removed from the IBM Sametime server cluster, you can now unregister the cluster from the Sametime System Console. After you unregister the cluster, it can no longer be administered from the Sametime System Console, which also serves as the Deployment Manager.

**Before you begin**

Before you start this task, verify that you have removed all nodes from the cluster.

**About this task**

Removing a cluster involves running a utility that removes the cluster from the Sametime System Console.

**Procedure**

1. On the Deployment Manager server, update the console.properties file on the Deployment Manager:
   a. Navigate to the InstallLocation/console directory.
Attention: The Gateway cluster’s Primary Node is installed on the same computer, so be sure to use the Deployment Manager profile.

b. Open the `console.properties` file for editing.
c. Fill in values for the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
<td>Type the fully qualified host name of the Sametime System Console server.</td>
</tr>
</tbody>
</table>
| SSCHTTPPort         | Type the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false."
|                     | To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the "HTTP transport port." The default profile name is STSCAppProfile. |
| SSCUserName         | Type the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is `wasadmin`. |
| SSCPassword         | Type the IBM WebSphere Application Server password associated with the SSCUserName. |

d. Save and close the file.

2. Open a command window and run the following command:

   - **IBM AIX, Linux, or Solaris**
     
     `removeWASClusterRegistration.sh`
   
   - **Microsoft Windows**
     
     `removeWASClusterRegistration.bat`

3. When prompted by the utility, enter the name of the cluster you are deleting, and press Enter.

**Results**

This utility deletes the cluster and generates a log file called `ConsoleUtility.log`, which it stores in the `console/log` directory.

**Unregistering Sametime Gateway:**

Before you uninstall an IBM Sametime Gateway server on IBM AIX, Linux, Solaris, or Microsoft Windows, remove it from the list of the Sametime System Console’s managed servers by running the unregister utility. You should only unregister Sametime Gateway when you will uninstall the server or perform some other activity that requires removal of the product from the console.

**About this task**

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- `console.properties`
- `productConfig.properties`

**Procedure**

1. Back up the `console.properties` and `productConfig.properties` files:
a. On the Sametime Gateway server, navigate to the `stgw_server_root/IBM/WebSphere/STgateway/console` directory.

b. Make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

2. Update the following values in the `console.properties` file and save the file.

<table>
<thead>
<tr>
<th>Table 72. <code>console.properties</code> settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCHostName</strong></td>
</tr>
<tr>
<td><strong>SSCHTTPPort</strong></td>
</tr>
<tr>
<td><strong>SSCUserName</strong></td>
</tr>
<tr>
<td><strong>SSCPASSWORD</strong></td>
</tr>
</tbody>
</table>

3. Verify that the settings in the `productConfig.properties` file are correct, modifying them as needed before saving and closing the file.

<table>
<thead>
<tr>
<th>Table 73. <code>productConfig.properties</code> settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DepName</strong></td>
</tr>
<tr>
<td><strong>NodeHostName</strong></td>
</tr>
</tbody>
</table>

4. Now unregister the server:

   a. Open a command window and run the unregistration utility with the following command:

   - **AIX, Linux, Solaris**: `unregisterWASProduct.sh -uninstall`
   - **Windows**: `unregisterWASProduct.bat -uninstall`

   The utility unregisters the server, generating a log file called `ConsoleUtility.log` and storing it in the `console/logs` directory. If the unregistration is successful, a `console.pid` will also be generated.
Related tasks

“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**Editing the multibroker.xml file before removing a cluster:**

Edit the multibroker.xml file to remove a specific line before removing the cluster.

**About this task**

Edit the multibroker.xml file to remove the following line:

```xml
<multibroker:DataReplicationDomain xmlns:multibroker="http://www.ibm.com/websphere/appserver/schemas/5.0/multibroker.xmi" xmi:id="DataReplicationDomain_1286203735111" name="stCellDRS"/>
```

In the example below, this is the multi-broker statement in bold face before the last line.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<multibroker:DataReplicationDomain xmlns:multibroker="http://www.ibm.com/websphere/appserver/schemas/5.0/multibroker.xmi" xmi:id="DataReplicationDomain_1285353668677" name="CsCellDRS">  
<defaultDataReplicationSettings xmlns:multibroker="http://www.ibm.com/websphere/appserver/schemas/5.0/multibroker.xmi" xmi:id="DataReplication_1285353669177" requestTimeout="5" encryptionType="NONE" numberOfReplicas="-1">  
<partition xmi:id="DRSPartition_1285353669474" partitionOnEntry="false"/>
<serialization xmi:id="DRSSerialization_1285353669490" entrySerializationKind="BYTES" propertySerializationKind="BYTES"/>
<pooling xmi:id="DRSConnectionPool_1285353669505" poolConnections="false"/>
</defaultDataReplicationSettings>
</multibroker:DataReplicationDomain>  
<multibroker:DataReplicationDomain xmlns:multibroker="http://www.ibm.com/websphere/appserver/schemas/5.0/multibroker.xmi" xmi:id="DataReplicationDomain_1286203735111" name="stCellDRS">  
<defaultDataReplicationSettings xmi:id="DataReplication_1286203735454" requestTimeout="5" encryptionType="NONE" numberOfReplicas="-1">  
<partition xmi:id="DRSPartition_1286203735689" partitionOnEntry="false"/>
<serialization xmi:id="DRSSerialization_1286203735704" entrySerializationKind="BYTES" propertySerializationKind="BYTES"/>
<pooling xmi:id="DRSConnectionPool_1286203735720" poolConnections="false"/>
</defaultDataReplicationSettings>
</multibroker:DataReplicationDomain>
</xmi:XMI>
```

**Removing a cluster from WebSphere Application Server on AIX, Linux, Solaris, or Windows:**

Remove the Sametime cluster from WebSphere Application Server network deployment.

**About this task**

After removing nodes and unregistering the cluster and individual servers from the Sametime System Console, remove the cluster from the network deployment. Use the Deployment Manager’s Integrated Solutions Console to remove the cluster.
Note: For additional information on deleting a cluster, see the Deleting clusters in the WebSphere Application Server 7 information center.

Procedure
1. In the Deployment Manager’s Integrated Solutions Console, click Servers > Clusters > WebSphere application server clusters.
2. Stop the cluster.
3. Select the cluster you want to delete, and click the Delete button.
4. Click OK.
5. Select Synchronize changes with Nodes, and then click the Save link in the "Messages" box at the top of the page.

Uninstalling a WebSphere-based Sametime server from a cluster:

Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

Before you begin
Remove the node from the Deployment Manager.

About this task
Running the install program on the Sametime server allows you to see the Uninstall option. You can uninstall any of these servers:
- Sametime System Console
- Sametime Proxy Server
- Sametime Meeting Server
- Sametime Media Manager
- Sametime Advanced

About uninstalling separate Media Manager components

The Media Manager is comprised of three components that work together: Packet Switcher, Conference Manager, and SIP Proxy and Registrar. When components are installed as non-clustered servers, you cannot uninstall a single component, but must uninstall them in sets of three, even if they are hosted on separate computers. Uninstall the components in this order: first Packet Switcher, then Conference Manager, and finally the SIP Proxy/Registrar.

If you configured clusters for the components, you can uninstall a single component from a cluster, provided you maintain at least one Packet Switcher, a SIP Proxy and Registrar cluster with at least one node, and a Conference Manager cluster with at least one node.

Procedure
1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
1. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   a. Stop the Sametime server.
   b. Stop WebSphere Application Server.
   c. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Working on the server you want to uninstall, run the Installation Manager.
   AIX, Linux, and Solaris
   /opt/IBM/InstallationManager/InstallationDirectory/eclipse/IBMIM
   Windows
   Select Start > Programs > IBM Installation Manager > IBM Installation Manager.
4. Choose the components to remove from the server. Click Next.
5. Click Uninstall.
   The Uninstall command removes the profile. The Repository Information section that appears after uninstalling the software will not have any files listed.
6. On the Deployment Manager, remove the Sametime application from the server by
   a. Start the Deployment Manager.
   b. Start WebSphere Application Server.
   c. Log in to the Integrated Solutions Console.
   d. Follow the steps for Uninstalling enterprise applications in the WebSphere Application Server information center.
7. If you uninstalled a Meeting server, you must also remove this node from the meeting_service_bus topology.
   a. On the Deployment Manager computer, start the Sametime server on the Deployment Manager if it is not already started.
   b. Log in to the Integrated Solutions Console.
   c. Click Service integration > Buses and click meeting_service_bus.
   d. In the content pane, under Topology, click Bus members.
   e. Select the node you uninstalled and click Remove
   f. Save your changes to the master configuration.
   g. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.
8. If you uninstalled an Advanced server, you must also remove this node from the bus topology.
   a. Start the Deployment Manager.
   b. Start WebSphere Application Server.
   c. Start the Sametime server.
   d. Log into the Integrated Solutions Console.
   e. Click Service integration > Buses.
   f. Click orgcollab_service_bus.
   g. In the content pane, under Topology, click Bus members.
h. Select the node you uninstalled and click **Remove**

i. Repeat the previous three steps to remove the bus member from the following buses:
   - rtc4web_cluster_service_bus
   - rtc4web_node_service_bus
   - MQTT_Bus

j. Save your changes to the master configuration.

k. If you have removed the only bus member for a server, you must disable the SIB Service at server startup.

9. If you are uninstalling a Media Manager that was installed on separate systems, repeat these steps on each remaining server that is connected to the Media Manager component you just uninstalled.

10. If you uninstalled only some nodes in a cluster, synchronize the remaining nodes:
   a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes in the cluster.
   c. Back in the navigator, click **System Administration > Node agents**.
   d. Click a node agent, and then click **Restart**; repeat for each node agent.

**What to do next**

During uninstallation, the server is unregistered from the Sametime System Console and the WebSphere Application Server profile removed. If you receive an error during the uninstallation process, refer to the following troubleshooting topics for instructions on manually completing the uninstallation process:

- Manually removing WebSphere Application Server
- “Unregistering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced” on page 1230
- Updating the Sametime System Console when server unregistration fails

**Related tasks**

“Removing a node from a Deployment Manager on AIX, Linux, Solaris, or Windows” on page 505

Before uninstalling an IBM Sametime server that was federated at install time or during registration, remove the node from the Deployment Manager.

*Uninstalling a Sametime Bandwidth Manager server node in a cluster on Linux or Windows:*

Uninstall IBM Sametime Bandwidth Manager on a server running Linux or Windows. This server runs on IBM WebSphere Application Server, similar to other Sametime servers, but requires a different process for uninstallation.

**Before you begin**

On the server node where you will uninstall the Bandwidth Manager, make sure the appropriate IBM WebSphere Application Server instance is running.

**Procedure**

1. On the server where you will uninstall the Bandwidth Manager, use a command line terminal or prompt, navigate to the \TMP\BWM folder containing the extracted uninstallation files.
2. Run the following command to uninstall the Bandwidth Manager:

   - **Linux**
     
     ```
     WAS_install_root/profiles/Profile_name/bin/ws_ant.sh uninstall
     ```
     
     where:
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application is installed, typically "AppServerProfile".
     - `WAS_install_root` is the root directory where WebSphere Application Server is installed. In Linux it is typically `/opt/IBM/WebSphere/AppServer`.
     
     For example:
     ```
     /opt/IBM/WebSphere/AppServer/profiles/AppServerProfile/bin/ws_ant.sh uninstall
     ```

   - **Microsoft Windows**
     
     ```
     WAS_install_root/profiles/Profile_name\bin\ws_ant.bat uninstall
     ```
     
     where:
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application is installed, typically "AppServerProfile".
     - `WAS_install_root` is the root directory where WebSphere Application Server is installed. In Microsoft Windows this is typically `C:\Program Files\WebSphere\AppServer` and in Linux it is typically `/opt/IBM/WebSphere/AppServer`.
     
     **Attention:** In Windows, you must use the DOS-shortened versions of the directory names; for example: `C:\PROGRA~1\IBM\WebSphere\AppServer`.  
     
     For example:
     ```
     C:\PROGRA~1\IBM\WebSphere\AppServer/profiles\AppServerProfile\bin\ws_ant.bat uninstall
     ```

     **Note:** Do not copy and paste the paths and parameters above because control characters may inadvertently be included in the command. For best results, type the command manually.

**Results**

The script makes the following changes:

- It removes the datasource DS_BWM created when you installed Bandwidth Manager.
- It removes these Websphere Application Server applications: BandwidthManagerSIPFrontend, BW_Pool_Application, and BandwidthManager.
- It removes the Bandwidth Manager node from the Sametime Servers portlet node.

**What to do next**

If you performed any manual steps during the original installation (such as LDAP federated repository configurations), you must now undo or reverse those steps manually.

**Uninstalling WebSphere and Sametime Gateway**

Uninstall the IBM WebSphere Application Server and IBM Sametime Gateway server applications on a computer running IBM AIX, Linux, Sun Solaris, or Microsoft Windows.
About this task

The procedure for uninstalling the WebSphere Application Server and Sametime Gateway products vary with the operating system:

Uninstalling WebSphere and Sametime Gateway on AIX, Linux, or Solaris:

Uninstall IBM Sametime Gateway on a server running IBM AIX, Linux, or Solaris.

Before you begin

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there's no need to uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

Note: WebSphere Application Server, the Sametime Gateway Profile, and Sametime Gateway must be uninstalled before installing anew. If all components are not removed, the VPD registry may determine that Sametime Gateway is still installed and believe that you are trying to install a second instance of Sametime Gateway.

Procedure

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Open a command window and navigate to the following directory:
   stgw_server_root/_uninst
4. Execute the appropriate command:
   • For GUI mode type ./uninstaller.bin
   • For Console mode type ./uninstaller.bin -console
5. Select the language you wish to use for the uninstall procedure and click OK. The Welcome screen is displayed.
6. Click Next to proceed. The Sametime Gateway features screen is displayed.
7. Select the check box for all available components/features and click Next. The Uninstall summary screen is displayed.
8. Click Uninstall to begin the procedure. The progress is displayed on the screen.
9. When the uninstall is complete, read the summary information and click Finish to exit the wizard.
10. Remove all Sametime Gateway install folders from your computer.
What to do next

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

Uninstalling WebSphere and Sametime Gateway on Windows:

Uninstall IBM Sametime Gateway on a server running Microsoft Windows.

Before you begin

Uninstalling Sametime Gateway automatically removes WebSphere Application Server as well. If you are reinstalling Sametime Gateway, there's no need to uninstall DB2 first. If you need to uninstall DB2, uninstall it separately according instructions in the DB2 Information Center at http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp.

Procedure

1. Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.
   a. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
   b. Stop the Sametime server.
   c. Stop WebSphere Application Server.
   d. Stop the Deployment Manager.
2. Close all browsers and command windows that are accessing the server you plan to uninstall.
3. Open a command window and navigate to the following directory:
   `stgw_server_root/_uninst`
4. Type the appropriate command to start the uninstall program:
   - For GUI mode, type `uninstaller.exe`
   - For console mode, type `uninstaller.exe -console`
5. Select the language you wish to use for the uninstall procedure and click OK. The Welcome screen is displayed.
6. Click Next to proceed. The Sametime Gateway features screen is displayed.
7. Select the check box for all available components/features and click Next. The Uninstall summary screen is displayed.
8. Click Uninstall to begin the procedure. The progress is displayed on the screen.
9. When the uninstall is complete, read the summary information and click Finish to exit the wizard.
10. Remove all Sametime Gateway install folders from your computer.
What to do next

WebSphere Application Server, the Sametime Gateway Profile, and the Sametime Gateway application must all be uninstalled before installing a new version of Sametime Gateway. If all components are not removed, the VPD registry may treat any new installation as an additional instance of Sametime Gateway rather than as an initial instance. If WebSphere Application Server did not uninstall completely, refer to Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows for instructions on manually removing WebSphere Application Server.

Uninstalling DB2 with the IBM Installation Manager

Use the Installation Manager to uninstall the version of IBM DB2 that was provided with IBM Sametime for Linux and Microsoft Windows.

Before you begin

DB2 must be running before starting uninstallation.

About this task

Run the installer on the DB2 server to see the Uninstall option.

Procedure

1. Run the Installation Manager.
   - Linux: /opt/IBM/InstallationManager/eclipse/IBMIM
   - Windows: Click Start > Programs > IBM Installation Manager > IBM Installation Manager
2. Choose the components to remove from the server, and then click Next.
3. Click Uninstall.
   - The Repository Information section that appears after uninstalling the software will not have any files listed.

Results

If the installation fails, click View Log File for more information.

Installation Manager logs are stored in the following locations:

- Linux: /var.ibm/InstallationManager/logs
  More detailed DB2 installation logs are stored in /tmp folder and are named db2setup.log, db2setup.his, and db2setup.err.
- Windows 2003: %ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
  More detailed DB2 installation logs are stored in %My Documents%\DB2LOG\.
  The log file name includes the date and time of the installation attempt; for example: C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log.
- Windows 2008: %ALLUSERSPROFILE%\IBM\Installation Manager\logs
  More detailed DB2 installation logs are stored in %My Documents%\DB2LOG\.
  The log file name includes the date and time of the installation attempt; for example: C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log.
Note: If uninstallation fails, you can remove DB2 manually as described in Manually removing DB2 data on AIX, Linux, Solaris, and Windows.

What to do next

Remove the rest of the DB2 files and data left on the system.
1. Remove all files in the local /tmp or temp directory.
2. Manually remove user and group information.
   - Linux
     Remove user home directories under /home.
     DB2 Instance user account: db2admin (or the administrator account specified during installation)
     DB2 Administration Server (DAS) user account: dasuser1
     DB2 users group: db2admin (or the same as the DB2 Instance user account name defined by user)
     DB2 Administration users group: dasadm1
   - Windows
     Remove DB2 users and groups:
     DB2 Instance user account: db2admin (or the administrator account specified during installation)
     DB2 Administration Server (DAS) user account: db2admin
     DB2 users group: DB2USERS
     DB2 Administration users group: DB2ADMNS
3. Remove these directories for DB2.
   The directories below show the Windows path. They will differ on Linux.
   - c:\documents and settings\all users\application data\ibm\db2
   - c:\documents and settings\all users\application data\ibm\db2history
   - c:\documents and settings\db2admin
   - c:\documents and settings\install user\application data\ibm\vshet
   - c:\documents and settings\install user\application data\ibm\db2
4. Delete the remaining DB2 directories.

Deploying the Sametime client to users

The IBM Sametime Connect client or Sametime client embedded in Notes have to be installed on users' machines to use instant messaging and meetings. This section gives you information about ways to install these clients.

Preparing for Sametime client installation and deployment

This section gives you information about preparing the web browser client to use meetings and instructions for customizing installations of Sametime Connect client and Sametime embedded client for Lotus Notes.

Installing the Java Runtime environment for browser-based clients

Users who will attend IBM Sametime meetings with a web browser may need to install the Java Runtime Environment.
About this task

Installing the Java Runtime environment for meetings

Users attending meetings with the browser-based client must install the Java Runtime environment under the following conditions:

• Meetings are hosted on Sametime Classic (meetings running on a legacy Domino server).
• Meetings are hosted on Sametime 8.5 or later and the user wants to share his or her screen with attendees. Install the IBM or Sun JRE 1.5 and 1.6 (you only need the JRE if you want to be able to share your screen during meetings).

If either of these conditions is true, the user must install a supported version of the JRE before attending online meeting:

• IBM JRE 1.5 or later
• Sun JRE 1.5 or later

Sametime Connect client considerations

There are several things you need to know before deploying the IBM Sametime Connect client to your users.

About this task

The Sametime Connect client must be installed on a user's workstation by someone with administrative privileges on that computer. Before installing the client, review the following points:

• Internet passwords required
  Internet passwords are required to log on to IBM Sametime connect. Before using Sametime Connect, each user must have an Internet password in their Person Document in the Domino Directory or stored in the LDAP Directory. You may need to inform users of their Internet passwords.

• Password character restrictions
  In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
  `: \ } ' " &`

• Supporting IPv6 addressing with the Connect client
  Supporting the IPv6 protocol in a Sametime deployment requires you to upgrade Sametime Connect clients to release 8.5 or later to ensure they can communicate with Sametime servers that use IPv6 addresses.
  If you support only IPv6 addressing, older clients will not generate error messages but will appear “broken” to users because they cannot communicate with the IPv6–enabled servers. To avoid lengthy investigations of problems caused by attempts to use older clients with servers where only IPv6 addressing is enabled, you should only use clients from release 8.0.2 or later.
  If you support both IPv4 and IPv6 addressing, all Sametime clients can communicate with the IPv6–enabled servers; just be sure to configure the servers to listen for IPv4–format addresses as well as IPv6–format addresses.

• Spell checker dictionaries
  The U.S. English spell check dictionary is installed automatically, but you can install spell checker dictionaries for additional languages. The additional dictionaries are provided as an update site on the client CD and downloaded image in the optional-components/optional-components-update.zip file. See “Distributing updates and optional features to clients” on page 598.
Configuring servers to support the Sametime web audio-visual plugin for browser-based clients

The IBM Sametime web audio-visual plugin adds audio and video conferencing features to browser-based clients.

**Configuring Sametime servers to support browser-based audio-visual conferencing**

After installing all servers, configure them for single sign-on (SSO) and anonymous authentication, which is a requirement for enabling browser-based video conferencing.

**About this task**

Use this checklist to ensure that you have met login requirements on the servers before deploying the Sametime web audio-visual plugin to users.

**Procedure**

1. Define a Sametime Proxy server so Sametime users can be detected when they are in Sametime meeting rooms.
2. Configure SSO between the servers.
   a. Set up SSO between the Sametime Meeting Server and the Sametime Community Server.
   b. Set up SSO between the Sametime SIP Proxy and Registrar server and the Sametime Community Server.
   c. Import the LTPA token into the SIP Proxy and Registrar server.
   d. Verify that the servers use the same SSO settings.
   e. Verify that you are able to get Sametime live names in the browser-based meetings client.
3. Configure anonymous authentication in the SIP Proxy and Registrar.
4. The Proxy Servers and the Media Manager Servers must be added to the Sametime Community Server’s trusted IP addresses.
5. If the Sametime Meeting Server and Sametime Proxy Server are on the same computer, change the host name of the Proxy Server so it does not match the Sametime Meeting Server and does not contain a wildcard character.
6. Verify that all servers are reachable by their host names: Sametime Community Server, Sametime Meeting Server, and Sametime Media Manager.
Providing an alternate download site for the Sametime web audio-visual plugin

The IBM Sametime web audio-visual plugin package is configured automatically by default for downloading from the Sametime Proxy Server. However, you can also post the plugin on another server and present that server as an alternate site from which browser-based clients can download the plugin.

About this task

Follow these steps to set up an HTTP server and configure an alternate URL for users to download the plugin.

Procedure

1. Download the Sametime web audio-visual plugin package from the Media Manager installation package under the WebAVBrowserInstalls directory and extract the files to a temporary directory.
2. Log in to the machine where the HTTP server is installed.
3. Navigate to the HTTP server directory.
4. Copy the following files to the directory:
   - STWebPlayer.CAB
   - STWebPlayerPDB.zip
   - STWebPlayer.xpi
   - STWebPlayerMac.xpi
   - STWebPlayerWin7.CAB
   - stwebsoftphone.CAB
   - stwebsoftphone.zip
   - VersionInfo.txt
5. Log in to the Sametime System Console.
7. In the Proxy Servers list, click the server with the configuration that you want to change.
8. In the Web AV Settings tab, provide the following details:
   - **URL**
     Specify the URL where the plugin will be hosted, including the port; for example:
     http://Host_name:HTTP_port/directory
   - **WebPlayer Version**
     Specify the value of the WebPlayer Version in the VersionInfo.txt file included with the Web Meeting Room client package.
   - **Softphone Plugin Version**
     Specify the value of the Plugin Version in the VersionInfo.txt file included with the Web Meeting Room client package.
9. Click Apply, then click OK.
10. Click System administration > Save changes to master repository.
11. Select Synchronize changes with Nodes. Click Save.
12. Restart the Proxy Server.
   - If the Sametime Proxy Server’s primary node is federated to the Sametime System Console deployment manager, then restart the System Console deployment manager, Proxy Server primary node agent, and Proxy Server.
   - If the Sametime Proxy Server is installed as a Cell profile, then restart the Proxy Server’s own deployment manager, node agent, and server.

### Installing and uninstalling Sametime web audio-visual plugin for browser-based meeting clients

Although you can attend meetings directly from a browser, you must install the IBM Sametime web audio-visual plugin before you can participate in an audio/video call during a meeting.

### About this task

The Sametime web audio-visual plugin works with Windows and Mac clients operating on Mozilla Firefox or Microsoft Internet Explorer. For more information about software requirements, see the System requirements for this release of the Sametime family of products, maintained as an IBM Tech Note at the following web address:


A keyboard user who uses the audio-visual plugin with Mozilla Firefox must use the Shift+Tab key combination two times to tab out of the “Join Call” button in the Voice and Video panel. For more information, see the Bugzilla web site:

https://bugzilla.mozilla.org/show_bug.cgi?id=618046

### Preparing to install the Sametime web audio-visual plugin

Prepare your browser before installing the IBM Sametime web audio-visual plugin.
Before you begin

You must have already prepared the servers, as described in "Configuring servers to support the Sametime web audio-visual plugin for browser-based clients."

Procedure

- For Internet Explorer browsers, provide access to allow the plugin to run.
  - If your site allows ActiveX controls to be installed on clients, follow these steps:
    1. From the browser, click **Tools > Internet Options**.
    2. On the Security tab, click **Custom level**.
    3. Verify or select these options:
      - **Binary and Script Behavior**: Enable
      - **Download signed ActiveX Controls**: Prompt
      - **Only allow approved domains to use ActiveX without prompt**: Enable
      - **Run ActiveX Controls and plug-ins**: Enable
      - **Script ActiveX controls marked safe for scripting**: Enable
    4. Click **OK** and **OK** again.
  - If your site does not allow ActiveX controls to be installed on clients, follow these steps to include the Sametime servers in the browser’s Trusted Sites list:
    1. In the browser, click **Tools > Internet Options** and click the Security tab.
    2. Click **Trusted Sites > Sites**.
    3. Add the host name for the Sametime servers and if applicable, the URL for an alternate update site:
      - Add the Sametime Meeting Server and Sametime Proxy Server host names.
      - If you use an Alternate Update site, provide the URL where the plugin will be hosted. This matches the URL you will provide in the Web AV Settings tab for the Proxy Server.
      - Do not select **Require server verification (https) for all sites in this zone**.
    4. Click **Close** and **OK** to save the changes.
- For all browsers, clear the cache and cookies to be sure that you download the latest plugin files.
  - For Firefox browsers, use the **Tools > Clear Recent History** command to delete cache and cookies.
  - For Internet Explorer 7 and 8, use the **Tools > Delete Browsing History** command to delete temporary Internet files and cookies.
Related tasks

“Configuring servers to support the Sametime web audio-visual plugin for browser-based clients” on page 544
The IBM Sametime web audio-visual plugin adds audio and video conferencing features to browser-based clients.

“Providing an alternate download site for the Sametime web audio-visual plugin” on page 545
The IBM Sametime web audio-visual plugin package is configured automatically by default for downloading from the Sametime Proxy Server. However, you can also post the plugin on another server and present that server as an alternate site from which browser-based clients can download the plugin.

Installing and uninstalling the Sametime web audio-visual plugin automatically from a browser
You can install the IBM Sametime web audio-visual plugin by entering a Meeting room and using the browser’s automatic install feature.

Procedure

1. In the browser, unblock popups for the IBM Sametime Meeting URL. If the plugin was already installed on the client machine, empty the browser's cache to ensure a successful upgrade.

2. On the operating system, verify that the deployment's Sametime Meeting Server and Sametime Proxy Server hosts (for example: 10.10.10.10xyz.abc.com) are registered in the client workstation's DNS. If not, then make an entry for both the hosts in the etc\hosts file, stored in the %WINDIR%\system32\drivers\etc\hosts directory. On the Macintosh, add the host name and IP address to the /etc/hosts file using a super user account.

3. Clients install the plugin for their browser:
   - Internet Explorer
     a. Enter the Meeting room.
     b. A popup prompts to install the ActiveX control “IBM Sametime WebPlayer.” There may be some delay, depending on the plugin size and network availability.
     c. Right-click the popup, and then click Allow “Install ActiveX Control”. An installation message prompts to install the “IBM Sametime WebPlayer” control.
     d. Click Install.

   After the plugin has been installed, the meeting room page is refreshed. The participant list shows all users in the meeting room, and the green telephone icon is enabled so you can start the call.

   - Mozilla Firefox
     a. Enter the Meeting room.
     b. A popup prompts to install the plugin.
     c. Click Allow.
     d. Click Install.

   After the plugin has been installed, Firefox prompts to restart the browser. The user must restart the browser to use the plugin in a meeting.

In the plugin does not install, check if "Block pop-up windows" is selected in the browser options Content panel. The option must be cleared for the installation to work.
Results

Uninstalling the plugin

Follow the instructions that apply to your operating system and browser to uninstall the Sametime web audio-visual plugin.

Internet Explorer on Microsoft Windows

- Internet Explorer 6:
  Open Explorer and navigate to the folder %WINDIR%\Downloaded Program Files and remove the entry “IBM Lotus Sametime WebPlayer” Control.

- Internet Explorer 7 and 8:
  Launch Internet Explorer and navigate to Tools > Manage Add-ons. Select Show All Add-ons. Double-click IBM Lotus Sametime WebPlayer and click Remove.

Mozilla Firefox on Microsoft Windows and Mac OSX

1. Launch Firefox and navigate to Tools > Add-ons. Open the Extensions Tab and select IBM Lotus Sametime WebPlayer. Click Uninstall.
2. Clean up folders that are no longer needed.
   Windows XP: Delete the folders %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\ and %APPDATA%\IBM\Lotus\Sametime WebPlayer\.
   Windows 7: Delete the folder %USERPROFILE%\AppData\LocalLow\ IBM\Lotus\Sametime WebPlayer\.
   Mac OSX: Delete the folder $HOME/Library/ApplicationSupport/IBM/Lotus/Sametime WebPlayer/.

Setting up the Sametime Web audio-visual plugin in an SSL-enabled environment

If the IBM Sametime servers are configured for SSL-enabled connections, you must first accept the server’s SSL certificates.

Before you begin

A meeting room must be set up and the servers must be running.

Procedure

1. In the browser, open the browser-based Sametime client. For example: https://hostname:port/stwebclient/index.jsp
2. Log in to the browser-based client and accept the security certificate.
3. Browse to the Sametime Meeting server URL.
4. Log in to the meeting client and enter into the Web audio-visual-enabled room.
5. When prompted, install the Web audio-visual plugin, which is an ActiveX control for Internet Explorer and a plugin for Firefox.
Related tasks
“Working with Sametime servers that are enabled for SSL” on page 787
Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

Installing and uninstalling the Sametime web audio-visual plugin using the installation program
If you prefer to install the IBM Sametime web audio-visual plugin before you join a meeting, you can install the program from the stand-alone installation program.

About this task
Follow the instructions for your operating system. The Web client plugin for Mac requires Mozilla Firefox. The Sametime web audio-visual plugin for Windows works with Internet Explorer and Mozilla Firefox. As an administrator, you can use this method to push the client installs to users who do not have administrative privileges.

Procedure
1. Log in to the computer with administrative privileges.
2. Locate the install program, which is part of the Media Manager Server installation package, located in this directory: disk1/WebAVDesktopInstalls
   If the package is extracted locally, it is located here:
   extract_directory/IBM/SametimeMediaManager/WebAVDesktopInstalls
3. Run the install program.
   Windows
   a. Run setup.exe.
   b. Choose “Complete” or “Custom” setup type. Choosing “custom” allows you to select the plugin for Microsoft Internet Explorer, Mozilla Firefox, or both.
   c. Complete the installation. If your browser is running, you will need to close it and re-run it before the plugins appear.
   By default, the installer will only install the plugins for the current user. To install for all users on the system, set the ALLUSERS property to 1 from the command line. For example:
   setup.exe /V"ALLUSERS=1"
   or
   msiexec /i setup.msi ALLUSERS=1
   Mac
   Execute same-time-webplayer.mpkg and complete install.

Results

Uninstalling
Follow the instructions that apply to your operating system to uninstall the Sametime web audio-visual plugin.

Microsoft Windows
1. From the Control Panel, use the Add or Remove Programs utility to remove the Sametime WebPlayer program.
Mac OSX
1. To uninstall, delete the following directories. You must have administrative privileges:
2. /Library/Application Support/IBM/Lotus/Sametime WebPlayer
3. /Library/Application Support/Mozilla/Extensions/{ec8030f7-c20a-464f-9b0e-13a3a9e97384}/34629D26-F36A-4a97-9A3C-D05EA007FEB7

Customizing client installation packages
Customize installation packages before deploying clients if you want default installations to include extra features or preferences. Examples of extra features are those included with Sametime, such as Microsoft Office Integration and custom features developed with the Sametime Software Development Kit.

Related tasks
“Configuring Sametime Connect client preferences with the Expeditor managed settings framework” on page 951
You can configure and manage user preferences for IBM Sametime Connect clients using the Expeditor managed settings framework.

Enabling installation of optional client features such as Microsoft Office Integration
IBM Sametime ships with a number of optional client features that are not included in the default installation package. You can add features to the installation package for new client installs and update already-installed clients by updating the installation manifest file.

About this task
These optional features are not installed by default; to make them available to your users, you must either update existing clients or customize the installation package for new clients.
- Microsoft Office Integration features
- Email integration features
- Spell checker dictionaries

Note: Microsoft Office Integration features are available only for clients running on Windows.

What to do next
After you decide which optional features to add to client installations, choose the method for installing the client and edit the client install package accordingly.
Related tasks
“Example: Customized install.xml file for the Sametime Connect client (CD or
download install)” on page 556
To make optional features and custom features available, you can customize the
install.xml file for IBM Sametime Connect clients on Linux, Mac, or Windows
operating systems. Repackage the CD or download image with the changes.
“Editing the install.xml file for use on the Sametime Welcome page” on page 562
To make optional features available, you can customize the install.xml file for
IBM Sametime Connect clients on Mac or Windows operating systems.
“Editing the install.addon.xml file for the Lotus Notes embedded client” on page
559
You can customize the install.addon.xml file for the Sametime client that is
embedded in Lotus Notes on Microsoft Windows and on Mac OS X. Optional
features are not available on the Linux embedded client.

Enabling installation of custom client features and extra
preferences
To set initial preferences that are unique to your site or to add custom features,
edit the plugin_customization.ini file used by the client installation program.
When the client starts for the first time, the preferences and features defined in the
plugin_customization.ini file go into effect.

Creating custom client features:
Some organizations create custom plugins that contain extra client features, such as
site-specific login messages or corporate branding and graphics. To include the
plugin in all client installations, copy the custom plugin to the installation kit, then
edit the install manifest file and plugin_customization.ini file to reference the
features to install.

Before you begin
Before you can build plug-ins, you must install:
• The Sametime software development kit
• Eclipse IDE (integrated development environment) version 3.2
• The JCL Desktop custom runtime environment for Windows and Linux
• the Eclipse J9 JDT launching plug-in for Windows and Linux
• a standard Java Runtime Environment (1.4.2 or higher version)
• Windows XP, Linux, or Mac operating system supported by Sametime 7.5. or
later
• For comprehensive information on setting up the integrated development
environment, and building and providing plug-ins to clients, see the IBM
Redbooks® publications at http://www.redbooks.ibm.com/abstracts/
sg247346.html.
For information on using a wizard to create plug-ins, see the Eclipse
documentation: http://help.eclipse.org/help32/topic/
org.eclipse.pde.doc.user/guide/tools/project_wizards/
new_project_wizards.htm.

Procedure
Put your compressed plug-in into the sametime-connect.mpkg\Contents folder.
What to do next

Sign the plugin, then edit the plugin_customization.ini file and edit the installation manifest file to include the custom features.

Related tasks

“Example: Writing custom messages for clients”
You can create a branding plugin that shows a custom message in the user’s “New contact” screen or in the login screen. For example, when you are creating a message for the new contact screen, if you connect a particular community to a public instant messaging network, you may want to tell the users which community to use to add a contact from that public network. This branding feature accepts text only.

“Editing the plugin_customization.ini file to add custom features and change default preferences” on page 554
You can customize the plugin_customization.ini file to add features from a custom plugin or to change the default installed preferences.

“Example: Customized install.xml file for the Sametime Connect client (CD or download install)” on page 556
To make optional features and custom features available, you can customize the install.xml file for IBM Sametime Connect clients on Linux, Mac, or Windows operating systems. Repackage the CD or download image with the changes.

“Editing the install.xml file for use on the Sametime Welcome page” on page 562
To make optional features available, you can customize the install.xml file for IBM Sametime Connect clients on Mac or Windows operating systems.

“Editing the install.addon.xml file for the Lotus Notes embedded client” on page 559
You can customize the install.addon.xml file for the Sametime client that is embedded in Lotus Notes on Microsoft Windows and on Mac OS X. Optional features are not available on the Linux embedded client.

Example: Writing custom messages for clients:

You can create a branding plugin that shows a custom message in the user’s "New contact" screen or in the login screen. For example, when you are creating a message for the new contact screen, if you connect a particular community to a public instant messaging network, you may want to tell the users which community to use to add a contact from that public network. This branding feature accepts text only.

Example

This is a sample branding plug-in:

```xml
<plugin>
  <extension
      id="com.ibm.collaboration.realtime.notes.branding"
      point="com.ibm.collaboration.realtime.ui.stbranding">
    <stbranding
      id="mypackage.messages"
      name="Custom Sametime Messages">
      <messages class="mypackage.Messages"/>
    </stbranding>
  </extension>
</plugin>
```

Below are some Sample Messages.java:
import org.eclipse.osgi.util.NLS;

private static final String BUNDLE_NAME = "messages";//$NON-NLS-1$

// Add Contacts dialog message for single community
public static String
com_ibm_collaboration_realtime_imhub_strings_messages
$singleCommunityDefMsgArea;

// Add Contacts dialog message for multiple communities
public static String
com_ibm_collaboration_realtime_imhub_strings_messages
$multiCommunityDefMsgArea;

static {
    NLS.initializeMessages(BUNDLE_NAME, Messages.class);}

Below are Sample resourcebundle messages.properties

Add a new contact by entering a name below.
com_ibm_collaboration_realtime_imhub_strings_messages$multiCommunityDefMsgArea=
Customize me:
Add a new contact by selecting the community where the contact exists.
Enter the user's name (or email address if adding an external contact.)

Customizing client installation files

Download the plugin_customization.ini and installation manifest files from the
client installation package and then customize them with the features and
preferences you want.

Downloading files for client installations from a CD or download image:

Download the plugin_customization.ini and installation manifest files from the
client installation package to prepare to edit them for a CD or download image
installation. For the Sametime Connect client, the installation manifest file is named
install.xml. For the Sametime embedded client for Lotus Notes, the installation
manifest file is named install.addon.xml.

Procedure

Follow the steps for the installation package you are editing.

Extract the files from the installation package.

- **Linux**
  Extract the files to the /etc/ibm/sametime-connect directory. A customized
  install file in the /etc/ibm/sametime-connect directory takes precedence over the
copy in the rpm.

- **Mac**
  Extract the files, maintaining the same folder structure. They are extracted to the
  install_mpkg\deploy folder.

- **Windows**
  If you are using the zipped version of the installation package, extract the files,
maintaining the same folder structure. They are extracted to the
  install-kit-base-dir\deploy\install.xml directory.

  If you are using the self-extracting .exe file, start the installation program. After
  you complete the step for entering a local directory path in the "Save files in
  folder" field and clicking **Next**, the files are downloaded. You can then exit the
  installation program.

Editing the plugin_customization.ini file to add custom features and change
default preferences:
You can customize the `plugin_customization.ini` file to add features from a custom plugin or to change the default installed preferences.

**Before you begin**

Download the client installation files to prepare them for customizing.

**Procedure**

Follow these steps to customize the `plugin_customization.ini` file.

1. Open the downloaded `plugin_customization.ini` file in a text editor.

   - **Linux**
     
     `/etc/ibm/sametime-connect/plugin_customization.ini`
   
   - **Mac**
     
     `install_mpkg\deploy\plugin_customization.ini`
   
   - **Windows**
     
     `install-kit-base-dir\deploy\plugin_customization.ini`

2. Change the default preferences that you want users to receive. For a list of preferences you can add, see Sametime client preferences.

   After installation, users can manually override the preferences set with the `plugin_customization.ini` file by using the Preferences dialog in their Sametime Connect clients. If you prefer to set preferences at runtime with the option of locking the preferences, use the Expeditor managed settings framework to set read-only preferences instead.

3. If you created a custom plugin, identify the features to install.

   a. Add the features to the `plugin_customization.ini` file. For example:

      ```ini
      #com.ibm.collaboration.realtime.community/
      SametimeServer=chaat1.sametime.example.com
      
      #com.ibm.collaboration.realtime.ui/
      stbranding=custom.branding.custom_feature
      ```

   b. If you did not sign the plugin, comment out these four lines from the `plugin_customization.ini` file. Otherwise the installation will fail:

      ```ini
      #com.ibm.rcp.security.update/
      VERIFICATION_LISTENER=com.ibm.rcp.security.update.DefaultVerificationListener
      com.ibm.rcp.security.update/EXPIRED_SIGNATURE_POLICY=PROMPT
      #com.ibm.rcp.security.update/UNSIGNED_PLUGIN_POLICY=PROMPT
      #com.ibm.rcp.security.update/UNTRUSTED_SIGNATURE_POLICY=PROMPT
      ```


5. Repackage the CD or download image before distributing it to your users. If you are making the client installation package available from the Sametime Welcome page, generate a new installation package.

**What to do next**

If you plan to install clients in silent mode, change the `CREATECOMMUNITYTEMPLATE` setting in the `silentinstall.ini` file to false.
Related tasks

“Configuring Sametime Connect client preferences with the Expeditor managed settings framework” on page 951
You can configure and manage user preferences for IBM Sametime Connect clients using the Expeditor managed settings framework.

“Preparing to install Sametime Connect clients in silent mode” on page 568
You can enable the silent installation of the IBM Sametime Connect Client on Windows using two files that are provided on the client standalone installer CD and the associated downloaded image.

“Making the client installation package available from the Sametime Welcome page” on page 566
Perform the following steps to make the network client installer available for installation from the Sametime Welcome page. If the Domino HTTP server has been configured to use SSL with a self-signed test certificate, users will not be able to download the zip from the Sametime Welcome page.

Example: Customized install.xml file for the Sametime Connect client (CD or download install):

To make optional features and custom features available, you can customize the install.xml file for IBM Sametime Connect clients on Linux, Mac, or Windows operating systems. Repackage the CD or download image with the changes.

Before you begin

Download the client installation files to prepare them for customizing.

About this task

Follow these steps to customize the install.xml file.

Procedure

1. Open the downloaded install.xml file in a text editor.
   - Linux
     /etc/ibm/sametime-connect/install.xml
   - Mac
     install_mpkg\deploy\install.xml
   - Windows
     install-kit-base-dir\deploy\install.xml
2. Customize the install.xml file to remove the comment markers from any optional features you wish to include in the install.
   Optional features are commented out like this:
   <!-- This is the beginning of a comment marker
   The following characters mark the end of the comment: -->
   Everything between the markers is ignored as a comment. To enable a feature, either copy it and place it outside of the commented section, or move the comment markers as needed to exclude the feature from the commented section.
3. If you created a custom plugin, add the custom features to install.
4. Save and close the file.
5. Test a base install.
6. Repackage the CD or download image before distributing it to your users.

Related tasks
“Creating custom client features” on page 552
Some organizations create custom plugins that contain extra client features, such as site-specific login messages or corporate branding and graphics. To include the plugin in all client installations, copy the custom plugin to the installation kit, then edit the install manifest file and plugin_customization.ini file to reference the features to install.

Example: Customized install.xml file for the Sametime Connect client:

The install.xml is the installation manifest, which lists all features shipped with IBM Sametime Connect. When you uncomment the optional features in the list, they become part of the base client install package. You can edit the install.xml file for installations from a CD, a downloadable image, or from a link on the Sametime Welcome page.

List of optional features

Optional features have these unique feature IDs in the .xml file.

Table 74. List of optional features

<table>
<thead>
<tr>
<th>Optional feature</th>
<th>Feature ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Office features</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Required</strong>: Sametime Connect client feature (required when you add any Microsoft Office optional features to the installation file for Sametime Connect clients)</td>
<td>com.ibm.collaboration.realtime.oi.standalone.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Office</td>
<td>com.ibm.collaboration.realtime.oi.smarttags.feature</td>
</tr>
<tr>
<td>Microsoft Outlook calendar availability</td>
<td>com.ibm.collaboration.realtime.exchange.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.toolbar.feature</td>
</tr>
<tr>
<td>Sametime meeting integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.webConfTab.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for SharePoint</td>
<td>com.ibm.collaboration.realtime.oi.sharepoint.feature</td>
</tr>
<tr>
<td><strong>Notes calendar integration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Required</strong>: Sametime Connect client feature (required when you add the Notes calendar integration optional feature to the installation file for Sametime Connect clients)</td>
<td>com.ibm.collaboration.realtime.notes.connector.standalone.feature</td>
</tr>
<tr>
<td>Sametime availability status updates based on person’s Lotus Notes calendar entries</td>
<td>com.ibm.collaboration.realtime.notes.connector.feature</td>
</tr>
</tbody>
</table>
Original file with no optional features enabled

This example shows the default settings, in which six Microsoft Office Integration features and two other optional features are commented out. The commented section begins with <!-- and ends with -->

Note: The lines below have been formatted for readability because it is important to move entire feature statements.

<!--
The following Sametime features are optional, and may be uncommented in order to be deployed.
<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.notes.connector.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="123"
    size="123" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.notes.connector.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add" url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add" url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
    size="4302" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.webConfTab.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3048"
    size="3048" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
-->

Modified file with some optional features enabled

Now the Microsoft Office Integration features have been moved outside of the comment, so they will install automatically. The remaining optional features are still commented out and will not be installed.

<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
Editing the install.addon.xml file for the Lotus Notes embedded client:

You can customize the install.addon.xml file for the Sametime client that is embedded in Lotus Notes on Microsoft Windows and on Mac OS X. Optional features are not available on the Linux embedded client.

Before you begin

Download the client installation files to prepare them for customizing.

About this task

Follow these steps to customize the install.addon.xml file to add optional features to the Lotus Notes embedded client installation package.

Procedure

1. Navigate to the .\deploy folder for the appropriate client operating system. Open the install.xml file in a text editor.
   - Mac
     \sametimeclient\MacOSX\deploy\install.addon.xml
   - Windows
     Save_files_in_folder_directory\deploy\install.addon.xml

2. Locate the section that starts with the following statement near the end of the file:
   The following Sametime features are optional, and may be uncommented in order to be deployed.
   -<feature id="com.ibm.collaboration.realtime.notes.connector.feature" version="8.5.0.20091027-2140" match="compatible" download-size="123" size="123" action="install" shared="true" mergeaction="add"
   url="${installer.root}"/>
   -<feature id="com.ibm.collaboration.realtime.notes.connector.standalone.feature" version="8.5.0.20091027-2140" match="compatible" download-size="7" size="7" action="install" shared="true" mergeaction="add"
   url="${installer.root}"/>

3. Remove the comment markers to enable desired features:
   - By default, all of the features in this section are disabled because they are commented out.
   - You can enable any combination of features.
   - You can enable any, or all, of these features by moving the comment markers to the appropriate position.
   - Make sure to comment entire features (from the opening <feature marker through the closing /> marker.
   - Begin a comment with this marker: <!--
For example, you may want to enable one or more Microsoft Office Integration features for clients running on Windows:

Table 75. Microsoft Office Integration features available on Windows

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.ibm.collaboration.realtime.exchange</td>
<td>Provides automatic availability status updates in Sametime livenames based on Microsoft Outlook calendar entries.</td>
</tr>
<tr>
<td>com.ibm.collaboration.realtime.oi.sharepoint.feature</td>
<td>Provides awareness and instant messaging among Sametime users who are using an Office SharePoint site.</td>
</tr>
<tr>
<td>com.ibm.collaboration.realtime.oi.toolbar</td>
<td>Provides an action toolbar in Microsoft Outlook containing Sametime instant messaging actions, including access to the contact list, status, and location information.</td>
</tr>
<tr>
<td>com.ibm.collaboration.realtime.oi.webConfTab</td>
<td>Provides the ability to reserve Sametime meetings from the Sametime tab in Microsoft Outlook meetings.</td>
</tr>
</tbody>
</table>

4. Save and close the deploy\install.addon.xml file.
5. Repackage the CD or download image before distributing to your users.

Example: Customized client install.addon.xml file for embedded client:

The install.addon.xml file is the installation manifest, which lists all features shipped with the IBM Sametime embedded client for Lotus Notes. When you uncomment the optional features in the list, they become part of the base client install package.

List of optional features

Optional features have these unique feature IDs in the .xml file.

Table 76. List of optional features

<table>
<thead>
<tr>
<th>Optional feature</th>
<th>Feature ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office features</td>
<td></td>
</tr>
<tr>
<td>Required: Sametime embedded client for Lotus Notes feature (required when you add any Microsoft Office optional features to the installation file for Sametime embedded clients for Lotus Notes)</td>
<td>com.ibm.collaboration.realtime.oi.embedded.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Office</td>
<td>com.ibm.collaboration.realtime.oi.smarttags.feature</td>
</tr>
</tbody>
</table>
### Table 76. List of optional features (continued)

<table>
<thead>
<tr>
<th>Optional feature</th>
<th>Feature ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Outlook calendar availability</td>
<td>com.ibm.collaboration.realtime.exchange.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.toolbar.feature</td>
</tr>
<tr>
<td>Sametime meeting integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.webConfTab.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for SharePoint</td>
<td>com.ibm.collaboration.realtime.oi.sharepoint.feature</td>
</tr>
<tr>
<td>Notes calendar integration</td>
<td>com.ibm.collaboration.realtime.notes.connector.feature</td>
</tr>
</tbody>
</table>

#### Original file with no optional features enabled

The set of optional features is enclosed in comment markers (all of the features are within a single comment):

**Note:** Lines have been formatted here for readability because it is important to make sure you move entire feature statements.

```xml
<feature id="com.ibm.rtc.meetings.embedded.feature"
    version="8.5.0.20091027-1957" match="compatible" download-size="5"
    size="5" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.rtc.meetings.feature" version="8.5.0.20091027-1957"
    match="compatible" download-size="23446" size="23446" action="install"
    shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.rtc.web.utils.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="139"
    size="139" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.collaboration.realtime.sslite.feature"
    version="1.0.0" match="greaterOrEqual" download-size="0" size="0"
    action="uninstall" shared="true"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
</!--

The following Sametime features are optional, and may be uncommented in order to be deployed.

```xml
<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.collaboration.realtime.oi.embedded.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
<feature id="com.ibm.collaboration.realtime.oi.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
```
Modified file with some optional features enabled

The first three optional features have been moved outside of the comment markers and are now enabled for installation:

```
<feature id="com.ibm.rtc.meetings.embedded.feature"
    version="8.5.0.20091027-1957" match="compatible" download-size="5"
    size="5" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.rtc.meetings.feature"
    version="8.5.0.20091027-1957" match="compatible" download-size="23446"
    size="23446" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.rtc.web.utils.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="139"
    size="139" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.collaboration.realtime.sslite.feature"
    version="1.0.0" match="greaterOrEqual" download-size="0"
    size="0" action="uninstall" shared="true"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<!-- These three features have been enabled by moving them outside of the comment: -->
```

```
<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.collaboration.realtime.oi.embedded.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<!-- The following Sametime features are optional, and may be uncommented in order to be deployed.
```

```
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.collaboration.realtime.oi.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
    size="4302" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<feature id="com.ibm.collaboration.realtime.oi.webConfTab.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3048"
    size="3048" action="install" shared="true" mergeaction="add"
    url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```

```
<!--
```

Editing the install.xml file for use on the Sametime Welcome page:

To make optional features available, you can customize the install.xml file for IBM Sametime Connect clients on Mac or Windows operating systems.
About this task

Complete these tasks to create a customized install.xml file and post it for users to download using a link on the Sametime Welcome page:

Editing the client install package on the network:

You can customize the Sametime Connect client installation package for Mac and Windows clients.

Editing the Mac client install package on the network:

You can customize the Sametime Connect client installation package for Mac clients.

About this task

Follow these steps to customize the install.xml file on the network.

1. Locate the Mac installer tar file and untar it:
   - Windows server
     C:\Program Files\lotus\domino\data\domino<html\sametime\network-install\install.mac\sametime.internal.macosx_build.tar
   - AIX, Linux, or Solaris servers
     /local/notesdata/domino/html/sametime/network-install/instal1.mac/sametime.internal.macosx_build.tar
   - IBM i server
     /STserver/domino/html/sametime/network-install/instal1.mac/sametime.internal.macosx_build.tar

2. Open the install.xml file in the directory where you untarred the installation package:
   `untar_directory/sametime-connect.mpkg/Contents/deploy/install.xml`

3. Edit the install.xml to uncomment any optional features you wish to include in the install.
   Optional features are commented out like this:
   ```xml
   <!--
            This is the beginning of a comment marker
   
   The following characters mark the end of the comment: -->
   
   Everything between the markers is ignored as a comment. To enable a feature, either copy it and place it outside of the commented section, or move the comment markers as needed to exclude the feature from the commented section.
   
   4. If you created a custom plugin, add the custom features to install.
   5. Save and close the file.
   6. Tar the customized Mac installation package and replace the existing one with the customized one.

Editing the Windows client install package on the network:

You can customize the Sametime Connect client installation package for Microsoft Windows clients.
About this task

Follow these steps to customize the install.xml file on the network.

1. Open the install.xml file in the network-install directory on the Sametime server:
   - Windows server: C:\Program Files\lotus\domino\data\domino\html\sametime\network-install\install\deploy\install.xml
   - AIX, Linux, or Solaris servers:
     /local/notesdata/domino/html/sametime/network-install/install/deploy/install.xml
   - IBM i server
     There is no default data directory but the name may be similar to this:
     /STserver/domino/html/sametime/network-install/install/deploy/install.xml

2. Edit the install.xml to uncomment any optional features you wish to include in the install.
   Optional features are commented out like this:
   <!-- This is the beginning of a comment marker
   The following characters mark the end of the comment: -->
   Everything between the markers is ignored as a comment. To enable a feature, either copy it and place it outside of the commented section, or move the comment markers as needed to exclude the feature from the commented section.

3. If you created a custom plugin, add the custom features to install.
4. Save and close the file.

Example: Customized install.xml file for the Sametime Connect client (network install):

The install.xml is the installation manifest, which lists all features shipped with IBM Sametime Connect. When you uncomment the optional features in the list, they become part of the base client install package. You can edit the install.xml file for installations from a CD, a downloadable image, or from a link on the Sametime Welcome page.

List of optional features

Optional features have these unique feature IDs in the .xml file.

<table>
<thead>
<tr>
<th>Optional feature</th>
<th>Feature ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office features</td>
<td></td>
</tr>
<tr>
<td>Required: Sametime Connect client feature (required when you add any Microsoft Office optional features to the installation file for Sametime Connect clients)</td>
<td>com.ibm.collision.realtime.oii.standalone.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Office</td>
<td>com.ibm.collision.realtime.oii.smarttags.feature</td>
</tr>
<tr>
<td>Microsoft Outlook calendar availability</td>
<td>com.ibm.collision.realtime.exchange.feature</td>
</tr>
</tbody>
</table>
### Table 77. List of optional features (continued)

<table>
<thead>
<tr>
<th>Optional feature</th>
<th>Feature ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Connect integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.toolbar.feature</td>
</tr>
<tr>
<td>Sametime meeting integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oi.webConfTab.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for SharePoint</td>
<td>com.ibm.collaboration.realtime.oi.sharepoint.feature</td>
</tr>
<tr>
<td>Notes calendar integration</td>
<td>com.ibm.collaboration.realtime.notes.connector.feature</td>
</tr>
</tbody>
</table>

**Notes calendar integration**

**Required:** Sametime Connect client feature (required when you add the Notes calendar integration optional feature to the installation file for Sametime Connect clients)

| Sametime availability status updates based on person’s Lotus Notes calendar entries | com.ibm.collaboration.realtime.notes.connector.standalone.feature |

### Original file with no optional features enabled

This example shows the default settings, in which six Microsoft Office Integration features and two other optional features are commented out. The commented section begins with `<!-- and ends with -->`

**Note:** The lines below have been formatted for readability because it is important to move entire feature statements.

`<!--
The following Sametime features are optional, and may be uncommented in order to be deployed.
<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.notes.connector.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="123"
    size="123" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.notes.connector.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
    size="4302" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.webConfTab.feature">

Chapter 11. Installing 565
Modified file with some optional features enabled

Now the Microsoft Office Integration features have been moved outside of the comment, so they will install automatically. The remaining optional features are still commented out and will not be installed.

<feature id="com.ibm.collaboration.realtime.exchange.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
    size="4302" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oi.webConfTab.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3048"
    size="3048" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>

<!--
The following Sametime features are optional, and may be uncommented
in order to be deployed.
<feature id="com.ibm.collaboration.realtime.notes.connector.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="123"
    size="123" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.notes.connector.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
-->

Making the client installation package available from the Sametime Welcome page:

Perform the following steps to make the network client installer available for installation from the Sametime Welcome page. If the Domino HTTP server has been configured to use SSL with a self-signed test certificate, users will not be able to download the zip from the Sametime Welcome page.

Before you begin

To customize the installation package before making it available to users, edit the install.xml, install.addon.xml, or plugin_customization.ini files to be specific to your site.
Procedure

1. Copy the entire contents of the network-install directory from the Sametime Connect Network Install Client CD or downloaded image to the following location on the Sametime Community Server.

server_data_directory\domino\html\sametime\network-install

Note: There are placeholder files in the directory; you must replace them with the real ones.

These are the default locations for the network-install directory:

Windows
c:\program files\lotus\domino\data\domino\html\sametime\network-install

AIX, Linux, and Solaris
/local/notesdata/domino/html/sametime/network-install

IBM i
There is no default data directory but the name may be similar to this:
/STserver/domino/html/sametime/network-install

2. Update the installer URL information.
   a. Open the \domino\html\sametime\network-install\applet\download.properties file in a text editor.
   b. Set the value of the installer.root.base property to match the correct URL for the network-install directory on your Sametime server.
      For example, if your Sametime server host name is stserver.com:
      installer.root.base=http://stserver.com/sametime/network-install
   c. Save your changes.

3. Use the ArchiveCreator tool to generate the installer archive zips for each platform.
   These zip files only include the base installer with the Expeditor/Eclipse platform and the install manifest which can be customized for your environment. This allows the user to download the zip file, extract it, and run the installer, which provisions the Sametime features from the update site included with the network-install directory.

Windows
a. Open a console window to the \domino\html\sametime\network-install\bin directory
b. Run the ArchiveCreator tool (ArchiveCreator.bat).

AIX, Linux, and Solaris
a. Open a console window to the \domino\html\sametime\network-install\bin directory
b. Run the ArchiveCreator tool (ArchiveCreator.sh).

IBM i
a. Run the following commands:
   QSH
   cd /server_data_directory/domino/html/sametime/network-install/bin
   ArchiveCreator_1505.sh
b. Press F3 to Exit QSH.

Installing Sametime clients

This section gives you information about ways to install the Sametime Connect client and Sametime embedded client for Lotus Notes.
Installing the Sametime Connect client from a CD

Users can install the IBM Sametime Connect client from the standalone client installer CD or corresponding downloaded image.

Installing the Sametime Connect client from CD on Windows:

Users can install the IBM Sametime Connect client from the standalone client installer CD or corresponding downloaded image on a Microsoft Windows client.

Before you begin

If the installation has been customized to install Microsoft Office Integration features, you must ensure that no Office or Outlook processes are running at the time of the install. For more information, see the IBM Tech Note 1307607 at:

www.ibm.com/support/docview.wss?rs=477&uid=swg21307607

About this task

Follow these steps to install the Sametime Connect client on a Windows client.

Procedure

1. If the Sametime Connect client is running, shut it down before attempting to install the newer version.
2. **Important:** Make a back-up copy of the directory where the earlier version of the client is installed, in case you need to revert to it.
3. Navigate to the root of the CD or downloaded image.
4. Double-click `setup.exe` to begin the installation.
   
   If you have previous releases of the Connect client installed:
   
   • Sametime Connect 7.5.x:
     
     The default operation is to uninstall an existing client, but because the 8.5 client installs to a different directory, you can choose to retain the 7.5.x client by running the new installation with a special flag, as follows:
     
     `setup.exe /v"STUNINSTALL75=0"
     
   • Sametime Connect 8.0.x:
     
     The 8.5.x client installs to the same path as the 8.0.x client, you cannot retain the older client when you install the 8.5.x client; the new client will replace the old client.
   
5. Enter the required information when prompted.
6. When the installation completes, launch the Sametime Connect client; by default Sametime Connect is installed to C:\Program Files\IBM\Lotus\Sametime Connect.

Related tasks

“Uninstalling the Sametime Connect client on Windows” on page 602

Uninstall or revert to an earlier version of the IBM Sametime Connect client on Windows.

Preparing to install Sametime Connect clients in silent mode:

You can enable the silent installation of the IBM Sametime Connect Client on Windows using two files that are provided on the client standalone installer CD and the associated downloaded image.
About this task

Copy the setup.bat and the silentinstall.ini files from the root of the CD or download, and then update them to tailor the installer to your requirements.

Updating the setup.bat file

The batch file (setup.bat) contains several different commands that can be used to perform different installation functions. Some of the commands are commented out by default but can be uncommented and updated if the function is needed. Detailed explanations are included in the setup.bat file.

• Uninstalling older, pre-7.5.x Sametime Connect clients

Three commands are provided to shutdown, uninstall, and cleanup an older, pre-7.5.x installation of the Sametime Connect client. These commands are commented-out by default. If this functionality is needed, uncomment these lines and configure the paths to the old Sametime install directory as needed for your environment.

• Several sample commands are provided for different methods of executing the silent install.

– The first option executes the installer silently and uses a silentinstall.ini file to preconfigure connection settings.

  This is the default. If you choose to use one of the other methods, comment out this command.

– The second option executes the installer silently and migrates the connection settings from an existing, earlier (pre-7.5) version of Sametime.

  This option does not use the silentinstall.ini file. If you choose to use this method, uncomment this command.

– The third option executes the MSI version of the installer silently, using a silentinstall.ini to preconfigure the connection settings. If you choose to use this method, uncomment this command.

The commands in the setup.bat file contain several configuration parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.log</td>
<td>The name of the log file created by the installer. The file is created in the same directory as the installer.</td>
</tr>
<tr>
<td>INSTALLDIR=[path]</td>
<td>Full path to the desired installation directory</td>
</tr>
<tr>
<td>STSILENTINIFILE=[name]</td>
<td>Name of the silentinstall.ini file</td>
</tr>
<tr>
<td>STSILENTINSTALL=TRUE</td>
<td>Must be TRUE for silent execution</td>
</tr>
<tr>
<td>STMIGRATESETTINGSPRE75CHK</td>
<td>Instructs the installer to migrate connection settings from an existing pre-7.5 version of Sametime.</td>
</tr>
<tr>
<td>LAPAGREE=</td>
<td>Set to YES to indicate acceptance of the license agreement. This must be specified on the command-line when the silentinstall.ini file is not used. When silentinstall.ini is used, LAPAGREE is set in that file.</td>
</tr>
</tbody>
</table>

Updating the silentinstall.ini file
The `silentinstall.ini` file contains configuration parameters for the Sametime Connect client. The settings are used to pre-populate the `community-config.xml` file with server connection information and other parameters required by the installer for silent execution.

Table 79. `silentinstall.ini` file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAPAGREE=NO</td>
<td>You must change this parameter to YES to indicate acceptance of the license agreement.</td>
</tr>
<tr>
<td>CREATECOMMUNITYTEMPLATE=true</td>
<td>When set to true, this parameter creates a <code>community-config.xml</code> file. If you use a custom <code>plugin_customization.ini</code> file to set initial preferences that are unique to your site or to add custom features, you must change this value to false. Otherwise, after installation, the client starts up without using the custom values defined in the <code>plugin_customization.ini</code> file.</td>
</tr>
<tr>
<td>STSERVERNAME=stservername.domain.com</td>
<td>Fully qualified host name of the Sametime community server. Normally this should be the same as the home Sametime server specified in the person document.</td>
</tr>
<tr>
<td>STCOMMUNITYNAME=YourCommunityName</td>
<td>Community name</td>
</tr>
<tr>
<td>STSERVERPORT=1533</td>
<td>Sametime community server IP Port number</td>
</tr>
<tr>
<td>STSENDKEEPALIVE=true</td>
<td>Flag for sending keep alive signal.</td>
</tr>
<tr>
<td>STKEEPALIVETIME=60</td>
<td>Default is 60 seconds. Indicates how often to check the connectivity between the client and server, allowing timely notification if disconnected.</td>
</tr>
<tr>
<td>STCONNECTIONTYPE75=direct</td>
<td>Connection type</td>
</tr>
<tr>
<td>STPROXYHOST=Proxy port number (leave blank if not used)</td>
<td>Proxy host name (leave blank if not used)</td>
</tr>
<tr>
<td>STPROXYPORT=</td>
<td>Proxy port number (leave blank if not used)</td>
</tr>
<tr>
<td>STRESOLVELOCALY75=</td>
<td>Proxy resolves local flag (TRUE/FALSE)</td>
</tr>
<tr>
<td>STPROXYUSERNAME=</td>
<td>Proxy user name (leave blank if not used)</td>
</tr>
<tr>
<td>STPROXYPASSWORD=</td>
<td>Proxy password (leave blank if not used)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>STCOUNTRYLANG=en</td>
<td>Specify one of the Language codes listed below to set the language used by the Sametime Connect client. If not specified, the client machine's default language will be used.</td>
</tr>
<tr>
<td></td>
<td>• cs - Czech</td>
</tr>
<tr>
<td></td>
<td>• da - Danish</td>
</tr>
<tr>
<td></td>
<td>• de - German</td>
</tr>
<tr>
<td></td>
<td>• el - Greek</td>
</tr>
<tr>
<td></td>
<td>• en - English</td>
</tr>
<tr>
<td></td>
<td>• es - Spanish</td>
</tr>
<tr>
<td></td>
<td>• fi - Finnish</td>
</tr>
<tr>
<td></td>
<td>• fr - French</td>
</tr>
<tr>
<td></td>
<td>• hu - Hungarian</td>
</tr>
<tr>
<td></td>
<td>• it - Italian</td>
</tr>
<tr>
<td></td>
<td>• ja - Japanese</td>
</tr>
<tr>
<td></td>
<td>• ko - Korean</td>
</tr>
<tr>
<td></td>
<td>• nl - Dutch</td>
</tr>
<tr>
<td></td>
<td>• no - Norwegian</td>
</tr>
<tr>
<td></td>
<td>• pl - Polish</td>
</tr>
<tr>
<td></td>
<td>• pt - Portuguese (Portugal)</td>
</tr>
<tr>
<td></td>
<td>• pt_BR - Portuguese (Brazil)</td>
</tr>
<tr>
<td></td>
<td>• ru - Russian</td>
</tr>
<tr>
<td></td>
<td>• sv - Swedish</td>
</tr>
<tr>
<td></td>
<td>• tr - Turkish</td>
</tr>
<tr>
<td></td>
<td>• zh_CN - Chinese (simplified)</td>
</tr>
<tr>
<td></td>
<td>• zh_TW - Chinese (traditional)</td>
</tr>
<tr>
<td>STAUTHSERVERURL=</td>
<td>Specifies the URL of the Auth Server for SSO Token Login (leave blank if not used)</td>
</tr>
<tr>
<td></td>
<td>See Configuring single sign-on with Microsoft Windows Active Directory for additional information.</td>
</tr>
<tr>
<td>STLOGINBYTOKEN=false</td>
<td>Login By Token flag. TRUE/FALSE</td>
</tr>
<tr>
<td>STUSEAUTHSERVER=false</td>
<td>Use Auth Server flag. TRUE/FALSE</td>
</tr>
<tr>
<td>STLOGINATSTARTUP=false</td>
<td>Login at startup flag. TRUE/FALSE</td>
</tr>
<tr>
<td>STUNINSTALL75=1</td>
<td>Uninstall Sametime 7.5.x client flag:</td>
</tr>
<tr>
<td></td>
<td>1=uninstall 7.5.x client if found</td>
</tr>
<tr>
<td></td>
<td>0=leave 7.5.x client installed</td>
</tr>
<tr>
<td>STUNINSTALLPRE75=1</td>
<td>Uninstall Sametime clients older than release 7.5:</td>
</tr>
<tr>
<td></td>
<td>1=uninstall pre-7.5 client if found (default)</td>
</tr>
<tr>
<td></td>
<td>0=leave pre-7.5 client installed</td>
</tr>
</tbody>
</table>
Related tasks
“Editing the plugin_customization.ini file to add custom features and change default preferences” on page 554
You can customize the plugin_customization.ini file to add features from a custom plugin or to change the default installed preferences.

Installing the Sametime Connect client from CD on RHEL or SLED:

Users can install the IBM Sametime Connect client from the client CD or downloaded image on a Red Hat Enterprise Linux Desktop (RLED) or SUSE Linux Enterprise Desktop (SLED) client.

Before you begin

If you are upgrading from release 8.0, the rpm upgrade command (-U) removes the 8.0 version of the client automatically; there is no option to retain the 8.0 version of the features.

About this task

To install the Sametime Connect client on a Linux client, perform the following steps:

Procedure
1. Log in to the workstation as the root user.
2. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
3. Red Hat Enterprise Linux only: Install the compat runtime library by running the following command:
   • Red Hat Enterprise Linux 5.x
     rpm -ivh compat-libstdc++-33-3.2.3-61.i386.rpm

   Note: There may be a later release of the compat library for your release.
4. Navigate to the Linux directory containing the install package.
5. Run the following install program:
   • Install:
     rpm -i sametime-connect-8.5.2-timestamp.i586.rpm
   • Upgrade:
     rpm -u sametime-connect-8.5.2-timestamp.i586.rpm
6. Launch the Sametime Connect client using the “Sametime Connect” desktop launcher in the Office category.
   Alternatively, use the following command:
   /usr/bin/sametime-connect
Related tasks
“Uninstalling the Sametime Connect client on Linux” on page 602
Uninstall or revert to an earlier version of the IBM Sametime Connect client on Linux.

Installing the Sametime Connect client from CD on Ubuntu:

Users can install the IBM Sametime Connect client from the client CD or downloaded image on an Ubuntu client.

About this task

To install the Sametime Connect client on an Ubuntu client, perform the following steps:

Procedure
1. Log in with the user account.
2. Navigate to the Linux directory containing the install package.
3. Double-click the following program to install the client:
   `sametime-connect-8.5.2.timestamp.i386.deb`
4. Launch the Sametime Connect client using the "Sametime Connect" desktop launcher in the Office category.
   Alternatively, use the following command:
   `/usr/bin/sametime-connect`

Related tasks
“Uninstalling the Sametime Connect client on Linux” on page 602
Uninstall or revert to an earlier version of the IBM Sametime Connect client on Linux.

Installing the Sametime Connect client from CD on Mac OS X:

Users can install the IBM Sametime Connect client from the client CD or downloaded image on a Mac OS X client.

About this task

To install the Sametime Connect client on a Mac OS X client, perform the following:

Procedure
1. If an earlier version of the Sametime Connect client is installed, exit it and drag it to the Trash before installing the newer version.
2. Navigate to the MacOSX directory on the client CD or downloaded image.
3. Double-click `sametime-connect.mpkg` to begin the installation.
   By default the connect client will be installed to the Applications folder on Mac HD.
4. Enter the required information when prompted.
5. When the installation completes, launch Sametime Connect by double-clicking on Sametime.
Related tasks
“Uninstalling the Sametime Connect client on the Macintosh” on page 603
Uninstall or revert to an earlier version of the IBM Sametime Connect client on the Macintosh.

Installing the Sametime Connect client from the network
Providing installation files on the network allows users to download the Sametime Connect Client without CDs or download images.

Installing the Sametime Connect client from the network on Windows:
When network installation files are available, users can install Sametime Connect from a web browser on Windows.

Procedure
1. (Optional) Set default preferences in the plugin_customization.ini file located in the \network-install\install.win\deploy directory.
2. Using a web browser, open the Sametime Welcome page on your Sametime server.
   For example, if the fully qualified host name of your Sametime server is stserver.example.com, you open http://stserver.example.com/stcenter.nsf.
3. Click Download Sametime Connect 8.5.2 Client to display the "Welcome to the IBM Sametime Connect 8.5.2 Client Download Site" page.
4. Click Install Now to begin the download and installation process.
   Once all files have been downloaded, the actual client installer will start.
   Follow the instructions in the installer and enter the required information to complete the installation.

   Tip: If there are problems running the network client installer applet, or if you want to install at a later time, you can select Save from the Welcome page instead. This shows you a downloads page where you can select the operating system of the installer you wish to save and follow the instructions for downloading the installer for later use.

Related tasks
“Uninstalling the Sametime Connect client on Windows” on page 602
Uninstall or revert to an earlier version of the IBM Sametime Connect client on Windows.

Installing the Sametime Connect client from the network on RHEL and SLED:
When network installation files are available, users can install IBM Sametime Connect from a web browser on a Red Hat Enterprise Linux Desktop (RLED) or SUSE Linux Enterprise Desktop (SLED) client.

About this task
To install the Sametime Connect client on a Red Hat Enterprise Linux Desktop (RLED) or SUSE Linux Enterprise Desktop (SLED) client perform the following steps:

Procedure
1. If you share a computer and another user already installed the Sametime Connect client, remove temporary files left by the previous installation:
a. Log on the computer as the root user.

b. Run the following command to remove the temporary files:
   
   ```bash
   rm -rf /tmp/deploy /tmp/sametime-connect-*.rpm /tmp/install.sh
   ```

2. Install the compat runtime library by running the following command:

   **RHEL 5.x**
   
   ```bash
   rpm -ivh compat-libstdc++-33-3.2.3-61.i386.rpm
   ```

   **Note:** There may be a later release of the compat library for your release.

3. Using a web browser, open the Sametime Welcome page on your Sametime server.

   For example, if the fully qualified host name of your Sametime server is `stserver.example.com`, you open `http://stserver.example.com/stcenter.nsf`.

4. Click **Download Sametime Connect 8.5.2 Client** to display the "Welcome to the IBM Sametime Connect 8.5.2 Client Download Site" page.

5. Click **Install Now** to begin the download and installation process.

   Once all files have been downloaded, the actual client installer will start and runs automatically.

   **Tip:** If there are problems running the network client installer applet, or if you want to install at a later time, you can select **Save** from the Welcome page instead. This shows you a downloads page where you can select the operating system of the installer you wish to save and follow the instructions for downloading the installer for later use.

**Related tasks**

“Uninstalling the Sametime Connect client on Linux” on page 602

Uninstall or revert to an earlier version of the IBM Sametime Connect client on Linux.

**Installing the Sametime Connect client from the network on Mac OS X:**

When network installation files are available, users can install Sametime Connect from a web browser on a Mac OS X client.

**Procedure**

1. If you share a computer and another user already installed the Connect client, remove temporary files left by the previous installation:
   a. Log on the computer as the root user.
   b. Run the following command to remove the temporary files:
      
      ```bash
      rm -rf /tmp/deploy /tmp/sametime-connect.mpkg.zip /tmp/setupmac.sh
      ```

2. Using a web browser, open the Sametime Welcome page on your Sametime server.

   For example, if the fully qualified host name of your Sametime server is `stserver.example.com`, you open `http://stserver.example.com/stcenter.nsf`.

3. Click **Download Sametime Connect 8.5.2 Client** to display the "Welcome to the IBM Sametime Connect 8.5.2 Client Download Site" page.

4. Click **Install Now** to begin the download and installation process.

   Once all files have been downloaded, the actual client installer will start. Follow the instructions in the installer and enter the required information to complete the installation.
Tip: If there are problems running the network client installer applet, or if you want to install at a later time, you can select **Save** from the Welcome page instead. This shows you a downloads page where you can select the operating system of the installer you wish to save and follow the instructions for downloading the installer for later use.

**Related tasks**

“Uninstalling the Sametime Connect client on the Macintosh” on page 603

Uninstall or revert to an earlier version of the IBM Sametime Connect client on the Macintosh.

**Installing the Sametime embedded client for Lotus Notes**

Install the IBM Sametime embedded client to a Lotus Notes client.

**Before you begin**

Verify the version of Lotus Notes that supports the embedded client you are deploying by reviewing the System Requirements at the following web address:

&uid=swg27019598

**Installing the embedded client on Windows:**

Install the IBM Sametime embedded clients on a Lotus Notes client running on Microsoft Windows.

**Before you begin**

You must install Lotus Notes 8.5.1 FP2 or later to use the embedded client. Lotus Notes 8.5.1 FP4 or later is recommended.

**About this task**

The Sametime embedded client installs directly into the Lotus Notes directory. If you have already installed a previous version of the embedded client, it is upgraded to this new version.

**Procedure**

1. Download the installation package for the Sametime embedded client if you have not already done so.
   
a. To download installation packages:
      
1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address:
   
&uid=swg24029128

Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows...
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

2. Stop the Lotus Notes client.

3. Double-click the `setup.exe` file to begin installation:
   a. Select a language and click **Next**.
   b. Click **Next** as needed to proceed through the installation screen.

4. Verify the installation:
   a. **Help > About IBM Lotus Notes**
   b. Click **Feature Details**.
   c. Verify that "Sametime Application" appears in the list of features with "8.5.2" at the beginning of its version information.
   d. Close the dialog box.

Related tasks

“Uninstalling the Sametime client embedded in Notes on Windows” on page 603

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client on Windows.

**Installing the embedded client on RHEL and SLED:**

Install the IBM Sametime embedded clients on a Lotus Notes client running on Red Hat Enterprise Linux Desktop (RLED) or SUSE Linux Enterprise Desktop (SLED).

**Before you begin**

You must install Lotus Notes 8.5.1 FP4 or later to use the embedded client.

You must uninstall Sametime if it is already installed.

```
rpm -e ibm_lotus_sametime
```

**Attention:** If you do not uninstall Sametime first, you can still upgrade Sametime to the new version, but if you subsequently upgrade to the Notes version, it fails. If you uninstall Sametime at this point, the uninstall is successful and the upgrade to Notes 8.5.2 is also successful, but Notes fails to start.
About this task

To install the Sametime embedded client on Red Hat Enterprise Linux Desktop (RLED) or SUSE Linux Enterprise Desktop (SLED), perform the following steps:

Procedure
1. Log in as root.
2. Download and extract the installation program:
   a. Download the file called SametimeEmbeddedClient.zip to the client workstation.
   b. Extract the following two files to a temporary location on the client workstation:
      • sametime-connect-embedded-8.5.2-timestamp.i586.rpm
      • sametime-connect-embedded-core-8.5.2-timestamp.i586.rpm
3. Stop the Lotus Notes client.
4. Double-click the following file to install the client program:
   sametime-connect-embedded-8.5.2-timestamp.i586.rpm

Related tasks
“Uninstalling the Sametime client embedded in Notes on Linux” on page 603
Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client.

Installing the embedded client on Ubuntu:

Install the IBM Sametime embedded clients on a Lotus Notes client running on Ubuntu.

Before you begin

You must install Lotus Notes 8.5.1 FP4 or later to use the embedded client.

About this task

To install the Sametime embedded client on Ubuntu, perform the following steps:

Procedure
1. Log in with the user account.
2. Download and extract the installation program:
   a. Download the file called SametimeEmbeddedClient.zip to the client workstation.
   b. Extract the following two files to a temporary location on the client workstation:
      • sametime-connect-embedded-8.5.2-timestamp.i386.deb
      • sametime-connect-embedded-core-8.5.2-timestamp.i386.deb
3. Stop the Lotus Notes client.
4. Double-click the following file to install the client program:
   sametime-connect-embedded-8.5.2-timestamp.i386.deb
Related tasks
“Uninstalling the Sametime client embedded in Notes on Ubuntu” on page 604
Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client.

Installing the embedded client on Mac:

Install the IBM Sametime embedded clients on a Lotus Notes client running on a Mac.

Before you begin

You must install Lotus Notes 8.5.1 FP4 or later to use the embedded client.

About this task

The Sametime embedded client installs directly into the Lotus Notes directory. If you have already installed a previous version of the embedded client, it is upgraded to this new version.

Procedure

1. Unpack `sametime.embedded.add-on.mac.XXXXXXXX-XXXX.zip` by right-clicking it and then selecting **Open with Archive Utility**.
2. Double-click on `sametime-embedded-addon.pkg` and follow the install wizard.

Related tasks

“Uninstalling the Sametime client embedded in Notes on Mac” on page 604
Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client on the Mac.

Enabling client features after installation

Depending on the licenses purchased for your site, the IBM Sametime Connect client or Sametime client embedded in Notes may be licensed to receive additional features. This section gives you information about ways to roll out those features to clients.

Installing Sametime Integration for Microsoft Office

IBM Sametime integration with Microsoft Office allows you to collaborate, create meetings, and chat with coworkers through Microsoft Office applications. Sametime integration with the Microsoft Office SharePoint Server allows similar collaboration features with coworkers who use Office SharePoint Server as their instant messaging application.

About this task

You can integrate Sametime with Microsoft Office to enable users to collaborate directly within Office applications. You can additionally integrate Sametime with the Office SharePoint Server to enable Sametime users to communicate with Office SharePoint Server users from a SharePoint site.

Office Integration

Integrating Sametime with Microsoft Office allows Sametime users to collaborate directly within Office products by providing awareness and messaging capabilities within each application. All users must be hosted on Sametime servers.
Clients can receive updates and patches if you set up an add-on site or give them instructions to install updates manually. You cannot use an update site with the Sametime update site URL policy for Instant Messaging to distribute updates for Office Integration.

**Requirements**

Sametime Office Integration features require the following applications:

- Microsoft Windows version XP, Vista, or Microsoft Windows 7

**Limitations**

- Office Integration does not support multiple users running Office Integration on a single machine simultaneously. In particular, Citrix environments are not supported.
- The Sametime Meeting integrator for Microsoft Outlook does not support delegation of access to the Outlook calendar (in that scenario, a user cannot delegate access to a coworker, for example).

**Upgrading the client does not automatically upgrade optional features**

If you do not upgrade them (by uncommenting them in the 8.5.2 manifest) or remove them (by uncommenting them and setting action="uninstall" in the 8.5.2 manifest) then they will be carried forward like any feature should be.

**Upgrading from Office Integration 7.5.1**

If you plan to upgrade from Office Integration 7.5.1, either skip uninstalling the older product during the upgrade or uninstall it first before installing Office Integration 8.5.2. If you do not follow one of these precautions, a defect of the 7.5.1 uninstaller causes Office SmartTags to be disabled. The problem will not happen if 7.5.1 is not uninstalled. The problem will only happen for the user installing the client (the administrator). Other users on the same machine will not be affected.

Follow these steps to re-enable the SmartTags if you have already encountered the problem:

1. In Windows Explorer, navigate to the following directory:
   
   \Sametime_connect_install_directory\shared\eclipse\plugins\com.ibm.collaboration.realtime.oi.smarttagsFiles_8.5.2.yyyymmdd_hhmm\.
   
2. Double-click this file:
   
   EnableOiSmartTags.reg

**Office SharePoint Server integration**

Integrating Sametime with Microsoft Office SharePoint Server extends collaboration capabilities by providing awareness and instant messaging among users whose names appear on a SharePoint site. Any Office SharePoint Server user's live name that can be resolved using the standard email address field will be recognized and will display its presence status to a user who is logged into Sametime. Clicking on an active SharePoint user displays a contextual Sametime menu. During a chat, the Sametime user is presented with the complete feature set of Sametime and its third-party plug ins, including emoticons, file sharing, image captures, multi-way chats, audio, video, telephony, screen sharing, and chat history.
Integration with Office SharePoint Server is achieved using documented interfaces from Microsoft Corporation. Deploying this feature requires modifying two template files on the Office SharePoint Server. In addition, Sametime Connect users will need to upgrade their installed client software.

Requirements

Sametime integration with the Microsoft Office SharePoint Server requires the following applications:

- Microsoft Internet Explorer browser, version 6 or higher
- Microsoft Office SharePoint Services version 2 or version 3, Microsoft Office SharePoint Portal Server 2003, or Microsoft Office SharePoint Server 2007 or 2010
- Sametime 8.5.2 client with the Sametime Connect Integrator for Microsoft Office
- Sametime server, release 8.5.2 or later

The Office SharePoint feature requires only a Sametime client; other Office Integration features need not be installed at all, or may be present in any combination. Complete the tasks below according to the features you wish to install. The client installation files or update site also need to be enabled to include the Office Integration features.

Related tasks

“Enabling installation of optional client features such as Microsoft Office Integration” on page 551
IBM Sametime ships with a number of optional client features that are not included in the default installation package. You can add features to the installation package for new client installs and update already-installed clients by updating the installation manifest file.
“Distributing updates and optional features to clients” on page 598
Set up updates site to distribute updates and optional features to clients.

Installing Office Integration:

IBM Sametime with Microsoft Office allows you to collaborate, create meetings, and chat with co-workers from Microsoft Office.

Before you begin

To install Office Integration, complete the following tasks first.

- Install Sametime servers.
- Install Microsoft Office.
- Install or upgrade Sametime Connect clients, including the Office Integration features they must have.

Microsoft Windows Vista and Windows 7 clients must run the installation program as an administrator and, when prompted, consent to run the program with elevated privileges. This allows proper creation of new application icons on the Windows Desktop or in the Windows Start Menu and proper creation of global registry keys. After installation, log on as a regular user, to restore the default security for the client.
About this task

Sametime Integration with Microsoft Office offers the following features:

- Sametime Connect integrator for Microsoft Office
- Microsoft Outlook calendar availability
- Sametime Connect integrator for Microsoft Outlook
- Sametime meeting integrator for Microsoft Outlook
- Sametime Connect integrator for SharePoint

**Note:** When you install Office Integration, you may have to close Office, Outlook, or Internet Explorer processes. The installer will notify you if those applications are running and need to be closed.

Installing the Office Integration features

Perform these steps after you have installed or upgraded the Sametime clients and enabled the Office Integration optional features the clients must have.

Enabling SmartTags

The Sametime Office Integration feature set adds the SmartTag recognizer which will start on either the names from the user's local buddy list or from internet-style email addresses, for example "jdoe@example.com".

**Note:** These are in addition to the Sametime menu items contributed to Person Name (English) from Sametime 7.5.1.

- To enable SmartTags, select the Person (Sametime Recognizer) entry from the AutoCorrect SmartTag dialog.
- The use of automatic hyperlinks in Office documents will interfere with the new SmartTag's ability to recognize email addresses -- you can regain the SmartTag function by disabling hyperlinks: Clear the "Internet and network paths with hyperlinks" option in "AutoFormat As You Type" tab from the Tools->Auto-Correct Options menu.

Known issues

- The Meeting Integrator feature can support Sametime meeting servers that require SSL by modifying the syntax of the server name specified in the Sametime Meeting properties: if SSL is required, include the protocol portion of the server URL, for example "https://sametime.mycompany.com". The syntax shown in the dialog example, "sametime.mycompany.com", is correct for servers that are accessible by ordinary, non-SSL http.
- If the default email fields read by the Outlook Toolbar are not the appropriate fields for a customer's enterprise, the Toolbar can be redirected to use other fields instead by modifying the file CustomProperties.ini in the Sametime install folder. The intent is that such modifications would be made by IT experts and the ini file (text) be distributed to users. If this optional file is not present, Toolbar uses its default field settings.

Limitations

- The local Outlook user email address must be resolvable in Sametime for the MyStatus button to properly display status.
- The Meeting Integrator feature is not included in a meeting request that begins from Outlook's "Plan A Meeting" dialog.
In a meeting which includes a Sametime meeting, if the Sametime meeting password is changed after the initial invitation is sent, then the message body will show more than one password -- the most recent password assignment is displayed last.

**Third Party Limitations**

- Microsoft Outlook will cache and retain forms despite the uninstall if the form is designated to be used.
  
  To fully uninstall and eliminate the ST OnlineMeeting, ST OnlineMeetingRTL, and STContact custom forms, the user must be sure to set Calendar and Contact "When posting..." properties back to IPM.Appointment and IPM.Contact respectively.

- Microsoft Outlook permits multiple user profiles but is designed to operate under one profile at a time, which must be selected at Outlook’s launch. Some Sametime features must keep the Outlook process running for their operation, which has implications when a user wants to select or switch profiles.
  
  Outlook can be configured to always use one default profile, or to prompt at start-up; if you later want to use Outlook with a different profile, you must exit Outlook, launch it again, and then select the new profile.

- If the Sametime client has been configured to use Outlook for either the Calendar AutoStatus feature or as the storage location for Chat History, and Outlook is not already running, Sametime will silently launch Outlook to access those features, and then keep it running as a background process with no user interface. If the user has multiple profiles with no default selected and Sametime executes this silent launch, a "Use Profile" dialog box will be provided by Outlook and will be used by the background process. When the user later starts Outlook, the profile chosen earlier during the Sametime start-up will automatically be used; if the user wants to change the profile, he or she must exit both Outlook and the Sametime client (which in turn stops the Outlook process running in the background).

**Installing the Meeting Integrator:**

IBM Sametime Meeting Integrator allows you to use the Calendar feature within Microsoft Office even though you do not have the Sametime Client installed.

**About this task**

**Note:** When you install Office Integration, you do not need to close Microsoft Outlook, but the Meeting Integrator becomes available only after you restart Outlook.

To install IBM Sametime Meeting Integrator (sametime-outlook-integrator-8.5.1.exe), launch the installer and work through the screens from install to license. If you have closed all the Outlook Processes Running during installing, the fix is installed successfully onto Outlook. If you have not closed all the Outlook Processes Running during installing, the fix is installed completely only after you restart Outlook.

**Known issues**

The Meeting Integrator feature can support Sametime meeting servers that require SSL by modifying the syntax of the server name specified in the Sametime Meeting properties: if SSL is required, include the protocol portion of the server URL, for
example "https://sametime.mycompany.com". The syntax shown in the dialog example, "sametime.mycompany.com", is correct for servers that are accessible by ordinary, non-SSL http.

Limitations

The Meeting Integrator feature is not included in a meeting request that begins from Outlook's "Plan A Meeting" dialog. In a meeting which includes a Sametime meeting, if the Sametime meeting password is changed after the initial invitation is sent, then the message body will show more than one password -- the most recent password assignment is displayed last.

The Meeting Integrator does not support delegation of the Outlook calendar access.

Setting up the Meeting Integrator for a secure connection:

Install the SSL certificate on the client to use the Meeting Integrator successfully on Sametime servers running on a secure connection. The Sametime Meeting Server runs on a secure HTTPS connection by default.

About this task

Follow these steps to install the certificate.

Procedure
1. Open Internet Explorer to connect to the Sametime server over HTTPS.
2. At the Security Alert dialog box, click View Certificate.
   - If you do not see a dialog box, double-click the lock icon located in the bottom right corner of the window.
3. The Certificate dialog box shows the certificate properties. Open the Certification Path tab.
   - The root certificate shows a red X because it is not yet trusted.
4. Select the root certificate and click View Certificate.
   - A dialog box shows the properties of the root certificate.
5. Click Install Certificate.
6. When the wizard starts, click Next.
7. On the next screen, select Automatically select the certificate store based on the type of certificate and click Next.
8. Click Finish.
   - At the prompt, click Yes to trust the root certificate.
9. After receiving a confirmation that the certificate was correctly installed, close and reopen Internet Explorer and connect to the Sametime server again.
   - If the certificate was installed properly, the Security Alert no longer appears.

Configuring Microsoft Office integration:

If the Microsoft Office integration does not work properly in your IBM Sametime deployment, you may need to adjust the Sametime server configuration.

Displaying Sametime user names in the Microsoft Outlook toolbar:

The Sametime Integrator for Microsoft Outlook (or "Outlook toolbar") works by asking Sametime to process an identifier phrase – in the case of Microsoft Outlook,
the phrase is an email address. If the server is not configured to resolve the email "phrases" found by the toolbar, the **Target Contact** button is not updated to show the LotusSametime display name and status, but instead continues to show an email address, such as “jsmith@example.com” or “JSMITH” (a CN portion of an X.400 address).

**About this task**

There will always be emails from external parties that will remain unresolved, but you can follow these steps to resolve the email addresses of Sametime users.

**Procedure**

1. Enable logging in the Sametime client.

   As any new email address is encountered, an XML message is sent from the Outlook toolbar to the Sametime client for lookup processing. These messages can be echoed into the client logs. The configuration information for a user is stored in a workspace under the user's Documents and Settings folder, under the path `Documents and Settings\User\Application Data\Lotus\Sametime\.config`. The `rcpinstall.properties` file located here is processed on each launch of the client.

   Open this and add the following line to the end of the file:

   ```
   com.ibm.collaboration.realtime.brokerbridge.level=FINE
   ```

   On all subsequent launches, the XML traffic between the Sametime client and the Office Integration features will be logged to the `trace-log-N.xml` files in the `Application Data\Lotus\Sametime\logs` folder.

   A few tips will simplify using these logs:

   - Focus the troubleshooting effort on just one Office application – so avoid opening other Office applications or SharePoint pages, because their message traffic will overlap the Outlook messages and make the logs larger.
   - The Sametime client usually needs to be exited to complete the writing of the logs – the easiest approach is to start Sametime, click a few problem emails, then exit the client and examine the logs.
   - The logs are designed to be opened in a browser from the `Application Data\Lotus\Sametime\logs` folder, which contains formatting files to create tables of output.

2. Find the resolution request.

   Once the trace log is opened, use the browser's function to search for text in the page and search for the phrase “liveNameResolve”. This XML message is the type used by Outlook toolbar to request resolutions – because email addresses map uniquely to one person, the toolbar is using the lookup service which returns only unique matches. Once the table row containing a liveNameResolve is found, the target phrase is located in the lookupName section – this in turn is an array of one or more phrases, in stringArray\data nodes. As a concrete example, an email within the STOIDEV enterprise from user John Doe might cause a liveNameResolve like this one:

   ```
   <messageSet version="1.0" encoding="utf-8" ?>
   <messageSet version="1.0" signed="false">
   <liveNameResolve typeVersion="1.0">
   <lookupNames valueType="stringArray"><stringArray length="1">
   <data><![CDATA[CN=John Doe,CN=Users,DC=stoidev,DC=com]]></data>
   </stringArray></lookupNames></liveNameResolve><signature />
   <messageSet>
   ```

   This example has been formatted for this page – it may appear as a single line in the logs. So the email address phrase here is `CN=John Doe,CN=Users,DC=stoidev,DC=com`.  

Chapter 11. Installing 585
Note that in this example (from a real Exchange test set-up) this particular format of the email address is NOT ordinarily displayed to the Outlook user – instead, the user sees “John Doe” or “jdoe@stoidev.com” displayed in Outlook documents and dialogs.

3. Check the phrase.

A quick check for resolution results can be accomplished by starting the Sametime client and clicking Add Contact. Then, paste the phrase from the liveNameRequest (CN=John Doe,CN=Users,DC=stoidev,DC=com in this example) into the User name field of the “New Contact” dialog box, and click Lookup. If the phrase returns a unique result, then the toolbar should likewise get that result and operate fully for that target contact. If there are no results, or if there are multiple results, then the toolbar resolution will not be able to display a Sametime user for that address.

4. Adjust the server configuration.

Both the Sametime client and the Outlook toolbar (working within the Sametime client), rely on the Sametime server to associate a particular phrase with a user. No other communications to directories are in use – if the Sametime server cannot establish the association, the Outlook toolbar can only assume that none exists. However, the Sametime server has great flexibility and can be directed to use any of the directory fields at its disposal when doing this processing.

The field called “Search filter for resolving person names” in the “Searching” settings of the LDAP Directory configuration for the Sametime Community Server dictates the query that is used. Notice that “mail=%s” is a recommended setting, and will be successful when the ID phrase is the SMTP email address “ajones@example.com”. For cases like the example above, the default settings for many Exchange deployments will have this address phrase, in its entirety, within an attribute called “legacyExchangeDN” – so a query term 

“(legacyExchangeDN=%s)” would typically be added as an addition to the “(mail=%s)” and others present in the filter string. Other cases could require inspecting available directory attributes to find a suitable match; for example:

(&objectclass=organizationalPerson)((mail=%s*)(cn=%s*)(legacyExchangeDN=%s)(userPrincipalName=%s*))

In addition, to ensure that the Microsoft Exchange contacts are correctly resolved and authenticated, add the query term (legacyExchangeDN=%s) to the Search filter to use when resolving a user name to a distinguished name field in the Searching settings of the LDAP directory configuration for the Sametime Community Server. For example:

(&objectclass=organizationalPerson)((cn=%s)(givenname=%s)(sn=%s)(mail=%s)(legacyExchangeDN=%s))

One final detail is that the Sametime server, by default, will skip over attribute values that are in LDAP canonical format as a single field, but it offers an override – this override would be required in the legacyExchangeDN case, for example. To establish the override behavior, edit the Sametime server’s sametime.ini configuration file and add this line:

ST_DB_LDAP_ALLOW_SEARCH_ON_DN=1

to the section labeled [Directory]. If there is no such section already, create one by appending the two lines at the end of the sametime.ini file:

[Directory]
ST_DB_LDAP_ALLOW_SEARCH_ON_DN=1

Allowing delegated users to create meetings in Microsoft Outlook:
If you have users in your organization who are delegated to create meetings for other people, you must publish the Sametime custom form for meetings to the server's Organizational Forms Library. When this form is available, delegated users do not encounter the "Object Not Found" message when creating a meeting for someone else.

**Before you begin**

Create an Organizational Forms Library as described on the Microsoft Support site at this URL: [http://support.microsoft.com/kb/933358](http://support.microsoft.com/kb/933358)

**Procedure**

Follow these steps to publish the meetings form and associate it with the person whose meetings are created by someone else.

1. Log in to a client computer that has Microsoft Outlook installed and can use the Administrator profile (for example, Administrator for the Microsoft Exchange Server).
2. Publish the STOnlineMeetings form to the Organizational Forms Library and give it a new name, such as STMeetingForm.
3. Working on the machine of the person who has delegated meeting creation to someone else, remove all the local forms from the cache associated with Calendar, and specify that the custom form you published in the previous step is to be used when posting appointments to the Calendar.

**Results**

When the person delegated to create meetings accesses the delegator’s calendar and creates a new appointment, the custom Sametime meetings form opens as the default form.

**Setting up Office SharePoint integration:**

Integrating IBM Sametime with Microsoft Office SharePoint Server extends collaboration capabilities by providing awareness and instant messaging between Sametime users who are using an Office SharePoint site. System administrators set up this feature by modifying template files on the Microsoft Office SharePoint Server as described below. Users add these new capabilities by using a customized install file to install the optional client feature called “Sametime Connect integrator for SharePoint.”

**About this task**

Complete the tasks below to set up Office SharePoint integration:

**Related tasks**

“Enabling installation of optional client features such as Microsoft Office Integration” on page 551

IBM Sametime ships with a number of optional client features that are not included in the default installation package. You can add features to the installation package for new client installs and update already-installed clients by updating the installation manifest file.

*Setting up the Office SharePoint Server:*
Set up integration with Microsoft Office SharePoint by modifying template files on the Microsoft Office SharePoint Server with which you want IBM Sametime to communicate.

Before you begin

The user plugin called “Sametime Connect integrator for SharePoint” is the client feature that responds to the server modifications described here. That feature can be installed on the client at any time, but it will remain dormant until Internet Explorer views a SharePoint web page from a server that has been modified as described in this topic. Likewise, the web pages from a modified server can be viewed from any client, but the extended functions will only be available on a client that is running Sametime Connect and the integrator for SharePoint plugin.

The Office SharePoint Server integration feature is an optional feature and is not necessary for enabling integration with Office applications. On the client, the Sametime Connect integrator for SharePoint plugin can be installed independently of other Office Integration features.

Note: Microsoft Communicator must not be configured to run against the Office SharePoint Server.

About this task

Setting up the SharePoint integration feature requires copying files to the Office SharePoint Server, using them to modify template files, and then restarting the server, as described below.

The files that you copy to the Office SharePoint Server in this procedure are available with the Sametime package. For details on downloading parts from the kits, see the Sametime Download document at:

www.ibm.com/support/docview.wss?rs=477&uid=swg24017299

Procedure

1. Copy the following files from the Sametime client packages to a temporary location on the Office SharePoint Server:
   These files are stored in the folder called sametimesharepoint:
   • SharePointImages.zip
   • EnsureIMNControl.js
   • Copy the appropriate version of this file for your version of SharePoint:
     – IMNGetStatusImage_SharePoint2003.js
     – IMNGetStatusImage_SharePoint2007.js

2. Open the folder called Common Files\Microsoft Shared\web server extensions\12\TEMPLATE.
   For most machines, the path will be: C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE. You will work in this folder for the remaining steps.

3. Extract the contents of the SharePointImages.zip file to the IMAGES subfolder.
   For example: C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\IMAGES.

4. Now open the folder called Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\LAYOUTS\Language_ID.
For example, an English installation will have the Language_ID 1033, and the path will be: C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\LAYOUTS\1033.

5. Make backup copies of the Init.js and OWS.js template files.

In each of these files, you will replace two functions with newer versions that support integration with Sametime, and modify two other functions to correctly support the presence icon.

6. Replace the EnsureIMNControl function in the Init.js file as follows:
   a. Open the Init.js file for editing.
   b. Open the EnsureIMNControl.js file that you copied to the server back in step 1.
   c. Copy the EnsureIMNControl function from this file (leave the file open for now).
   d. Back in the Init.js file, search for its own version of the EnsureIMNControl function, delete that, and paste the newer version in its place.

7. Now replace the IMNGetStatusImage function in the same manner:
   a. Open the IMNGetStatusImage200x.js file that you also copied in step 1.
   b. Copy the IMNGetStatusImage function from this file (you can also leave this file open for now).
   c. Back in the Init.js, search for its own version of the IMNGetStatusImage function, delete that, and paste the newer version in its place.

8. Make two changes to the IMNRC(name, elem) function within the Init.js file as follows:
   a. Locate the function called IMNRC(name, elem).
   b. Locate the following statement (approximately 30 lines into the function):
      ```
      if (typeof(IMNDictionaryObj[id])=='undefined')
      ```
   c. Change the assignment from IMNDictionaryObj[id]=1 to IMNDictionaryObj[id]=0 so the "if" statement looks like this:
      ```
      if (typeof(IMNDictionaryObj[id])=='undefined')
      {
        IMNDictionaryObj[id]=0;
      }
      ```
   d. At the bottom of the same IMNRC(name, elem) function, there is a section that looks like this:
      ```
      if (fFirst)
      {
        var objRet=IMNGetOOUILocation(obj);
        objSpan=objRet.objSpan;
        if (objSpan)
        {
          objSpan.onmouseover=IMNShowOOUIMouse;
          objSpan.onclick=IMNShowOOUIKyb;
          objSpan.onmouseout=IMNHideOOUI;
          objSpan.onfocusout=IMNHideOOUI;
        }
      }
      ```
   e. Add the following statement as the last assignment within that section:
      ```
      objSpan.tabIndex=0;
      ```

Now that section should look like this (make sure you inserted the statement in the right place):

Chapter 11. Installing 589
if (fFirst)
{
    var objRet=IMNGetOOUILocation(obj);
    objSpan=objRet.objSpan;
    if (objSpan)
    {
        objSpan.onmouseover=IMNShowOOUIMouse;
        objSpan.onfocusin=IMNShowOOUIKyb;
        objSpan.onmouseout=IMNHideOOUI;
        objSpan.onfocusout=IMNHideOOUI;
        objSpan.tabIndex=0;
    }
}

9. Finally, modify the IMNIIsOnlineState function as explained here:
   a. Locate the IMNIIsOnlineState function.
   b. Change the condition from state==1 to state==0 so that the function looks like this:
      function IMNIIsOnlineState(state){
          if (state==0)
          {
              return false;
          }
      return true;
    }

10. Save and close the Init.js file.
    Next you will make similar changes to the OWS.js file.

11. Replace the EnsureIMNControl function in the OWS.js file as follows:
    a. Open the OWS.js file for editing.
    b. Open the EnsureIMNControl.js file that you copied to the server back in step 1.
    c. Copy the EnsureIMNControl function from this file (leave the file open for now).
    d. Back in the OWS.js file, search for its own version of the EnsureIMNControl function, delete that, and paste the newer version in its place.
    e. Close the EnsureIMNControl.js file.

12. Now replace the IMNGetStatusImage function in the same manner:
    a. Open the IMNGetStatusImage.js file that you also copied in step 1.
    b. Copy the IMNGetStatusImage function from this file (you can also leave this file open for now).
    c. Back in the OWS.js file, search for its own version of the IMNGetStatusImage function, delete that, and paste the newer version in its place.
    d. Close the IMNGetStatusImage.js file.

13. Make two changes to the IMNRC(name, elem) function within the OWS.js file as follows:
    a. Locate the function called IMNRC(name, elem).
    b. Locate the following statement (approximately 30 lines into the function):
       if (typeof(IMNDictionaryObj[id])=='undefined')
    c. Change the assignment from IMNDictionaryObj[id]=1 to IMNDictionaryObj[id]=0 so the "if" statement looks like this:
       if (typeof(IMNDictionaryObj[id])=='undefined')
       {
           IMNDictionaryObj[id]=0;
       }
d. At the bottom of the same IMNRC(name, elem) function, there is a section that looks like this:

```javascript
if (fFirst)
{
  var objRet=IMNGetOOUILocation(obj);
  objSpan=objRet.objSpan;
  if (objSpan)
  {
    objSpan.onmouseover=IMNShowOOUIMouse;
    objSpan.onfocusin=IMNShowOOUIKyb;
    objSpan.onmouseout=IMNHideOOUI;
    objSpan.onfocusout=IMNHideOOUI;
  }
}
```

e. Add the following statement as the last assignment within that section:

```javascript
objSpan.tabIndex=0;
```

Now that section should look like this (make sure you inserted the statement in the right place):

```javascript
if (fFirst)
{
  var objRet=IMNGetOOUILocation(obj);
  objSpan=objRet.objSpan;
  if (objSpan)
  {
    objSpan.onmouseover=IMNShowOOUIMouse;
    objSpan.onfocusin=IMNShowOOUIKyb;
    objSpan.onmouseout=IMNHideOOUI;
    objSpan.onfocusout=IMNHideOOUI;
    objSpan.tabIndex=0;
  }
}
```

14. Finally, modify the IMNIsOnlineState function as explained here:

a. Locate the IMNIsOnlineState function.

b. Change the condition from state==1 to state==0 so that the function looks like this:

```javascript
function IMNIsOnlineState(state){
  if (state==0)
  {
    return false;
  }
  return true;
}
```

15. Save and close the OWS.js file.

16. Restart the Office SharePoint Server.

Related reference

“Troubleshooting Office SharePoint integration” on page 593

If the Microsoft Office SharePoint integration does not work properly in your IBM Sametime deployment, you may need to modify how Sametime processes the identifier phrase being used by the Office SharePoint Server.

Verifying the Office SharePoint integration setup:

Use the IBM Sametime Connect client with the Sametime Connect integrator for SharePoint to verify that the Microsoft Office SharePoint integration feature is working correctly.
Before you begin

Set up the Office SharePoint Server by modifying template files as described in "Setting up the Office SharePoint server." On the client machine, install Sametime Connect with the optional feature called "Sametime Connect integrator for SharePoint."

About this task

When a web page like the My Site page is loaded, the Sametime SharePoint control will display a presence icon for names on the page that represents online Sametime users. For example, a green square indicates an online user whose status is Available. No icon appears when a name is unresolved. Log in to the Sametime Connect client and navigate to a SharePoint site to ensure that the presence icons are displaying correctly.

Procedure

1. If online users are displaying appropriate Sametime presence icons, integration is correctly configured and you have finished. Skip the remainder of this topic.
2. If icons are missing, check for the following situations:
   - **Names on this page are missing icons entirely.** You know that a particular name should have a presence icon but only displays it when you mouse-over the name.
     In this case, the client control is loading and resolving the name, but the icon update within the page is not complete. The most likely cause is incorrect editing of the template files on the server; return to the previous topic and verify that you made the changes properly.
   - **Names are missing icons and a mouse-over shows the control as a gray "X".**
     In this case, the client control is loading but is not receiving positive resolutions for the person data being set by the page. Verify that the Sametime Connect client is running and logged into the Sametime server. If the problem persists, check the following topic, "Troubleshooting Office SharePoint integration".
   - **A mouse-over does not show any change in the presence icon and does not have a gray "X".**
     In this case, either:
     - The optional Sametime Connect integrator for SharePoint feature was not installed on the client. Install it now and repeat this procedure to verify that integration is working correctly.
     - the JavaScript library edits have not been applied on the server hosting this web page. Return to the previous topic and apply the template changes directly on the Office SharePoint Server where the page being tested is hosted.
Related tasks
“Enabling installation of optional client features such as Microsoft Office Integration” on page 551
IBM Sametime ships with a number of optional client features that are not included in the default installation package. You can add features to the installation package for new client installs and update already-installed clients by updating the installation manifest file.

Related reference
“Troubleshooting Office SharePoint integration”
If the Microsoft Office SharePoint integration does not work properly in your IBM Sametime deployment, you may need to modify how Sametime processes the identifier phrase being used by the Office SharePoint Server.

Troubleshooting Office SharePoint integration:
If the Microsoft Office SharePoint integration does not work properly in your IBM Sametime deployment, you may need to modify how Sametime processes the identifier phrase being used by the Office SharePoint Server.

Sametime and Office SharePoint user directories
In some enterprises, the Office SharePoint integration may function immediately with no additional configuration updates besides the JavaScript library changes described in “Setting up Office SharePoint Server integration”. The most likely scenario to encounter this immediate functionality is one where Sametime and Office SharePoint have both been configured to use the same Active Directory, sharing this one LDAP for their backend directory. However, sharing a common LDAP is not a prerequisite for success with the Sametime SharePoint integration.

Enterprises where the Sametime server uses a different directory server are workable, even in cases where Sametime is configured to use IBM Lotus Domino and Office SharePoint is configured to use Active Directory. The key to the functionality is the concept of Sametime “resolving” a phrase to match a Sametime user. The Office SharePoint Server creates and delivers web pages to the local browser, and the live names on the page include JavaScript code that initializes names with presence controls.

Ensuring that Sametime can resolve an Office SharePoint server phrase
In Office SharePoint 2007, the function that provides a Sametime user name with a presence icon is called IMNRC. This function will appear in the page source wherever Office SharePoint intends to place a presence icon. The IMNRC function is passed an identifier phrase, typically an SMTP-format email address for the user; so alongside the name “Alice Jones” will be a presence initializer like IMNRC(“ajones@example.com”). The Sametime control that is loaded into the browser will be passed this ID (the “ajones@example.com” string).

The primary requirement for successful use of the Sametime SharePoint integration is that the ID phrase be uniquely resolvable by the Sametime server. Sametime does not require the Office SharePoint Server to use a particular data field as its ID for users, but you must configure the Sametime server to recognize the field you
choose. The exact setting used by the Sametime server is described in the “Table 6,
Authentication settings for the LDAP directory” in the LDAP directory settings
topic within this information center.

The first table entry, called "Search filter to use when resolving a user name to a
distinguished name", dictates the query that is used. Notice that "mail=%s" is a
recommended setting, and will be successful when the ID phrase is the SMTP
email address "ajones@example.com".

To summarize, the user data that is configured as an ID for presence by Office
SharePoint Server must be made available to the Sametime server (even if in a
second directory), and then specified in the "Search filter... when resolving a user
name” field. A quick troubleshooting check is to take the ID phrase found in the
presence initializing function, and paste it into the Lookup text field of the "Add
Contact” dialog in the Sametime Connect Client. If it is a unique match, the ID
phrase will resolve in the proper Office SharePoint integration.

Related tasks
“Setting up the Office SharePoint Server” on page 587
Set up integration with Microsoft Office SharePoint by modifying template files on
the Microsoft Office SharePoint Server with which you want IBM Sametime to
communicate.

“Verifying the Office SharePoint integration setup” on page 591
Use the IBM Sametime Connect client with the Sametime Connect integrator for
SharePoint to verify that the Microsoft Office SharePoint integration feature is
working correctly.

Enabling Sametime features on Linux clients
Optional features are installed on Linux clients automatically, but they are disabled
until users enable the features they want.

About this task
Users can enable the optional features in the Manage Plug-ins utility in their clients
by following these steps.

Procedure
1. Log in to the Sametime client.
2. Go to Tools > Plug-ins > Manage Plug-ins.
3. Click the Show Disabled Feature icon on the toolbar.
4. Find the optional feature you want to install and select it.
5. Click Enable to enable the selected feature.

Enabling Sametime Unified Telephony, extended status, and
telephony status in the client
The IBM Sametime Connect client and the Sametime embedded client for Lotus
Notes include plug-ins that can be enabled to support Sametime Unified Telephony
features.

• Sametime Unified Telephony plug-ins
  These plug-ins provide access to Sametime Unified Telephony features for users
  who have access to an Sametime Unified Telephony infrastructure and are
  provisioned to use it. In previous releases, the Sametime Unified Telephony
  client plug-ins were provided as a client add-on in the Sametime Unified
  Telephony product, and were installed using an add-on installer or update site.
• **Extended status plug-in** (com.ibm.collaboration.realtime.status.ext)
  This plug-in provides the ability to display custom live name status icons. This is typically used to display telephony status icons, but this mechanism can be used to display any custom status icons. This plug-in first appeared in Sametime 7.5.1, and prior to Sametime 8.5.1, this plug-in was only available in the Sametime SDK and as part of the Sametime Unified Telephony client add-on.

• **Telephony status plug-in** (com.ibm.collaboration.realtime.telephony.status)
  This plug-in, which was added for Sametime 8.0, makes use of the extended status plug-in to display telephony status icons for live names. This plug-in is used in conjunction with the Sametime Telephony Presence Adapter server component, which integrates the Sametime server with Sametime Unified Telephony and third-party telephony presence systems. The Sametime server obtains telephony status from the Telephony Presence Adapter and publishes status changes via Sametime user attributes. The telephony status plug-in responds to telephony status user attributes by displaying the appropriate telephony status icon next to the Sametime presence icon. Like the extended status plug-in, the telephony status plug-in was only available in the Sametime SDK and Sametime Unified Telephony client add-on in previous releases.

The remainder of this topic describes how the Sametime Unified Telephony, extended status, and telephony status plug-ins are enabled or disabled in the Sametime Connect 8.5.1 client. Since the different plug-ins are somewhat dependent on one another, it’s important for both administrators and third-party developers to understand how to enable or disable them and the impact of doing so.

**New client preferences**

A number of different options were considered that would allow administrators to enable or disable the Sametime Unified Telephony, extended status, and telephony status plug-ins. The two best options were client preferences and new policies, because either one could be applied to specific users and groups, but client preferences were chosen. Unlike policies, client preferences can be used to prevent plug-ins from loading at startup if the plug-ins will not be used, improving startup time, and client preferences can be used with older Sametime servers.

This section describes the new client preferences, which are listed below. The default value in all cases is false, which means the corresponding feature is disabled. To enable a feature, set the preference value to true. To disable the feature after enabling it, set the preference to false again.

• `com.ibm.collaboration.realtime/enableSUT=false`
  Set this preference to true to enable Sametime Unified Telephony features in the client. Once enabled, the client will only be able to make use of Sametime Unified Telephony telephony service (and Sametime audio/video service), so don’t enable this preference for users who are not provisioned to use Sametime Unified Telephony, since that will prevent them from getting access to other telephony services. When this preference is enabled (true), both telephony status and extended status are used, regardless of the values of the other preferences.

• `com.ibm.collaboration.realtime/enableTelephonyStatus=false`
  Set this preference to true to enable the display of telephony presence status icons for live names on the contact list or elsewhere. This is used for telephony presence published using the Sametime Telephony Presence Adapter, used by both Sametime Unified Telephony and third-party telephony presence solutions. Enabling telephony status also enables extended status. It is not necessary to
enable both preferences. In environments that include both Sametime Unified Telephony and non-Sametime Unified Telephony users, this preference can be enabled for the non-Sametime Unified Telephony users, to allow them to see telephony status for Sametime Unified Telephony users.

- `com.ibm.collaboration.realtime/enableExtendedStatus=false`

  Set this preference to true to enable the use of non-telephony extended status icons for live names on the contact list or elsewhere. Although extended status icons are most often used for telephony presence status, some third-party applications use extended status icons for other purposes. To display telephony status icons for applications that use the Sametime Telephony Presence Adapter, enable telephony status rather than this preference.

- `com.ibm.collaboration.realtime.telephony.ui/showCallComputer=false`

  Set this preference to true to enable the Call Computer action on the call menu and livename context menu. The Call Computer action starts a computer audio (voice chat) call using Sametime Audio/Video Conferencing, regardless of the selected preferred device and service provider preference. This action is primarily intended for Sametime Unified Telephony users, but can be enabled for any user.

The following table summarizes how these preferences affect extended status icons and telephony status:

<table>
<thead>
<tr>
<th>enableExtendedStatus</th>
<th>enableTelephony</th>
<th>enableSUT</th>
<th>Extended status icons displayed</th>
<th>Telephony status displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>any value</td>
<td>any value</td>
<td>true</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>any value</td>
<td>true</td>
<td>any value</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>false</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

### Modifying client preferences

Sametime provides different options for administrators to change client preferences, without requiring any action from end users. Any of these options can be used to modify the three client preferences described previously, however, IBM recommends the managed preferences mechanism is for changing these and other client preferences. Here’s an overview of the managed preferences mechanism:

- It was first supported by the Sametime Connect 8.5 client, but does not require a Sametime 8.5 server.
- You place a file named `managed-settings.xml` (example follows) on your server at the location specified by the administration update site URL. This is the same URL that specifies where the client looks for updated features posted by the administrator, which are automatically installed. This URL is specified by a Sametime user policy, so a different URL can be used for different users and groups.
- Sametime Connect 8.5 and later clients use the administration update site URL to look for updated features, but also look for a `managed-settings.xml` file at that location. If found, the `managed-settings.xml` settings are read and processed by the client.
- Older clients use the administration update site URL to look for updated features, but ignore any `managed-settings.xml` file at that location.
This is the format of the managed-settings.xml file used to enable or disable the three preferences described in this topic, with the default values:

```xml
<ManagedSettings>
    <settingGroup name="com.ibm.collaboration.realtime">
        <setting name="enableSUT" value="false"/>
        <setting name="enableTelephonyStatus" value="false"/>
        <setting name="enableExtendedStatus" value="false"/>
    </settingGroup>
</ManagedSettings>
```

For more information on using managed settings, see Configuring client preferences with the Expeditor managed settings framework.

**Note:** Unlike other client preferences, changes to the three preferences described here do not take effect until the client is restarted. Because the end user is unaware of preference changes made using the managed preferences mechanism, a dialog box with the following message appears if changes are detected to any of the three preferences:

Sametime has detected a configuration change from the administrator and needs to restart.

From the dialog, the user can choose to restart the client.

**Enabling Sametime Advanced persistent chat rooms and broadcast communities after installing**

The IBM Sametime Connect client, both standalone and integrated with Lotus Notes, includes plug-ins that were available separately in previous releases.

**About this task**

Administrators have different options to enable the Advanced plug-ins for users who are licensed to use Sametime Advanced. Administrators must explicitly enable the Advanced plug-ins even for clients upgrading from earlier releases of Sametime Advanced.

```plaintext
com.ibm.collaboration.realtime/enableAdvanced=false
```

Set this preference to `true` to enable the Sametime Advanced client.

**Configuring client connectivity to the Community Mux**

After you have configured the Community Server multiplexer, give users the DNS name of the multiplexer and instruct them to set up their Sametime Connect preferences to connect to the multiplexer instead of the Sametime Community Server.

**About this task**

Each user must update the Sametime Connect client with the DNS name of the multiplexer. If you have deployed multiple Community Server multiplexers, distribute users evenly among the machines. For example, with two multiplexers, direct half of your users to use multiplexer 1 and the other half to use multiplexer 2.

**Procedure**

1. Open Sametime Connect.
2. Choose **File > Preferences > Server Communities**.
3. In the Server Community field, type the DNS name of the Community Server multiplexer machine, such as messaging.example.com, as instructed by the administrator.

**Distributing updates and optional features to clients**

Set up updates site to distribute updates and optional features to clients.

**Before you begin**

A basic Eclipse update site is provided in the optional-components directory of the standalone client install CD and downloaded image. It includes all of the optional features distributed with Sametime, including Microsoft integration features and spell checker dictionaries for various languages. You can make updates to this site yourself to remove features you do not plan to distribute, to add your own features, or to add fixes.

**About this task**

Configuring update sites allows you to:

- Distribute optional Sametime client features to Windows and Mac clients. (Linux client installations include the optional features, but they are hidden until users enable them.)
- Install new client features that you have purchased from a third party or developed yourself using the Sametime SDK.
- Install client fixes from Lotus.

**Note:** To be able to install updates, Microsoft Windows Vista and Windows 7 clients must right-click the client program and choose to log on as an administrator, and when prompted, consent to run the program with elevated privileges. This allows the installation of new updates temporarily. After installation, log on as a regular user, to restore the default security for the client.

**Pushing updates to installed clients automatically**

Administrators can push a uniform set of updates and features to all clients automatically each time users log in to Sametime. This distribution method is supported for all features except the Sametime Office Integration for Microsoft Office features and patches.

**Before you begin**

Set up required update sites and make a note of their URLs.

**About this task**

Follow these steps to add the update sites to the Sametime update site URL policy for Instant Messaging on each of your Sametime servers.

**Procedure**

1. Log in to the Sametime System Console, open that server's Integrated Solutions Console, select Sametime System Console, and then click Manage Policies > Instant Messaging.
2. Locate the "Sametime update site URL" setting in the Instant Messaging section of the policy.
3. Specify one or more URLs for update sites where you will post required updates. Separate multiple URLs with semi-colons or commas.

4. Repeat these steps on each server.

**Results**

When the user logs in, the client checks the Sametime update site URL setting for the appropriate policy on the default Sametime server. The client connects to the specified update site and silently downloads all updated features it finds and installs them. The client then prompts the user to restart the client after the updates are installed. The user can delay the restart for five minutes or continue to delay every five minutes until it is convenient to restart. After the restart, the client checks again to see if there are more updates, and if it finds none, the user is not interrupted again. This update process takes place each time the user restarts his client and logs in.

**Note:** If the URL has not been specified or the setting is not found, the client will search the preferences.ini file located in the update plugin (com.ibm.collaboration.realtime.update\preferences.ini) root directory for the adminUpdatePolicyURL value. (The policy setting was not available prior to Sametime 7.5.1.)

**Giving users the option of installing new features when they log in**

Administrators can allow users to decide which features and updates to install. Configure the optional updates sites before users install the product, so they can choose the optional features and updates they want immediately after installation. With subsequent logins, users also continue to have the option to install features and updates. Users need administrator access to their machines to be able to install the Sametime Integration for Microsoft Office feature.

**Before you begin**

Set up optional update sites and make a note of their URLs.

**About this task**

Follow these steps to add the update sites to the Sametime optional add-on site URLs policy for Instant Messaging on each of your Sametime servers.

**Procedure**

1. Log in to the Sametime System Console, open that server’s Integrated Solutions Console, select Sametime System Console, and then click Manage Policies > Instant Messaging.
2. Locate the “Sametime optional add-on site URLs” setting in the Instant Messaging section of the policy.
3. Specify one or more URLs for update sites where you will post optional updates. Separate multiple URLs with semi-colons or commas.
4. Repeat these steps on each server.

**Results**

When the user logs in as a user with administrative access, the client scans all of the optional update sites specified in the “Sametime optional add-on site URLs” policy on the default Sametime server. The client then displays the updates that
match the client configuration and allows the user to disable further checking on startup. The user selects which updates to install, if any.

**Note:** If the URL has not been specified or the setting is not found, the client will search the preferences.ini file located in the update plugin (com.ibm.collaboration.realtime.update\preferences.ini) root directory for the optionalUpdatePolicyURL value. (The policy setting was not available prior to Sametime 8.0.)

**Letting users install updates manually**
Administrators either distribute update sites (zip or jar files) or post them to a web server and provide the users with instructions for manually installing the updates from their clients.

**About this task**
Provide Sametime Connect clients with these instructions to install updates manually that you have added to update sites or posted on a web server.

Users need to log in to their systems with administrative privileges if the optional Microsoft Office Integration features are included in the installation.

**Procedure**
1. In Sametime Connect, click **Tools > Plug-ins > Install plug-ins**.
2. Select **Search for new features to install**, and then click **Next**.
3. Add an update site:
   - If remote, select **Add Remote Location...**, specify a name for the update site and provide the URL for the site.
   - If a local directory, select **Add Folder Location...**, and select the directory where the update site exists.
   - If a local archive, select **Add Zip / Jar Location...** and select the update site archive.
     For example, if you have access to the Standalone client install D or downloaded image, you can click **New Archive Site...**. Then navigate to the optional-components directory and select **optional-components-update-site.zip**.
4. Click **OK** to add the new update site, and then click **Finish**. After a short time, the Update window appears.
5. Expand the update site and select the updates you wish to install from the available list. Then click **Next**.
6. You must agree to the license terms to continue.
7. In the next window, click **Finish** to install. Verify by clicking **Install**.
8. Restart the client.

**Creating an update site for plug-in access**
If you want to provide additional IBM Sametime plug-ins for your users, you can create an update site by using tools available from Eclipse.org. Users can use the site to update features or to get new features for their Instant Messaging component.

**Creating an update site**
You can create an update site using the wizard at http://www.eclipse.org.
To start the wizard:

1. Choose File > new project.
2. In the new project wizard, choose Plug-in development > update site project. The new update site wizard appears.
3. In Project Name, name your site.
4. In Location, use the format of HTTP_DOC_Root\myupdatesite.
5. Deselect Use default location.
6. Select Generate a web page listing all available features within the site.
7. Click Finish.
8. In the site.xml page, in "Category Properties", create the name and label for the category. The label appears on the page as a feature for the user to select.
9. In the Feature selection dialog box, add the feature you want to provide to users.
10. Click the Build All button to build the feature and the feature’s required plug-in.

User downloads

If you want to manually provision the plug-in, make sure that the policy Allow user to install plug-ins is assigned to the user. To deploy the plug-in to a larger audience, you can use software distribute system or a Sametime update site. For more information on using Sametime update sites, see Methods of pushing down Sametime 7.5.x & 8.0 client updates. In Sametime Connect, the user can select the feature from the Sametime Connect client.

2. Select Search for new features to install, and then click Next.
3. Select the site to include in the search and click Finish.
4. In the Search Results, select the features to install and click Next.
5. In the next window, click Finish to install. Verify by clicking Install.
6. Restart the client.

Update existing features

If Automatic Updates are selected in the Connect Client, the user receives a dialog box that states that new updates are available, and asks the user if he or she wants to install them now. The user can select Yes or No.

Client automatic update process

To ensure all clients have the same features, enable the update policy key to have the server push updates out to the IBM Sametime clients.

Administrators can provision new or update existing Sametime client features in a push mode so each client employs the same set of features as the others do. The push method enables the client to install Sametime features or updates automatically when a user logs in to Sametime.

Setting up automatic updates

When the user logs in from the client, the client looks in the preferences.ini file located in the update plugin (com.ibm.collaboration.realtime.update\preferences.ini) root directory for the existence of the "runme" property. If the property is present and is set to 'true,' then the update plugin continues. The client
then checks the policy key CONNECT_UPDATE_URL on the default Sametime Community Server. If the server is 7.5.x or later then you, as Administrator, can define the policy to tell the client where the update site is located. If the policy key is not set on the server (see the section on User Policy in this documentation), it is missing for one of two reasons:

1. The administrator did not set the key in the stpolicy.nsf file on the Sametime Community Server.
2. The Sametime Community Server is a pre-7.5.1 version.

If the key is not found, the client will search the preferences.ini file located in the update plugin (com.ibm.collaboration.realtime.update\preferences.ini) root directory for the adminUpdatePolicyURL value. The client then silently downloads all updated features it finds in the administrator’s update site and install them. Updates of features from this site are required so the client does not have the option of not installing them. Once installation is complete, the user receives a message announcing that new updates have been installed and that the user should restart the Sametime client. The user can click the restart button or press a five-minute delay button. If the user is involved in chats with other users, he or she can continue to delay restart by continuing to press the restart button at five-minute intervals. After the restart, the client checks again to see if there are more updates, and if it finds none, the user is not interrupted again. This update process takes place each time the user restarts the client and logs in into the default server.

**Uninstalling the Sametime client**

Follow the instructions in this section to uninstall the Sametime Connect client or the Sametime embedded client for Lotus Notes.

**Uninstalling the Sametime Connect client**

Uninstall or revert to an earlier version of the IBM Lotus Sametime Connect client.

**Uninstalling the Sametime Connect client on Windows:**

Uninstall or revert to an earlier version of the IBM Sametime Connect client on Windows.

**About this task**

To uninstall Sametime Connect, use the Windows Add-Remove Programs utility.

**Uninstalling the Sametime Connect client on Linux:**

Uninstall or revert to an earlier version of the IBM Sametime Connect client on Linux.

**Procedure**

1. Log in as root.
2. At the Linux command line, run the following command:
   ```
   rpm -e sametime-connect
   ```

**Uninstalling the Sametime Connect client on Unbuntu:**

Uninstall or revert to an earlier version of the IBM Sametime Connect client on Unbuntu.
Procedure
1. Log in with the user account.
2. At the command line, run the following command:
   `sudo dpkg -r sametime-connect`

Uninstalling the Sametime Connect client on the Macintosh:

Uninstall or revert to an earlier version of the IBM Sametime Connect client on the Macintosh.

Procedure
1. To uninstall the Sametime Connect client on the Macintosh, put `Sametime.app` in the trash.
2. Remove the workspace folder, stored in the `/Users/user_name/Library/Application Support/Lotus Sametime Data` folder.

Uninstalling the Sametime client embedded in Notes

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client.

Uninstalling the Sametime client embedded in Notes on Windows:

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client on Windows.

Procedure
1. From a DOS command prompt, navigate to the directory where the `setup.exe` file for the Sametime embedded client for Lotus Notes is stored.
2. Run the following command:
   `setup.exe /v"EMBEDDED_UNINSTALL=true"
   This command removes the Sametime client user interface, but does not remove the core Sametime features that are required for Notes to function.

What to do next

To revert to an earlier version of the Sametime client embedded in Notes, you must uninstall and reinstall Notes.

Uninstalling the Sametime client embedded in Notes on Linux:

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client.

Procedure

Follow these steps to uninstall the Sametime client and revert the Lotus Notes client to its original state.

1. Uninstall the Sametime client using the following command:
   `rpm -e sametime-connect-embedded`

   Note: At this point, the Lotus Notes client cannot start until you reinstall the Sametime client or follow the steps below to revert the Lotus Notes client to its previous state.
2. Uninstall any Notes fixpacks with the following command:
   
   `rpm -e ibm-lotus-notes-fixpack`

3. Reinstall `ibm_lotus_sametime` from the Notes install.

4. Reinstall any Notes fixpacks that were previously installed.

**Uninstalling the Sametime client embedded in Notes on Ubuntu:**

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client.

**Procedure**

Follow these steps to uninstall the Sametime client and revert the Lotus Notes client to its original state.

1. Uninstall the Sametime client using the following command:
   
   `sudo dpkg -r sametime-connect-embedded`

   **Note:** At this point, the Lotus Notes client cannot start until you reinstall the Sametime client or follow the steps below to revert the Lotus Notes client to its previous state.

2. Uninstall any Notes fixpacks with the following command:

   `sudo dpkg -r ibm-lotus-notes-fixpack`

3. Reinstall `ibm_lotus_sametime` from the Notes install.

4. Reinstall any Notes fixpacks that were previously installed.

**Uninstalling the Sametime client embedded in Notes on Mac:**

Uninstall or revert to an earlier version of the IBM Sametime embedded client running on a Lotus Notes client on the Mac.

**About this task**

The uninstall command should be run from the directory that contains the addonUninstall executable. This is normally downloaded along with the installer.

**Procedure**

From the Mac OSX command line, run the following command on one line:

**Sametime 8.5.2 client**

```
./addonUninstall -rcphome /Applications/Notes.app/Contents/MacOS -addonID sametime.852.embedded.addon
```

**Sametime 8.5.1 client**

```
./addonUninstall -rcphome /Applications/Notes.app/Contents/MacOS -addonID sametime.851.embedded.addon
```

**Sametime 8.5 client**

```
./addonUninstall -rcphome /Applications/Notes.app/Contents/MacOS -addonID sametime.850.embedded.addon
```

This command removes the Sametime client user interface, but does not remove the core Sametime features that are required for Notes to function.

**What to do next**

To revert to an earlier version of Sametime client embedded in Notes, you must uninstall and reinstall Notes.
Chapter 12. Migrating and upgrading

Migrate data from a previous version of Sametime and upgrade one or more servers to take advantage of the latest features.

This section contains information about installing and configuring IBM Sametime, while maintaining as much legacy data as possible, if you have used previous versions of the product.

Upgrading from Sametime 8.5 or 8.5.1

Upgrade servers in an IBM Sametime deployment to take advantage of the latest features.

About this task

Upgrading any Sametime 8.5 or 8.5.1 server requires that you run the installation program on that server; only files that changed in the newer release will be updated. Begin your upgrade with the Sametime System Console so that other servers can be registered with the console as they are upgraded.

Related concepts

“Planning for migration from an earlier release” on page 245
Planning an upgrade from an earlier release of IBM Sametime takes into account which release of Sametime you are upgrading from and whether you want to upgrade all servers and clients to this release in phases or at one time.

Upgrading Sametime 8.5 or 8.5.1 on AIX, Linux, Solaris, or Windows

Upgrade an IBM Sametime 8.5 deployment running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Before you begin

To help track your progress, print this page and use it as a checklist.

About this task

If you have a cluster of Sametime servers, you must upgrade all servers in the cluster; a cluster cannot support servers running different releases of Sametime.

Follow the instructions for the components you will upgrade:

Related concepts

“Planning server upgrades” on page 245
The tasks involved in planning an upgrade from an earlier release of IBM Sametime will vary, depending on your current release of Sametime, whether you have enabled online meetings, and how you want to support those meetings in the future.

Upgrading DB2 from a Sametime 8.5 or 8.5.1 installation on AIX, Linux, Solaris, and Windows

Upgrade to a newer version of DB2.
Upgrading DB2 from a Sametime 8.5 installation on AIX, Linux, Solaris, and Windows:

IBM DB2 9.7 is supported with this release of IBM Sametime, but you can continue to use DB2 9.5 if you prefer. If you do not already have one of the supported versions, you can use the following information to upgrade to DB2 9.7 on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Before you begin

- Verify that no applications are accessing or using the DB2 server or databases while you upgrade the server and databases.
- Back up your Sametime System Console, Meeting Server, and Gateway databases using the DB2 Control Center or the db2 backup database database_name command. For example, from the DB2 Command Line Processor tool, back up the Sametime System Console database named STSC with this command:
  
  ```
  db2 backup database STSC
  ```

  By default, the Meeting Server database is named STMS and the Gateway database is named STGW.

About this task

These instructions explain how to upgrade to the version of DB2 integrated with the Sametime installation package. Use this version of DB2 if you are unfamiliar with DB2 and would prefer a less complex deployment on Windows and Linux operating systems. The DB2 installation provided with Sametime supports Linux 32-bit or 64-bit systems and Windows 32-bit or 64-bit systems.

Linux: Upgrading from DB2 9.5 to DB2 9.7 is not supported on Linux. In addition, 64-bit DB2 is recommended on Linux now.

If you are familiar with DB2 deployments or are installing on other operating systems, download and install one of the unmodified DB2 limited use installation packages that are available at the following web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

IBM i includes DB2.

Linux: The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

Linux: If you are installing using the GUI mode, the full X11 desktop environment is required.

Procedure

Follow these steps to upgrade the DB2 server to the version of DB2 integrated with the Sametime installation package.
Attention: You must log in with the same administrative user ID that you used when you installed DB2 or the upgrade will fail.

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
3. Download the Sametime DB2 installation package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
      Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      AIX
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      mount -v cdrfs -o ro /dev/cd0 /cdrom
      Linux
      Mount the CD or DVD using a command similar to the following command:
      mount /dev/cdrom /cdrom
      Solaris
      Mount the CD or DVD.
4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   • Linux./launchpad.sh
   • Windows\launchpad.exe
Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

`sametime_server_package/IM/platform`

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM DB2, then click Install IBM DB2 again.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation. If you do not see a prompt, continue to the next step.

8. Click Update to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that Update All is not selected, and then click Next.

   The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the I accept the terms in the license agreements option and click Next.

11. Review the summary, then click Update.

   The process can take up to 20 minutes. You receive confirmation when it is complete.

12. Click Finish to close the screen.

13. Click Exit to close the Installation Manager.

14. Run the DB2 upgrade command to complete the upgrade of every database.

   **AIX, Linux, and Solaris**

   Log in as the db2admin user who installed DB2 originally and run the DB2 upgrade command.

   ```
   su db2admin
   db2 upgrade database database_name
   ```

   **Windows**

   Run the DB2 upgrade command.

   ```
   db2 upgrade database database_name
   ```

   Repeat this step for each database to be upgraded. The default names are STSC for the Sametime System Console, STMS for the Meeting Server database, and STGW for the Gateway database, but your database names may be different.

**Results**

If the installation fails, click View Log File for more information.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media. Ignore any warning about a missing `versionInfo.properties` file. It does not apply to DB2 installations and upgrades.

Installation Manager logs are stored in the following locations.
Linux /var.ibm/InstallationManager/logs

Windows 2008
%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

More detailed DB2 installation logs are stored in the following locations.

Linux The logs are stored in the /tmp folder and are named db2setup.log,
db2setup.his, and db2setup.err.

Windows
%My Documents%\DB2LOG\n
The log file name includes the date and time of the installation attempt; for
example:
C:\Documents and settings\administrator\my documents\db2log\DB2-ES-NE-
Wed Jun 21 11_59_37 2006.log

Upgrading DB2 from a Sametime 8.5.1 installation on AIX, Linux, Solaris, and
Windows:

IBM DB2 9.7 is supported with this release of IBM Sametime, but you can continue
to use DB2 9.5 if you prefer. If you do not already have one of the supported
versions, you can use the following information to upgrade to DB2 9.7 on IBM
AIX, Linux, Sun Solaris, or Microsoft Windows.

Before you begin
• Verify that no applications are accessing or using the DB2 server or databases
while you upgrade the server and databases.
• Back up your Sametime System Console, Meeting Server, and Gateway
databases using the DB2 Control Center or the db2 backup database
database_name command. For example, from the DB2 Command Line Processor
tool, back up the Sametime System Console database named STSC with this
command:
db2 backup database STSC
By default, the Meeting Server database is named STMS and the Gateway
database is named STGW.

About this task

These instructions explain how to upgrade to the version of DB2 integrated with
the Sametime installation package. Use this version of DB2 if you are unfamiliar
with DB2 and would prefer a less complex deployment on Windows and Linux
operating systems. The DB2 installation provided with Sametime supports Linux
32-bit or 64-bit systems and Windows 32-bit or 64-bit systems.

Linux: Upgrading from DB2 9.5 to DB2 9.7 is not supported on Linux. In addition,
64-bit DB2 is recommended on Linux now.

If you are familiar with DB2 deployments or are installing on other operating
systems, download and install one of the unmodified DB2 limited use installation
packages that are available at the following web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

Chapter 12. Migrating and upgrading 609
IBM i includes DB2.

**Linux** The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**Linux:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**Procedure**

Follow these steps to upgrade the DB2 server to the version of DB2 integrated with the Sametime installation package.

**Attention:** You must log in with the same administrative user ID that you used when you installed DB2 or the upgrade will fail.

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the **SELINUX** setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
3. Download the Sametime DB2 installation package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477
         &uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

   - **Linux**./launchpad.sh
   - **Windows** launchpad.exe

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

   `sametime_server_package/IM/platform`

   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM DB2, then click Install IBM DB2 again.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose File > Preferences.

   b. Uncheck Search service repositories during installation and updates and click OK.

9. Click Update to upgrade from a previous release.

10. Select the packages you want to upgrade, make sure that Update All is not selected, and then click Next.

    The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the I accept the terms in the license agreements option and click Next.

12. Validate the DB2 application user ID and password. Then click Next.

13. Review the summary, then click Update.

    The installation can take up to 20 minutes. You receive confirmation when it is complete.
14. Click **Finish** to close the installation screen.
15. Click **Exit** to close the Installation Manager.
16. Run the DB2 upgrade command to complete the upgrade of every database.
   **AIX, Linux, and Solaris**
   Log in as the db2admind user who installed DB2 originally and run the DB2 upgrade command.
   ```
   su db2admin
db2 upgrade database database_name
   ```
   **Windows**
   Run the DB2 upgrade command.
   ```
   db2 upgrade database database_name
   ```
   Repeat this step for each database to be upgraded. The default names are STSC for the Sametime System Console, STMS for the Meeting Server database, and STGW for the Gateway database, but your database names may be different.

**Results**

If the installation fails, click **View Log File** for more information.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media. Ignore any warning about a missing versionInfo.properties file. It does not apply to DB2 installations and upgrades.

Installation Manager logs are stored in the following locations.

**Linux**  `/var.ibm/InstallationManager/logs`

**Windows 2008**
`%ALLUSERSPROFILE%\IBM\Installation Manager\logs`

**Windows 2003**
`%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs`

More detailed DB2 installation logs are stored in the following locations.

**Linux**  The logs are stored in the `/tmp` folder and are named `db2setup.log`, `db2setup.his`, and `db2setup.err`.

**Windows**
`%My Documents%\DB2LOG\`

The log file name includes the date and time of the installation attempt; for example:

`C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log`

**Upgrading the Sametime 8.5 or 8.5.1 System Console on AIX, Linux, Solaris, or Windows**

Upgrade the IBM Sametime Community Server and Meeting Server to Release 8.5.1.1. Then upgrade the Sametime System Console running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.
Before you begin

Before upgrading the Sametime System Console to 8.5.2, you must do an interim upgrade of the Community Server and Meeting Server. The Community Server must be upgraded to Release 8.5.1.1 before you upgrade the Sametime System Console or nested groups will not work. The Sametime Meeting Server must be upgraded to Release 8.5.1.1 or group policies will not work.

About this task

Be sure to update the database used by the Sametime System Console before attempting to upgrade the console itself:

Updating the Sametime 8.5 database for the Sametime System Console on AIX, Linux, Solaris, and Windows:

If you are upgrading a Sametime System Console running on AIX, Linux, Solaris, and Windows from Release 8.5 to 8.5.2, update the database that stores its data. This step does not apply if you are upgrading from 8.5.1 to 8.5.2.

Before you begin

The DB2 administrator must have administrator rights to be able to create and update tables in the database. Make sure the DB2 server is running.

About this task

Run the scripts that come with Sametime in the DB2 installation package to update the database before upgrading the Sametime System Console.

Procedure

1. Back up the data stored in the Sametime System Console database.
   For instructions, see Backing up the console database.
2. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation if you are not already logged in.
   Linux and Windows: Now proceed to Step 4.
   AIX and Solaris: Now proceed to Step 3.
3. Download the DB2 installation package if you have not already done so.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         &uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**

Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**

Mount the CD or DVD using a command similar to the following command:

```bash
mount /dev/cdrom /cdrom
```

**Solaris**

Mount the CD or DVD.

4. Open a command prompt and navigate to the folder where you extracted the DB2 installation package.

5. Update the database by running one of the following commands from the SametimeDB2 folder:

**AIX, Linux, and Solaris**

```bash
./update_85_SCDb.sh STSC dbadmin
```

**Windows**

```bash
update_85_SCDb.bat STSC dbadmin
```

Replace "STSC" in the command if you used a different name when you created the database.

Replace "dbadmin" with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.

6. Close the command window.

7. Open the DB2 Control Center.

**AIX, Linux, and Solaris**

Open the IBM DB2 folder on the desktop and click Control Center.

**Windows**

Click **Start > Programs > IBM DB2 > installed_DB2_instance > General Administration Tools > Control Center.**

8. Verify that the database was updated.

The update script adds the following to the database:

- A table called VERSIONINFO
- A field called DISPLAYVERSION in the DEPLOYMENT table
- A field called CLUSTERVERSION in the CLUSTERDEPLOYMENT table

By looking at these elements in the DB2 control center, you can confirm that the database was updated.

**Upgrading a Sametime 8.5 or 8.5.1 System Console on AIX, Linux, Solaris, and Windows:**

Upgrade a Sametime System Console from 8.5 or 8.5.1.
Upgrade the IBM Sametime System Console on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing a newer version over an existing version.

**Before you begin**

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- The IBM DB2 database has been updated, and the server is running (you can use the `db2start` command).
- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (`install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x`) to ensure that the installation program can function properly.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   
   For more information, see the `backupConfig` command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator (Microsoft Windows) or as root (IBM AIX, Linux, Solaris).

   **Solaris only:** Solaris installs must be performed by the root user using `su` or a normal login session. Third-party sudo packages are not supported on Solaris.

3. Prepare to use the Sametime System Console installation package.
   
   a. To download installation packages:
      
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      
      2) Open this release's Download document at the following web address:
         
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

   **Tip:** When extracting downloads on Windows operating systems, use a short path location such as `C:\` and not a long path location such as the user's desktop or `TEMP` directories. When extracting to long path locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following command:
```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**:
     ```
     /launchpad.sh
     ```
   - **Windows**:
     ```
     launchpad.exe
     ```

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

   ```
   sametime_server_package/IM/platform
   ```

   *sametime_server_package* is the installation package name for this server.

   *platform* is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click **Install IBM Sametime System Console** and click **Launch IBM Sametime System Console 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. Click **Update** to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that **Update All** is not selected, and then click **Next**.

   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the **I accept the terms in the license agreements** option and click **Next**.

11. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

12. Click **Update**.

13. Click **Finish** when the installation process is complete.

14. Click **Exit** to close the Installation Manager.
Results

After a successful installation, the three components that are needed to run the
console start automatically: the Deployment Manager, the node agent, and the
Sametime System Console server. These must always be started before you can use
the system console.

If the installation was not successful, look at the installation logs for more
information about what occurred during the installation attempt. Fix any problems,
then uninstall all components and reinstall. Find information in the logs directory
and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the
root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs

SSC connection log:
/tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Upgrading a Sametime 8.5.1 System Console on AIX, Linux, Solaris, and Windows:

Upgrade the IBM Sametime System Console on IBM AIX, Linux, Sun Solaris, or
Microsoft Windows by installing a newer version over an existing version.

Before you begin

Stop all of the Sametime servers in the deployment except the server being
upgraded. For more information, see the Command reference for starting and
stopping servers in this information center.

Make sure your server meets the following requirements:
• The IBM DB2 database has been updated, and the server is running (you can
  use the db2start command).
• Linux: The launchpad install program needs to be able to launch a web browser. You
  will need to work directly on the console or have an X server and a web
  browser installed and configured (VNC or a remote X term session will work as
  well).
• Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
• If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

Procedure
1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator (Microsoft Windows) or as root (IBM AIX, Linux, Solaris).
   Solaris only: Solaris installs must be performed by the root user using su or a normal login session. Third-party sudo packages are not supported on Solaris.
3. Prepare to use the Sametime System Console installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
      b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
         AIX
         Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
         mount -v cdrfs -o ro /dev/cd0 /cdrom
         Linux
         Mount the CD or DVD using a command similar to the following command:
         mount /dev/cdrom /cdrom
         Solaris
         Mount the CD or DVD.
4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   **AIX, Linux, Solaris**
   
   ./launchpad.sh
   **Windows**
   launchpad.exe

5. Select a language from the “Select a language” list.

6. Click **Install IBM Sametime System Console** and click **Launch IBM Sametime System Console 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install Installation Manager. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose **File > Preferences**.
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

9. Click **Update** to upgrade from a previous release.

10. Select the packages you want to upgrade, make sure that **Update All** is **not** selected, and then click **Next**.
   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. At the Licenses screen, click **I accept the terms in the license agreements** and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Click **Update**.

14. Click **Finish** when the installation process is complete.

15. Click **Exit** to close the Installation Manager.

**Results**

After a successful installation, the three components that are needed to run the console start automatically: the Deployment Manager, the node agent, and the Sametime System Console server. These must always be started before you can use the system console.

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the **ant** and **native** subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var/ibm/InstallationManager/logs

**SSC connection log:**
Upgrading Sametime 8.5 or 8.5.1 Community Server on AIX, Linux, Solaris, or Windows

Upgrade an IBM Sametime 8.5 Community Server running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Before you begin

Before you can upgrade a Sametime Community Server, the Sametime System Console must be upgraded and running. The server is registered with the Sametime System Console during the upgrade process.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

Procedure

1. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.

2. Stop the Sametime and Lotus Domino servers running on this computer. For more information, see the instructions for your computer’s operating system:
   • AIX, Linux, Solaris: Stopping Domino and a Sametime Community Server on AIX, Linux, or Solaris
   • Windows: Stopping Domino and a Sametime Community Server on Windows

3. Prepare to use the Sametime Community Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files for Sametime and open the Server folder. Start the installation program by running one of the following commands:

**AIX**

```
./setupaix.bin
```

**Linux**

```
./setuplinux.bin
```

**Solaris**

```
./setupsolaris.bin
```

**Windows**

```
setupwin32.exe
```

5. Select the language to use for the installation and click **OK**.

6. At the Welcome screen, click **Next**.

7. Click the **I accept the terms in the license agreements** option and click **Next**.

8. Choose **Upgrading existing instance** and click **Next**.

9. Review the summary, then click **Install** to start the upgrade.

10. Click **Finish** to close the installation screen.

11. If prompted, click **Finish** to reboot the system.

12. **Windows 2008 only**

    After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is...
C:\Program Files (x86)\IBM\Lotus\Domino. Check for the following line to the [Config] section and add it if it is missing to ensure continuous connections for Sametime components:

```
BREAK_CONN_ON_ZERO_BYTES_SENT=0
```

Close and save the file, then restart the server.

**Results**

The `Domino_data_directory\stsetup_exit_status.txt` file contains a zero ("0") if the upgrade is successful. If the installation was not successful, look at the logs for more information about what occurred during the upgrade attempt. Fix the problem, then try installing again. The logs are stored in the following locations.

**AIX, Linux, or Solaris**

- **Domino data directory**: SametimeInstall.log, stsetup.log, stsetup_exit_status.txt
- **SametimeIniParser.log**: This log may be in /tmp or in the Domino data directory.
- **SSC connection log**: /tmp/SSCLogs/ConsoleUtility0.log

The default Domino data directory is /local/notesdata/.

**Windows**

- **Domino data directory**: SametimeInstall.log, stsetup.log, and stsetup_exit_status.txt
- **Domino program directory**: stsetup_exit_code_windows.txt
- **SametimeIniParser.log**: This log may be in %TEMP% or in the Domino data directory.
- **SSC connection log**: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

The default Domino data directory is c:\program files\ibm\lotus\domino\data\ and the Domino program directory is c:\program files\ibm\lotus\domino.

**Connecting with older Sametime Community Servers and Connect clients:**

IBM Sametime Community Servers connect with one another by recognizing a shared connection group ID set by the VP_SECURITY_LEVEL parameter in the `sametime.ini` file. New and upgraded Community Servers receive this parameter with a setting of 7000 automatically.

**About this task**

For Community Servers running releases prior to Sametime 8.5.1 on AIX, Linux, Solaris, or Windows, you must update the parameter in each older server’s `sametime.ini` file. Follow these steps to change the VP_SECURITY_LEVEL parameter for each older Community Server.

**Procedure**

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server installation directory. The default directories are listed below:
   - AIX: /local/notesdata
   - Linux: /local/notesdata
   - Solaris: /local/notesdata
   - Windows: C:\Lotus\Domino
3. In the **Config** section, change the value to match the following:
   For environments where all clients are using Sametime Connect 7.x or later or Sametime embedded in Notes 8.5.x or later clients:
   ```plaintext
   VP_SECURITY_LEVEL=7000
   ```
   For environments where clients are using releases prior to Sametime Connect 7.x or Sametime embedded in Notes 6.5.x, 7.x, or Notes Basic 8.x.:
   ```plaintext
   VP_SECURITY_LEVEL=6510
   ```
4. Save the sametime.ini file.

**What to do next**

If you changed the VP_SECURITY_LEVEL to 6510, you must also change the default sametime.ini setting from 7000 to 6510 on all new and upgraded Sametime Community servers running 8.5.x to maintain the connection between all servers.

**Upgrading a Sametime 8.5 or 8.5.1 Community Server cluster on AIX, Linux, Solaris, or Windows:**

Upgrade a cluster of IBM Sametime 8.5 Community Servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

**About this task**

Upgrade all of the servers in the cluster to ensure proper operation. After all of the servers have been upgraded, update the cluster's registration with the Sametime System Console.

**Upgrading a clustered Sametime 8.5 or 8.5.1 Community Server on AIX, Linux, Solaris, Windows:**

Upgrade an IBM Sametime 8.5 Community Server on AIX, Linux, Solaris, or Windows by installing the update over the existing product.

**Before you begin**

Before you can upgrade a Sametime Community Server, the Sametime System Console must be upgraded and running. The server is registered with the Sametime System Console during the upgrade process.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**Procedure**

1. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
**Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

2. Stop the Sametime and Lotus Domino servers running on this computer. For more information, see the instructions for your computer's operating system:
   - **AIX, Linux, Solaris:** Stopping Domino and a Sametime Community Server on AIX, Linux, or Solaris
   - **Windows:** Stopping Domino and a Sametime Community Server on Windows

3. Prepare to use the Sametime Community Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      `mount -v cdrfs -o ro /dev/cd0 /cdrom`

      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      `mount /dev/cdrom /cdrom`

      **Solaris**
      Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files for Sametime and open the Server folder. Start the installation program by running one of the following commands:
   - **AIX**
     ./setupaix.bin
   - **Linux**
     ./setuplinux.bin
   - **Solaris**
5. Select the language to use for the installation and click **OK**.
6. At the Welcome screen, click **Next**.
7. Click the **I accept the terms in the license agreements** option and click **Next**.
8. Choose **Upgrading existing instance** and click **Next**.
9. Review the summary, then click **Install** to start the upgrade.
10. Click **Finish** to close the installation screen.
11. If prompted, click **Finish** to reboot the system.

**Windows 2008 only**

After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is 
C:\Program Files (x86)\IBM\Lotus\Domino. Check for the following line to the [Config] section and add it if it is missing to ensure continuous connections for Sametime components:

```
BREAK_CONN_ON_ZERO_BYTES_SENT=0
```

Close and save the file, then restart the server.

**Results**

The **Domino data directory\stsetup_exit_status.txt** file contains a zero ("0") if the upgrade is successful. If the installation was not successful, look at the logs for more information about what occurred during the upgrade attempt. Fix the problem, then try installing again. The logs are stored in the following locations.

**AIX, Linux, or Solaris**

**Domino data directory:** SametimeInstall.log, stsetup.log, stsetup_exit_status.txt

**SametimeIniParser.log:** This log may be in /tmp or in the Domino data directory.

**SSC connection log:** /tmp/SSCLogs/ConsoleUtility0.log

The default Domino data directory is /local/notesdata/.

**Windows**

**Domino data directory:** SametimeInstall.log, stsetup.log, and stsetup_exit_status.txt

**Domino program directory:** stsetup_exit_code_windows.txt

**SametimeIniParser.log:** This log may be in %TEMP% or in the Domino data directory.

**SSC connection log:** Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

The default Domino data directory is c:\program files\ibm\lotus\domino\data\ and the Domino program directory is c:\program files\ibm\lotus\domino.

**Connecting with older Sametime Community Servers and Sametime Connect clients:**

Chapter 12. Migrating and upgrading 625
IBM Sametime Community Servers connect with one another by recognizing a shared connection group ID set by the VP_SECURITY_LEVEL parameter in the sametime.ini file. New and upgraded Community Servers receive this parameter with a setting of 7000 automatically.

About this task

For Community Servers running releases prior to Sametime 8.5.1 on AIX, Linux, Solaris, or Windows, you must update the parameter in each older server's sametime.ini file. Follow these steps to change the VP_SECURITY_LEVEL parameter for each older Community Server.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server installation directory. The default directories are listed below:
   - AIX: /local/notesdata
   - Linux: /local/notesdata
   - Solaris: /local/notesdata
   - Windows: C:\Lotus\Domino
3. In the Config section, change the value to match the following:
   For environments where all clients are using Sametime Connect 7.x or later or Sametime embedded in Notes 8.5.x or later clients:
   
   VP_SECURITY_LEVEL=7000
   
   For environments where clients are using releases prior to Sametime Connect 7.x or Sametime embedded in Notes 6.5.x, 7.x, or Notes Basic 8.x.:
   
   VP_SECURITY_LEVEL=6510
4. Save the sametime.ini file.

What to do next

If you changed the VP_SECURITY_LEVEL to 6510, you must also change the default sametime.ini setting from 7000 to 6510 on all new and upgraded Sametime Community servers running 8.5.x to maintain the connection between all servers.

Registering the upgraded Community Server cluster with the System Console:

After upgrading an IBM Sametime cluster to a Sametime Community Server cluster on IBM AIX, Linux, Sun Solaris, or Microsoft Windows, register the cluster with the Sametime System Console, so you can manage all of the Sametime servers from a central location.

Before you begin

Make sure each of these servers is ready for the cluster registration task:

- Each of the upgraded Sametime Community Servers in the cluster must be registered with the Sametime System Console, and must be started.
- The Sametime System Console must be started.
- The LDAP server must be started, and must be connected to the Sametime System Console.
Procedure

1. Verify that each of the servers in the cluster has been registered with the Sametime System Console.

2. Run the registration utility using the appropriate command below:

   **Upgrading from 8.5 and 8.5.1**
   - AIX, Linux, Solaris: ./registerSTCluster.sh -upgradeCluster
   - Windows: registerSTCluster.bat -upgradeCluster

   **Upgrading from 8.0.x and 7.5.1**
   - AIX, Linux, Solaris: ./registerSTCluster.sh
   - Windows: registerSTCluster.bat

3. As the registration utility runs, you will be prompted to enter the following information:

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Type the name you created when you configured the cluster, and press Enter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of notes.ini file</td>
<td>This is the user name and password that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the full path to the directory containing the notes.ini file, and press Enter. For example, on Windows: C:\Lotus\Domino</td>
</tr>
<tr>
<td>Lotus Domino administrator user name</td>
<td>This is the account that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the Lotus Domino administrator's user name, and press Enter.</td>
</tr>
<tr>
<td>Lotus Domino administrator password</td>
<td>Type the password associated with the Lotus Domino administrator user account, and press Enter.</td>
</tr>
</tbody>
</table>

   The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory.

4. Restart the Sametime Community Server.

Upgrading a stand-alone Community Mux from Sametime 8.5 or 8.5.1:

If your previous IBM Sametime deployment included a stand-alone Community Mux, you can upgrade the multiplexer to this release.

**Before you begin**

This task only applies to a stand-alone Community Mux; the multiplexer that installs directly on the Sametime Community Server was upgraded automatically when you upgraded that server.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

This release of Sametime supports a stand-alone Community Mux installed with an earlier version of the product; however if you plan to support IPv6 addressing in
your deployment, you must upgrade the Community Mux to at least release 8.0.2 (IPv6 addressing was introduced in Sametime 8.0.2).

If you have more than one stand-alone Community Mux, upgrade all of them:

**Procedure**

1. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

2. Prepare to use the Sametime Community Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         &uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

      **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      `mount -v cdrfs -o ro /dev/cd0 /cdrom`

      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      `mount /dev/cdrom /cdrom`

      **Solaris**
      Mount the CD or DVD.

3. Navigate to the folder where you stored the downloaded files for Sametime and open the Server folder. Start the installation program by running one of the following commands:
   **AIX**
   `./setupaix.bin`

   **Linux**
   `./setuplinux.bin`
Solaris
./setsolarsis.bin

Windows
setupwin32.exe

4. Choose the option to install the Community Services Mux.
5. At the "Select a language" screen, select a language for the installer, and then click OK.
6. At the "Welcome" screen, click Next.
7. At the license agreement screen, click I accept both the IBM and the non-IBM terms, and then click Next.
8. Click Upgrade.
9. At the summary screen, click Install.
10. At the "successfully installed" screen, click Finish.

11. Windows 2008 only

   After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is C:\Program Files (x86)\IBM\Lotus\Domino. Check for the following line to the [Config] section and add it if it is missing to ensure continuous connections for Sametime components:
   
   BREAK_CONN_ON_ZERO_BYTES_SENT=0
   
   Close and save the file, then restart the server.

Verifying a remote Conversion Server after upgrading:

If your IBM Sametime deployment includes a remote conversion server and you will continue to host meetings on one or more upgraded Sametime servers, you should upgrade the conversion server as well. If you upgraded the conversion server from an earlier release to 8.5 or later, you do not need to upgrade the conversion server again because there have been no changes since 8.5.

About this task

Your Sametime Community Server may already be configured to use a particular conversion server and port number. If you used a remote conversion server in a previous release of Sametime, the configuration was migrated during the upgrade. You may have specified the configuration when you installed Sametime or when you added Sametime to a Domino server (IBM i). Verify that the information is correct, or update the server configuration.

Procedure

1. On the upgraded Sametime Community server, verify the conversion server configuration:
   a. Open the stconvservices.properties file, which is located in the Sametime server data stconversion subdirectory.
   b. Check the value for RemoteConversionURL setting:
      • If no remote conversion server has been configured, the setting looks like:
        
        #RemoteConversionURL=http://conversions1.ibm.com:8081;
        http://conversions2.ibm.com:8081/servlet/stconversion

Chapter 12. Migrating and upgrading  629
• When one remote conversion server is configured, the # is absent at the start of the line, the server name is correct, and everything between the semicolon and the end of the line is deleted. For example:
  RemoteConversionURL=http://stconv.example.com:19610/servlet/stconversion
  Note the port number (19610 in the example) to use when you run the installation program.

• If more than one conversion server is configured, there is no # sign, and data for each server is separated by a semicolon. For example:
  RemoteConversionURL=http://stconv1.example.com:19610/servlet/stconversion;
  http://stconv2.example.com:8081/servlet/stconversion
  Find the entry for the conversion server that you plan to install, and note the port number.

  c. Save and close the file.
  d. If you updated the file, restart the Sametime server now.

2. Upgrade the remote conversion server:
   The Sametime Conversion Services installation program is located in the Sametime Community Server package.
   a. Move to the computer hosting the remote conversion server that you will upgrade.
   b. Download the conversion server installation program or insert the CD containing it, and start the installation.
   c. Select a language for the installer, and click Next.
   d. Select the option to install Sametime Conversion Services, and click Next.
   e. Follow the prompts presented to complete the installation.
   f. When you are prompted for the port on which the conversion service will listen, specify the port number you noted when you verified the Sametime server configuration in Step 1.
   g. If you installed Conversion Services on Microsoft Windows 2000, restart the server.
   h. If your users will be posting documents that contain text for languages other than English, verify that the locale for your Conversion Server is set appropriately.

Results

The conversion services component starts automatically when you restart the server. To start the conversion services manually, click Start > Administrative tools > Services.

Preparing for SSL encryption after upgrading:

If SSL is enabled, upgrade the GSKit environment to work with this release of IBM Sametime.

About this task

For an upgrade, take only the steps needed to update the components that allow SSL encryption between this release of Sametime Community Server and the LDAP server. Steps 1 and 2 are required for all upgrades. Step 3 only applies if you are running Tivoli Directory Server as your LDAP server.
Procedure

1. Upgrade GSKit on the Sametime Community Server to release 8.0.4.16.
2. Update the .jar files for the iKeyMan utility on the Community Server.
3. If you are using Tivoli Directory Server as the LDAP server, upgrade GSKit to a supported release. The server must be running GSKit 7.0.4.28 or later.

Related tasks

“Working with Sametime servers that are enabled for SSL” on page 787
Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

Upgrading Sametime 8.5 or 8.5.1 Proxy Server on AIX, Linux, Solaris, or Windows

Follow the instructions for your operating system to upgrade one or more Sametime Proxy Servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Upgrading a Sametime 8.5 or 8.5.1 Proxy Server on AIX, Linux, Solaris, or Windows:

Upgrade a Sametime System Console from 8.5 or 8.5.1.

Upgrading a Sametime 8.5 Proxy Server on AIX, Linux, Solaris, or Windows:

Upgrade an IBM Sametime Proxy Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure
1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.
3. Prepare to use the Sametime Proxy Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
      b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
         **AIX**
         Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
         `mount -v cdrfs -o ro /dev/cd0 /cdrom`
         **Linux**
         Mount the CD or DVD using a command similar to the following command:
         `mount /dev/cdrom /cdrom`
         **Solaris**
         Mount the CD or DVD.
4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris** `./launchpad.sh`
- Windows launchpad.exe

Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

sametime_server_package/IM/platform

platform is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM Sametime Proxy Server and click Launch IBM Sametime Proxy Server 8.5.2 installation.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.
If you do not see a prompt, continue to the next step.

8. Click Update to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that Update All is not selected, and then click Next.

The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the I accept the terms in the license agreements option and click Next.

11. Validate the WebSphere Application Server administrator ID and password, and then click Next.

12. Enter the fully qualified Sametime System Console server host name. Do not use an IP address or short host name.

13. Enter the Sametime System Console user ID and password, then click Validate.

14. After the Validate button changes to Validated, click Next.

15. Click Update.

16. Click Finish when the installation process is complete.

17. Click Exit to close the Installation Manager.

18. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded Sametime Proxy Server's EAR file to the System Console.

If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

a. Locate the SametimeProxy.ear file on the upgraded Sametime Proxy Server:

install_root/SametimeProxyServerOffering/SametimeServer/STProxy/proxy/installableApps/SametimeProxy.ear

b. Copy the file to the following location on the Sametime System Console:

WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs

SSC connection log:

/tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Upgrading a Sametime 8.5.1 Proxy Server on AIX, Linux, Solaris, or Windows:

Upgrade an IBM Sametime Proxy Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.
**AIX, Linux, and Solaris**: If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   
   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   **Solaris only**: The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Prepare to use the Sametime Proxy Server installation package.
   
   a. To download installation packages:
      
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      
      2) Open this release’s Download document at the following web address:
         
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         
         **Tip**: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
      
      b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

      **AIX**
      
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      
      `mount -v cdrfs -o ro /dev/cd0 /cdrom`
      
      **Linux**
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX, Linux, and Solaris**: `./launchpad.sh`
- **Windows**: `launchpad.exe`

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (``install`` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

*platform* is the installation package name for this server.

5. If necessary, select a language other than English from the Select a language list.

6. Click **Install IBM Sametime Proxy Server** and click **Launch IBM Sametime Proxy Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose **File > Preferences**.
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

9. Click **Update** to upgrade from a previous release.

10. Select the packages you want to upgrade, make sure that **Update All** is not selected, and then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Enter the fully qualified Sametime System Console server host name.

    Do not use an IP address or short host name.

14. Enter the Sametime System Console user ID and password, then click **Validate**.

15. After the **Validate** button changes to **Validated**, click **Next**.

16. Click **Update**.

17. Click **Finish** when the installation process is complete.

18. Click **Exit** to close the Installation Manager.
19. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded Sametime Proxy Server's EAR file to the System Console.

If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

a. Locate the SametimeProxy.ear file on the upgraded Sametime Proxy Server:
   
   ```
   install_root/SametimeProxyServerOffering/SametimeServer/
   STProxy/proxy/installableApps/SametimeProxy.ear
   ```

b. Copy the file to the following location on the Sametime System Console:
   
   ```
   WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
   ```

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the `logs` directory and the `ant` and `native` subdirectories.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media.

**AIX, Linux, or Solaris**

```
/var.ibm/InstallationManager/logs
```

**SSC connection log:**

```
/tmp/SSCLogs/ConsoleUtility0.log
```

**Windows 2008**

```
%ALLUSERSPROFILE%\IBM\Installation Manager\logs
```

**Windows 2003**

```
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
```

**SSC connection log:**

```
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log
```

**Upgrading a cluster of Sametime 8.5 or 8.5.1 Proxy Servers on AIX, Linux, Solaris, or Windows:**

Upgrade a cluster of IBM Sametime 8.5 Proxy Servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows. Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**About this task**

Upgrading a cluster of Sametime Proxy Servers requires you to stop the Deployment Manager and all nodes in the cluster before upgrading the individual...
servers. After the individual nodes have been upgraded, you will start the cluster and complete its configuration by running the clustering guided activity.

**Note:** Remember to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

*Preparing the Sametime 8.5 or 8.5.1 Proxy Server cluster for an upgrade on AIX, Linux, Solaris, or Windows:*

Before upgrading servers in a cluster of IBM Sametime Proxy Servers, prepare the cluster by stopping the Deployment Manager as well as servers running on each node.

**Procedure**

1. On each node in the cluster, open a command window and stop the following servers:

   **Note:** On each node, leave the WebSphere Application Server running so you can back up its configuration and validate the administrator credentials in the next task.

   a. Stop the Sametime Proxy Server:
      
      **AIX, Linux, Solaris:**
      
      .\stopServer.sh STProxy_Server_name -username WAS_admin_username -password WAS_admin_password
      
      **Windows:**
      
      stopServer.bat STProxy_Server_name -username WAS_admin_username -password WAS_admin_password

   b. If a WebSphere proxy server is hosted on this node, stop it now:
      
      **AIX, Linux, Solaris:**
      
      .\stopServer.sh WAS_proxy_server_name
      
      **Windows:**
      
      stopServer.bat WAS_proxy_server_name

   c. Stop the node agent:
      
      **AIX, Linux, Solaris:**
      
      .\stopNode.sh WAS_admin_username -username WAS_admin_username -password WAS_admin_password
      
      **Windows:**
      
      stopNode.bat WAS_admin_username -username WAS_admin_username -password WAS_admin_password

   d. Repeat for every node in the cluster.

2. On the server hosting the Deployment Manager, open a command window and stop the cluster’s Deployment Manager:

   **AIX, Linux, Solaris:**
   
   .\stopManager.sh dmgr -username WAS_admin_username -password WAS_admin_password
   
   **Windows:**
   
   stopManager.bat dmgr -username WAS_admin_username -password WAS_admin_password

*Upgrading a Sametime 8.5 or 8.5.1 Proxy Server node on AIX, Linux, Solaris, or Windows:*

Upgrade a Sametime System Console from 8.5 or 8.5.1.

*Upgrading a Sametime 8.5 Proxy Server node on AIX, Linux, Solaris, or Windows:*

Upgrade an IBM Sametime Proxy Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.
Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   
   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.
3. Prepare to use the Sametime Proxy Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         &uid=swg24029128
Locate the components that you need in the document's listing, then
download the packages labelled with the corresponding part numbers
to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a
short path location such as C:\ and not a long path location such as
the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:
```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following
command:
```bash
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the
installation program by running one of the following commands:
- **AIX, Linux, and Solaris**:
  ```bash
  /launchpad.sh
  ```
- **Windows**:
  ```bash
  launchpad.exe
  ```

**Note:** If you do not have a web browser, go to the Installation Manager
package directory and run the installation program (**install** for Linux or
**install.exe** for Windows). Find the Installation Manager package directory
here:

```
sametime_server_package/IM/platform
```

**sametime_server_package** is the installation package name for this server.

```
platform is the operating system on which you are installing.
```

5. If necessary, select a language other than English from the **Select a language**
list.

6. Click **Install IBM Sametime Proxy Server** and click **Launch IBM Sametime
Proxy Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it.
Do so, then click **Finish** to restart the Installation Manager and continue with
the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. Click **Update** to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that **Update All** is *not*
selected, and then click **Next**.
The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the I accept the terms in the license agreements option and click Next.

11. Validate the WebSphere Application Server administrator ID and password, and then click Next.

12. Enter the fully qualified Sametime System Console server host name.
    Do not use an IP address or short host name.

13. Enter the Sametime System Console user ID and password, then click Validate.

14. After the Validate button changes to Validated, click Next.

15. Click Update.

16. Click Finish when the installation process is complete.

17. Click Exit to close the Installation Manager.

18. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded Sametime Proxy Server's EAR file to the System Console.
    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.
    a. Locate the SametimeProxy.ear file on the upgraded Sametime Proxy Server:
       install_root/SametimeProxyServerOffering/SametimeServer/STProxy/proxy/installableApps/SametimeProxy.ear
    b. Copy the file to the following location on the Sametime System Console:
       WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs

SSC connection log:
/tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:
Upgrading a Sametime 8.5.1 Proxy Server node on AIX, Linux, Solaris, or Windows:

Upgrade an IBM Sametime Proxy Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version “7.0.0.9” (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure
1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.
3. Prepare to use the Sametime Proxy Server installation package.
   a. To download installation packages:
1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

   Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   AIX
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   ```sh
   mount -v cdrfs -o ro /dev/cd0 /cdrom
   ```

   Linux
   Mount the CD or DVD using a command similar to the following command:
   ```sh
   mount /dev/cdrom /cdrom
   ```

   Solaris
   Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - AIX, Linux, and Solaris: /launchpad.sh
   - Windows: launchpad.exe

   Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

   sametime_server_package/IM/platform

   sametime_server_package is the installation package name for this server.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM Sametime Proxy Server and click Launch IBM Sametime Proxy Server 8.5.2 installation.
7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.
8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.
9. Click Update to upgrade from a previous release.
10. Select the packages you want to upgrade, make sure that Update All is not selected, and then click Next.
    The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.
11. Click the I accept the terms in the license agreements option and click Next.
12. Validate the WebSphere Application Server administrator ID and password, and then click Next.
13. Enter the fully qualified Sametime System Console server host name. Do not use an IP address or short host name.
14. Enter the Sametime System Console user ID and password, then click Validate.
15. After the Validate button changes to Validated, click Next.
16. Click Update.
17. Click Finish when the installation process is complete.
18. Click Exit to close the Installation Manager.
19. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded Sametime Proxy Server's EAR file to the System Console.
    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.
   a. Locate the SametimeProxy.ear file on the upgraded Sametime Proxy Server:
      
      install_root/SametimeProxyServerOffering/SametimeServer/STProxy/proxy/installableApps/SametimeProxy.ear
   b. Copy the file to the following location on the Sametime System Console:
      
      WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs
Starting servers in the upgraded Sametime Proxy Server cluster on AIX, Linux, Solaris, or Windows:

In an IBM Sametime deployment, start the servers in the upgraded cluster of Sametime Proxy Servers.

Before you begin

Upgrade all nodes in the cluster before you start the cluster.

Procedure

1. On the server hosting the Deployment Manager, open a command window and start the cluster's Deployment Manager:
   
   AIX, Linux, Solaris: ./startManager.sh dmgr
   Windows: startManager.bat dmgr

2. On each node in the cluster, open a command window and start the following servers:
   
   a. WebSphere Application Server should already be running, but if it is not, start it now:
      
      AIX, Linux, Solaris: ./startServer.sh server1
      Windows: startServer.bat server1
   
   b. Start the node agent:
      
      AIX, Linux, Solaris: ./startNode.sh
      Windows: startNode.bat
   
   c. If a WebSphere proxy server is hosted on this node, Start it now:
      
      AIX, Linux, Solaris: ./startServer.sh WAS_proxy_server_name
      Windows: startServer.bat WAS_proxy_server_name
   
   d. Start the Sametime Proxy Server:
      
      AIX, Linux, Solaris: ./startServer.sh STProxy_Server_name
      Windows: startServer.bat STProxy_Server_name
   
   e. Repeat for every node in the cluster.
Upgrading Sametime 8.5 or 8.5.1 Meeting Server on AIX, Linux, Solaris, or Windows

Follow the instructions for your operating system to upgrade one or more Sametime Meeting Servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Upgrading a Sametime 8.5 or 8.5.1 Meeting Server on AIX, Linux, Solaris, and Windows:

Upgrade a Sametime Meeting Server from 8.5 or 8.5.1.

Upgrading a Sametime 8.5 Meeting Server on AIX, Linux, Solaris, or Windows:

Upgrade an IBM Sametime Meeting Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.15" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

**Solaris only**: The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         **Tip**: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      ```
      mount -v cdrfs -o ro /dev/cd0 /cdrom
      ```

      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      ```
      mount /dev/cdrom /cdrom
      ```

      **Solaris**
      Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**: `./launchpad.sh`
   - **Windows**: `launchpad.exe`

   **Note**: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (`install` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

   ```
   sometime_server_package/IM/platform
   ```

   `sometime_server_package` is the installation package name for this server.
*platform* is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language** list.

6. Click **Install IBM Sametime Meeting Server** and click **Launch IBM Sametime Meeting Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.

8. Click **Update** to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that **Update All** is *not* selected, and then click **Next**.
   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the **I accept the terms in the license agreements** option and click **Next**.

11. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

12. Enter the fully qualified Sametime System Console server host name.
   Do not use an IP address or short host name.

13. Enter the Sametime System Console user ID and password, then click **Validate**.

14. After the **Validate** button changes to **Validate**ed, click **Next**.

15. Click **Update**.

16. Click **Finish** when the installation process is complete.

17. Click **Exit** to close the Installation Manager.

18. If this is the Primary Node for a cluster and the Sametime System Console does *not* function as the cluster's Deployment Manager, copy the upgraded Sametime Meeting Server's EAR file to the System Console.
   If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

   a. Locate the meetingserver.ear file on the upgraded Sametime Meeting Server:
   ```
   install_root/SametimeMeetingServerOffering/SametimeServer/
   STM Meeting/meeting/installableApps/meeting.server.ear
   ```

   b. Copy the file to the following location on the Sametime System Console:
   ```
   WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
   ```

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the **ant** and **native** subdirectories.

You can use the **collectLogs** utility to gather the logs; **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**

```
/var.ibm/InstallationManager/logs
```
Upgrading a Sametime 8.5.1 Meeting Server on AIX, Linux, Solaris, or Windows:

Upgrade an IBM Sametime Meeting Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version “7.0.0.15” (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.
Procedure

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      ```
      mount -v cdrfs -o ro /dev/cd0 /cdrom
      ```
      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      ```
      mount /dev/cdrom /cdrom
      ```
      **Solaris**
      Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris** ./launchpad.sh
   - **Windows** launchpad.exe
Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.
6. Click Install IBM Sametime Meeting Server and click Launch IBM Sametime Meeting Server 8.5.2 installation.
7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.
8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.
9. Click Update to upgrade from a previous release.
10. Select the packages you want to upgrade, make sure that Update All is not selected, and then click Next.
    The Update All option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.
11. Click the I accept the terms in the license agreements option and click Next.
12. Validate the WebSphere Application Server administrator ID and password, and then click Next.
13. Enter the fully qualified Sametime System Console server host name.
    Do not use an IP address or short host name.
14. Enter the Sametime System Console user ID and password, then click Validate.
15. After the Validate button changes to Validated, click Next.
16. Click Update.
17. Click Finish when the installation process is complete.
18. Click Exit to close the Installation Manager.
19. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded Sametime Meeting Server's EAR file to the System Console.
    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.
   a. Locate the meetingserver.ear file on the upgraded Sametime Meeting Server:
      ```
      install_root/SametimeMeetingServerOffering/SametimeServer/
      STMeeting/meeting/installableApps/meeting.server.ear
      ```
   b. Copy the file to the following location on the Sametime System Console:
```
      WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
```
Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs; collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris

/var.ibm/InstallationManager/logs

SSC connection log:
/tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Upgrading a cluster of Sametime 8.5 or 8.5.1 Meeting Servers on AIX, Linux, Solaris, or Windows:

Upgrading a cluster of IBM Sametime Meeting Servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows. Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

About this task

Upgrading a cluster of Sametime Meeting Servers requires you to stop the Deployment Manager and all nodes in the cluster before upgrading the individual servers. After the individual nodes have been upgraded, you will start the cluster and complete its configuration by running the clustering guided activity.

Note: Remember to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Preparing the Sametime 8.5 or 8.5.1 Meeting Server cluster for an upgrade on AIX, Linux, Solaris, or Windows:

Before upgrading servers in a cluster of IBM Sametime Meeting Servers, prepare the cluster by stopping the Deployment Manager as well as servers running on each node.
About this task

All members of the cluster must be stopped before you upgrade any nodes.

Procedure

1. On each node in the cluster, open a command window and stop the following servers:

   **Note:** On each node, leave the WebSphere Application Server running so you can back up its configuration and validate the administrator credentials in the next task.

   a. Stop the Sametime Meeting Server:
      
      **AIX, Linux, Solaris:** ./stopServer.sh Meeting_Server_name -username WAS_admin_username -password WAS_admin_password
      
      **Windows:** stopServer.bat Meeting_Server_name -username WAS_admin_username -password WAS_admin_password

   b. If a WebSphere proxy server is hosted on this node, stop it now:
      
      **AIX, Linux, Solaris:** ./stopServer.sh WAS_proxy_server_name
      
      **Windows:** stopServer.bat WAS_proxy_server_name

   c. Stop the node agent:
      
      **AIX, Linux, Solaris:** ./stopNode.sh -username WAS_admin_username -password WAS_admin_password
      
      **Windows:** stopNode.bat -username WAS_admin_username -password WAS_admin_password

   d. Repeat for every node in the cluster.

2. On the server hosting the Deployment Manager, open a command window and stop the cluster's Deployment Manager:

   **AIX, Linux, Solaris:** ./stopManager.sh dmgr -username WAS_admin_username -password WAS_admin_password

   **Windows:** stopManager.bat dmgr -username WAS_admin_username -password WAS_admin_password

**Upgrading a Sametime 8.5 or 8.5.1 Meeting Server node on AIX, Linux, Solaris, or Windows:**

Upgrade a Sametime Meeting Server from 8.5 or 8.5.1.

**Upgrading a Sametime 8.5 Meeting Server node on AIX, Linux, Solaris, or Windows:**

Upgrade an IBM Sametime Meeting Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.

**Before you begin**

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:
• Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
• Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
• If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.15" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using **su** or a normal login session. Independent sudo packages are not supported on Solaris.
3. Download the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
   
   **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   **AIX**
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   ```bash
   mount -v cdrfs -or /dev/cd0 /cdrom
   ```

   **Linux**
   Mount the CD or DVD using a command similar to the following command:
   ```bash
   mount /dev/cdrom /cdrom
   ```

   **Solaris**
   Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris.** `./launchpad.sh`
   - **Windows** `launchpad.exe`

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

   ```bash
   sametime_server_package/IM/platform
   ```

   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language** list.

6. Click **Install IBM Sametime Meeting Server** and click **Launch IBM Sametime Meeting Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. Click **Update** to upgrade from a previous release.

9. Select the packages you want to upgrade, make sure that **Update All** is not selected, and then click **Next**.

   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

10. Click the **I accept the terms in the license agreements** option and click **Next**.

11. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

12. Enter the fully qualified Sametime System Console server host name.

   Do not use an IP address or short host name.
13. Enter the Sametime System Console user ID and password, then click **Validate**.

14. After the **Validate** button changes to **Validated**, click **Next**.

15. Click **Update**.

16. Click **Finish** when the installation process is complete.

17. Click **Exit** to close the Installation Manager.

18. If this is the Primary Node for a cluster and the Sametime System Console does **not** function as the cluster's Deployment Manager, copy the upgraded Sametime Meeting Server's EAR file to the System Console.

   If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

   a. Locate the meetingserver.ear file on the upgraded Sametime Meeting Server:

      install_root/SametimeMeetingServerOffering/SametimeServer/
      STMeeting/meeting/installableApps/meeting.server.ear

   b. Copy the file to the following location on the Sametime System Console:

      WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs; collectLogs is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var.ibm/InstallationManager/logs

**SSC connection log:**

/tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

**SSC connection log:**

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Upgrading a Sametime 8.5.1 Meeting Server node on AIX, Linux, Solaris, or Windows:**

Upgrade an IBM Sametime Meeting Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing the update over the existing product.
Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.15" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.
3. Download the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         &uid=swg24029128
Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX**, **Linux**, and **Solaris**. `/launchpad.sh`
- **Windows** `launchpad.exe`

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language** list.

6. Click **Install IBM Sametime Meeting Server** and click **Launch IBM Sametime Meeting Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

a. In the Installation Manager window, choose **File > Preferences**.
b. Uncheck **Search service repositories during installation and updates** and click OK.

9. Click **Update** to upgrade from a previous release.

10. Select the packages you want to upgrade, make sure that **Update All** is not selected, and then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Enter the fully qualified Sametime System Console server host name.

    Do not use an IP address or short host name.

14. Enter the Sametime System Console user ID and password, then click **Validate**.

15. After the **Validate** button changes to **Validated**, click **Next**.

16. Click **Update**.

17. Click **Finish** when the installation process is complete.

18. Click **Exit** to close the Installation Manager.

19. If this is the Primary Node for a cluster and the Sametime System Console does **not** function as the cluster's Deployment Manager, copy the upgraded Sametime Meeting Server's EAR file to the System Console.

    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

    a. Locate the meetingserver.ear file on the upgraded Sametime Meeting Server:

       ```
       install_root/SametimeMeetingServerOffering/SametimeServer/STMeeting/meeting/installableApps/meeting.server.ear
       ```

    b. Copy the file to the following location on the Sametime System Console:

       ```
       WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/>
       ```

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs; collectLogs is located at the root of the installation media.

**AIX, Linux, or Solaris**

```
/var.ibm/InstallationManager/logs
```

**SSC connection log:**

```
/tmp/SSCLogs/ConsoleUtility0.log
```

**Windows 2008**

```
%ALLUSERSPROFILE%\IBM\Installation Manager\logs
```
Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Starting servers in the upgraded Sametime Meeting Server cluster on AIX, Linux, Solaris, or Windows:

In an IBM Sametime deployment, start the servers in the upgraded cluster of Sametime Meeting Servers.

Before you begin

Upgrade all nodes in the cluster before you start the cluster.

Procedure

1. On the server hosting the Deployment Manager, open a command window and start the cluster's Deployment Manager:
   AIX, Linux, Solaris: ./startManager.sh dmgr
   Windows: startManager.bat dmgr
2. On each node in the cluster, open a command window and start the following servers:
   a. WebSphere Application Server should already be running, but if it is not, start it now:
      AIX, Linux, Solaris: ./startServer.sh server1
      Windows: startServer.bat server1
   b. Start the node agent:
      AIX, Linux, Solaris: ./startNode.sh
      Windows: startNode.bat
   c. If a WebSphere proxy server is hosted on this node, start it now:
      AIX, Linux, Solaris: ./startServer.sh WAS_proxy_server_name
      Windows: startServer.bat WAS_proxy_server_name
   d. Start the Sametime Meeting Server:
      AIX, Linux, Solaris: ./startServer.sh Meeting_Server_name
      Windows: startServer.bat Meeting_Server_name
   e. Repeat for every node in the cluster.

Upgrading Sametime 8.5 or 8.5.1 Media Manager on Linux or Windows

Follow the instructions for your operating system to upgrade one or more Sametime Media Manager servers running on Linux or Microsoft Windows.

Upgrading a stand-alone Sametime 8.5 or 8.5.1 Media Manager:

Upgrade a single IBM Sametime Media Manager server on Linux or Microsoft Windows. You can upgrade a server that contains all Media Manager components, or individual components residing on different computers.
About this task

The basic process for upgrading a server containing a single Media Manager component is the same as the process for upgrading a server containing all of the components; however you will need to complete an additional security configuration task for servers hosting individual components.

Upgrading a Sametime 8.5 or 8.5.1 Media Manager:

Upgrade a Sametime Media Manager from 8.5 or 8.5.1.

Upgrading a Sametime 8.5 Media Manager:

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- **Linux**: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- **Graphics libraries** must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

**AIX, Linux, and Solaris**: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Use these instructions to upgrade any of the following Sametime Media Manager deployments:

- A stand-alone or a clustered Conference Manager component
- A stand-alone or a clustered SIP Proxy and Registrar component
- A Packet Switcher component
- All three Media Manager components installed on a single computer

The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   
   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the installation package for the Sametime Media Manager.

   a. To download installation packages:
      
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

      2) Open this release’s Download document at the following web address:
         &uid=swg24029128

         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C: and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

      **AIX**

      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

      `mount -v cdrfs -o ro /dev/cd0 /cdrom`

      **Linux**

      Mount the CD or DVD using a command similar to the following command:

      `mount /dev/cdrom /cdrom`

      **Solaris**

      Mount the CD or DVD manually.

4. **Linux only:** If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), you will need to mount the CD or DVD manually.
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

See your operating system's documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX, Linux, and Solaris**: `./launchpad.sh`
- **Windows**: `launchpad.exe`

**Note**: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (`install` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

6. If necessary, select a language other than English from the **Select a language** list.

7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

9. Click **Update** to upgrade from a previous release.

10. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Enter the fully qualified Sametime System Console server host name. Do not use an IP address or short host name.

14. Enter the Sametime System Console user ID and password, then click **Validate**.

15. After the **Validate** button changes to **Validated**, click **Next**.

16. Click **Update**.

17. Click **Finish** when the installation process is complete.

18. Click **Exit** to close the Installation Manager.

19. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console.

    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

   a. Locate the appropriate files on the upgraded server:
      - Conference Manager cluster's Primary Node:
install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ConferenceFocus.ear

- SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
  - install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ProxyAppl-8.5.2.ear
  - install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarAppl-8.5.2.ear

b. Copy the files to the following location on the Sametime System Console:

WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs; collectLogs is located at the root of the installation media.

Linux

/var.ibm/InstallationManager/logs

SSC connection log:

tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Upgrading a Sametime 8.5.1 Media Manager:

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:
• Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).

• Graphics libraries must be installed in the operating system so that Installation Manager can function properly.

• If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version “7.0.0.9” (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

Use these instructions to upgrade any of the following Sametime Media Manager deployments:
• A stand-alone or a clustered Conference Manager component
• A stand-alone or a clustered SIP Proxy and Registrar component
• A Packet Switcher component
• All three Media Manager components installed on a single computer

The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the installation package for the Sametime Media Manager.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
Locate the components that you need in the document's listing, then
download the packages labelled with the corresponding part numbers
to the system on which you are installing.

Tip: When extracting downloads on Windows operating systems, use a
short path location such as C:\ and not a long path location such as
the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:

```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following
command:

```bash
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. **Linux only:** If you are installing from physical media and your operating
system mounts CDs or DVDs automatically with execution privileges turned
off (such as on some Linux distributions), you will need to mount the CD or
DVD manually.

Mount the CD or DVD using a command similar to the following command:

```bash
mount /dev/cdrom /cdrom
```

See your operating system's documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the
installation program by running one of the following commands:

- **AIX, Linux, and Solaris:** `./launchpad.sh`
- **Windows:** `launchpad.exe`

**Note:** If you do not have a web browser, go to the Installation Manager
package directory and run the installation program (**install** for Linux or
**install**.exe for Windows). Find the Installation Manager package directory
here:

```
sametime_server_package/IM/platform
```

**sametime_server_package** is the installation package name for this server.

**platform** is the operating system on which you are installing.

6. If necessary, select a language other than English from the **Select a language**
list.
7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

If you do not see a prompt, continue to the next step.

9. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose **File > Preferences**.
   
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

10. Click **Update** to upgrade from a previous release.

11. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

12. Click the **I accept the terms in the license agreements** option and click **Next**.

13. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

14. Enter the fully qualified Sametime System Console server host name.

   Do not use an IP address or short host name.

15. Enter the Sametime System Console user ID and password, then click **Validate**.

16. After the **Validate** button changes to **Validated**, click **Next**.

17. Click **Update**.

18. Click **Finish** when the installation process is complete.

19. Click **Exit** to close the Installation Manager.

20. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console.

   If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

   a. Locate the appropriate files on the upgraded server:

      - Conference Manager cluster's Primary Node:
        
        `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ConferenceFocus.ear`

      - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
        
        `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ProxyAppl-8.5.2.ear`
        
        `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarAppl-8.5.2.ear`

   b. Copy the files to the following location on the Sametime System Console:

   
   `WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/`
Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs; collectLogs is located at the root of the installation media.

Linux

/var.ibm/InstallationManager/logs

SSC connection log:
/tmp/SSCLogs/ConsoleUtility0.log

Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Enabling ports for Transport Layer encryption for an upgraded Sametime Media Manager:

After upgrading an IBM Sametime Media Manager, edit settings in the stavconfig.xml file to specify secure ports for TLS encryption. Do this only if all clients are running 8.5.1 or later; otherwise older clients cannot connect to the upgraded Media Manager.

Before you begin

Make a note of the values you need to transfer to stavconfig.xml from the SIP/Proxy Registrar, Conference Manager, and Packet Switcher servers. Open the WebSphere Application Server Integrated Solutions Console for each server and click Application servers > STMediaServer > Ports.

Find the values for a non-clustered or clustered environment.

Non-clustered environment

- SIP/Proxy Registrar
  
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE

- Conference Manager

  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

- Packet Switcher

  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
Clustered environment

- **SIP/Proxy Registrar**
  - SIP_ProxyRegHOST/SIP_ProxyRegSECURE
  - (Clustered node) WebSphere Application Server proxy host
  - (Clustered node) WebSphere Application Server proxy secure port

- **Conference Manager**
  - SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
  - (Clustered node) WebSphere Application Server proxy host
  - (Clustered node) WebSphere Application Server proxy secure port

- **Packet Switcher**
  - SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

About this task

The default settings in the stavconfig.xml file specify non-secure ports and must be modified for use with TLS encryption. Edit the stavconfig.xml files on the Conference Manager and Packet Switcher to reflect this update by changing the non-secure ports to secure ports. Follow these steps on both machines. This file is not used by the SIP Proxy and Registrar.

Follow these steps to update the stavconfig.xml file for every instance of the Media Manager components. When multiple profiles are installed on the same computer, each profile uses its own copy of the file and requires the updates.

Procedure

1. Log in to the Integrated Solutions Console for the machine.
2. On the server hosting the Conference Manager, Packet Switcher, or SIP Proxy and Registrar, navigate to the following directory:
   \dm_install_root\config\cells\cell_name\nodes\node_name\servers\server_name
3. In a text editor, open the stavconfig.xml file.
4. Modify the following settings:
   - The ConferenceServerPort setting should contain the SIP_DEFAULTHOST_SECURE port value from the Conference Manager server.
   - The SIPProxyServerPort setting should contain the SIP_ProxyRegSECURE port value from the SIP Proxy/Registrar server.
   - The port setting in the [packetswitches] section should contain the SIP_DEFAULTHOST_SECURE port value from the Packet Switcher server.
   - **Clustered environment only**: Change the SIPProxyServerTransportProtocol setting value to TLS.
5. (Packet Switcher only) Add these three attributes if they are missing.
   <configuration lastUpdated="1226425838277" name="IsEncryptedConferenceEnabled" value="false"/></configuration>
   <configuration lastUpdated="1226425838277" name="AudioRTCPEnabled" value="false"/></configuration>
   <configuration lastUpdated="1226425838277" name="VideoRTCPEnabled" value="true"/></configuration>

   **Note:** If you have Sametime 8.5.0 clients in your environment, set the third attribute for "VideoRTCPEnabled" to "false" instead.
6. **(Clustered environment only)**
   Make these additional changes in the file if you are configuring on a clustered node server.
Conference Manager node

- SIPProxyServerHost field
  SIP Proxy/Registrar WAS proxy host

- SIPProxyServerPort field
  SIP Proxy/Registrar WAS proxy secure port

Packet Switcher node

- SIPProxyServerHost field
  SIP Proxy/Registrar WebSphere Application Server proxy host

- SIPProxyServerPort field
  SIP Proxy/Registrar WebSphere Application Server proxy secure port

- ConferenceServerHost field
  Conference Manager WebSphere Application Server proxy host

- ConferenceServerPort field
  Conference Manager WebSphere Application Server proxy secure port

7. Close and save the updated file.
8. Synchronize all nodes in the Deployment Manager that manages the component.
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Click Full Resynchronize.

Results

Communications will now take place over the secure ports. If you later switch back to (nonencrypted) TCP or UDP transport protocol, you must change the port settings back to their original values. For SIP transport, you should use either TLS or TCP transport protocols.

Upgrading a cluster of Conference Manager components on Linux or Windows:

Upgrade a cluster of IBM Sametime Media Manager Conference Manager components running on Linux or Microsoft Windows. Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

About this task

Upgrading a cluster of Conference Manager components requires you to stop the Deployment Manager and all nodes in the cluster before upgrading the individual servers. After the individual nodes have been upgraded, you will start the cluster and complete its configuration by running the clustering guided activity.

Note: Remember to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Preparing the Conference Manager cluster for an upgrade on Linux or Windows:

Before upgrading servers in a cluster of IBM Sametime Conference Manager components, prepare the cluster by stopping the Deployment Manager as well as servers running on each node.
About this task

All members of the cluster must be stopped before you upgrade any nodes.

Procedure

1. On each node in the cluster, open a command window and stop the following servers:

   **Note:** Leave the WebSphere Application Server itself running.
   a. Stop the Conference Manager:
      - **Linux:** `./stopServer.sh Conference_Manager_name -username WAS_admin_username -password WAS_admin_password`
      - **Windows:** `stopServer.bat Conference_Manager_name -username WAS_admin_username -password WAS_admin_password`
   b. If a WebSphere proxy server is hosted on this node, stop it now:
      - **Linux:** `./stopServer.sh WAS_proxy_server_name`
      - **Windows:** `stopServer.bat WAS_proxy_server_name`
   c. Stop the node agent:
      - **Linux:** `./stopNode.sh -username WAS_admin_username -password WAS_admin_password`
      - **Windows:** `stopNode.bat -username WAS_admin_username -password WAS_admin_password`
   d. Repeat for every node in the cluster.

2. On the server hosting the Deployment Manager, open a command window and stop the cluster’s Deployment Manager:

   **Linux:** `./stopManager.sh dmgr -username WAS_admin_username -password WAS_admin_password`
   **Windows:** `stopManager.bat dmgr -username WAS_admin_username -password WAS_admin_password`

**Upgrading an 8.5 or 8.5.1 Conference Manager node:**

Upgrade a Sametime Media Manager from 8.5 or 8.5.1.

**Upgrading an 8.5 Conference Manager node:**

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

**Before you begin**

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- **Linux:** The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
Graphics libraries must be installed in the operating system so that Installation Manager can function properly.

If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**About this task**

Use these instructions to upgrade any of the following Sametime Media Manager deployments:

- A stand-alone or a clustered Conference Manager component
- A stand-alone or a clustered SIP Proxy and Registrar component
- A Packet Switcher component
- All three Media Manager components installed on a single computer

The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

**Procedure**

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   
   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the installation package for the Sametime Media Manager.
   
   a. To download installation packages:
      
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      
      2) Open this release's Download document at the following web address:
         
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```bash
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following command:

```bash
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. **Linux only**: If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), you will need to mount the CD or DVD manually.

   Mount the CD or DVD using a command similar to the following command:

   ```bash
   mount /dev/cdrom /cdrom
   ```

   See your operating system's documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**: `./launchpad.sh`
   - **Windows**: `launchpad.exe`

   **Note**: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (`install` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

   ```
   sametime_server_package/IM/platform
   ```

   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

6. If necessary, select a language other than English from the **Select a language** list.

7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.
9. Click **Update** to upgrade from a previous release.

10. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Enter the fully qualified Sametime System Console server host name.

    Do not use an IP address or short host name.

14. Enter the Sametime System Console user ID and password, then click **Validate**.

15. After the **Validate** button changes to **Validated**, click **Next**.

16. Click **Update**.

17. Click **Finish** when the installation process is complete.

18. Click **Exit** to close the Installation Manager.

19. If this is the Primary Node for a cluster and the Sametime System Console does not function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console.

    If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

    a. Locate the appropriate files on the upgraded server:

        - Conference Manager cluster's Primary Node:
          
            ```
            install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ConferenceFocus.ear
            ```

        - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
          
            ```
            install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ProxyAppl-8.5.2.ear
            install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarAppl-8.5.2.ear
            ```

    b. Copy the files to the following location on the Sametime System Console:

        ```
        WAS_install_root/AppServer/profiles/STSCMgrProfile/config/temp/
        ```

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the **ant** and **native** subdirectories.

You can use the **collectLogs** utility to gather the logs; **collectLogs** is located at the root of the installation media.

**Linux**

```
/var.ibm/InstallationManager/logs
```

**SSC connection log:**

```
/tmp/SSCLogs/ConsoleUtility0.log
```
Windows 2008

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Windows 2003

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

SSC connection log:

Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Upgrading an 8.5.1 Conference Manager node:

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Use these instructions to upgrade any of the following Sametime Media Manager deployments:

- A stand-alone or a clustered Conference Manager component
- A stand-alone or a clustered SIP Proxy and Registrar component
- A Packet Switcher component
- All three Media Manager components installed on a single computer

The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:

1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure
1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent `sudo` packages are not supported on Solaris.
3. Download the installation package for the Sametime Media Manager.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      ```bash
      mount -v cdrfs -o ro /dev/cd0 /cdrom
      ```
      **Linux**
      Mount the CD or DVD using a command similar to the following command:
      ```bash
      mount /dev/cdrom /cdrom
      ```
      **Solaris**
      Mount the CD or DVD.
4. **Linux only:** If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), you will need to mount the CD or DVD manually.

   Mount the CD or DVD using a command similar to the following command:

   ```
   mount /dev/cdrom /cdrom
   ```

   See your operating system's documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

   - **AIX, Linux, and Solaris**
     ```
     ./launchpad.sh
     ```
   - **Windows**
     ```
     launchpad.exe
     ```

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

   ```
   sametime_server_package/IM/platform
   ```

   *sametime_server_package* is the installation package name for this server.
   *platform* is the operating system on which you are installing.

6. If necessary, select a language other than English from the **Select a language** list.

7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

9. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose **File > Preferences**.
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

10. Click **Update** to upgrade from a previous release.

11. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

   The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

12. Click the **I accept the terms in the license agreements** option and click **Next**.

13. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

14. Enter the fully qualified Sametime System Console server host name.

   Do not use an IP address or short host name.

15. Enter the Sametime System Console user ID and password, then click **Validate**.

16. After the **Validate** button changes to **Validated**, click **Next**.

17. Click **Update**.
18. Click **Finish** when the installation process is complete.
19. Click **Exit** to close the Installation Manager.
20. If this is the Primary Node for a cluster and the Sametime System Console does **not** function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console.
   If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.
   a. Locate the appropriate files on the upgraded server:
      - Conference Manager cluster's Primary Node:
        ```
        install_root/SametimeMediaServerOffering/SametimeServer/media/installableApps/ConferenceFocus.ear
        ```
      - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
        ```
        install_root/SametimeMediaServerOffering/SametimeServer/media/installableApps/ProxyAppl-8.5.2.ear
        install_root/SametimeMediaServerOffering/SametimeServer/media/installableApps/RegistrarAppl-8.5.2.ear
        ```
   b. Copy the files to the following location on the Sametime System Console:
      ```
      WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
      ```

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the `logs` directory and the `ant` and `native` subdirectories.

You can use the `collectLogs` utility to gather the logs; `collectLogs` is located at the root of the installation media.

**Linux**

```
/var.ibm/InstallationManager/logs
```

**SSC connection log:**

```
/tmp/SSCLogs/ConsoleUtility0.log
```

**Windows 2008**

```
%ALLUSERSPROFILE%\IBM\Installation Manager\logs
```

**Windows 2003**

```
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
```

**SSC connection log:**

```
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log
```

*Enabling ports for Transport Layer encryption for an upgraded Conference Manager:*
After upgrading an IBM Sametime Media Manager, edit settings in the
stavconfig.xml file to specify secure ports for TLS encryption. Do this only if all
clients are running 8.5.1 or later; otherwise older clients cannot connect to the
upgraded Media Manager.

Before you begin

Make a note of the values you need to transfer to stavconfig.xml from the
SIP/Proxy Registrar, Conference Manager, and Packet Switcher servers. Open the
WebSphere Application Server Integrated Solutions Console for each server and
click Application servers > STMediaServer > Ports.

Find the values for a non-clustered or clustered environment.

Non-clustered environment

- SIP/Proxy Registrar
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE
- Conference Manager
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
- Packet Switcher
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

Clustered environment

- SIP/Proxy Registrar
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE
    (Clustered node) WebSphere Application Server proxy host
    (Clustered node) WebSphere Application Server proxy secure port
- Conference Manager
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
    (Clustered node) WebSphere Application Server proxy host
    (Clustered node) WebSphere Application Server proxy secure port
- Packet Switcher
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

About this task

The default settings in the stavconfig.xml file specify non-secure ports and must
be modified for use with TLS encryption. Edit the stavconfig.xml files on the
Conference Manager and Packet Switcher to reflect this update by changing the
non-secure ports to secure ports. Follow these steps on both machines. This file is
not used by the SIP Proxy and Registrar.

Follow these steps to update the stavconfig.xml file for every instance of the Media
Manager components. When multiple profiles are installed on the same computer,
each profile uses its own copy of the file and requires the updates.

Procedure

1. Log in to the Integrated Solutions Console for the machine.
2. On the server hosting the Conference Manager, Packet Switcher, or SIP Proxy
   and Registrar, navigate to the following directory:
   
   $dm_install_root/config/cells/cell_name/nodes/node_name/servers/server_name

Chapter 12. Migrating and upgrading  679
3. In a text editor, open the stavconfig.xml file.

4. Modify the following settings:
   - The ConferenceServerPort setting should contain the SIP_DEFAULTHOST_SECURE port value from the Conference Manager server.
   - The SIPProxyServerPort setting should contain the SIP_ProxyRegSECURE port value from the SIP Proxy/Registrar server.
   - The port setting in the [packetswitches] section should contain the SIP_DEFAULTHOST_SECURE port value from the Packet Switcher server.
   - **Clustered environment only**: Change the SIPProxyServerTransportProtocol setting value to TLS.

5. (Packet Switcher only) Add these three attributes if they are missing.
   ```xml
   <configuration lastUpdated="1226425838277" name="IsEncryptedConferenceEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="AudioRTCPEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="VideoRTCPEnabled" value="true"/>
   
   **Note:** If you have Sametime 8.5.0 clients in your environment, set the third attribute for "VideoRTCPEnabled" to "false" instead.

6. **(Clustered environment only)**
   Make these additional changes in the file if you are configuring on a clustered node server.

   **Conference Manager node**
   - **SIPProxyServerHost field**
     SIP Proxy/Registrar WAS proxy host
   - **SIPProxyServerPort field**
     SIP Proxy/Registrar WAS proxy secure port

   **Packet Switcher node**
   - **SIPProxyServerHost field**
     SIP Proxy/Registrar WebSphere Application Server proxy host
   - **SIPProxyServerPort field**
     SIP Proxy/Registrar WebSphere Application Server proxy secure port
   - **ConferenceServerHost field**
     Conference Manager WebSphere Application Server proxy host
   - **ConferenceServerPort field**
     Conference Manager WebSphere Application Server proxy secure port

7. Close and save the updated file.

8. Synchronize all nodes in the Deployment Manager that manages the component.
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   b. Click **Full Resynchronize**.

**Results**

Communications will now take place over the secure ports. If you later switch back to (nonencrypted) TCP or UDP transport protocol, you must change the port settings back to their original values. For SIP transport, you should use either TLS or TCP transport protocols.
Starting servers in the upgraded Conference Manager cluster:

In an IBM Sametime deployment, start the servers in the upgraded cluster of Conference Manager components.

Before you begin

Upgrade all nodes in the cluster before you start the cluster.

Procedure

1. On the server hosting the Deployment Manager, open a command window and start the cluster's Deployment Manager:
   - Linux: ./startManager.sh dmgr
   - Windows: startManager.bat dmgr

2. On each node in the cluster, open a command window and start the following servers:
   a. WebSphere Application Server should already be running, but if it is not, start it now:
      - Linux: ./startServer.sh server1
      - Windows: startServer.bat server1
   b. Start the node agent:
      - Linux: ./startNode.sh
      - Windows: startNode.bat
   c. If a WebSphere proxy server is hosted on this node, Start it now:
      - Linux: ./startServer.sh WAS_proxy_server_name
      - Windows: startServer.bat WAS_proxy_server_name
   d. Start the Sametime Meeting Server:
      - Linux: ./startServer.sh Conference_Manager_name
      - Windows: startServer.bat Conference_Manager_name
   e. Repeat for every node in the cluster.

Upgrading a cluster of SIP Proxy and Registrar components on Linux or Windows:

Upgrade a cluster of IBM Sametime Media Manager SIP Proxy and Registrar components running on Linux or Microsoft Windows. Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

About this task

Upgrading a cluster of SIP Proxy and Registrar components requires you to stop the Deployment Manager and all nodes in the cluster before upgrading the individual servers. After the individual nodes have been upgraded, you will start the cluster and complete its configuration by running the clustering guided activity.

Note: Remember to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Preparing the SIP Proxy and Registrar cluster for an upgrade on Linux or Windows:
Before upgrading servers in a cluster of IBM Sametime SIP Proxy and Registrar components, prepare the cluster by stopping the Deployment Manager as well as servers running on each node.

**About this task**

All members of the cluster must be stopped before you upgrade any nodes.

**Procedure**

1. On each node in the cluster, open a command window and stop the following servers:

   **Note:** Leave the WebSphere Application Server itself running.
   a. Stop the SIP Proxy and Registrar:
      - **Linux:** `/stopServer.sh SIP_Proxy_and_Registrar_name -username WAS_admin_username -password WAS_admin_password`
      - **Windows:** `stopServer.bat SIP_Proxy_and_Registrar_name -username WAS_admin_username -password WAS_admin_password`
   b. If a WebSphere proxy server is hosted on this node, stop it now:
      - **Linux:** `/stopServer.sh WAS_proxy_server_name`
      - **Windows:** `stopServer.bat WAS_proxy_server_name`
   c. Stop the node agent:
      - **Linux:** `/stopNode.sh -username WAS_admin_username -password WAS_admin_password`
      - **Windows:** `stopNode.bat -username WAS_admin_username -password WAS_admin_password`
   d. Repeat for every node in the cluster.

2. On the server hosting the Deployment Manager, open a command window and stop the cluster's Deployment Manager:

   - **Linux:** `/stopManager.sh dmgr -username WAS_admin_username -password WAS_admin_password`
   - **Windows:** `stopManager.bat dmgr -username WAS_admin_username -password WAS_admin_password`

**Upgrading an 8.5 or 8.5.1 SIP Proxy and Registrar node:**

Upgrade a Sametime Media Manager from 8.5 or 8.5.1.

**Upgrading an 8.5 SIP Proxy and Registrar node:**

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

**Before you begin**

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:
Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).

Graphics libraries must be installed in the operating system so that Installation Manager can function properly.

If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Use these instructions to upgrade any of the following Sametime Media Manager deployments:

- A stand-alone or a clustered Conference Manager component
- A stand-alone or a clustered SIP Proxy and Registrar component
- A Packet Switcher component
- All three Media Manager components installed on a single computer

The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure

1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.

   For more information, see the backupConfig command in the WebSphere Application Server information center.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.

3. Download the installation package for the Sametime Media Manager.

   a. To download installation packages:

      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

      2) Open this release's Download document at the following web address:
Locate the components that you need in the document’s listing, then download the packages labeled with the corresponding part numbers to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. **Linux only:** If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), you will need to mount the CD or DVD manually.

Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

See your operating system’s documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX, Linux, and Solaris**
  ```
  ./launchpad.sh
  ```
- **Windows**
  `launchpad.exe`

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (``install`` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

6. If necessary, select a language other than English from the **Select a language** list.
7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

9. Click **Update** to upgrade from a previous release.

10. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

13. Enter the fully qualified Sametime System Console server host name. Do not use an IP address or short host name.

14. Enter the Sametime System Console user ID and password, then click **Validate**.

15. After the **Validate** button changes to **Validated**, click **Next**.

16. Click **Update**.

17. Click **Finish** when the installation process is complete.

18. Click **Exit** to close the Installation Manager.

19. If this is the Primary Node for a cluster and the Sametime System Console does **not** function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console.

   If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.

   a. Locate the appropriate files on the upgraded server:
      
      - Conference Manager cluster's Primary Node:
        
        ```
        install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/
        installableApps/ConferenceFocus.ear
        ```
      
      - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
        
        ```
        install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/
        installableApps/ProxyAppl-8.5.2.ear
        install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/
        installableApps/RegistrarAppl-8.5.2.ear
        ```
      
   b. Copy the files to the following location on the Sametime System Console:
      
      ```
      WAS_install_root/AppServer/profiles/STSCDMgrProfile/config/temp/
      ```

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the `logs` directory and the `ant` and `native` subdirectories.

You can use the `collectLogs` utility to gather the logs; `collectLogs` is located at the root of the installation media.
Upgrading an 8.5.1 SIP Proxy and Registrar node:

Upgrade an IBM Sametime Media Manager server or one of its components running on Linux or Windows by installing the update over the existing product.

Before you begin

Stop all of the Sametime servers in the deployment to prevent users from using the system during the upgrade. Leave WebSphere Application Server running. For more information, see the Command reference for starting and stopping servers in this information center.

Make sure your server meets the following requirements:

- Linux: The launchpad install program needs to be able to launch a web browser. You will need to work directly on the console or have an X server and a web browser installed and configured (VNC or a remote X term session will work as well).
- Graphics libraries must be installed in the operating system so that Installation Manager can function properly.
- If the IBM WebSphere Update Installer is already installed on this server, it must reside in a directory named lower than version "7.0.0.9" (install_root/IBM/WebSphere/UpdateInstaller/7.0.0.x) to ensure that the installation program can function properly.

AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

Use these instructions to upgrade any of the following Sametime Media Manager deployments:

- A stand-alone or a clustered Conference Manager component
- A stand-alone or a clustered SIP Proxy and Registrar component
- A Packet Switcher component
- All three Media Manager components installed on a single computer
The deployment plan used for the original installation determines which components are upgraded.

Upgrade cluster components in the following order:
1. Deployment Manager (if the Sametime System Console is not serving as the Deployment Manager)
2. Primary Node
3. Secondary Nodes

Be sure to upgrade all nodes in the cluster because Sametime does not support clusters in which nodes are running different versions of the product.

Procedure
1. Back up the WebSphere Application Server configuration so that you can roll it back if you need to cancel the upgrade.
   For more information, see the backupConfig command in the WebSphere Application Server information center.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.
3. Download the installation package for the Sametime Media Manager.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.
         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user’s desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.
   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.
      **AIX**
      Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
      `mount -v cdrfs -o ro /dev/cd0 /cdrom`
      **Linux**
      Mount the CD or DVD using a command similar to the following command:
mount /dev/cdrom /cdrom

Solaris
Mount the CD or DVD.

4. **Linux only:** If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off (such as on some Linux distributions), you will need to mount the CD or DVD manually.

Mount the CD or DVD using a command similar to the following command:
mount /dev/cdrom /cdrom

See your operating system's documentation for instructions.

5. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - AIX, Linux, and Solaris: `./launchpad.sh`
   - Windows: `launchpad.exe`

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (`install` for Linux or `install.exe` for Windows). Find the Installation Manager package directory here:

   `sametime_server_package/IM/platform`

   `sametime_server_package` is the installation package name for this server.
   
   `platform` is the operating system on which you are installing.

6. If necessary, select a language other than English from the Select a language list.

7. Click **Install IBM Lotus Sametime Media Manager** and click **Launch IBM Sametime Media Manager 8.5.2 installation**.

8. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

9. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.
   
   a. In the Installation Manager window, choose **File > Preferences**.
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

10. Click **Update** to upgrade from a previous release.

11. Select the package you want to update and make sure that **Update all** is not selected; then click **Next**.

    The **Update All** option does not work as expected and may cause the upgrade to fail, so IBM recommends that you do not use it.

12. Click the **I accept the terms in the license agreements** option and click **Next**.

13. Validate the WebSphere Application Server administrator ID and password, and then click **Next**.

14. Enter the fully qualified Sametime System Console server host name. Do not use an IP address or short host name.
15. Enter the Sametime System Console user ID and password, then click **Validate**.
16. After the **Validate** button changes to **Validated**, click **Next**.
17. Click **Update**.
18. Click **Finish** when the installation process is complete.
19. Click **Exit** to close the Installation Manager.
20. If this is the Primary Node for a cluster and the Sametime System Console does *not* function as the cluster's Deployment Manager, copy the upgraded component server's EAR file to the System Console. If this server is not the cluster's Primary Node or the cluster uses the Sametime System Console as its Deployment Manager, skip this step.
   a. Locate the appropriate files on the upgraded server:
      - Conference Manager cluster's Primary Node:
        - `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ConferenceFocus.ear`
      - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
        - `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/ProxyAppl-8.5.2.ear`
        - `install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarAppl-8.5.2.ear`
   b. Copy the files to the following location on the Sametime System Console:
      - `WAS_install_root/AppServer/profiles/STSCMgrProfile/config/temp/`

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the `logs` directory and the `ant` and `native` subdirectories.

You can use the `collectLogs` utility to gather the logs; `collectLogs` is located at the root of the installation media.

**Linux**

```
/var.ibm/InstallationManager/logs
```

**SSC connection log:**

```
/tmp/SSCLogs/ConsoleUtility0.log
```

**Windows 2008**

```
%ALLUSERSPROFILE%\IBM\Installation Manager\logs
```

**Windows 2003**

```
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
```

**SSC connection log:**

```
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log
```
Starting servers in the upgraded SIP Proxy and Registrar cluster:

In an IBM Sametime deployment, start the servers in the upgraded cluster of SIP Proxy and Registrar components.

Before you begin

Upgrade all nodes in the cluster before you start the cluster.

Procedure

1. On the server hosting the Deployment Manager, open a command window and start the cluster's Deployment Manager:
   Linux: ./startManager.sh dmgr
   Windows: startManager.bat dmgr
2. On each node in the cluster, open a command window and start the following servers:
   a. WebSphere Application Server should already be running, but if it is not, start it now:
      Linux: ./startServer.sh server1
      Windows: startServer.bat server1
   b. Start the node agent:
      Linux: ./startNode.sh
      Windows: startNode.bat
   c. If a WebSphere proxy server is hosted on this node, Start it now:
      Linux: ./startServer.sh WAS_proxy_server_name
      Windows: startServer.bat WAS_proxy_server_name
   d. Start the Sametime Meeting Server:
      Linux: ./startServer.sh SIP_Proxy_and_Registrar_name
      Windows: startServer.bat SIP_Proxy_and_Registrar_name
   e. Repeat for every node in the cluster.

Configuring Transport Layer security for the upgraded Sametime Media Manager:

Configuring the IBM Media Manager SIP Proxy and Registrar component to use SIP authentication and authorization requires some additional steps.

About this task

Follow the instructions in this section to configure Transport Layer Security (TLS) if you chose it as the encryption protocol and to set up user authentication.

Distributing certificates for Transport Layer encryption to all upgraded Media Manager components:

If you installed Media Manager components on separate machines or as separate cell profiles, you must extract the signed security certificate from the SIP Proxy and Registrar server. Then add the certificate to all Conference Manager and Packet Switcher servers. This step does not apply if you installed all components of the media manager on the same cell profile.
Before you begin

Extract the certificate used by the SIP Proxy and Registrar and copy it to a location from which each Media Manager component can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the SIP Proxy and Registrar certificate.

2. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   - In a non-clustered environment, the certificate is on the same machine as the SIP Proxy and Registrar component.
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the SIP Proxy and Registrar.

3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.

4. Type a unique file name for the signed certificate.

5. Copy the extracted certificate to a location from which the Media Manager component can retrieve the file.

About this task

Follow these steps to add a signed certificate to each Media Manager component.

Procedure

1. Log in to the Media Manager component’s Integrated Solutions Console.

2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.

   Note: If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.

3. Click Add.

4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.

5. In the File name field, type the path to the certificate file; for example: c:\sip-pr.cer

6. Click OK.

7. Click Save.

8. Restart the server.

9. Repeat these steps for each Media Manager component.

Distributing certificates for Transport Layer encryption to the upgraded SIP Proxy and Registrar:

If you installed the SIP Proxy and Registrar on separate machines or as a separate cell profile from the other IBM Sametime Media Manager components, you must extract the signed security certificate from the Conference Manager and Packet Switcher components and add the certificates to the SIP Proxy and Registrar. This step does not apply if you installed all components of the Sametime Media Manager and SIP Proxy and Registrar on the same cell profile.
Before you begin

Extract the certificate used by each Conference Manager and Packet Switcher component and copy it to a location from which the SIP Proxy and Registrar can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Manager certificate.
2. Click Security > SSL Certificates and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   - In a non-clustered environment, the certificate is on the same machine as the Sametime Media Manager component (Conference Manager or Packet Switcher)
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.

   Note: The Packet Switcher does not run in a cluster.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the SIP Proxy and Registrar component can retrieve the file.
6. Repeat this procedure for the Packet Switcher.

About this task

Follow these steps to add from the Conference Manager and Packet Switcher components the signed certificates to the SIP Proxy and Registrar.

Procedure

1. Log in to the SIP Proxy and Registrar component's Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.

   Note: If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.
3. Click Add.
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example:
   c:\cm-pr.cer or c:\ps-pr.cer
6. Click OK.
7. Click Save.
8. Restart the server.
9. Repeat these steps for each Media Manager component.

Exchanging certificates between the upgraded Packet Switcher and the upgraded Conference Manager:

The Packet Switcher component of the IBM Sametime Media Manager opens a TLS connection to the Conference Manager, so you need to exchange certificates
between the Packet Switcher and the Conference Manager. You must extract the certificate used by the Conference Manager and then add this certificate to the Packet Switcher.

**Before you begin**

Extract the certificate used by the Conference Manager component and copy it to a location from which the Packet Switcher component can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Focus certificate.
2. Click **Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.**
   - In a non-clustered environment, the certificate is on the same machine as the Conference Manager component.
   - In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the Packet Switcher component can retrieve the file.

**About this task**

Follow these steps to add a signed certificate to the Packet Switcher.

**Procedure**

1. Log in to the Packet Switcher component’s Integrated Solutions Console.
2. Click **Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.**
   - **Note:** If **CellDefaultTrustStore** is not in the table then choose **NodeDefaultTrustStore**.
3. Click **Add.**
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example:
   - c:\conf-focus.cer
6. Click **OK.**
7. Click **Save.**
8. Restart the server.

*Adding trusted IP addresses to the upgraded SIP Proxy and Registrar:*

The Sametime SIP Proxy and Registrar accepts connections from the Sametime Media Manager components – Conference Manager and Packet Switcher. To ensure that the SIP Proxy and Registrar trusts these components when they establish a connection, you must add a custom SIP container property that uses the IP address or fully qualified domain name for these trusted components as its value.
About this task

Complete these steps for each server in a Sametime SIP Proxy and Registrar cluster or for every SIP Proxy/Registrar in a multiple-server deployment.

Procedure

1. Log in to the Sametime Media Manager's Integrated Solutions Console.
   If you installed the SIP Proxy/Registrar component on a separate server, log in to the SIP Proxy and Registrar's Integrated Solutions Console.
2. Click Servers > Server Types > WebSphere Application Servers.
3. Click the name of the Media Manager server.
   In a clustered environment, click the name of a cluster member.
4. Under Container settings, click SIP Container Settings > SIP container.
5. Click Custom Properties.
6. Add this new property if it does not exist:
   com.ibm.ws.sip.security.trusted.iplist
7. Add the Conference Manager and Packet Switcher as trusted IP addresses.
   Use commas to separate multiple values if you are using multiple servers.
   In a non-clustered environment, use the servers' IP addresses or fully qualified domain names.

   Note: If the Conference Manager operates in a cluster, use the IP address or fully qualified domain name for the WebSphere Application Server proxy used by the Conference Manager cluster instead.
8. Click OK.
9. Click Save.
10. Restart the Sip Proxy and Registrar server.

Upgrading policies from Release 8.5 or 8.5.1

Changes in the way policies are defined on the backend require you to take steps after upgrading the servers to ensure that your IBM Sametime Release 8.5 or 8.5.1 policies work with the new design.

Before you begin

Before following the steps in this procedure, you must have completed these required upgrades:

• Upgrade the Community Server, Proxy Server, and Meeting Server to Release 8.5.1.1.
• Upgrade the Sametime System Console to this release.
• Then upgrade the Community Server, Proxy Server, and Meeting Server to this release.
• Also upgrade the Media Manager to this release if appropriate.

About this task

Upgrade policies by working with the Manage Policies page and the LDAP deployment in the Sametime System Console.
Procedure
1. Log in to the Sametime System Console.
2. On the Manage Policies page, click **Upgrade Policies**.
3. Upgrade the LDAP deployment for each LDAP directory that you connected to the Sametime System Console:
   a. Expand **Sametime Prerequisites** and click **Connect to LDAP Servers**.
   b. Select the LDAP deployment to be upgraded and click **Edit**.
   c. Click **Next** and continue through the deployment pages. You do not need to make any changes unless you made changes through the Advanced LDAP configuration. If you did make changes, check that the values are correct.
   d. Click **Finish** to complete the upgrade.
   e. Repeat these steps if you have more than one LDAP deployment.
4. Restart the Deployment Manager.
5. Return to the console Manage Policies page and click **Verify Policy Assignments**.
   a. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime Community Server.
   b. Open the LDAP document you created for the server.
   c. Add the UUID property to these two fields: **Search filter for resolving person names** and **Search filter for resolving group names**. 
      Apply the UUID and value that is appropriate to the LDAP directory you use. For example, for Microsoft Active Directory, you could use the value: `objectguid=%s`
      - Lotus Domino LDAP: dominounid
      - IBM Tivoli Directory Server: ibm-entryuuid
      - Microsoft Active Directory: objectguid
      - Novell eDirectory: guid
      - Sun ONE: nsuniqueid
   d. Close and save the document.
   e. Close the Lotus Notes client.
7. Restart the Community Server.

Results
Use a test user and test group to verify that policies work for Instant Messaging, Meetings, and Media Manager.

What to do next
If you created custom Java resolve filters that are used on the Community server, the specified UUID attributes listed above must also be added to the customized Java code.
Related tasks
“Creating custom Java classes for searching the LDAP” on page 332
Create custom Java classes that provide greater control over how the Sametime Community server conducts name searches of an LDAP directory and how results are formatted.

“Using nested groups in policy assignments” on page 1068
You can configure whether or not Sametime considers nested groups when it applies policies and how many levels deep that Sametime searches for the highest weighted group.

Upgrading from Sametime 8.0.x and 7.5.1
Upgrading from the 8.0.x and 7.5.1 releases of IBM Lotus Sametime introduces many new features and components. You can upgrade your existing Sametime servers in place and optionally add new components to your deployment.

Upgrading Sametime on AIX, Linux, Solaris, or Windows
Upgrade from previous releases of IBM Sametime on the IBM AIX, Linux, Sun Solaris, or Microsoft Windows operating system.

About this task
You can upgrade from the following types of Sametime deployments:
• Sametime (release 7.5.1)
• Sametime Instant Messaging Limited Use (release 8.0, 8.0.1, and 8.0.2)
• Sametime Entry (release 8.0, 8.0.1, and 8.0.2)
• Sametime Standard (release 8.0, 8.0.1, and 8.0.2)

The upgrade process is the same for all servers up to a point; if you have meetings enabled on your server there will be additional tasks to complete if you want to migrate existing meetings to a new Sametime 8.5 Meeting Server.

Note: If you have a cluster of Sametime servers, you must upgrade all servers in the cluster. A cluster cannot support servers running different releases of Sametime.

Upgrading Sametime 8.0.x and 7.5.1 on AIX, Linux, Solaris, or Windows
Upgrade one or more IBM Sametime servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

Removing meeting rooms from Enterprise Meeting Server:
If you have meeting services enabled on your IBM Sametime server and you clustered the meeting rooms with Sametime Enterprise Meeting Server, you must remove those servers from Enterprise Meeting Server before upgrading them.

About this task
Beginning with release 8.5, Sametime no longer supports the Sametime Enterprise Meeting Server. Instead, you deploy one or more Sametime Meeting Servers and optionally cluster them using an IBM WebSphere network deployment. Then you can set up URL redirects from your upgraded Sametime servers to the new Meeting Servers so that when a user clicks a link to create or attend a meeting on an upgraded server, the link is automatically redirected to the new Meeting Server.
If you do not wish to install the Sametime Meeting Server yet, you can still create and host meetings on an upgraded Sametime classic server, but you cannot cluster the meeting rooms.

**Upgrading the Sametime server on AIX, Linux, Solaris, or Windows:**

After you have completed the preliminary steps to prepare the environment, upgrade each of your IBM Sametime servers.

**About this task**

If you are upgrading a cluster, be sure to upgrade each of the servers in the cluster (and register each server with the Sametime System Console) before you configure the cluster and register the cluster itself.

**Checking for supported releases for Lotus Domino and Sametime:**

Before upgrading to this release of IBM Sametime, determine whether you first need to upgrade your Lotus Domino and your operating system releases. You also need to determine whether your current level of Sametime is supported by the Sametime upgrade process.

**About this task**

Follow these steps to ensure that the server you intend to upgrade is running on a supported level of the operating system and that the current releases of Lotus Domino and Sametime are supported by the upgrade process. If the server includes an unsupported release of any product, you must complete an interim upgrade to a supported product.

**Procedure**

1. Check the operating system level on the computer where Sametime is installed. Make sure that your currently installed server releases, and product releases, are all supported on the new operating system level.
   
   System requirements for this release are available at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg27019598

2. Check the Lotus Domino release on the server to be upgraded.
   
   Sametime requires Lotus Domino release 8.0 or later. Before installing a newer release of Sametime to upgrade a Sametime server, verify that host Lotus Domino server is at a supported level.

   If your Sametime server is running on a version of Lotus Domino earlier than 8.0, you must upgrade the Lotus Domino server to a supported version before installing Sametime. The Sametime upgrade will fail for any server that is not running a supported release of Lotus Domino, and can only be corrected by upgrading the level of Lotus Domino and reinstalling Sametime.

   If the server is running Lotus Domino 8.0 or later, continue to the next step. Otherwise, install a supported level of Lotus Domino before proceeding. For details, see Installing a Sametime Community Server and supporting software.

3. Check the Sametime release on the server to be upgraded.
   
   Sametime supports direct upgrades from Sametime 7.5.1 or later. If your server is running an earlier release of Sametime, you must complete an interim upgrade to one of the following releases of Sametime: 7.5.1, 8.0, 8.0.1, or 8.0.2; then you can upgrade that release to this release of Sametime directly.
**Backing up the Sametime data:**

Before installing a new release of IBM Sametime, you should back up all important server data.

**Before you begin**

When upgrading Sametime on Microsoft Windows, IBM AIX, Linux or Solaris, the install program provides the option of preserving your existing Sametime data, which includes meeting information, contact lists and configuration settings, or overwriting this information.

The IBM i installation program always preserves the Sametime data on existing servers. If you do not want to preserve the Sametime data, remove Sametime from the server with the RMVLSTDOM command before installing the new release. After the installation completes, run the ADDLSTDOM command to add Sametime to the server again.

**About this task**

When backing up your Sametime data, include the following information:

*Table 81. Sametime server data to back up*

<table>
<thead>
<tr>
<th>Data to back up</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>names.nsf</td>
<td>This is optional if you can replicate from another Domino server. After upgrading to this release of Sametime, you will need to convert the native Domino Directory to use LDAP format in order to register the server with the Sametime System Console.</td>
</tr>
<tr>
<td>notes.ini</td>
<td>Back up this file for possible reference after upgrade.</td>
</tr>
<tr>
<td>da.nsf</td>
<td>Back up this file if you are using directory assistance.</td>
</tr>
<tr>
<td>vpuserinfo.nsf</td>
<td>This contains user storage and privacy information, such as contacts lists. If you upgrade from a release earlier than 7.5, you will need to upgrade the design on this database.</td>
</tr>
<tr>
<td>sametime.ini, stconfig.nsf</td>
<td>It is not necessary to backup these files on IBM i as they are saved automatically during the upgrade process. The original sametime.ini and stconfig.nsf files are saved in a subdirectory of the server data directory. The name of the subdirectory is ST&lt;previous_version&gt;BU. For example, the subdirectory name is ST751BU if you upgraded from Sametime 7.5.1, and ST80BU if you upgraded from Sametime 8.0.</td>
</tr>
<tr>
<td>All customized data files, templates or applications (.ntf, .mdm, .scr, .bmp, .mac, .smi, .tbl)</td>
<td></td>
</tr>
<tr>
<td>All ID files, desktop.dsk, and pubnames.ntf</td>
<td></td>
</tr>
</tbody>
</table>
Table 81. Sametime server data to back up (continued)

<table>
<thead>
<tr>
<th>Data to back up</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>meetingserver.ini</td>
<td>(Sametime Standard only) It is not necessary to back up this file on IBM i because it is saved automatically during the upgrade process; the original meetingserver.ini file is saved in the server data directory as meetingserver.bak.</td>
</tr>
<tr>
<td>All recorded meeting files (.rap)</td>
<td>(Sametime Standard only)</td>
</tr>
</tbody>
</table>

Upgrading the Sametime server application:

After you have verified that your server is running a supported version of IBM Lotus Domino as well as a version of Sametime that can be upgraded directly, upgrade the Sametime server application by installing the newer release on top of it.

Before you begin

Complete any pending reboot actions you may have from installing other applications. Make sure that all applications on the server computer (including the Domino Server Administrator and the web browser) are closed. All Domino services must be stopped. Otherwise, you might corrupt any shared files and the installation program might not run properly.

AIX, Linux, or Solaris

If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

The Sametime Community Server installs directly over the existing Sametime 8.0.x or 7.5 server and uses the existing version of Lotus Domino.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator (Microsoft Windows) or as root (IBM AIX, Linux, Solaris).
   Solaris only: Solaris installs must be performed by the root user using su or a normal login session. Third-party sudo packages are not supported on Solaris.
3. Prepare to use the Sametime Community Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
2) Open this release’s Download document at the following web address:
&uid=swg24029128

Locate the components that you need in the document’s listing, then
download the packages labelled with the corresponding part numbers
to the system on which you are installing.

**Tip:** When extracting downloads on Windows operating systems, use a
short path location such as C:\ and not a long path location such as
the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

**AIX**
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

**Linux**
Mount the CD or DVD using a command similar to the following
command:

```
mount /dev/cdrom /cdrom
```

**Solaris**
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files for Sametime
and open the Server folder. Start the installation program by running one of
the following commands:

**AIX**

```
./setupaix.bin
```

**Linux**

```
./setuplinux.bin
```

**Solaris**

```
./setupsolaris.bin
```

**Windows**

```
setupwin32.exe
```

5. Select the language to use for the installation and click **OK**.

6. At the Welcome screen, click **Next**.

7. Click the **I accept the terms in the license agreements** option and click **Next**.

8. Select the option to install **without** the Sametime System Console. Click **Next**.

9. **Server Host Name.**

   Provide the fully qualified host name for this Sametime Community Server.
   Do not use an IP address or the host's short name.

10. **Connect to Domino Server.**

    Enter the existing Domino administrator’s user ID and password, and then
click **Next**.
Use the common-name portion of the ID (not the hierarchical name that includes slashes). The Sametime System Console validates the administrator credentials on the Domino server.

11. Slide Conversion.
   Do one of the following:
   Select Use the Sametime server to host the slide conversion feature on the current server, and then click Next.
   Select Use Sametime slide conversion server to host the slide conversion feature on a different Community Server, provide the host name and port to connect to that server, and then click Next.

12. Connect to an LDAP Server.
   Select the user directory to be used with the Sametime Community Server, and then click Next.

13. HTTP Tunneling.
   To allow Sametime clients to make HTTP-tunneled connections on port 80 to a server with a single IP address, click Enable HTTP Tunneling, and then click Next.
   Selecting this feature increases the possibility that users in restrictive network environments can exchange data in chats on a Sametime Community Server that is extended to the Internet.

14. Review the summary, then click Install to start the installation.

15. Click Finish to close the installation screen.

16. If prompted, click Finish to reboot the system.

17. Windows 2008 only
   After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is C:\Program Files (x86)\IBM\Lotus\Domino. Add the following line in the [Config] section to ensure continuous connections for Sametime components:
   BREAK_CONN_ON_ZERO_BYTES_SENT=0
   Then close and save the file.

Connecting with older Community Servers and clients on AIX, Linux, Solaris, or Windows:

IBM Sametime Community Servers connect with one another by recognizing a shared connection group ID set by the VP_SECURITY_LEVEL parameter in the sametime.ini file. New and upgraded Community Servers receive this parameter with a setting of 7000 automatically.

About this task

For Community Servers running releases prior to Sametime 8.5.1 on AIX, Linux, Solaris, or Windows, you must update the parameter in each older server’s sametime.ini file. Follow these steps to change the VP_SECURITY_LEVEL parameter for each older Community Server.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server installation directory. The default directories are listed below:
3. In the **Config** section, change the value to match the following:

   For environments where all clients are using Sametime Connect 7.x or later or Sametime embedded in Notes 8.5.x or later clients:
   
   VP_SECURITY_LEVEL=7000
   
   For environments where clients are using releases prior to Sametime Connect 7.x or Sametime embedded in Notes 6.5.x, 7.x, or Notes Basic 8.x:
   
   VP_SECURITY_LEVEL=6510

4. Save the *sametime.ini* file.

**What to do next**

If you changed the VP_SECURITY_LEVEL to 6510, you must also change the default *sametime.ini* setting from 7000 to 6510 on all new and upgraded Sametime Community servers running 8.5.x to maintain the connection between all servers.

*Migrating data from pre-7.5 releases of Sametime:*

The format for storing IBM Sametime user privacy information changed in release 7.5. If you are upgrading from a release prior to 7.5, complete these tasks to migrate user privacy information to the new format.

*Upgrading the *vpuserinfo.nsf* template:*

As part of upgrading IBM Sametime, you will need to replace the design of the *vpuserinfo.nsf* database.

**About this task**

As part of a product upgrade, you will need to replace the design of the *vpuserinfo.nsf* database with the *stuserin.ntf* template:

**Procedure**

1. Start the Lotus Notes client.
2. Click **File > Application > Open**.
3. Select the Community Server you upgraded (select "Local" for the current server).
4. Select the Configuration folder.
5. In the file name field, type *vpuserinfo.nsf* and then click **Open**.
6. Once the database is open, click **File > Application > Replace Design**.
7. Select the newly installed Sametime Community Server as the template server, and then click the **Show advanced templates** option to locate the "Sametime User Information" (*stuserin.ntf*) template.
8. Click the *stuserin.ntf* template to select it, and then click **Replace** to update the database's design to match the template.
9. When you have finished, you can exit the Lotus Notes client.

*Migrating user privacy information:*
If you are upgrading from a version of IBM Sametime earlier than release 7.5, you will need to migrate privacy information to the newer format.

**Before you begin**

The format for storing privacy information changed in Sametime 7.5. If you are upgrading from a release prior to 7.5, and your users have stored privacy information ("Who can see me") from the earlier release, then you need to migrate this information by running a utility after upgrading. If the information is not migrated, privacy information from the earlier release appears to be lost after upgrading.

**Note:** There is no need to run this utility unless you have upgraded from a release prior to 7.5 and your users have stored privacy data from the earlier release.

**Considerations:**

- If you delay running the utility, users may create additional privacy data on the upgraded server. In this situation, the new data is stored in addition to the existing data and it is not predictable which privacy record will be used. Running the upgrade utility will not solve the problem. If necessary, the administrator can manually delete one of the privacy records from `vpuserinfo.nsf`.

- If you have multiple Sametime servers within a single community (but have not configured them as a Community Services cluster), each of the servers maintains a separate version of `vpuserinfo.nsf`. It is highly recommended that you run the upgrade utility on each of the servers in the community immediately after upgrading it to the new Sametime Community Server.

- If you have clustered the Sametime servers to support server failover and load balancing, it is best to upgrade all of the servers at the same time, if possible. Immediately run the upgrade utility on just one of the Sametime servers in the cluster and allow the `vpuserinfo.nsf` updates to replicate to the other servers.

- If it is not possible to upgrade all of the servers in the cluster at the same time, consider advising your users to avoid creating additional privacy data until all of the servers have been upgraded. If users who are connected to a server running a release prior to 7.5 create new privacy data, it will be stored in the older format. This may conflict with privacy data that has already been migrated to the newer format. More than one privacy record for a user and conflicts between the records can cause unexpected results. Running the upgrade utility again will not solve the problem. If necessary, the administrator can manually delete one of the privacy records from `vpuserinfo.nsf`.

- The time required to run the utility depends on the size of `vpuserinfo.nsf`. For example, running the utility for a 2 GB `vpuserinfo.nsf` file may take 30 minutes.

- When the utility runs, two files are created in the Sametime server data directory:
  - `vpuserinfo.nsf` (time stamp): backup copy of `vpuserinfo.nsf` before it was modified by the utility
  - `vpuserinfo.nsf.log` (time stamp): log of activity which occurred when the utility ran

**Running the privacy migration utility on Windows:**

Run the privacy migration utility to migrate user privacy information that was stored prior to IBM Sametime 7.5 to the new format. An optional parameter allows you to migrate privacy data for only a specified subset of your Sametime users.
Before you begin

This example assumes the default Domino installation directory (\Program Files\Lotus\Domino).

Example

1. If you intend to migrate privacy information for only a specified subset of your Sametime users, create a text file containing the names of the users. For example, create a text file called upgrade_util_filter.txt and save it in the Domino installation directory or another accessible location. The file should have each user specified on a separate line in the following format:
   CN=John Smith/O=example
   CN=Jane Doe/O=example
   CN=Sally Brown/O=example

2. Stop the Sametime server

3. Open a Windows command prompt

4. Run the following commands:
   c:\program files\lotus\Domino> upgrade_util.cmd
   <sametime_server_data_directory> <upgrade_util_filter_file> (where "c:\program files\lotus\Domino" is the directory where the Domino server is installed).
   • If you do not specify the server data directory (the first parameter shown above), the SametimeDirectory entry in the sametime.ini file is used.
   • If you do not specify the upgrade util filter file (the second parameter shown above), the UpgradeUtilFilter entry in the sametime.ini file is used.
   • If there is no such entry in the sametime.ini, no filter will be used, meaning migrating privacy information of all Sametime users.

   Note: If you intend to use the <upgrade_util_filter_file> parameter, it should be the second parameter, meaning you should also specify the <sametime_server_data_directory> parameter.

5. Check the vpuserinfo.nsf.log file which has the latest time stamp to verify that the utility ran successfully.

Running the privacy migration utility on AIX, Linux or Solaris:

Run the privacy migration utility to migrate user privacy information that was stored prior to IBM Sametime 7.5 to the new format. To migrate privacy information from AIX, Solaris, or Linux to the new format. An optional parameter allows you to migrate privacy data for only a specified subset of your Sametime users.

Example

To run the utility after upgrading to Sametime 8, follow these steps:

1. If you intend to migrate privacy information for only a specified subset of your Sametime users, create a text file containing the names of the users. For example, create a text file called upgrade_util_filter.txt and save it in the server data directory or another accessible location. The file should have each user specified on a separate line in the following format:
   CN=John Smith/O=example
   CN=Jane Doe/O=example
   CN=Sally Brown/O=example

2. Change directory to the data directory.
3. Make the script executable by running the following command.
   
   - chmod u+x upgrade_util.sh

4. Stop the Sametime server.

5. Run the upgrade utility as the user defined for your Domino and Sametime deployment, typically "notes":
   
   upgrade_util.sh <domino_program_directory>
   <sametime_server_data_directory> [ <upgrade_util_filter_file> ]
   
   - The first two parameters should be specified, and the last parameter is optional.
   - If you do not specify the upgrade util filter file (the third parameter shown above), the UpgradeUtilFilter entry in the sametime.ini file is used.
   - If there is no such entry in the sametime.ini, no filter will be used, meaning migrating privacy information of all Sametime users.

6. Check the vpuserinfo.nsf.log file which has the latest time stamp to verify that the utility ran successfully.

Upgrading a stand-alone 8.0 or 7.5.1 Community Mux:

If your previous IBM Sametime deployment included a stand-alone Community Mux, you can upgrade it.

Before you begin

This task only applies to a stand-alone Community Mux; the multiplexer that installs directly on the Sametime server was upgraded automatically when you upgraded that server.

About this task

Sametime supports a stand-alone Community Mux installed with an earlier version of the product; however if you plan to support IPv6 addressing in your deployment, you must upgrade the Community Mux (IPv6 addressing was introduced in Sametime 8.0.2).

If you have more than one stand-alone Community Mux, upgrade all of them:

Procedure

1. Insert the Sametime CD into the Community Services multiplexer machine, start the installation program, and choose the option to install the Community Services Mux.
2. At the "Select a language" screen, select a language for the installer, and then click OK.
3. At the "Welcome" screen, click Next.
4. At the license agreement screen, click I accept both the IBM and the non-IBM terms, and then click Next.
5. At the "Directory name" screen, browse to a the directory where you want to install the Community Mux (or accept the default), and then click Next.
6. At the "Host name or IP address" screen, enter the fully qualified host name of the Sametime Community Server that this Community Mux will serve.
   
   For best results, do not use an IP address.
7. At the summary screen, click Install.
8. At the "successfully installed" screen, click Finish.
9. **Windows 2008 only**

After installation, perform the following required configuration step. In a text editor, open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is `C:\Program Files (x86)\IBM\Lotus\Domino`. Check for the following line to the [Config] section and add it if it is missing to ensure continuous connections for Sametime components:

```
BREAK_CONN_ON_ZERO_BYTESSENT=0
```

Close and save the file, then restart the server.

**Upgrading a remote 8.0 or 7.5.1 Conversion Server:**

If your IBM Sametime deployment includes a remote conversion server and you will continue to host meetings on one or more upgraded Sametime servers, you should upgrade the conversion server as well. If you upgraded the conversion server from an earlier release to 8.5 or later, you do not need to upgrade the conversion server again because there have been no changes since 8.5.

**About this task**

Your Sametime Community Server may already be configured to use a particular conversion server and port number. If you used a remote conversion server in a previous release of Sametime, the configuration was migrated during the upgrade. You may have specified the configuration when you installed Sametime or when you added Sametime to a Domino server (IBM i). Verify that the information is correct, or update the server configuration.

**Procedure**

1. On the upgraded Sametime Community server, verify the conversion server configuration:
   a. Open the `stconvservices.properties` file, which is located in the Sametime server data `stconversion` subdirectory.
   b. Check the value for `RemoteConversionURL` setting:
      - If no remote conversion server has been configured, the setting looks like:
        ```
        #RemoteConversionURL=http://conversions1.ibm.com:8081;
        http://conversions2.ibm.com:8081/servlet/stconversion
        ```
      - When one remote conversion server is configured, the # is absent at the start of the line, the server name is correct, and everything between the semicolon and the end of the line is deleted. For example:
        ```
        RemoteConversionURL=http://stconv.example.com:19610/servlet/stconversion
        ```
        Note the port number (19610 in the example) to use when you run the installation program.
      - If more than one conversion server is configured, there is no # sign, and data for each server is separated by a semicolon. For example:
        ```
        RemoteConversionURL=http://stconv1.example.com:19610/servlet/stconversion;
        http://stconv2.example.com:8081/servlet/stconversion
        ```
        Find the entry for the conversion server that you plan to install, and note the port number.
   c. Save and close the file.
   d. If you updated the file, restart the Sametime server now.

2. Upgrade the remote conversion server:
The Sametime Conversion Services installation program is located in the Sametime Community Server package.

a. Move to the computer hosting the remote conversion server that you will upgrade.
b. Download the conversion server installation program or insert the CD containing it, and start the installation.
c. Select a language for the installer, and click Next.
d. Select the option to install Sametime Conversion Services, and click Next.
e. Follow the prompts presented to complete the installation.
f. When you are prompted for the port on which the conversion service will listen, specify the port number you noted when you verified the Sametime server configuration in Step 1.
g. If you installed Conversion Services on Microsoft Windows 2000, restart the server.
h. If your users will be posting documents that contain text for languages other than English, verify that the locale for your Conversion Server is set appropriately.

Results

The conversion services component starts automatically when you restart the server. To start the conversion services manually, click Start > Administrative tools > Services.

Upgrading a stand-alone Sametime Reflector:

Audio and video services provided by the IBM Sametime Reflector will not be available in this release to assist client-to-Sametime client audio/video communication.

About this task

The Sametime Reflector is a server application that helps to establish audio/video sessions between Sametime clients across a firewall. This release of Sametime does not include a Reflector component; the service may appear to be running, but will not function. In this release, the Sametime client can only establish audio and video connections with Sametime 8.5 and 8.5.1 clients.

Release 8.5 and 8.5.1 audio/video services can co-exist with release 7.5.x and 8.0.x audio/video services, with the following restrictions:

• The 8.5 or 8.5.1 client cannot establish an audio or video call with 7.5.x or 8.0.x clients
• The 7.5.x and 8.0.x clients cannot establish an audio or video call with the 8.5 or 8.5.1 client
• The 8.5 or 8.5.1 client cannot use the Sametime Reflector

Next steps:

After you have completed an upgrade of one or more IBM Sametime servers, the instant messaging, awareness, and presence features are ready to use. If your previous deployment included the online meetings feature, you can either use them on the upgraded server (as in previous releases) or migrate meetings to the Sametime Meeting Server.
About this task

If your Sametime server does not have the online meetings feature enabled, or meetings are enabled but you intend to continue creating and hosting them on the upgraded servers, then your upgrade is complete and you are ready to begin using the new version of Sametime.

You only need to continue to next upgrade section if your Sametime server has the online meetings feature enabled and you want to migrate them to the new Sametime Meeting Server. To migrate meetings, you will need to set up an LDAP directory (if you are currently using native Domino authentication), install new Sametime components, and then set up URL redirects from the upgraded servers to one or more newly installed Meeting Servers. All of these tasks are discussed in detail in the next section.

Expanding the deployment to host meetings on a Sametime Meeting Server

If you have upgraded one or more IBM Sametime servers and have the meetings feature enabled, you can choose to migrate the meetings to a Sametime Meeting Server and take advantage of new features such as persistent meeting rooms.

About this task

This section applies only to deployments where the upgraded servers have online meetings enabled and you want to migrate them to the new Sametime Meeting Server. To migrate meetings, you will need to set up an LDAP directory, install new Sametime components, and then set up URL redirects from the upgraded servers to one or more newly installed Meeting Servers. All of these tasks are discussed in detail in this section.

Note: This section only discusses installing new Sametime components; information on topics such as configuration, administration, tuning, and troubleshooting appears elsewhere in this information center.

Replacing the Domino Directory with an LDAP directory:

If you configured IBM Sametime to use a native IBM Lotus Domino directory for user authentication in a previous release, you must convert the directory to LDAP format for use with the upgraded Sametime deployment.

About this task

Beginning in release 8.5, Sametime requires the use of an LDAP directory for user authentication. Rather than installing a new LDAP directory, you can convert your existing Lotus Domino Directory to LDAP format. Complete this task before installing the Sametime System Console for the new deployment.

Shutting down the Sametime services while keeping the Domino services active:

To replace the Domino directory with an LDAP directory, shut down the Sametime services while you make configuration changes on the Sametime server.

About this task

You must leave the Domino server running so you can access Domino databases on the server.
Procedure
1. Open the Domino server console on the Sametime/Domino server.
2. In the Domino server console, type the following command:
   For Windows, AIX, Linus, and Solaris servers:
   Tell STADDIN Quit
   For IBM i servers:
   Tell STADDIN2 Quit

Creating a Directory Assistance database:

Setting up Directory Assistance enables web browser users to authenticate against entries in the LDAP directory when accessing databases on the Sametime server that require basic password authentication. Sametime Connect clients do not require Directory Assistance.

About this task

Because Sametime uses Directory Assistance to access an LDAP server, you must ensure that a Directory Assistance database exists on the Sametime server either by creating a new database or replicating an existing one. Use the same process to set up Directory Assistance for a Sametime server as you would for a Domino server without Sametime.

Follow these steps to create a new Directory Assistance database.

Procedure
1. Open a Lotus Notes client.
2. Choose File > Database > New.
3. Select the Sametime server (or select the Local server if you are running Sametime on a Windows server and you opened the Notes client on the server).
4. Create the Directory Assistance database on the server using the template DA50.NTF. Provide a database name and file name (for example, da.nsf) for the Directory Assistance database.

What to do next

To replicate a database instead of creating a new one, create a new replica of the Directory Assistance database on the Sametime server. Then create a Connection document to schedule replication of the database. See your Domino server administration documentation for information on replication.

Identifying the Directory Assistance database on the Sametime server:

After you have ensured that a Directory Assistance database exists on the Sametime server, you must identify the Directory Assistance database on the Sametime server.

About this task

Enter the database filename in the "Directory Assistance database name" field in the Basics section of the Sametime server's Server document.
Procedure
1. From a Notes client, choose File > Database > Open.
2. Select the Sametime server (or select the Local server if you are running Sametime on a Windows server and you opened the Notes client on the server).
3. Select the Domino directory (names.nsf) and click Open.
4. Select Server > Servers to open the Servers view.
5. Double-click the name of the Sametime server to open the Server document.
6. If necessary, select the Basics tab of the Server document.
7. Click Edit Server.
8. In the "Directory Assistance database name" field, enter the filename (for example, da.nsf) of the Directory Assistance database.
9. Click Save & Close.

Creating a Directory Assistance document:
The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the LDAP server.

About this task
Follow these steps to create the Directory Assistance document for the LDAP server. You can change the suggested values shown below as required by your environment.

Procedure
1. From the Notes client, open the Directory Assistance database (usually named da.nsf) on the Sametime server.
2. Click Add Directory Assistance.
3. In the Basics tab, make these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Select LDAP.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter any descriptive name; the name must be different from any other in Directory Assistance. Do not use the Domino domain name.</td>
</tr>
<tr>
<td>Company name</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Search order</td>
<td>The suggested value is 1. The search order specifies the order this directory is searched relative to other directories in Directory Assistance.</td>
</tr>
<tr>
<td>Make this domain available to:</td>
<td>Both Notes clients and LDAP clients choices are checked by default.</td>
</tr>
</tbody>
</table>
Setting | Value
--- | ---
Group authorization | The suggested setting is Yes. This setting enables Directory Assistance to examine the contents of groups in the LDAP directory. This capability is necessary if you enter the name of a group defined in the LDAP directory in the ACL of a database on the Sametime server.

Nested group expansion | The suggested setting is Yes. This setting enables Directory Assistance to examine the content of an LDAP directory group that is a member of another LDAP directory group. This capability is also used when an LDAP directory group name is entered in the ACL of a database on the Sametime server.

Enabled | Set to Yes to enable Directory Assistance for the LDAP Directory.

4. Select the Naming contexts (Rules) tab. Configure Rule 1 as needed for your Domino environment. The suggested values for Rule 1 are as follows:
- The OrgUnit1, OrgUnit2, OrgUnit3, OrgUnit4, Organization, and Country fields should all contain an asterisk. Using all asterisks in this setting ensures that all entries in the LDAP directory can be searched and authenticated.
- The "Enabled" and "Trusted for Credentials" fields should both be set to "Yes."

5. Select the LDAP tab. The LDAP tab contains the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The fully qualified host name for the LDAP server (for example, ldap.example.com).</td>
</tr>
<tr>
<td>Optional Authentication Credential:</td>
<td>Binding parameters to the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>If entries exist in the &quot;Administrator distinguished name&quot; and &quot;Administrator password&quot; fields in the LDAP Directory-Connectivity settings of the Sametime Administration Tool, the Sametime server binds to the LDAP server as an authenticated user.</td>
</tr>
<tr>
<td></td>
<td>If there are no entries in the &quot;Administrator distinguished name&quot; or &quot;Administrator password&quot; fields, the Sametime server binds to the LDAP server as an anonymous user.</td>
</tr>
<tr>
<td>Username</td>
<td>Complete this field if you want your Sametime server to bind to the LDAP server as an authenticated user. Otherwise, leave this field empty. Suggested values for Microsoft Active Directory server are: cn=qadmin, cn=users, dc=ubq-qa, dc=com</td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Complete this field if you want your Sametime server to bind to the LDAP server as an authenticated user. Otherwise, leave this field empty. Enter the password for the Username specified above.</td>
</tr>
<tr>
<td>Base DN for search</td>
<td>Specify a search base. A search base defines where in the directory tree a search should start. Suggestions for this setting are:</td>
</tr>
<tr>
<td></td>
<td><strong>Domino directory</strong> - An example value is &quot;O=DomainName,&quot; where &quot;DomainName&quot; is the Lotus Notes domain (for example O=Example).</td>
</tr>
<tr>
<td></td>
<td><strong>Microsoft Exchange 5.5 directory</strong> - An example value is &quot;CN=recipients, OU=ServerName,O=NTDomainName,&quot; where ServerName is the Windows server name and NTDomainName is the Windows NT Domain (for example, CN=recipients,OU=Server1,)</td>
</tr>
<tr>
<td></td>
<td>O=NTExampledomain).</td>
</tr>
<tr>
<td></td>
<td>The Microsoft Exchange 5.5 example above assumes that the directory is using the default directory schema. If you have changed the schema of the Microsoft Exchange 5.5 directory, the entry in the Base DN for search field must reflect the new schema.</td>
</tr>
<tr>
<td></td>
<td><strong>Microsoft Active Directory</strong> - An example value is &quot;CN=users, DC=DomainName, DC=com.&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>Netscape LDAP directory</strong> - Use the format O= followed by the organizational unit that was specified during the Netscape server setup. If you are uncertain about this entry, use the administrative features of the Netscape server to determine the appropriate entry.</td>
</tr>
<tr>
<td>Channel encryption</td>
<td>Select None. For information on using Secure Sockets Layer (SSL) to encrypt the connection between the Sametime server and the LDAP server, see Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number used to connect to the LDAP server. The default setting is port 389.</td>
</tr>
<tr>
<td>Accept expired SSL certificates</td>
<td>Choose the option that suits your environment.</td>
</tr>
<tr>
<td>SSL protocol version</td>
<td>Choose the option that suits your environment.</td>
</tr>
<tr>
<td>Verify server name with remote server’s certificate</td>
<td>Choose the option that suits your environment.</td>
</tr>
<tr>
<td>Advanced options</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeout</td>
<td>The suggested setting is 60 seconds. This setting specifies the maximum number of seconds allowed for a search of the LDAP directory.</td>
</tr>
<tr>
<td>Maximum number of entries returned</td>
<td>The suggested setting is 100. This setting specifies the maximum number of names the LDAP server will return for the name searched. If the LDAP server also has a maximum setting, the lower setting takes precedence.</td>
</tr>
<tr>
<td>De-reference alias on search</td>
<td>Choose the option that suits your environment, usually set to &quot;Never.&quot;</td>
</tr>
<tr>
<td>Preferred mail format</td>
<td>Depends upon the directory; the options are Internet mail address and Notes mail address.</td>
</tr>
<tr>
<td>Attribute to be used as Notes Distinguished Name</td>
<td>Should always be blank.</td>
</tr>
<tr>
<td>Type of search filter to use</td>
<td>Options are standard, Active Directory or custom; depends upon your directory. Most often 'standard' is used. If you use Active Directory, choose AD, and if you want complete control over how directory assistance searches the directory, choose 'custom.' There is additional 'hover-over' help with each option: custom, AD, and standard.</td>
</tr>
</tbody>
</table>

6. Click **Save & Close**. The warning message notifies you that your connection does not include SSL settings; you can ignore the warning and continue with the procedure.

*Creating an LDAP document in the Configuration database:*

The LDAP document in the Configuration database holds the LDAP Directory settings that enable the Sametime Community Server to search and authenticate against entries in the LDAP directory.

*About this task*

Follow these steps to create an LDAP document in the Configuration database on the Sametime Community Server.

**Procedure**

1. Use a Lotus Notes client to open the Sametime Configuration database (stconfig.nsf) on the Sametime Community Server.
2. Select **Create > LDAPServer**.
   - A document opens that contains the LDAP administration settings. Choose File > Save to save the LDAP document.
3. Close the LDAP document and close the Lotus Notes client.

*Specifying LDAP as the directory type in the Sametime.ini file:*

Edit the sametime.ini file to replace the Domino Directory with an LDAP directory.
Procedure
1. Use a text editor to open the sametime.ini file located in the Sametime server data directory.
2. In the [Directory] section of the sametime.ini file, edit the DirectoryType= parameter so that it specifies LDAP as shown below:
   
   DirectoryType=LDAP

3. Save and close the file.

Changing names to an LDAP format:

Run the Name Change task to ensure that the user and group names that are stored in the vpuserinfo.nsf database on the Sametime server are converted from the native Domino directory name format to an LDAP directory format.

About this task

Running the name conversion utility updates Sametime Community Server user or group names with the latest directory changes. The name conversion utility uses a comma-separated value list that you compile to change names, delete names, or convert all names from Domino to Domino LDAP formatted names.

Users create a contact list, a privacy list, and an alert-me-when list in the IBM Sametime Connect client by selecting user names or group names from the Domino or Domino LDAP directory that is used with the IBM Sametime Community server. These contact, privacy, alert-me-when lists are stored in the user information database (vpuserinfo.nsf) on Sametime Community servers. When a user starts the Sametime Connect client, the lists are downloaded from the database to update the lists stored on the client’s local computer.

You do not need to run the name conversion utility when you add new users or groups to the Domino or LDAP directory.

Run the name conversion utility manually on a stand-alone Sametime Community server, or on a server in a cluster which will replicate the change throughout the cluster.

Note: Be sure to stop the Domino server before you run the name conversion utility.

Configuring LDAP:

Specify the LDAP Directory settings that enable the Sametime Community Server to search the LDAP directory on the LDAP server and authenticate Sametime users against entries in the LDAP directory.

About this task

Configuring the LDAP Directory settings requires previous experience with LDAP; in particular you will need to know the following information:

- The structure (directory tree) of the LDAP directory the Sametime server will access
- The schema of Person and Group entries in the LDAP directory
- How to construct LDAP search filters to access the attributes of Person and Group entries in the LDAP directory
Procedure
1. In the Sametime server home page, click **Administer the Server**.
2. Click **LDAP Directory**.
3. Enter the settings to enable your LDAP directory to access Sametime Community Servers.
4. Click **Save**.
5. Restart the Sametime server to enable your settings.

Related reference
“LDAP directory settings” on page 271
Find more details about LDAP settings for the guided activity, "Sametime prerequisite: Connecting to an LDAP server."

Updating search settings for policies:

Replace the Notes policy key in sametime.ini with a key for the LDAP directory and verify that the search filter settings are correct for the LDAP server.

About this task
To switch from the Domino directory to an LDAP configuration, make the following changes:

Procedure
1. Stop the Sametime Policy service.
2. In the Policy section of the Sametime.ini file, replace the key:
   ```
   POLICY_DIRECTORY_BB_IMPL=com.ibm.sametime.policy.directorybb.notes.DirNotesBlackBox
   ```
   with this key:
   ```
   POLICY_DIRECTORY_BB_IMPL=com.ibm.sametime.policy.directorybb.ldap.DirLdapBlackBox
   ```
4. Click **Administer the Server**.
5. In the navigation pane, click **LDAP Directory > Searching**.
   The top two search filter settings are for LDAP, and the lower two search filter settings are for Policy.
6. Verify that the LDAP Server document holds the proper values for the BaseMembership and GroupMembership fields.
   The most effective policy search through the LDAP Directory may be using a memberOf attribute. In this case, the Policy filter field contains this attribute name, so if your LDAP Server provides the memberOf attribute, you should know how to configure the use of this feature.
7. Save stconfig.nsf.
8. Using the “tell http restart” command in the Domino console, restart the Domino HTTP server.
9. Restart the Sametime Policy service.

Reconfiguring the UserInfo servlet after switching from Domino to LDAP:

The UserInfo servlet must be reconfigured after switching from Domino to LDAP to enable the Business Card to work.
About this task

To reconfigure the UserInfo servlet, follow these steps:

Procedure
1. Open UserInfoConfig.xml in a text editor and replace all its contents with the following, then save the file:

```xml
<UserInformation>
    <ReadSTConfigUpdates value="true"/>
    <Resources>
        <Storage type="LDAP">
            <StorageDetails HostName="hera.haifa.ibm.com" Port="389" UserName="" Password="" SslEnabled="false" SslPort="636" BaseDN="" Scope="2" SearchFilter=""/>
            <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
            <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
            <SslProperties KeyStorePath="" KeyStorePassword=""/>
        </Storage>
    </Resources>
    <ParamsSets>
        <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
        <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    </ParamsSets>
    <BlackBoxConfiguration>
        <BlackBox type="LDAP" name="com.ibm.sametimeuserinfo.UserInfoLdapBB" MaxInstances="5"/>
    </BlackBoxConfiguration>
</UserInformation>
```
2. Open the Sametime server home page and log in as an administrator.
3. Click **Administer the server**.
4. Click **Configuration > Business Card**.
5. Choose the attributes to display in user business cards:
   - Photo
   - Name
   - Company
   - Email address
   - Telephone
   - Address or location
   - Title
6. Click **Update**.
7. Stop and restart Domino and Sametime.

Related concepts

“Starting and stopping servers running on Lotus Domino” on page 492

The IBM Sametime Community Server is configured as a set of services that start and stop automatically when the Domino server is stopped or started.

Installing DB2 on Linux or Windows for the expanded deployment:

Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store
Before you begin

These instructions explain how to install the version of DB2 integrated with the Sametime installation package. Use this version of DB2 if you are unfamiliar with DB2 and would prefer a less complex deployment on Windows and Linux operating systems. The DB2 installation provided with Sametime supports Linux 64-bit systems and Windows 32-bit or 64-bit systems.

If you are familiar with DB2 deployments or are installing on other operating systems, download and install one of the unmodified DB2 limited use installation packages that are available at the following web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

IBM i includes DB2.

Linux The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

Linux: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

If you are running in an enterprise deployment, install DB2 on a separate computer. In a small deployment, you can install DB2 on the same computer on which you plan to install Sametime system console.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
3. Download the Sametime DB2 installation package if you have not already done so.
   a. To download installation packages:
1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.

2) Open this release's Download document at the following web address:
https://www-304.ibm.com/support/docview.wss?rs=477 &uid=swg24029128
Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

Linux
Mount the CD or DVD using a command similar to the following command:

```
mount /dev/cdrom /cdrom
```

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- Linux./launchpad.sh
- Windows\launchpad.exe

Note: If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

`sametime_server_package/IM/platform`

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click Install IBM DB2, then click Install IBM DB2 again.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click Finish to restart the Installation Manager and continue with the next step of the Sametime installation.

If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose File > Preferences.
   b. Uncheck Search service repositories during installation and updates and click OK.
9. Click Install.
10. Click the I accept the terms in the license agreements option and click Next.
11. Accept the default locations and click Next.
12. Accept the default location for the package group and click Next.
13. Select Create a new package group and accept the default location. Click Next.
14. Confirm that all available features are selected, then click Next.
15. Create a DB2 application user ID that does not exist on the system. Then, supply a password that meets the operating system password policy requirements and any additional requirements imposed by your company. Confirm the password.
   The user specified, dasadm1, and the group db2admin does not exist on the system.
   For information about passwords, see the Password Rules topic in the DB2 information center.

   **Important:** This user cannot previously exist on the system. This user will be created as a local operating system user during the DB2 installation process; if your organization does not allow creation of local operating system users for security reasons, exit this installer and install DB2 using a different package. This installer does not check to see if the user exists.

   Make a note of the DB2 application user name and password. This user has database administration authority and you must supply the name and password when you install the Sametime system console and when you connect to DB2 databases later.

   Click Next.
16. Review the summary, then click Install to start the installation.
   The installation can take up to 20 minutes. You receive confirmation when it is complete.
17. Click Finish.
18. Click Exit to close the Installation Manager.
19. (Linux only) The DB2 server does not start by default when you restart the computer. To start a database instance automatically when the server restarts, use the db2iauto command.

   For more information, see db2iauto - Autostart instance command.

**Results**

If the installation fails, click View Log File for more information.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media. Ignore any warning about a missing versionInfo.properties file. It does not apply to DB2 installations and upgrades.

Installation Manager logs are stored in the following locations.

**Linux**  
/var.ibm/InstallationManager/logs

**Windows 2008**  
%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Windows 2003**  
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs
More detailed DB2 installation logs are stored in the following locations.

**Linux**  The logs are stored in the /tmp folder and are named db2setup.log, db2setup.his, and db2setup.err.

**Windows**
%My Documents%\DB2LOG\n
The log file name includes the date and time of the installation attempt; for example:
C:\Documents and settings\administrator\my documents\db2log\DB2-ESE-Wed Jun 21 11_59_37 2006.log

**What to do next**

If you are installing DB2 for Sametime Advanced, you must also install DB2 Net Search Extender to allow database content to be searchable and persistent. See the instructions for your operating system in the DB2 9.7 information center:
- Installing Net Search Extender on IBM DB2 9.7 for UNIX
- Installing Net Search Extender on IBM DB2 9.7 for Windows

**Related information**

- IBM DB2 Database for Linux, UNIX, and Windows Information Center

**Setting up the Sametime System Console:**

A new IBM Sametime deployment uses a system console as the central point for administering servers; all new Sametime components must connect to the console. Set up the Sametime System Console and its prerequisite components before you install a Sametime Meeting Server.

**About this task**

Setting up the Sametime System Console involves creating a database to store console data, connecting the console to existing servers, and creating policy settings on the console.

*Installing the Sametime System Console for the expanded deployment:*

The IBM Sametime System Console is your focal point for administering and configuring all Sametime servers.

**About this task**

Install and configure prerequisite applications, then install the IBM Sametime System Console, which you use for preparing for server installations and for managing your Sametime deployment.

*Creating a database for the system console for the expanded deployment:*

Before installing the IBM Sametime System Console on AIX, Linux, Solaris, or Windows, create a database to store its data.

**Before you begin**

Make sure that you have installed DB2. To install the Sametime System Console server, the DB2 application user ID must have administrator rights to be able to
create and update tables in the database. If the user does not have administrator rights, you must perform an additional step after creating the database to create tables needed for installation.

About this task

Run the scripts that come with the Sametime System Console package. They are also included with Sametime in the DB2 installation package.

Procedure

1. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation.
   
   If you are logging in for the first time, create a DB2 profile if you are prompted to do so, then close the Welcome to First Steps window.

2. Open a command prompt and navigate to the folder where you extracted the SametimeSystemConsole installation package.

3. Create the database by entering one of the following commands from the SametimeDB2 folder. Wait until you see confirmation that the database has been created and the command has finished.

   - AIX, Linux, or Solaris: `/createSCDb.sh STSC dbadmin`
   - Windows: `createSCDb.bat STSC dbadmin`

   Replace `STSC` in the command if you want to choose a different database name. Names can be from 1 - 8 characters, but cannot contain special or multibyte characters.

   Replace `dbadmin` with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.

   When naming DB2 objects, follow the rules for your operating system.

4. Close the command window.

5. Open the DB2 control center.

   - AIX, Linux, or Solaris
     
     Open the IBM DB2 folder on the desktop and click Control Center.

   - Windows
     
     Click Start > Programs > IBM DB2 > General Administration Tools > Control Center.

6. Find the database name to verify that the new database was created.

What to do next

If corporate policy prevents the DB2 application user ID from having administrator rights to the DB2 server, perform these additional steps after creating the database and before installing the Sametime System Console.

Connect to the system console database (for example, STSC). Then enter the `createSchedTable.ddl` command to create additional tables in the database.

AIX, Linux, or Solaris

`db2 connect to STSC`

`db2 -tf createSchedTable.ddl`

Windows
db2cmd

db2 connect to STSC

db2 -tf createschedTable.ddl

**Related tasks**

“Installing DB2 on Linux or Windows” on page 251
Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store information about servers, users, bandwidth configuration, and meetings. Sametime Advanced uses DB2 to store information about persistent chats and broadcast communities.

*Installing the console for the expanded deployment:*

Run the installation program to set up the system console on AIX, Linux, Solaris, or Windows.

**Before you begin**

Ensure that your IBM DB2 server is installed and running with the `db2start` command, and that the Sametime System Console database has been created. If you are upgrading, make sure that you have completed the database update before proceeding.

**IPv4 and IPv6 addressing:** When installing the Sametime System Console on a system that supports both IPv4 and IPv6 addressing, the IPv4 and IPv6 addresses associated with the system console must be mapped to the same host name. Additional host names cause problems in the system console because SSL certificates can be generated using either the IPv4 or IPv6 host name, which might not match during authentication.

**Linux**
The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The `/home` directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**
If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:** Check the `hosts` file and remove any lines that start with the following:

- `127.0.0.1 fully_qualified_domain_name short_name`
- `::1 fully_qualified_domain_name short_name`

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.
Procedure

Follow these steps to install the system console.

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.

3. Prepare to use the installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         &uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

   b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

   **AIX**
   Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
   ```bash
   mount -v cdrfs -o ro /dev/cd0 /cdrom
   
   Linux
   Mount the CD or DVD using a command similar to the following command:
   ```bash
   mount /dev/cdrom /cdrom
   
   **Solaris**
   Mount the CD or DVD.
4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
   - **AIX, Linux, and Solaris**
     `./launchpad.sh`
   - **Windows**
     `launchpad.exe`

   **Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (**install** for Linux or **install.exe** for Windows). Find the Installation Manager package directory here:

   `sametime_server_package/IM/platform`

   `sametime_server_package` is the installation package name for this server.

   `platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click **Install IBM Sametime System Console** and click Launch IBM Sametime System Console 8.5.2 installation.

7. If the IBM Installation Manager is not installed, you are prompted to install it.
   Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.
   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose **File > Preferences**.
   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

9. Click **Install**.

10. Select the packages that you want to install and click **Next**.

11. Click the I accept the terms in the license agreements option and click **Next**.

12. Accept the location for shared installation files and click **Next**.

13. Select Create a new package group. Accept the installation directory and click **Next**.

14. Verify that **IBM Sametime System Console server 8.5.2** is selected as the feature to install and click **Next**.

15. In the Common Configurations window, verify the cell, node, and host name.
   The Sametime System Console is a deployment manager and administers a cell and any nodes federated into the cell for other Sametime servers. In an enterprise deployment, the servers are in one geographic region and in a small deployment, the servers are all installed on one computer.

   **Windows**
   Avoid using a node name that is longer than 10 characters if possible.
   Installation creates a profile name based on the selection you make here. The maximum number of characters for a profile is 80 characters. If installation fails, reinstall the product using a shorter directory path and a shorter node name.

   - **Cell:** The name of the WebSphere Application Server cell that is created for the system console, such as `systemNameSSCCell`.
• **Node:** The name of the WebSphere Application Server node that runs the Sametime applications in the system console. It is federated into the cell during the installation process.

• **Host Name:** Use the fully qualified DNS name of the server that you are installing the system console on. Make sure this DNS name is resolvable from other servers you will be installing products on. Do not use an IP address, a short host name, or localhost.

16. Create the WebSphere Application Server user ID. Avoid a name that contains spaces. Supply a password and confirm it. Click **Next**.

If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

This user must be one that is not on the operating system or in an LDAP directory. The user is created in a WebSphere Application Server local file system repository and is used to administer the Sametime System Console server.

Make a note of the ID and password because you use them later for additional product installations and configuration. You also use them to administer the Sametime System Console server.

17. In the Configure DB2 for the System Console window, provide information for connecting to the system console database.

• **Host Name:** Use the fully qualified domain name of the server where you installed DB2. Do not use an IP address or a short host name.

• The **Port** field shows the default port of 50000. Accept the default unless you specified a different port during DB2 installation or your server is using a different port.

On Linux, the default is typically 50000, but varies based on port availability. Check the `/etc/services` file on the DB2 server to verify the port number that is being used.

• **Database Name for the System Console/Policy:** Enter the name of the database that you want to connect to. If you used the suggested name when you created the system console database, the name is STSC.

Use only upper- and lower-case English characters, numbers, and the following punctuation characters:

`! ( ) + . , [ ] _ ` ~

• **Application user ID:** Enter the name of the database administrator that you created when installing DB2. The default is `db2admin`.

• **Application password:** Specify the password that you created when you installed DB2, such as `db2password`.

18. Click **Validate**.

19. When the button label changes to **Validated**, click **Next**.

If the database connection is not successful, use the `dbverify.log` file to debug the problem. The log can be found in the temporary directory for your operating system.

**AIX, Linux, or Solaris**

/tmp

**Windows**

%TEMP%

20. Review the summary, then click **Install** to start the installation.
21. When installation is complete, click Exit to close the Installation Manager.

**Results**

After a successful installation, three components must be started before using the console: the deployment manager, the node agent, and the Sametime System Console server.

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the `collectLogs` utility to gather the logs. `collectLogs` is located at the root of the installation media.

**AIX, Linux, or Solaris**

/var.ibm/InstallationManager/logs

**Console connection log:** /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

**Console connection log:** Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

**Console connection log:** Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

What to do next

“Logging in to the console” on page 483

Related tasks

“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505

Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

*Logging in to the console for the expanded deployment:*

Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

**About this task**

Log in to the Sametime System Console on the system where you installed the cell profile. If you deployed a cluster using a dedicated Deployment Manager, the cell is managed on a system other than the one where you installed the Sametime System Console.
Related tasks

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Logging in to the Sametime system console for the expanded deployment:

Use the IBM Sametime system console to use guided activities to perform configuration tasks and administer any Sametime servers that are managed by the console.

Procedure

With the Sametime system console started, follow these steps to log in.

1. From a browser, enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the Sametime System Console server. For AIX, Linux, Solaris, or Windows, specify port 8700 for HTTP and 8701 for HTTP over SSL.
   
   During the installation process, WebSphere Application Server security is enabled. SSL is enabled as part of the security process and you are directed to another port that listens for HTTPS connections.
   
   `http://serverhostname.domain:port/ibm/console`
   
   For example:
   
   `http://sametime.example.com:8700/ibm/console`
   `https://sametime.example.com:8701/ibm/console`

   **Note:** On IBM i, the port number cannot be 8700. Use the port that was listed in the system console installation results summary. To check the port, open the `AboutThisProfile.txt` file for the system console deployment manager profile and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:

   `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt`

2. The WebSphere Application Server Integrated Solutions Console opens. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.
   
   The default name is wasadmin.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

Logging in to the console for a cell profile in the expanded deployment:

If you chose the configuration type “Cell Profile” when you installed Sametime servers, you installed a self-contained set of WebSphere Application Server components for each server. This configuration type installs a WebSphere Application Server Integrated Solutions Console as part of the server's cell profile.

Before you begin

The Deployment Manager of the Sametime server must be started.
About this task

With the Deployment Manager of the Sametime server started, follow these steps to log in to the WebSphere Application Server Integrated Solutions Console.

Procedure

1. From a browser, enter the following URL to log into the console. Replace serverhostname.domain with the fully qualified domain name and port for the server.

   Note: During the install process, WebSphere security is enabled. SSL is enabled as part of the WebSphere security process and you will be directed to another port which listens for https connections.

   • Sametime Proxy Server
   Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
   http://serverhostname.domain:8600/ibm/console
   8600 is the default port when the Proxy Server is installed as a Cell Profile.
   For example:
   http://sametime.example.com:8600/ibm/console

   Note: (IBM i) The port number may not be the default listed above. Use the port that was listed in the Sametime Proxy Server installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime Proxy Deployment Manager Profile on the server and use the setting specified for the "Administrative console port." For the default profile name (STPDMgrProfile), the file is located here:

   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPDMgrProfile/logs/AboutThisProfile.txt

   • Sametime Media Manager (Linux and Windows)
   Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
   http://serverhostname.domain:8800/ibm/console
   8800 is the default port when the Media Manager is installed as a Cell Profile.
   For example: http://sametime.example.com:8800/ibm/console

   • Sametime Meeting Server
   Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
   http://serverhostname.domain:8500/ibm/console
   8500 is the default port when the Meeting Server is installed as a Cell Profile.
   For example: http://sametime.example.com:8500/ibm/console

   Note: (IBM i) The port number may not be the default listed above. Use the port that was listed in the Sametime Meeting Server installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime Meeting Deployment Manager Profile on the server and use the setting specified for the "Administrative console port." For the default profile name (STMDMgrProfile), the file is located here:
The WebSphere Application Server Integrated Solutions Console opens.

2. Enter the WebSphere Application Server User ID and password that you created when you installed the Sametime server.
   The default name is wasadmin.

**Related concepts**

“Ports used by Sametime servers” on page 208

IBM Sametime uses a number of ports on the servers in your deployment. This topic lists the default ports and their uses; a range of ports means that the application can select any port in that range, in case one or more of those ports are already in use by other applications.

*Logging in to the console for a cluster in the expanded deployment:*

In a cluster, you log in to the console used by the Deployment Manager.

**About this task**

With the cluster's Deployment Manager started, follow these steps to log in.

**Note:** If you deployed the cluster using the Sametime System Console as the Deployment Manager, log in to the System Console. If you deployed the cluster using a dedicated Deployment Manager, log in to that server's console.

**Procedure**

1. From a browser, enter the following URL, replacing `serverhostname.domain` with the fully qualified domain name of the Sametime System Console server.
   Specify port 8700 for all platforms except IBM i.
   `http://serverhostname.domain:8700/ibm/console`
   For example:
   `http://sametime.example.com:8700/ibm/console`

   **Note:** Another option is to enter the following URL. Note that this is `https` and the port number is 8701:
   `https://serverhostname.domain:8701/ibm/console`

   **IBM i:** The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime System Console Deployment Manager Profile and use the setting specified for the "Administrative console port." For the default profile name (STSCDmgrProfile), the file is located here:
   `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt`

   **Note:** During the install process, WebSphere security is enabled. SSL is enabled as part of the WebSphere security process and you will be directed to another port which listens for `https` connections.
   The WebSphere Application Server Integrated Solutions Console opens.

2. Enter the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.
   The default name is wasadmin.

3. Click the **Sametime System Console** task to open it in the navigation tree.
What to do next

“Connecting to an LDAP server” on page 265

Related tasks

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Connecting to an LDAP server for the expanded deployment:

Use the IBM Sametime system console to connect IBM Sametime servers to an LDAP server that has already been installed and configured. An LDAP server is required for these server offerings: community server, meeting server, media manager, and gateway.

Before you begin

Start the LDAP server and the Sametime system console.

Procedure

If you have not already opened the Connect to LDAP Servers activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified host name of the Sametime System Console server.
   
   http://serverhostname.domain:8700/ibm/console
   
   For example: http://sametime.example.com:8700/ibm/console
   
   If you are prompted with a security exception, accept the certificate, and continue.

   IBM i: The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime System Console Deployment Manager Profile and use the setting specified for the "Administrative console secure port." For the default profile name (STSCDMgrProfile), the file is located here:

   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/
   STSCDMgrProfile/logs/AboutThisProfile.txt

2. Enter the WebSphere Application Server user ID and password that you created when you installed the system console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Expand Sametime Prerequisites, and click Connect to LDAP Servers.
Related concepts
“Planning for an LDAP directory” on page 232
The IBM Sametime 8.5 multiple-server environment requires an LDAP directory for user authentication. The LDAP server should be set up and running before deploying Sametime.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Sametime prerequisite: Connecting to an LDAP server for the expanded deployment:
This activity takes you through the steps for identifying users and groups in an LDAP directory that need access to IBM Sametime.

Before you begin
An LDAP server must be installed and configured.

About this task
Connect IBM Sametime servers to the LDAP server. After your Sametime server connects to the LDAP server, it can search the LDAP directory and authenticate Sametime users. If you have already connected Sametime to an LDAP server, but now you want to edit or delete a connection, use this activity.

Procedure
1. Connect to LDAP server.
   In Connect to LDAP servers, click Add.
   If you want to edit or delete an LDAP connection instead, then click the appropriate button.
   If you edit an LDAP connection for a Cell-based WebSphere Application Server product that is already installed, you must manually update the product’s LDAP configuration. The System Console Cell’s LDAP is updated and the changes are also pushed to a connected LDAP server. You can delete an LDAP connection if it is not being used by an installed product.
2. Bind to LDAP.
   a. Click Authenticated access to ensure that the Sametime server uses credentials to authenticate with the LDAP server.
      Provide the Bind distinguished name (DN) and Password when you are prompted to enter this information.
      Select Anonymous access only if you are certain that all attributes are accessible when the Sametime server binds to the LDAP server.
   b. Enter a Deployment Name for this LDAP connection to identify the connection for future reference. It does not need to map to any existing server name or value.
   c. Enter the fully qualified domain name of the LDAP server that you want to connect to in the Host name field. Do not use an IP address or a short host name.
   d. Enter the Port of the LDAP server. The default value is 389. If your LDAP server is running on a different port, enter the correct port value here.
e. To use an SSL connection with the LDAP server, click **Is secure LDAP connection**.
   
   **Attention:** Selecting this option requires additional configuration for Sametime Community Servers. When you set up the deployment plan for either of these servers, you must elect to configure the LDAP server manually. After installation, set up trust with the LDAP server’s SSL certificates and then manually configure the LDAP directory to finish setting up the secure LDAP connection. See “Enabling encryption between Sametime and the LDAP server” for more information.

f. If you selected **Is secure LDAP connection**, click **Import SSL Certificate**.
   
   This action imports the LDAP server's SSL certificate into the Default Cell Trust Store. You only need to do this once.

g. If you selected **Authenticated access**, enter the **Bind distinguished name (DN)** and **Password** fields. These are the user credentials you will use to authenticate with your LDAP server. If you have selected **Anonymous Access**, these fields are not shown. For example:

   cn=John Smith,ou=managers,o=example,st=Massachusetts,c=US

h. Click **Next**.
   
   When designating an authenticated user, create a unique directory entry that is used only for the purpose of authenticating connections from the Sametime server to the LDAP server. After creating the directory entry, you must ensure that this directory entry has at least read access to the attributes of the LDAP directory entries.

3. **Base Distinguished Name and Filter for Searches.**

   Enter the base distinguished name and filter for searches information.

   a. Select your base distinguished name and filter for searches from the list or enter a value. You specify the basic LDAP parameters required to conduct searches for people and groups in the LDAP directory. Some of these parameters are also necessary for displaying the names of users in the Sametime user interface.

   Failure to specify a base distinguished name prevents authenticated users from creating and attending meetings on the meeting server.

   **Restriction:** The list displays a base DN that is detected by the guided activity; however, the list does not display for a Lotus Domino LDAP directory. Additionally, Lotus Domino LDAP is the only LDAP directory that uses a blank base DN. WebSphere Application Server requires a base DN for federating repositories and does not let you use an empty base DN. It sets the base DN to C=US. The LDAP repositories are listed by base DN after they are federated.

   b. Optional: To specify the search filter and basic LDAP settings for person and group entries, click **Configure advanced LDAP settings**.

   c. Click **Next**.

4. **Collect Person Settings.** To search for a user name, users enter a text string in the Sametime user interface. This setting defines the LDAP search filter responsible for selecting a user name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory person entries.

   a. Enter the attributes of an LDAP person entry.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>Specifies a set of attributes used to describe an object that identifies the entry as a person. Sametime determines whether a directory entry returned by a search is a person or a group. Groups are represented by entries with a unique object class. The name of the object class specified in this setting is compared to the object class values.</td>
</tr>
<tr>
<td>LDAP user search base</td>
<td></td>
</tr>
<tr>
<td>Policy ID for users and groups</td>
<td>Specifies which ID to search for when the administrator selects User ID as the search criteria for managing policies.</td>
</tr>
<tr>
<td></td>
<td><strong>UUID</strong> is the default. Select <strong>Distinguished Name</strong> to use the distinguished name of users and groups instead if the default UUID attribute does not exist in the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>New and existing custom Java classes for searching the Community Server’s LDAP directory must include the appropriate UUID attribute for the LDAP directory if UUID is used with policy assignments or Sametime user login IDs:</td>
</tr>
<tr>
<td></td>
<td>• Lotus Domino LDAP: dominounid</td>
</tr>
<tr>
<td></td>
<td>• IBM Tivoli Directory Server: ibm-entryuuid</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory: objectguid</td>
</tr>
<tr>
<td></td>
<td>• Novell eDirectory: guid</td>
</tr>
<tr>
<td></td>
<td>• Sun ONE: nsuniqueid</td>
</tr>
<tr>
<td>Display name</td>
<td>Displays a user’s name in Sametime user interfaces. The attribute must not be the same as the one you use for Similar name distinguisher or Email address due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Differentiates between two users that have the same common name (cn) attribute. The attribute must not be the same as the one you use for Display name or Email address due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td>Email address</td>
<td>Contains the user's email address in the field. The attribute must not be the same as the one you use for Display name or Similar name distinguisher due to WebSphere Application Server configuration rules.</td>
</tr>
</tbody>
</table>
**Table 82. Person attributes (continued)**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Sametime server</td>
<td>Enter the name of the LDAP Attribute that contains a user's Home Sametime server. The Home Sametime server is a community server Domino name or a community server cluster name that indicates which community server or cluster a user should use. If your environment includes multiple community servers or you have deployed other applications enabled with Sametime technology, every user must be assigned to a home community server or cluster.</td>
</tr>
<tr>
<td>Membership attribute</td>
<td>Enter the attribute that specifies which groups a user belongs to if your LDAP server supports this feature.</td>
</tr>
</tbody>
</table>

b. Enter the search and authentication attributes of an LDAP person entry.

**Table 83. Search and filter**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authentication attributes| Allows the user to authenticate with more than one attribute of the user's entry. For example, if this field is set to mail;cn the user can authenticate with either of these names.                                      

The guided activity allows the use of any of these three properties: mail, cn, and uid. When forming the search filters, the mail, cn, and uid properties are replaced with the attributes specified above. For example if the "Similar name distinguisher" or uid is set to sAMAccountName, the attribute sAMAccountName is used in the filter. Similarly, if "Display Name" maps to "cn", the attribute "cn" is used in the filter and if "Email address" maps to "mail," the attribute "mail" is used in the filter. **Important:** For the meeting server to work, the first field of the Authentication attribute must be set to mail and must be listed first. Add other fields, separated by a semicolon (;). For example, the Authentication attribute can be set to mail;cn;uid. |
| Search attributes        | Specifies the fields used for searching the directory for users. The fields must be separated by a semicolon (;). For example, the Search attribute can be set to mail;cn;uid.                                              |

c. Click Next.

5. Collect Group Settings. To search for a group name, users enter a text string in the Sametime user interface. This setting defines the LDAP search filter.
responsible for selecting a group name from the LDAP directory. The search filter matches the text string to information contained within the attributes of LDAP directory group entries.

a. Enter the attributes of an LDAP group entry.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>Specifies the attribute of a directory entry that identifies the entry as a group. Sametime determines whether a directory entry returned by a search is a person or a group. Groups are represented by entries with a unique object class. The name of the object class specified in this setting is compared to the object class values.</td>
</tr>
<tr>
<td>LDAP group search base</td>
<td></td>
</tr>
<tr>
<td>Display name</td>
<td>Displays a group's name in Sametime user interfaces.</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Differentiates between two groups that have the same common name (cn) attribute.</td>
</tr>
<tr>
<td>Group membership attribute</td>
<td>Specifies the name of the attribute in the group entry that contains names of individual people or subgroups that belong to the group. If users add a group to a presence list, privacy list, or a list that restricts meeting attendance, Sametime must obtain the list of members within the group.</td>
</tr>
</tbody>
</table>

b. Click Next.

6. Task Completion Summary.
   Review the configuration details in the **Task Completion Summary** table, and click **Finish** to connect to the LDAP server.

7. If you selected the **Import SSL Certificate**, restart the system console deployment manager.

8. Restart the system console deployment manager to complete the LDAP federation process.

9. (Optional) To push the LDAP changes to all nodes, go to **System Administration > Nodes**. Select all nodes and click **Synchronize**.
Related tasks

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Assign users and groups to policies” on page 1051
You can assign users and groups to specific user policies to grant or limit access to features in IBM Sametime.

“Enabling encryption between Sametime and the LDAP server” on page 805
Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

Related reference

“LDAP directory settings” on page 271
Find more details about LDAP settings for the guided activity, "Sametime prerequisite: Connecting to an LDAP server."

“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Connecting to a Sametime Community Mux server for the expanded deployment:

Use the IBM Sametime System Console to connect to a Sametime Community Mux and validate its settings.

Before you begin

Start the Sametime Community Mux if it is not already running.

Procedure

If you have not already opened the Connect to Sametime Community Mux Servers activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified host name of the Sametime System Console server (for example stconsole.example.com).
   http://serverhostname.domain:8700/ibm/console
   For example: http://sametime.example.com:8700/ibm/console
   If you are prompted with a security exception, accept the certificate, and continue.

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the Sametime System Console task to open it.

4. Expand Sametime Prerequisites, and click Connect to Sametime Community Mux Servers.
Related concepts
“Planning for an LDAP directory” on page 232
The IBM Sametime 8.5 multiple-server environment requires an LDAP directory for user authentication. The LDAP server should be set up and running before deploying Sametime.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

*Sametime prerequisite: Connecting to a Sametime Community Mux Server for the expanded deployment:*
Validate the host name and ports specified for a new IBM Sametime Community Mux server.

**Before you begin**
Use this page to validate the host name of a new Community Mux, along with the ports on which it will listen for client connections. This ensures you have a working multiplexer before you attempt to connect it to a Sametime community server or cluster.

**Procedure**
1. Connect to Sametime Community Mux Servers.
   Click **Add** to begin the guided activity, which lets you validate your installed Sametime Community Mux servers before connecting them to community servers.
   You can optionally edit or delete connections to Community Mux servers. Click **Refresh** to view your most recent changes.
2. Add Sametime Community Mux Servers.
   a. In "Connect to Sametime Community Mux Servers", click **Add**.
   b. In the **Host Name** field, type the fully qualified host name of the new Sametime Community Mux (for example: *mux1.example.com*).
   c. Accept the default settings for the **Client Port** and **Client HTTP Port** fields.
      These settings indicate the ports that the multiplexer will listen on for connections from Sametime Connect clients and from web clients, respectively.
   d. Click **Save**.
      The connection to the Sametime Community Mux is validated when you save the settings.

**Registering an upgraded Community Server with the System Console:**

After upgrading an IBM Sametime server to a Sametime Community Server on IBM AIX, Linux, Sun Solaris, or Microsoft Windows, register it with the Sametime System Console, so you can manage all of the Sametime servers from a central location. If you upgraded a cluster, you must register each individual server before registering the cluster.

**Before you begin**
Make sure the following servers are ready for the registration task:
The upgraded Sametime Community Server must be configured to use an LDAP directory, and must be started.

The Sametime System Console must be started.

The LDAP server must be started, and must be connected to the Sametime System Console.

About this task

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

Procedure

1. If you enabled SSL encryption on the previous version of the Sametime server, complete these substeps on the upgraded server:
   - If SSL is not enabled, skip this step.
   - a. Locate the directory where the SSL certificate is stored and note the path (for example, C:\server.cer).
   - b. Navigate to the directory where Java is installed.
      - For example, on Microsoft Windows: C:\Lotus\Domino\JVM\bin.
   - c. Open a command window and run the following command:
      
      ```
      keytool -import -alias serverSSL -file "C:\server.cer" -keystore ../lib/security/cacerts -storepass changeit -noprompt
      ```
      
      where C:\server.cer represents the path where the SSL certificate is stored.

2. Back up the console.properties and productConfig.properties files:
   - a. Navigate to the Community Server's Sametime console directory:
      - **AIX, Linux, Solaris:** The console directory is under the Community Server data directory; for example: /opt/IBM/domino85/notesdata/console
      - **Windows:** The console directory is under the Domino directory; for example: C:\Lotus\Domino\console
   - b. Make back-up copies (using different names) of the console.properties and productConfig.properties files.

3. Update the following values in the console.properties file and save the file.

   **Table 85. console.properties settings**

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCCSSLEnabled is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
</tbody>
</table>
Table 85. console.properties settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

4. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file. Only the required values in this file are listed here:

Table 86. productConfig.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the Community Server that is being registered.</td>
</tr>
</tbody>
</table>

5. Now register the server:
   a. Run the registration utility with the following command:
      **Upgrading from 8.0.x and 7.5.1**
      - AIX, Linux, Solaris: registerSTServerNode.sh
      - Windows: registerSTServerNode.bat
   b. As the registration utility runs, you will be prompted to enter the following information:

      | Setting                      | Description                                                                 |
      |------------------------------|-----------------------------------------------------------------------------|
      | Location of notes.ini file   | This is the user name and password that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the full path to the directory containing the notes.ini file, and press Enter. For example, on Windows: C:\Lotus\Domino |
      | Lotus Domino administrator user name | This is the account that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the Lotus Domino administrator's user name, and press Enter. |
      | Lotus Domino administrator password | Type the password associated with the Lotus Domino administrator user account, and press Enter. |

   The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the registration is successful, a console.pid will also be generated.

6. (Optional) If you plan to recreate your current set of policies on the system console in the Sametime 8.5 deployment, review existing policy settings and copy them down now.
The upgraded Sametime Administration Tool no longer displays Policies after
you restart the server in the next step. The only way to find policies later is to
open the stpolicy.nsf database directly.

7. Restart the Sametime Community Server.

After you restart the server, the SSCUserName and SSCPassword settings will be
removed from the console.properties file and replaced with a new
SSCEncodedAuthorization setting; for example:

SSCEncodedAuthorization=d2FzYWRtaW46MTIz

Registering the upgraded Community Server cluster with the System Console:

After upgrading an IBM Sametime cluster to a Sametime Community Server
cluster on IBM AIX, Linux, Sun Solaris, or Microsoft Windows, register the cluster
with the Sametime System Console, so you can manage all of the Sametime servers
from a central location.

Before you begin

Make sure each of these servers is ready for the cluster registration task:

- Each of the upgraded Sametime Community Servers in the cluster must be
  registered with the Sametime System Console, and must be started.
- The Sametime System Console must be started.
- The LDAP server must be started, and must be connected to the Sametime
  System Console.

Procedure

1. Verify that each of the servers in the cluster has been registered with the
   Sametime System Console.

2. Run the registration utility using the appropriate command below:

Upgrading from 8.5 and 8.5.1

- AIX, Linux, Solaris: ./registerSTCluster.sh -upgradeCluster
- Windows: registerSTCluster.bat -upgradeCluster

Upgrading from 8.0.x and 7.5.1

- AIX, Linux, Solaris: ./registerSTCluster.sh
- Windows: registerSTCluster.bat

3. As the registration utility runs, you will be prompted to enter the following
   information:

<table>
<thead>
<tr>
<th>Cluster name</th>
<th>Type the name you created when you configured the cluster, and press Enter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of notes.ini file</td>
<td>This is the user name and password that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the full path to the directory containing the notes.ini file, and press Enter. For example, on Windows: C:\Lotus\Domino</td>
</tr>
<tr>
<td>Lotus Domino administrator user name</td>
<td>This is the account that you use to manage the upgraded Sametime Community Server from the Community Server Administration Tool. Type the Lotus Domino administrator's user name, and press Enter.</td>
</tr>
</tbody>
</table>
Lotus Domino administrator password

| Lotus Domino administrator password | Type the password associated with the Lotus Domino administrator user account, and press Enter. |

The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory.

4. Restart the Sametime Community Server.

**Installing a Sametime Proxy Server for the expanded deployment:**

The IBM Sametime Proxy Server enables browser-based clients to participate in Sametime instant messaging and online meetings. In addition, the Sametime Proxy Server works with Sametime Community Server or Connections to enable the business card feature in Sametime, and with Sametime Unified Telephony or other TCSP-enabled products to enable the Sametime click-to-call feature. The Sametime Proxy Server also provides live names awareness, and can replace the Links Toolkit used in earlier releases of Sametime.

**About this task**

**Important:** If you will be supporting the use of LiveNames in your Sametime deployment, you should deploy all Sametime Meeting Servers and Sametime Proxy Servers within the same subnet. It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

**Related concepts**

“Configuring a Sametime Proxy Server” on page 1021
Configure connection settings to enable the IBM Sametime Proxy Server to communicate with other servers in the deployment.

**Preparing to install a Sametime Proxy Server for the expanded deployment:**

Use the Sametime System Console to prepare to install an IBM Sametime Proxy Server by pre-populating values required for installation.

**Before you begin**

Start the Sametime System Console if it is not already running.

**Procedure**

If you have not already opened the Install Sametime Proxy Server guided activity, follow these steps:

1. From a browser, enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the Sametime System Console server.
   http://serverhostname.domain:8700/ibm/console
   For example: http://sametime.example.com:8700/ibm/console

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Sametime Guided Activities > Install Sametime Proxy Server**.
Related tasks

“Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine” on page 371
When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server on the same machine using the same server host name, conflicts with cookies that are used by each server can occur. If you install both servers on the same machine, then configure the Sametime Proxy Server with a host alias as a different host name.

“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install a Sametime Proxy Server for the expanded deployment:

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.

Before you begin

The following servers must be installed and running:
• LDAP server
• Sametime System Console
• Sametime Community Server, installed using a deployment plan created on the System Console

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Proxy Server.

Procedure

1. Plan a product installation.
   In the Install Sametime Proxy Server portlet, click Create a New Deployment Plan, and then click Next.
2. Deployment Name.
   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.
   The name should include the installation and node type, such as stProxy_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.
   Select the product version you want to install, and then click Next.
4. Choose the configuration type.
   Select Primary Node if this is the first server of its type. Select Secondary Node for additional servers. Then click Next.
   The Cell option is reserved for special-use cases in which the server must be self-contained. If you select Cell, you must provide a host name, user ID, and password when prompted to do so.
5. Node Federation at Install Time.
This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click **Next**.

**Attention:** Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

6. **WebSphere Profile Settings.**
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click **Next**.

   If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.

   **Important:** This must be a unique user ID that does not exist in the LDAP directory.

7. **Connect to Community Server.**
   Select the deployment plan that represents the Community Server to which this Proxy server connects, and then click **Next**.

8. **Deployment Summary.**
   Review the summary screen, and then click **Finish**.

   The deployment plan is ready to be used for the server installation. If you need to make any changes, click **Modify an Existing Deployment Plan** and update the plan. All changes must be made prior to running installation.

**What to do next**

“Installing a Sametime Proxy Server on AIX, Linux, Solaris, or Windows” on page 349

*Installing a Sametime Proxy Server for the expanded deployment on AIX, Linux, Solaris, or Windows:*

Run the installation program on the machine where you plan to install a Sametime Proxy Server.

**Before you begin**

You should have already created a deployment plan for the Sametime Proxy Server. Verify that the deployment plan is in the “Ready to Install” state and start the Sametime System Console server.

**Linux** The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the
Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

**AIX, Linux, and Solaris:**
If you are installing using the GUI mode, the full X11 desktop environment is required.

**Attention:** Check the `hosts` file and remove any lines that start with the following:
- `127.0.0.1 fullyQualifiedName shortName`
- `::1 fullyQualifiedName shortName`

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.

**About this task**
By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

**Procedure**
1. **Red Hat Enterprise Linux only:** Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the `/etc/selinux/config` file for editing.
   c. Locate the `SELINUX` setting. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.
2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.
   **Solaris only:** The installation must be performed by the root user using `su` or a normal login session. Independent sudo packages are not supported on Solaris.
3. **Prepare to use the Proxy Server installation package.**
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release's Download document at the following web address:
         https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document's listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         **Tip:** When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path
locations or deeply nested directories and using the built-in Windows
extract utility, corruption is sometimes seen without any warning. This
corruption occurs when maximum path lengths on some Windows
versions are exceeded.

b. If you are installing from physical media and your operating system
mounts CDs or DVDs automatically with execution privileges turned off,
mount the CD or DVD manually instead.

AIX
Mount the CD or DVD using the SMIT utility or the appropriate version of
the following command:

```
mount -v cdrfs -o ro /dev/cd0 /cdrom
```

Linux
Mount the CD or DVD using a command similar to the following
command:

```
mount /dev/cdrom /cdrom
```

Solaris
Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the
installation program by running one of the following commands:

- AIX, Linux, and Solaris
  ```
  /launchpad.sh
  ```
- Windows
  ```
  launchpad.exe
  ```

**Note:** If you do not have a web browser, go to the Installation Manager
package directory and run the installation program (**install** for Linux or
**install.exe** for Windows). Find the Installation Manager package directory
here:

```
sametime_server_package/IM/platform
```

*platform* is the operating system on which you are installing.

5. If necessary, select a language other than English from the **Select a language**
list.

6. Click **Install IBM Sametime Proxy Server** and click **Launch IBM Sametime
Proxy Server 8.5.2 installation.**

7. If the IBM Installation Manager is not installed, you are prompted to install it.
Do so, then click **Finish** to restart the Installation Manager and continue with
the next step of the Sametime installation.

If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the
automatic web update search to allow the installation to run successfully.

a. In the Installation Manager window, choose **File > Preferences.**

b. Uncheck **Search service repositories during installation and updates** and
   click **OK.**

9. Click **Install.**

10. Select the packages that you want to install and click **Next.**

11. Click the **I accept the terms in the license agreements** option and click **Next.**

12. Select a package group option and accept the installation directory. Then click
**Next.**
Select **Create a new package group** if you have not installed any other Sametime software on this machine.

Leave **Use the existing package group** selected if you are installing several Sametime servers on the same machine.

13. Select **IBM Sametime Proxy Server** as the feature to install and select **Use Sametime System Console to install**. Click **Next**.

14. At the Common Configurations screen, supply values for connecting to the Sametime System Console.

   - **Host Name**: Provide the Host Name for the Sametime System Console. The Host Name was determined when you installed the Sametime System Console. The host name must be the actual host name and not a DNS alias.
   - **Use SSL**: Leave this option selected to run the server over a secure connection.
   - **HTTPs Port**: Leave 9443 as the default value.
   - **User ID and password**: Provide the WebSphere Application Server User ID and password that you created when you installed the Sametime System Console.

15. Provide the host name for the machine you are currently using, which is the same name you used when you created the deployment plan for this installation.

   Do not use an IP address or short host name.

16. Click **Validate** to log in to the Sametime System Console.

   The button name changes to **Validated** after you log in.

17. When you are logged in, click **Next**.

18. Select the Sametime Proxy Server deployment plan you created earlier with the Sametime System Console guided activity. Then click **Next**.

19. Review the deployment settings, then click **Next**.

20. Review the summary, then click **Install** to start the installation.

21. When installation is complete, click **Exit** to close the Installation Manager.

22. If the Sametime Proxy server is installed on a system with multiple active IP addresses, follow these steps for each Proxy Server in the cell. Otherwise the Community Server may reject connections from the Proxy Server.

   a. Add the Proxy Server’s IP address to the stproxyconfig.xml file used by the Proxy Server's deployment manager. Complete this step for each Proxy Server in the cell.

      1) Find the stproxyconfig.xml file in the Proxy Server's deployment manager profile configuration in this location:

         ```
         dm_server_root/profiles/
         STPDMgrProfile/config/cells/ProxyCell_Name/nodes/
         ProxyNode_Name/servers/STProxyServer
         ```

      2) Add a `localip` setting with the IP address that corresponds to the host name of the Proxy Server specified during Proxy Server installation.

      Save the file.

      For example:

      ```xml
      <?xml version="1.0" encoding="UTF-8" ?>
      <configuration>
      <server>
      <host>stcommunityserver.example.com</host>
      <port>1516</port>
      <clusterlist />
      ```
b. Synchronize the Proxy Server deployment manager with each Proxy Server application server node.
   1) Log in to the Proxy Server deployment manager's Integrated Solutions Console.
   2) Choose System Administration > Nodes.
   3) For each Proxy Server application node, select the node and click Full Resynchronize.

c. Restart the Proxy Server.

Results

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the logs directory and the ant and native subdirectories.

You can use the collectLogs utility to gather the logs. collectLogs is located at the root of the installation media.

AIX, Linux, or Solaris
/var.ibm/InstallationManager/logs

Console connection log: /tmp/SSCLogs/ConsoleUtility0.log

Windows 2008
%ALLUSERSPROFILE%\IBM\Installation Manager\logs

Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

Windows 2003
%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

Console connection log: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.

What to do next

“Managing trusted IP addresses” on page 1081
Related tasks
“Guided activity: Preparing to install a Sametime Proxy Server” on page 347
This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.
“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.
“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Verifying a Sametime Proxy Server installation for the expanded deployment on AIX, Linux, Solaris, or Windows:

Open the IBM Sametime browser-based client to verify that the installation of a primary node was successful.

About this task
Follow these steps to verify the installation on a primary node. These instructions do not apply to verifying the installation on a secondary node because it does not have installed applications. To verify installation on a secondary node, verify that the installation completed successfully.

Procedure
1. Using a browser, log in to the Sametime Proxy Server application with the following URL:
   http://serverhostname.domain:port/stwebclient/index.jsp
   Replace serverhostname.domain with your server name and add the port number.
   For example:
   http://stproxy1.example.com:9080/stwebclient/index.jsp

   Tip: To verify the port number being used by the application, log in to the console on the Sametime Proxy Server:
   a. Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
      http://serverhostname.domain:8600/ibm/console
      8600 is the default port when the Proxy Server is installed as a Cell Profile.
      For example:
      http://stproxy1.example.com:8600/ibm/console
   b. Enter the WebSphere Application Server User ID and password that you created when you installed the server.
c. Click Servers > WebSphere application servers > STProxyServer > ports > WC_defaulthost to find the port number.

You can also verify the HTTP port number being used by the Sametime Proxy Server by opening the AboutThisProfile.txt file for the Sametime Proxy Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is short_host_nameSTPPNProfile1 when you use a deployment plan to install the server.

2. Verify that you can create or view contacts.

Related tasks
“Logging in to the console” on page 483
Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

Adding the expanded deployment's Sametime Proxy Server to the Sametime Community Server's trusted IP addresses:

Whenever you install a server that communicates with a community server, you must add the new server's IP address to the community server's settings.

About this task

The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server's IP address to the community server.

If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to complete include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).

You do not need to add the system console's IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the Connectivity tab.
5. Under Trusted Servers, enter the IP address of the server that must connect to the Sametime Community Server in the New IP Address field, and click Add.

Note:
If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.

For the media manager, enter the Conference Manager server IP address.

To delete an IP address from the list, select it and click Delete Selected.

6. Click OK.

7. Restart the community server for the change to take effect.

Installing the FIPS Server for the expanded deployment:

IBM Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2). Installing the FIPS Server is only necessary if your Sametime deployment must be FIPS-compliant; otherwise, it is optional.

Before you begin

You should have already installed the IBM Sametime System Console and the Sametime Proxy Server. If you want to administer the FIPS Server from the Sametime System Console, you should have already installed the FIPS administration portlet.

If you did not install the FIPS administration portlet, you can manage the FIPS Server using information in FIPS Support for IBM Sametime 8.

About this task

The FIPS administration portlet can connect to the FIPS Server only if the server is installed on the Sametime Proxy Server. You cannot have multiple FIPS Servers running on the same machine.

Note: Currently, you cannot administer the per-node configuration or vertical clustering of FIPS on the Sametime System Console. The administrative portlet only administers and therefore shows registered cell deployments or horizontal cluster deployments. It will not show individual primary or secondary nodes of the cluster.

Procedure

1. On the server where you will install the FIPS server, enable FIPS on the WebSphere Application Server by following the procedure in Configuring Federal Information Processing Standard Java Secure Socket Extension files.

2. Copy sametimefipsproxy.war from setup\STIPLaunchpad\disk1\FIPSProxy on the image disk to your local drive.

3. Log in to the Integrated Solutions Console on the machine where you are installing the FIPS Server.

4. Click Applications > Application Types > Websphere Enterprise Applications.

5. On the Enterprise Applications page, click Install.

6. Under Path to the new application, browse to the sametimefipsproxy.war file. Keep the default settings to install the server, and then click Next.

7. Enter the context root that you want for the FIPS Server, for example, /fipsProxy.

8. Click Finish and save the configuration.
9. Restart the Sametime Proxy Server to automatically start the FIPS Server.

10. Log in to the Integrated Solutions Console.

11. Click **Sametime System Console > Sametime Servers > FIPS Proxy Servers.**
    You can only edit data for FIPS if the FIPS war is running on the installed server. Make sure that your FIPS Server is running in order to administer it.

12. Click the FIPS Server that you installed.

13. Enter a fully qualified inbound host name and port and an outbound host name and port to which FIPS connects.
    If you are using the FIPS administration portlet, also replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server. Click **OK.**

14. Restart the Sametime Proxy Server again to automatically start the FIPS Server.

15. In a text editor, open the `sametimeProxy.xml` file. This file defines the port routing so the TLS connections can use the proxy to access the Sametime server.
    The file is located in the `\WebSphere\AppServer\profiles\profile_name\installedApps\cell_name\sametimefipsproxy_war.ear\sametimefipsproxy.war` directory.

16. If you are using the FIPS administration portlet, skip to the next step.
    If you are not using the FIPS administration portlet, edit the **SametimeProxyChannel properties** in the `sametimeProxy.xml` file. Replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server.
    In the following entries, replace "temp.sametimeserver.com" with your Sametime server name, for example, "yourserver.yourdomain.com".
    ```xml
    <channel name="SametimeProxyChannel" factory="com.ibm.sametime.proxy.channel.impl.SametimeProxyChannelFactory" sequence="2" weight="1">
      ...
      <property name="serverAddress1" value="temp.sametimeserver.com:8081" />
      <property name="clientAddress2" value="*:1533" />
      <property name="serverAddress2" value="temp.sametimeserver.com:1533" />
      <property name="clientAddress3" value="*:554" />
      <property name="serverAddress3" value="temp.sametimeserver.com:554" />
      ...
    </channel>
    ...
    </channel>
    ```

17. Edit the **TLSInboundChannel properties** in the `sametimeProxy.xml` file:
    - For the `com.ibm.ssl.keyStore` property, replace the `wccmDefault` value of `DummyServerKeyFile.jks` with the actual `keyFileName` and location for the keystore on this WebSphere Application Server. Replace the file: //c: designation with the operating system's absolute path to the file.
    - For the `com.ibm.ssl.trustStore` property, replace the `wccmDefault` value of `DummyServerTrustFile.jks` with the actual `trustFileName` and location for the keystore on this WebSphere Application Server. Replace the file: //c: designation with the operating system's absolute path to the file.
    ```xml
    <channel name="TLSInboundChannel" factory="com.ibm.ws.ssl.channel.impl.SSLChannelFactory" sequence="2" weight="1">
      ...
      <wccmProperty name="com.ibm.ssl.keyStore" wccmPropertyName="keyFileName" wccmPropertyGroup="SecurityPropertyGroup" wccmDefault="C:/WebSphere/AppServer/profiles/profile_name/installedApps/cell_name/sametimefipsproxy_war.ear/sametimefipsproxy.war">
        ...
      </wccmProperty>
      <wccmProperty name="com.ibm.ssl.trustStore" wccmPropertyName="trustFileName" wccmPropertyGroup="SecurityPropertyGroup" wccmDefault="C:/WebSphere/AppServer/profiles/profile_name/installedApps/cell_name/sametimefipsproxy_war.ear/sametimefipsproxy.war">
        ...
      </wccmProperty>
    </channel>
    ```
    - For the `com.ibm.ssl.protocol` property, replace the SSLv3 value with TLSv1.

18. Close and save the file.

19. Restart the Sametime Proxy Server again to put the configuration changes into effect.
Results

Sametime Connect clients use the “Direct connection using TLS” Connection option when setting up the server community connected to the FIPS-enabled server.

Setting up a Sametime Meeting Server:

Before you can migrate meetings from an upgraded IBM Sametime server, you must install a Sametime Meeting Server and then set up URL redirects from the upgraded server to the Sametime Meeting Server.

Installing a Sametime Meeting Server for the expanded deployment:

Follow the instructions for your operating system to install an IBM Sametime Meeting Server.

About this task

Important: If you will be supporting the use of LiveNames in your Sametime deployment, you should deploy all Sametime Meeting Servers and Sametime Proxy Servers within the same subnet. It is suggested that you configure WebSphere Application Server Network Deployment with a single subnet for network traffic. You can use one Network interface card (NIC) on a physical machine or logical partition (LPAR). You can also reference a single Domain name system (DNS) server in the network configuration for the physical machine or LPAR.

Related tasks

“Configuring a Sametime Meeting Server” on page 1031
This section describes how to configure a Sametime Meeting Server.

Creating a database for the Sametime Meeting Server for the expanded deployment on AIX, Linux, Solaris, or Windows:

Before installing the IBM Sametime Meeting Server on AIX, Linux, Solaris, or Windows, create a database to store its data.

About this task

Run the scripts that come with the Sametime Meeting Server package. They are also included with Sametime in the DB2 installation package.

Procedure

1. On the DB2 server, log in to the system as the DB2 administrator created during DB2 installation.
2. Open a command prompt and navigate to the folder where you extracted the SametimeMeetingServer installation package.
3. Create the database by entering one of the following commands from the SametimeDB2 folder. Wait until you see confirmation that the database has been created and the command has finished.
   - AIX, Linux, or Solaris: ./createMeetingDb.sh STMS dbadmin
   - Windows: createMeetingDb.bat STMS dbadmin

Replace STMS in the command if you want to choose a different database name. Names can be from 1 - 8 characters, but cannot contain special or multibyte characters.
Replace \textit{dbadmin} with the DB2 Application User ID you created when you installed DB2. This user has database administration authority.

When naming DB2 objects, follow the rules for your operating system.

4. Close the command window.

5. Open the DB2 control center.
   \begin{itemize}
   \item \textbf{AIX, Linux, or Solaris}
     Open the IBM DB2 folder on the desktop and click \texttt{Control Center}.
   \item \textbf{Windows}
     Click \texttt{Start} > \texttt{Programs} > \texttt{IBM DB2} > \texttt{General Administration Tools} > \texttt{Control Center}.
   \end{itemize}

6. Find the database name to verify that the new database was created.

Related tasks

"Installing DB2 on Linux or Windows" on page 251

Sametime requires a IBM DB2 installation. IBM DB2 9.7 is available for installing with this release of IBM Sametime. The Sametime system console, the Sametime Bandwidth Manager, and the Sametime Meeting Server, use DB2 databases to store information about servers, users, bandwidth configuration, and meetings. Sametime Advanced uses DB2 to store information about persistent chats and broadcast communities.

\textit{Connecting to a DB2 database for the expanded deployment:}

Use the Sametime System Console to connect to the Sametime Meeting Server, Sametime Gateway, or Sametime Advanced database before installing the server from the System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

\textbf{Before you begin}

Start the Sametime System Console if it is not already running.

\textbf{Procedure}

If you have not already opened the Connect to DB2 Databases activity, follow these steps:

1. From a browser, enter the following URL, replacing \texttt{serverhostname.domain} with the fully qualified domain name of the Sametime System Console server.
   \begin{quote}
   \texttt{http://serverhostname.domain:8700/ibm/console}
   \end{quote}
   For example:
   \begin{quote}
   \texttt{http://sametime.example.com:8700/ibm/console}
   \end{quote}

   \textbf{IBM i:} The port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary or use the setting specified for the Administrative console secure port in the AboutThisProfile.txt file. For the Sametime System Console Deployment Manager Profile (STSCDmgrProfile), the file is located in the following path:
   \begin{quote}
   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/
   STSCDmgrProfile/logs/AboutThisProfile.txt
   \end{quote}

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.
3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Sametime Prerequisites > Connect to DB2 Databases**.

**Related tasks**

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Sametime prerequisite: Connecting to a DB2 database for the expanded deployment:**

This activity takes you through the steps for connecting to the Meeting Server, Gateway, or Advanced Server database you created.

**Before you begin**

**AIX, Linux, Solaris, Windows:** Ensure that IBM DB2 has been installed and that you have created the Sametime Meeting Server, Gateway, or Sametime Advanced database.

**IBM i:** Ensure that you have created the required database schemas and tables.

In the **Connect to DB2 Databases** portlet, verify that the Sametime System Console database you created earlier is already displayed in the list of databases.

**About this task**

Follow these steps to connect to the Meeting Server, Gateway, or Advanced Server database. You must do this before you can install the Meeting Server or the Advanced Server using the Sametime System Console. If you installed the server without using the System Console (as is the case with the Sametime Meeting Server on IBM i and Sametime Gateway on any platform), do this step before registering the server with the System Console.

**Procedure**

1. **DB2 Configuration Guided Activity.**
   
   Click **Add** to begin the guided activity that will connect your server to the DB2 database. If a connection already exists, you can optionally edit or delete it.

2. **Add a new database.**
   
   a. In the **Connect to DB2 Databases** portlet, click **Add**.
      
      If you want to edit or delete a database instead, then select one, and click the appropriate button.

   b. Enter the fully qualified host name of the DB2 server in the **Host name** field.
      
      Do not enter an IP address or a short host name.

   c. The **Port** field shows the default port of 50000. Accept the default unless you specified a different port during DB2 installation or your server is using a different port.
      
      Linux: Check the `/etc/services` file on the DB2 server to verify the port number being used.

   d. In the **Database name** field, enter the name of the database you want to connect to.

   e. In the **Application user ID** field, supply the DB2 application's administrative user name that you created when you installed DB2, such as
db2admin. This user has database administration authority and you will use this user ID and password whenever you work with DB2 databases for Sametime. On IBM i, this is the user profile you specified as the owner of the Meeting Server database schemas in your copy of the stms.default.response.properties file or the user profile you logged in with when you created the Gateway database schemas.

f. In the **Application password** field, enter the password for the DB2 administrative user ID.

**g. (Meeting Server or Gateway databases)** If you are connecting to a database on an IBM i server, click **Hosted on IBM i**.

h. Click **Finish**.

---

**Preparing to install a Sametime Meeting Server for the expanded deployment:**

Use the Sametime System Console to prepare to install a Sametime Meeting Server by pre-populating values required for installation.

**Before you begin**

Start the Sametime System Console if it is not already running.

**Procedure**

If you have not already opened the Install Sametime Meeting Server guided activity, follow these steps:

1. From a browser, enter the following URL, replacing `servername.domain` with the fully qualified domain name of the Sametime System Console server.
   
   `http://servername.domain:8700/ibm/console`
   
   For example: `http://sametime.example.com:8700/ibm/console`

2. Enter the WebSphere Application Server user ID and password that you created when you installed the Sametime System Console.

3. On the left side of the navigation tree, click the **Sametime System Console** task to open it.

4. Click **Sametime Guided Activities > Install Sametime Meeting Server**.

**Related tasks**

“Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine” on page 371

When you deploy an IBM Sametime Proxy Server and a Sametime Meeting Server on the same machine using the same server host name, conflicts with cookies that are used by each server can occur. If you install both servers on the same machine, then configure the Sametime Proxy Server with a host alias as a different host name.

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Guided activity: Preparing to install a Sametime Meeting Server for the expanded deployment:**

This guided activity takes you through the steps of creating a deployment plan, which collects information that pre-populates installation screens.
Before you begin

You have set up an IBM DB2 database and an LDAP server, and have run the guided activities for connecting to the DB2 database and to the LDAP server.

About this task

Follow these steps to store a deployment plan on the Sametime System Console to be used when you run the installation program for Sametime Meeting Server.

Procedure

1. Plan a product installation.
   In the Install Sametime Meeting Server portlet, click Create a New Deployment Plan, and then click Next.

2. Deployment Name.
   Give the deployment plan a unique, recognizable name, which will be shown only in the Sametime System Console, and then click Next.
   The name should include the installation and node type, such as stMeeting_primary. You can include multibyte characters, symbols, and spaces in the name. The name can be up to 256 characters and is not case sensitive.

   Select the product version you want to install, and then click Next.

4. Choose the configuration type.
   Select Primary Node if this is the first server of its type. Select Secondary Node for additional servers. Then click Next.
   The Cell option is reserved for special-use cases in which the server must be self-contained. If you select Cell, you must provide a host name, user ID, and password when prompted to do so.

5. Node Federation at Install Time.
   This panel appears if you selected Primary Node or Secondary Node. You can only federate one Primary Node for this type of server in the cell. Select the Sametime System Console cell that will manage this server and then click Next.
   Attention: Each Deployment Manager (including the Sametime System Console when it is used as a Deployment Manager) can support one cluster of each Sametime product. For example, a single Deployment Manager can support a Sametime Proxy server cluster, a Media Manager cluster, and a Meeting server cluster. To create additional clusters for a particular product, install the first server using Cell as the configuration type, which designates it as the Deployment Manager and the primary node for the cluster.

6. WebSphere Profile Settings.
   a. Type the fully qualified host name of the server where you will be installing the Sametime server.
   b. Enter a user name that does not contain any spaces to be used as the WebSphere Application Server administrator on the Sametime server. Supply a password, and then click Next.
      If you must create a user name that contains a space, you may notice that the system console portlet does not appear in the WebSphere Application Server Integrated Solutions Console for the first time. This can be resolved by restarting the system console.
      **Important:** This must be a unique user ID that does not exist in the LDAP directory.
7. Choose a database for this deployment. This panel appears if you selected Primary node or Cell as the configuration type. Select the Sametime Meeting Server database that you configured with the Sametime System Console activity, and then click Next.

8. Connect to an LDAP Server. This panel appears if you selected Cell as the configuration type. Select the LDAP directory that you configured with the Sametime System Console guided activity, and then click Next.

   Review the summary screen, and then click Finish.
   The deployment plan is ready to be used for the server installation. If you need to make any changes, click Modify an Existing Deployment Plan and update the plan. All changes must be made prior to running installation.

What to do next

“Installing a meeting server on AIX, Linux, Solaris, or Windows” on page 438

Installing a Sametime Meeting Server for the expanded deployment on AIX, Linux, Solaris, or Windows:

Run the installation program on the machine where you plan to install a Sametime Meeting Server.

Before you begin

You should have already created a deployment plan for the Sametime Meeting Server. Verify that the deployment plan is in the "Ready to Install" state and start the Sametime System Console server. Be sure there are no firewalls or connectivity problems to the LDAP server or the installation will fail.

Linux
The launchpad installation program launches a web browser to start. You need to be on the console or have an X server and a web browser installed and configured. (VNC or a remote X term session works as well). The graphical library pages must also be installed for Linux so that the Installation Manager works correctly. The /home directory must be writable so that the home directories for the users created by the install are created on the system.

AIX, Linux, and Solaris:
If you are installing using the GUI mode, the full X11 desktop environment is required.

Attention: Check the hosts file and remove any lines that start with the following:
- 127.0.0.1 fully_qualified_domain_name short_name
- ::1 fully_qualified_domain_name short_name

These lines must be removed before installing any Sametime server running on WebSphere Application Server. An issue with WebSphere Application Server causes the server installation to fail if these lines are in the file. Save the file if you make changes.
About this task

By using the deployment plan you created earlier, you have fewer selections to make when you run the installation program.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server deployments.

Procedure

1. Red Hat Enterprise Linux only: Disable Security Enhanced Linux on any Red Hat operating system.
   a. Log in as root on the Linux Red Hat server where you will install the software.
   b. Open the /etc/selinux/config file for editing.
   c. Locate the SELINUX setting. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.

2. Log in to your computer as the system administrator on Microsoft Windows operating systems or as root on Linux operating systems.

   Solaris only: The installation must be performed by the root user using su or a normal login session. Independent sudo packages are not supported on Solaris.

3. Prepare to use the Meeting Server installation package.
   a. To download installation packages:
      1) To download installation packages, you must have an IBM Passport Advantage account. For information on using Passport Advantage, see the topic Using Passport Advantage to download IBM products.
      2) Open this release’s Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
         Locate the components that you need in the document’s listing, then download the packages labelled with the corresponding part numbers to the system on which you are installing.

         Tip: When extracting downloads on Windows operating systems, use a short path location such as C:\ and not a long path location such as the user's desktop or TEMP directories. When extracting to long path locations or deeply nested directories and using the built-in Windows extract utility, corruption is sometimes seen without any warning. This corruption occurs when maximum path lengths on some Windows versions are exceeded.

      b. If you are installing from physical media and your operating system mounts CDs or DVDs automatically with execution privileges turned off, mount the CD or DVD manually instead.

         AIX
         Mount the CD or DVD using the SMIT utility or the appropriate version of the following command:
         mount -v cdrfs -o ro /dev/cd0 /cdrom

         Linux
Mount the CD or DVD using a command similar to the following command:
```
mount /dev/cdrom /cdrom
```

**Solaris**

Mount the CD or DVD.

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:

- **AIX, Linux, and Solaris**
  
  ```
  ./launchpad.sh
  ```

- **Windows**
  
  ```
  launchpad.exe
  ```

**Note:** If you do not have a web browser, go to the Installation Manager package directory and run the installation program (install for Linux or install.exe for Windows). Find the Installation Manager package directory here:

```
sametime_server_package/IM/platform
```

`sametime_server_package` is the installation package name for this server.

`platform` is the operating system on which you are installing.

5. If necessary, select a language other than English from the Select a language list.

6. Click **Install IBM Sametime Meeting Server** and click **Launch IBM Sametime Meeting Server 8.5.2 installation**.

7. If the IBM Installation Manager is not installed, you are prompted to install it. Do so, then click **Finish** to restart the Installation Manager and continue with the next step of the Sametime installation.

   If you do not see a prompt, continue to the next step.

8. If the server is connected to the Internet, skip this step. Otherwise, disable the automatic web update search to allow the installation to run successfully.

   a. In the Installation Manager window, choose **File > Preferences**.

   b. Uncheck **Search service repositories during installation and updates** and click **OK**.

9. Click **Install**.

10. Select the packages that you want to install and click **Next**.

11. Click the **I accept the terms in the license agreements** option and click **Next**.

12. Select a package group option and accept the installation directory. Then click **Next**.

   Select **Create a new package group** if you have not installed any other Sametime software on this machine.

   Leave **Use the existing package group** selected if you are installing several Sametime servers on the same machine.

13. Select **IBM Sametime Meeting Server 8.5.2** as the feature to install and select **Use Sametime System Console to install**. Click **Next**.

14. At the Common Configurations screen, supply values for connecting to the Sametime System Console.

   **Host Name:** Provide the fully qualified domain name in the Host Name field for the Sametime System Console. The host name was determined when you installed the Sametime System Console. The host name must be the actual host name and not a DNS alias.
• **Use SSL**: Leave this option selected to run the server over a secure connection.

• **HTTPs Port**: Leave 9443 as the default value.

• **User ID and password**: Provide the WebSphere Application Server User ID and password that you created when you installed the Sametime System Console.

15. Provide the host name for the machine you are currently using, which is the same name you used when you created the deployment plan for this installation.
Do not use an IP address or short host name.

16. Click **Validate** to log in to the Sametime System Console.
The button name changes to **Validated** after you log in.

17. When you are logged in, click **Next**.

18. Select the Sametime Meeting Server deployment plan you created earlier with the Sametime System Console guided activity. Then click **Next**.

19. Review the deployment settings, then click **Next**.

20. Review the summary, then click **Install** to start the installation.

21. When installation is complete, click **Exit** to close the Installation Manager.

**Results**

If the installation was not successful, look at the installation log files for more information about what occurred during the installation attempt. Fix any problems, then uninstall all components and reinstall. Find information in the **logs** directory and the ant and native subdirectories.

You can use the **collectLogs** utility to gather the logs. **collectLogs** is located at the root of the installation media.

**AIX, Linux, or Solaris**
/var.ibm/InstallationManager/logs

*Console connection log*: /tmp/SSCLogs/ConsoleUtility0.log

**Windows 2008**

%ALLUSERSPROFILE%\IBM\Installation Manager\logs

*Console connection log*: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

**Windows 2003**

%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs

*Console connection log*: Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log

If the logs warn that the node was not federated to the cell after installation, you can register the server manually, a process that also federates the node.
Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 481
Starting and stopping IBM Sametime servers that run on WebSphere Application Server involves other server components such as the Deployment Manager and the node agent.
“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 505
Uninstall IBM Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, or Sametime Advanced on a server running IBM AIX, Linux, Sun Solaris, or Microsoft Windows. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.
“Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows” on page 1223
If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Verifying a Sametime Meeting Server installation for the expanded deployment:

Log in to the Sametime Meeting Server to verify that the installation was successful.

About this task
Verify the installation by logging in to the server. Then try creating a new meeting room.

Procedure
1. From a web browser, navigate to the Meeting Room Center by entering the following URL:
   http://serverhostname.domain/stmeetings
   Replace serverhostname.domain with your server name. For example:
   http://stmeet1.example.com/stmeetings

   Tip: To verify the port number being used by the application, log in to the console on the Sametime Meeting Server:
   a. Enter the following URL, replacing serverhostname.domain with the fully qualified domain name of the server.
      http://serverhostname.domain:8600/ibm/console
      8600 is the default port when the Meeting Server is installed as a Cell Profile.
      For example:
      http://stmeet1.example.com:8600/ibm/console
   b. Enter the WebSphere Application Server User ID and password that you created when you installed the server.
   c. Click Servers > WebSphere application servers > STMeetingServer > ports > WC_defaulthost to find the port number.

You can also verify the HTTP port number being used by the Sametime Meeting Server by opening the AboutThisProfile.txt file for the Sametime
Meeting Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is short_host_nameSTMPNProfile1 when you use a deployment plan to install the server. On IBM i, look for the AboutThisProfile.txt file in the following location:
/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs/AboutThisProfile.txt

2. Click Log In and then enter your User name and Password to log in to the Meeting Center. Use the name and password that is in the LDAP directory connected to the Sametime System Console.

3. Click New Meeting Room, then fill in the fields and click Save.

4. The new meeting appears in the list of meetings that you own. Click Enter Meeting Room below the name of the new meeting to join the meeting.

Setting up calendar integration with the Sametime Meeting Server:

Integrate the IBM Sametime Meeting server with Lotus Domino internet email so that users can receive notifications for online meetings. Each notification contains a link that directs a user to the appropriate Sametime online meeting room.

Before you begin

This feature requires a Lotus Domino server for internet-based email; you cannot use the Sametime Community Server for this purpose.

About this task

Enable calendar integration between the Sametime Meeting Server and a Lotus Domino email server. When a user creates a meeting invitation, the invitation is delivered to the external email address that is set up in these steps. The calendar integration application polls this external email address, and populates the meeting room with the necessary data. Clicking the meeting link contained in the email directs the user to the appropriate Sametime meeting room.

Procedure

1. Configure the Domino server as your internet mail box.
   a. Start the Domino Administrator client.
   b. Click the Configuration tab.
   c. Click the Server section, and then click All Server Documents.
   d. Open the server document for the Domino server you want to edit.
   e. Click Ports > Internet Ports > Mail, and enable the POP and SMTP ports:
   f. Click Save and Close.
   g. Stop and restart the Domino server for the changes to take effect.
   h. When the Domino server starts, the POP service has to be loaded by typing the following in the Domino administration console (or the notes.ini file has to be edited to always start POP when the server starts): load POP3.

2. Make sure SMTP listener task is enabled.
   a. Click the Server section, and then click All Server Documents.
   b. Open the server document for the Domino server you want to edit.
   c. Click Basics, and enable SMTP listener tasks.

3. Edit the person document and enter the Internet address password for your user.
   a. Start the Domino Administrator client.
b. Click the People and Groups tab.

c. Click People and select the user information to be modified, and then click Edit Person.

d. Enter the Internet email address and password for the user.

e. Click Save and Close.

Note: If you want the mail-in messages to go to an external email address and not a Domino user account, enable SMTP routing to external domains by following the instructions in "Setting up SMTP routing to external Internet domains" in the Domino Administrator Help and entering the external address in your online meeting place resource. The external address points to the Sametime Mail-in Database in the resource reservation database by default. Change this to the Internet mail box that has been set up. The user account should also have access of at least reader access to use the online meeting place.

4. Set the Sametime server field in the Domino Administrator client.
   a. Click People & Groups.
   b. Click Mail-in Databases and Resources.
   c. Expand Online Meetings.
   d. Click the online meeting place and enter the name of the Sametime Meeting Server.
   e. Click Save and Close.

5. Create a mail session on the Sametime Meeting Server so that the email account is polled and a Sametime 8.5 meeting room is created for each email in that account.
   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Click Resources > Mail > Mail sessions.
   c. Click CalendarIntegrationMailSession. If a mail session does not exist, create one with the following parameters:
      • Name - CalendarIntegrationMailSession
      • Jndi name - mail/CalendarIntegrationMailSession
      • Enter outgoing and incoming mail properties based on the Internet mail box that you set up previously.
      • Add a custom property to the mail session, _pass and set the value as the password of the incoming email account you used.
   d. Click Apply, and then click Save.

   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
   c. In the Meeting Servers list, click a server with the configuration that you want to change.
   d. Click the Server Configuration tab.
   e. Scroll down to the calinteg.enabled custom configuration key, and click Edit....
   f. Change the value to true.
   g. Click OK.

Setting up URL redirects to migrate meetings:
After you install the new IBM Sametime Meeting Server, you are ready to migrate meetings. Rather than transfer meeting schedules and associated data from the legacy server to the new server, you will set up URL redirects that automatically link users to the appropriate meeting room on the new server.

**Configuring the upgraded server to issue redirects to a Meeting Server:**

Configure an upgraded IBM Sametime Standard server to issue a redirect to a URL hosted on the new Sametime Meeting Server.

**About this task**

You can complete this task on the following servers:

- One or more upgraded Sametime Classic Servers (with meetings enabled)
- One or more pre-8.5 Sametime Standard servers (with meetings enabled)
- Two or more pre-8.5 Sametime Standard servers that are clustered with the Sametime Enterprise Meeting Server

Beginning in release 8.5, Sametime does not directly support the Sametime Enterprise Meeting Server, so you cannot cluster upgraded meeting rooms as in previous releases. However, you can set up URL redirects from pre-8.5 servers that are clustered with the Sametime Enterprise Meeting Server. When a user clicks an old meeting room link, the URL redirect automatically points the browser to the new Meeting Server.

**Procedure**

1. **Enable redirects on the Sametime Community Mux:**
   a. Open the `sametime.ini` file on the server where the Community Mux is hosted.
      
      On AIX, Linux, Windows, and Solaris, the `sametime.ini` file is stored in the Sametime server installation directory; for example on Microsoft Windows, the default path is: `C:\program files\lotus\domino`. On IBM i, the `sametime.ini` file is stored in the Sametime server data directory.
      
      If the Community Mux is local, use the Sametime server's own `sametime.ini` file. If you deployed a stand-alone Community Mux, open the `sametime.ini` file on that server.
   b. Add the following statement to the `[Config]` section of the file:

      `VPMX_HTTP_REDIRECT_ENABLE_RELATIVE=0`
   c. Close and save the file.
   d. Restart the stand-alone Community Mux so the change can take effect.
      
      For a local Community Mux, there's no need to restart the Sametime server yet, as you will do that when you complete the redirect task.
   e. If you deployed multiple stand-alone Community Mux servers, repeat this process on each one.

2. **On the upgraded Sametime server, establish a redirect to the new Meeting Server:**
   a. Log in to a Lotus Notes client.
   b. Click **File > Application > Open**.
   c. In the **Server** field, select the Sametime server where you want to enable the redirect.
      
      Click **Local** to select the current server.
   d. Locate and select the "Domino Directory" (`names.nsf`), and then click **Open**.
e. In the Domino Directory, click **Configuration > Servers > All Server Documents.**

f. In the list of servers, select the Sametime server where you want to create the URL redirect.

g. On the tool bar, click **Web > Create URL/Mapping Redirection.**
   A new page appears, where you can create the redirection/mapping information.

h. On the "Basics" tab, click **URL > Redirection URL.**
i. On the "Mapping" tab, fill in the **Incoming URL path** and **Redirection URL string** fields as follows:
   The redirection documents can be added in stages, depending on which part of the Sametime user interface should be redirected. Use the type of redirect that best suits your needs:

   **Table 87. URL redirect options for various user scenarios**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Incoming URL path</th>
<th>Redirection URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to attend previously scheduled meetings on the upgraded Sametime server, but have all new meetings created as rooms on the Sametime Meeting Server.</td>
<td>/stconf.nsf/frmConference*</td>
<td>[http://host_name/stmeetings/*]</td>
</tr>
<tr>
<td>Only redirect users that access the Welcome page in the meeting center on the upgraded Sametime server.</td>
<td>/stcenter.nsf*</td>
<td>[http://host_name/stmeetings/*]</td>
</tr>
<tr>
<td>Redirect URL that lead directly to individual meetings.</td>
<td>/stconf.nsf/meeting/*</td>
<td>[http://host_name/stmeetings/migration.jsp?mid=*]</td>
</tr>
<tr>
<td>Redirect all other URL paths in stconf.nsf to the new Meeting Server.</td>
<td>/stconf.nsf*</td>
<td>[http://host_name/stmeetings/*]</td>
</tr>
<tr>
<td>Redirect invited server URLs. For each invited server, the redirect document needs to be directed at a single Sametime Meeting Server where the rooms will be created. This avoids creating additional rooms on different Meeting Servers each time a redirect from the invited server is encountered.</td>
<td>/stconf.nsf/WebLookupMeeting?OpenAgent&amp;mid=*</td>
<td>[http://invited_server_host_name/stmeetings/migration.jsp?mid=*]</td>
</tr>
</tbody>
</table>

j. Save your changes and close the Domino Directory.
k. Repeat this process for every upgraded Sametime server that you want to redirect to a new Meeting Server.

---

**Configuring the Meeting Server to accept redirects from the upgraded Sametime server:**

Configure an IBM Sametime Meeting Server to accept URL redirects from an upgraded Sametime server or from a Sametime Enterprise Meeting Server cluster.
About this task

Establishing URL redirect to a Sametime Meeting Server uses the REST API provided by the Sametime Online Meeting Toolkit (included in the Sametime Software Development Kit). The Meeting Server uses the Online Meeting Toolkit to transfer meeting data from the upgraded Sametime server to the new Meeting Server.

The enable the redirect, the new Meeting Server must be configured to be associated with URL of a particular Sametime server.

You can complete this task on the following servers:

- One or more upgraded Sametime 8.5 servers with meetings
- One or more pre-8.5 Sametime server with meetings enabled
- Multiple pre-8.5 Sametime servers (with meetings enabled) that are clustered with the Sametime Enterprise Meeting Server

Sametime 8.5 does not directly support the Sametime Enterprise Meeting Server, so you cannot cluster upgraded Sametime 8.5 meeting rooms as in previous releases. However, you can set up URL redirects from pre-8.5 servers that are clustered with the Sametime Enterprise Meeting Server.

Procedure

1. Log in to the Sametime System Console as the Sametime administrator.
2. Click Sametime Servers > Sametime Meeting Servers.
3. In the 'Meeting Servers' list, click the name of the server that will accept redirects from a particular Sametime server.
4. Click the Server Configuration tab.
5. Click Edit.
6. Type restapi.migrationUrl as the name of the new configuration key.
7. Now assign one of the following values to the key, depending on whether the Sametime server is clustered with Sametime Enterprise Meeting Server:
   - **Sametime server (non-clustered)**: http://host_name/servlet/meeting/
   - **Sametime Enterprise Meeting Server (cluster)**: http://host_name/iwc/sametime/meeting/
     For **host_name**, supply the Sametime server's fully qualified host name; for example: ststd1.example.com
8. Click OK.

Enhancing the deployment with optional components:

After you have upgraded your IBM Sametime deployment and migrated meetings to the new Sametime Meeting Server, you may want to integrate additional components into your deployment.

About this task

The following components are not required for upgrading a Sametime server and migrating meetings, but provide additional capabilities to a Sametime deployment:

- **Sametime Media Manager**: Provides audio and video features for instant messaging and online meetings.
  For more information, see Planning a Sametime Media Manager installation.
• **Sametime Gateway**: Provides instant messaging with external communities, including:
  – Sametime communities deployed outside of your firewall
  – AOL Instant Messenger
  – Google Talk

  For more information, see Planning a Sametime Gateway installation.

**Preparing for SSL encryption after upgrading from Sametime 8.0.x or 7.5.1:**

If SSL is enabled, upgrade the GSKit environment to work with this release of IBM Sametime.

**About this task**

For an upgrade, take only the steps needed to update the components that allow SSL encryption between this release of Sametime Community Server and the LDAP server. Steps 1 and 2 are required for all upgrades. Step 3 only applies if you are running Tivoli Directory Server as your LDAP server.

**Procedure**

1. Upgrade GSKit on the Sametime Community Server to release 8.0.4.16.
2. Update the .jar files for the iKeyMan utility on the Community Server.
3. If you are using Tivoli Directory Server as the LDAP server, upgrade GSKit to a supported release. The server must be running GSKit 7.0.4.28 or later.

**Related tasks**

“Working with Sametime servers that are enabled for SSL” on page 787

Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

**Migrating policy settings from releases earlier than 8.5**

You must manually migrate your pre-8.5 IBM Sametime policy settings from the Administration Tool to new policy settings in the Sametime System Console. Review the settings used in the Administration Tool on the community server and write them down; recreate them on the new system console.

**Note**: Once a Sametime Community server has been registered with the Sametime System Console, the pre-8.5 Administration Tool policy settings are no longer valid.

To see the policy settings on your pre-8.5 Sametime server, click **Administer the Server** on the Sametime server home page (Sametime Welcome page), and then click **Policies**. To set policies in the Sametime System Console, see Creating new user policies.

The following table maps the old policy setting to the new policy and policy setting.

**Note**: Although Sametime Classic meetings are still managed on the server itself, you can set user policy for Sametime Classic meetings on the Sametime System Console.
<table>
<thead>
<tr>
<th>Pre-8.5 Setting</th>
<th>New Policy</th>
<th>New Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must set this server community as the default server community</td>
<td>Instant messaging</td>
<td>User must set this community as the default server community</td>
</tr>
<tr>
<td>Allow file transfer</td>
<td>Instant messaging</td>
<td>Allow user to transfer files</td>
</tr>
<tr>
<td>Allow file transfer - Maximum file size</td>
<td>Instant messaging</td>
<td>Maximum file transfer in Kilobytes</td>
</tr>
<tr>
<td>Allow client to client file transfer</td>
<td>Instant messaging</td>
<td>Allow client-to-client file transfer</td>
</tr>
<tr>
<td>Use exclude file types list</td>
<td>Instant messaging</td>
<td>Use exclude file types transfer list</td>
</tr>
</tbody>
</table>
| Allow telephony                                     | Media manager              | Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings.  
|                                                     |                             | • The pre-8.5 value of Contact lists, instant messaging, and instant meetings is the equivalent of selecting this setting.  
|                                                     |                             | • The pre-8.5 value of No is the equivalent of not selecting this setting. |
| Allow changes to preferred numbers                   | Media manager              | Allow changes to preferred numbers                                          |
| Allow changes to the permanent call routing rule     | Media manager              | Allow changes to the permanent call routing rule                           |
| Allow use of Offline status in call routing rules    | Media manager              | Allow use of "Offline" status in call routing rules                         |
| Allow user to create instant meetings and breakout sessions | Meetings               | Allow user to create instant (nonpersistent) meeting rooms          
|                                                     | Meetings (Sametime Classic Meetings only) | Allow users to create instant meetings and breakout sessions          |
| Allow Sametime IP audio and video for instant meetings and breakout sessions | Meetings (Sametime Classic Meetings only) | Allow Sametime IP audio and video in instant meetings and breakout sessions |
| Allow participation in meeting room chats            | Meetings                   | Meeting room group chats                                                    
<p>|                                                     | Meetings (Sametime Classic Meetings only) | Allow participation in meeting room chats                                    |
| Allow screen sharing                                 | Meetings                   | Allow screen sharing                                                        |
|                                                     | Meetings (Sametime Classic Meetings only) | Allow screen sharing                                                        |
| Allow user to control another user’s shared screen  | Meetings                   | Allow user to control another user’s shared screen                          |
|                                                     | Meetings (Sametime Classic Meetings only) | Allow user to control another user’s shared screen                          |</p>
<table>
<thead>
<tr>
<th>Pre-8.5 Setting</th>
<th>New Policy</th>
<th>New Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow to save chat transcripts</td>
<td>Instant messaging</td>
<td>Allow user to save chat transcripts</td>
</tr>
<tr>
<td>Allow to save chat transcripts - Automatically save chat transcripts</td>
<td>Instant messaging</td>
<td>Automatically save chat transcripts</td>
</tr>
<tr>
<td>Allow to save chat transcripts - Delete automatically saved chat transcripts</td>
<td>Instant messaging</td>
<td>Maximum days to save automatically saved chat transcripts</td>
</tr>
<tr>
<td>Allow client to client voice call</td>
<td>Media Manager</td>
<td>Voice and video capabilities available through the Sametime Media Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with Audio only selected. If Allow client to client voice call was not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>selected in pre-8.5 policy, then select None.</td>
</tr>
<tr>
<td>Set UDP port for voice call</td>
<td>Not a policy. Sametime Media</td>
<td>Sametime System Console &gt; Sametime Servers &gt; Sametime Media Manager &gt;</td>
</tr>
<tr>
<td></td>
<td>Manager server setting.</td>
<td>server-name &gt; Configuration tab. Click Starting UDP port for audio calls.</td>
</tr>
<tr>
<td>Allow client to client video call</td>
<td>Media Manager</td>
<td>Voice and video capabilities available through the Sametime Media Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with Audio and video selected. Video requires audio.</td>
</tr>
<tr>
<td>Set UDP port for video call</td>
<td>Not a policy. Sametime Media</td>
<td>Sametime System Console &gt; Sametime Servers &gt; Sametime Media Manager &gt;</td>
</tr>
<tr>
<td></td>
<td>Manager setting.</td>
<td>server-name &gt; Configuration tab. Click Starting UDP port for video calls.</td>
</tr>
<tr>
<td>Allow custom emoticons</td>
<td>Instant messaging</td>
<td>Allow custom emoticons</td>
</tr>
<tr>
<td>Allow screen captures and images</td>
<td>Instant messaging</td>
<td>Allow screen capture and images</td>
</tr>
<tr>
<td>Set maximum image size for custom emoticons, screen captures and inline images</td>
<td>Instant messaging</td>
<td>Set maximum image size for custom emoticons, screen captures, and inline</td>
</tr>
<tr>
<td>Allow mobile client</td>
<td>Instant messaging</td>
<td>Allow mobile client</td>
</tr>
<tr>
<td>Allow multiple server communities</td>
<td>Instant messaging</td>
<td>Allow user to add multiple server communities</td>
</tr>
<tr>
<td>Allow users to add external users using the Sametime Gateway</td>
<td>Instant messaging</td>
<td>Allow user to add external users using Sametime Gateway communities</td>
</tr>
<tr>
<td>Sametime update site URL</td>
<td>Instant messaging</td>
<td>Sametime update site URL</td>
</tr>
<tr>
<td>Sametime optional add-on site URLs</td>
<td>Instant messaging</td>
<td>Sametime optional plug-in site URLs</td>
</tr>
</tbody>
</table>
Table 88. Migrating policy settings (continued)

<table>
<thead>
<tr>
<th>Pre-8.5 Setting</th>
<th>New Policy</th>
<th>New Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow plug-ins installation</td>
<td>Instant messaging</td>
<td>Allow user to install plug-in</td>
</tr>
<tr>
<td>Limit size of contact list</td>
<td>Instant messaging</td>
<td>Limit contact list size</td>
</tr>
<tr>
<td>Allow all Sametime Connect features to be used with</td>
<td>Instant messaging</td>
<td>Allow all Sametime Connect features to be used</td>
</tr>
<tr>
<td>integrated clients</td>
<td></td>
<td>with integrated clients</td>
</tr>
</tbody>
</table>

Upgrading Sametime clients

Use the information in this section to help users upgrade their Sametime Connect or Notes Embedded 8.0.2 clients to this release.

About this task

It is not necessary to uninstall existing client software before upgrading the Sametime Connect client; you can install the new client directly over the existing version.

For more information, see Upgrading the IBM Sametime client embedded in IBM Lotus Notes to Sametime 8.5.1 in the Sametime wiki.

Related concepts

“Planning client upgrades” on page 247

Sametime Connect and Sametime embedded clients running release 7.5.1 or later can be upgraded directly to this release.

Considerations for upgrading the Sametime Connect client

There are several things you need to know before users upgrade the IBM Sametime Connect client.

About this task

Before upgrading the Sametime Connect client, note the following changes for this release:

- **Upgrading the client will not change the workspace location.**
  Upgrading continues to use the existing location.

- **Upgrading the client will not upgrade the optional Office Integration features.**
  If you do not upgrade them (by uncommenting them in the 8.5.2 manifest) or remove them (by uncommenting them and setting action="uninstall" in the 8.5.2 manifest), the older version will be carried forward.

- **Interoperability between servers and clients installed with different Sametime releases**
  A Sametime client installed with a release prior to 8.5 works with an 8.5.x Community Server without Media Manager installed.
  A Sametime 8.5.x client works with Sametime servers installed with a release prior to 8.5; however, new policies and configurations are not available without a Sametime System Console.

- **Sametime Unified Telephony plugin must be uninstalled before upgrading the Connect client**
Clients running the Sametime Unified Telephony plugin from a release prior to Release 8.5.1 must uninstall the plugin before upgrading the Connect client because the plugin is not compatible with newer releases. Remove the older plugin using operating-system features such as Microsoft Windows Add/Remove Programs.

- **Preferences**
  The location of the workspace does not change for this release. There is no special preference migration required when upgrading from previous Sametime 8.0.x releases.

- **Upgrading the Connect client on Windows**
  When upgrading from an 8.0.x client, the existing install location is presented as a read-only text box. The only option is to upgrade the client instance in the existing location.
  When installing on a Windows machine that already has an existing 7.5.x version of Sametime Connect installed, the existing program directory for 7.5.x should not be used for the upgrade installation because the default installation directory for this release is different from the default location used for 7.5.x. Do not manually change the installation directory to install into an existing 7.5.x location. This will result in a nonfunctioning installation, because the installer will by default attempt to remove 7.5.x at the end of the install. When 7.5.x is removed, its installation directory is cleaned up, which will also remove the newly installed files.

- **Upgrading the Connect client on Linux**
  When upgrading from an 8.0.x client, the RPM command first installs the new client and then uninstalls the older client.

- **Upgrading the Connect client on Mac OS X**
  When upgrading from an 8.0.x client, the installer will replace the older client.

- **Audio/video (A/V) interoperability between releases**
  - All 8.5.x clients (8.5.0, 8.5.1, and 8.5.2) can interoperate with each other and use any 8.5.0, 8.5.1, or 8.5.2 servers.
  - IBM Sametime Connect clients or Sametime embedded clients require a Sametime Media Manager server running Release 8.5.1 or later to be able to make or receive computer audio (voice chat) or video calls.
  - Microsoft Windows XP Tablet PC is not supported.
  - Sametime Media Manager includes additional security and audio-visual quality features that work with clients running Release 8.5.1 or later only. To support 7.5.x, 8.0.x, or 8.5 clients running on an 8.5.1 or later server, disable these features until all clients are running 8.5.1 or later:
    - SRTP
    - TLS
    - RTCP for N-way
  If you leave these features enabled, 8.5 and earlier clients cannot use audio-visual features provided by the Media Manager.

**Supporting older Sametime clients during migration**
Maintaining a flexible login policy during a migration to a new release of IBM Sametime is especially important in environments that include a large number of older Sametime clients. Immediately enforcing a minimum client version can result in a high volume of users experiencing login problems.
You can configure how servers respond to login requests from older client versions. The `sametime.ini` and `STsecurity.ini` files provide settings that enable you to perform the following tasks:

**Specifying the minimum allowed client version**

Each IBM Sametime Community Server is configured to allow logins from a minimum client version.

**About this task**

By default, the Sametime Community Server allows logins from Sametime 7 clients and later. If you have older clients, including those running on Notes 6.5, 7.x and Notes Basic 8.x, you must change the value of the `ST_MINIMAL_CLIENT_VERSION` setting in the `sametime.ini` file so they can continue to login.

All servers in the community **must** have the same `ST_MINIMAL_CLIENT_VERSION` and same `VP_SECURITY_LEVEL` settings (described in "Connecting with older Community Servers on AIX, Linux, Solaris, or Windows") or they cannot communicate with one another.

**Procedure**

1. Open the `sametime.ini` file in a text editor. By default the file is located in the Sametime Community Server installation folder, for example, `C:\Lotus\Domino\Sametime.ini`.
2. In the `[Config]` section of the `sametime.ini` file, specify the minimum Sametime client version that can log in to the server by providing one of the following values for the `ST_MINIMAL_CLIENT_VERSION` setting:

<table>
<thead>
<tr>
<th>Value</th>
<th>Sametime client version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Allows logins for all clients regardless of version</td>
</tr>
<tr>
<td>6510</td>
<td>Sametime 6.5.1 and all Sametime clients running on Notes 6.5, 7.x, and Notes Basic 8.x</td>
</tr>
<tr>
<td>7000</td>
<td>Sametime 7.0 (Default)</td>
</tr>
<tr>
<td>7500</td>
<td>Sametime 7.5</td>
</tr>
<tr>
<td>7501</td>
<td>Sametime 7.5.01</td>
</tr>
<tr>
<td>7510</td>
<td>Sametime 7.5.1</td>
</tr>
<tr>
<td>8000</td>
<td>Sametime 8</td>
</tr>
<tr>
<td>8010</td>
<td>Sametime 8.0.1</td>
</tr>
<tr>
<td>8020</td>
<td>Sametime 8.0.2</td>
</tr>
<tr>
<td>8500</td>
<td>Sametime 8.5</td>
</tr>
<tr>
<td>8510</td>
<td>Sametime 8.5.1</td>
</tr>
</tbody>
</table>

   The client version correlates to the version of the product, and the value is logged in stlog.nsf.
3. Save and close the file.
What to do next

After you specify a minimum version, you can then specify other settings to control how the server responds to login requests from client versions earlier than the specified minimum version.

Related tasks
“Connecting with older Community Servers and clients on AIX, Linux, Solaris, or Windows” on page 701
IBM Sametime Community Servers connect with one another by recognizing a shared connection group ID set by the VP_SECURITY_LEVEL parameter in the sametime.ini file. New and upgraded Community Servers receive this parameter with a setting of 7000 automatically.

Allowing logins from clients that do not conform to the minimum level
By default, the IBM Sametime Community Server automatically logs out users who attempt to connect from clients of versions earlier than the specified minimum. To allow users with earlier clients to continue to access the server during the transition to the new server version, you can configure the server to allow logins from client versions earlier than the specified minimum.

About this task
Maintaining a flexible login policy is especially important in environments that include a large number of older Sametime clients. In such an environment, immediately enforcing a minimum client version can result in a high volume of help desk calls. To avoid locking users out of Sametime, give users several weeks to upgrade and use the ST_FORCE_LOGOUT_OLD_CLIENT_VERSION setting to enable servers to continue to accept logins from earlier client versions. After the deadline for upgrading passes, change the value of the setting to block logins from clients that do not meet the minimum security level.

The ST_FORCE_LOGOUT_OLD_CLIENT_VERSION setting determines whether or not users of old clients are allowed to stay logged in to the community. By default, when this setting is true (a value of 1), old client versions are disconnected. When the setting is false (a value of 0), the users of old clients remain online an usually a message is sent to them.

Note: The VP_SECURITY_ALLOW_USER setting was renamed ST_FORCE_LOGOUT_OLD_CLIENT_VERSION in Sametime 8.5. In order to smooth migration, ST_FORCE_LOGOUT_OLD_CLIENT_VERSION overrides VP_SECURITY_ALLOW_USER from prior versions. If it is not present, then its default value will be 1 and VP_SECURITY_ALLOW_USER or its own default value takes affect.

Procedure
1. Open the sametime.ini file in a text editor. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\Sametime.ini.
2. In the [Config] section of the sametime.ini file, specify whether to allow logins from clients earlier than the minimum allowed version by providing one of the following values for the ST_FORCE_LOGOUT_OLD_CLIENT_VERSION setting:
   • 0 - Allows logins from all clients, regardless of version.
   • 1 - This default setting, rejects login attempts from clients of versions earlier than allowed by the ST_MINIMAL_CLIENT_VERSION setting.
Save and close the file.

**Configuring the server to send announcements to clients that do not conform to the minimum version**

You can use the ST_OLD_CLIENT_VERSION_WARNING_MESSAGE setting in the STSecurity.ini file to provide additional information to users who attempt to log in to the server from Sametime clients running versions earlier than what is allowed by the specified version level.

**About this task**

The ST_OLD_CLIENT_VERSION_WARNING_MESSAGE setting configures the server to automatically respond to login requests from clients that do not conform to the server’s minimum version level by sending an announcement containing specified text. The message you specify functions as either a warning message or a disconnection notification, depending on whether the value of the ST_MINIMAL_CLIENT_VERSION setting allows logins from earlier clients. If the ST_MINIMAL_CLIENT_VERSION setting allows logins, use the text of the message to warn users that they need to upgrade and to explain how to obtain and install the client upgrade. If the ST_MINIMAL_CLIENT_VERSION setting does not allow logins, use the text of the message to explain why login was denied.

Note the following before you configure the settings in the STSecurity.ini file:

- All platforms - Double-byte characters are not allowed in the message text or sender name.
- All platforms - If you want to use accented characters (for example, Æ,é,ä,ñ) in the message text or sender name, you should use Notepad on a Windows client or server to edit the file. When you finish making your changes with Notepad, save the STSecurity.ini file as a UTF-8 file (select File-Save As And specify UTF-8 as the Encoding option, then save the file).
- IBM i platform only - It is recommended that you map a network drive to make the STSecurity.ini file on the server accessible from your workstation. Then you can run Notepad from your workstation and update the file directly on your IBM i server. (By default, the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\STSecurity.ini).
  Alternatively, you can copy the file from the IBM i server to your client workstation using any convenient means (for example, dragging and dropping from IBM i Navigator or FTP), edit the file on your workstation using Notepad, and then copy the updated file back to the server.
- IBM i platform only - When you have updated the file on your IBM i server, ensure that the file is owned by QNOTES. To update the file ownership, run the following command:

  ```
  CHGOWN OBJ('server_data_directory/stsecurity.ini') NEWOWN(QNOTES)
  ```

Use the following procedure to configure the server to send an announcement to users who attempt to log in from client versions earlier than the specified minimum.

**Procedure**

1. Use a text editor to open the STSecurity.ini file. By default the file is located in the Sametime installation folder, for example, C:\Lotus\Domino\STSecurity.ini.
### Value Description

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>(Default) Do not send an announcement.</td>
</tr>
<tr>
<td>text</td>
<td>Specifies the text of the announcement that is sent in response to login requests from clients that do not conform to the server's security level.</td>
</tr>
</tbody>
</table>

The `ST_FORCE_LOGOUT_OLD_CLIENT_VERSION` setting determines whether or not users of old clients are allowed to stay logged in to the community. By default, when this setting is true (a value of 1), old client versions are disconnected. When the setting is false (a value of 0), the users of old clients remain online and usually a message is sent to them.

If the `ST_FORCE_LOGOUT_OLD_CLIENT_VERSION` setting is set to 0 (allow logins from client versions earlier than the specified minimum), and you provide a value for `ST_OLD_CLIENT_VERSION_WARNING_MESSAGE`, the text you provide serves as a warning message. The server allows the login and then sends the specified text. You can use the message to provide users with information on upgrading. For example, you can include an address that specifies the location of a download site. After receiving the announcement with the address link, users can click the address link to open the link location.

**Note:** The `VP_SECURITY_ALLOW_USER` setting was renamed `ST_FORCE_LOGOUT_OLD_CLIENT_VERSION` in Sametime 8.5. In order to smooth migration, `ST_FORCE_LOGOUT_OLD_CLIENT_VERSION` overrides `VP_SECURITY_ALLOW_USER` from prior versions. If it is not present, then its default value will be 1 and `VP_SECURITY_ALLOW_USER` or its own default value takes effect.

To include non-ASCII characters in the message text, save the STSecurity.ini file in UTF-8 format.

2. Save and close the file.

### Configuring the pause in the server before sending an announcement:

Follow these steps to configure the pause in the IBM Sametime Community Server before sending announcement to clients that do not conform to the minimum client version level.

**About this task**

By default, the server waits one second before sending the announcement to users who attempt to log in to the server from IBM Sametime clients running versions earlier than what is allowed by the specified minimum version level. This pause is needed since the full initialization time for some client versions is longer than the others, and without the pause the announcement would reach the client before it could handle it.

In case some users that should get the announcement do not receive it, the pause can be extended to more than one second.
Procedure
1. Use a text editor to open the `sametime.ini` file. By default the file is located in the Sametime installation folder, for example, `C:\Lotus\Domino\sametime.ini`.
2. In the `[Config]` section in `sametime.ini` specify the number of milliseconds that the server waits before sending the announcement in the `VP_SECURITY_PAUSE_INTERVAL` setting.
3. Save and close the file.

Installing the new Sametime client
To upgrade the IBM Sametime Connect or Sametime embedded client, you can install the newer version directly over the existing version.

About this task
For detailed instructions on installing the Sametime Connect or Sametime embedded client, see Deploying the Sametime client to users.

Important:
Clients running the Sametime Unified Telephony plugin from a release prior to Release 8.5.1 must uninstall the plugin before upgrading the Connect client because the plugin is not compatible with newer releases. Remove the older plugin using operating-system features such as Microsoft Windows Add/Remove Programs.

Upgrading the Sametime web audio-visual plugin
Upgrade the IBM Sametime web audio-visual plugin package by copying a newer package to the appropriate server update site.

Updating the Sametime web audio-visual plugin package on the default update site
If you allowed the IBM Sametime web audio-visual plugin package to be configured automatically on the Sametime Proxy Server and have a newer version to deploy, copy the newer package to the host location on the server.

About this task
Follow these steps to copy the upgraded plugin package files to the default location where the Sametime Proxy Server is installed.

Procedure
1. On the Sametime Proxy Server, navigate to the folder where the Sametime Proxy .ear file is installed and web audio-visual plugin is hosted. For example:
   `C:\Program Files\IBM\WebSphere\AppServer\profiles\Proxy_PROFILE_NAME\installedApps\Proxy_CELL_NAME\SametimeProxy.ear\stwebav.war`
2. Back up the original plugin package to a backup folder.
3. Copy the upgraded plugin package to the folder.
4. Restart the Sametime Proxy Server.
Updating the Sametime web audio-visual plugin on an alternate update site

If you posted the IBM Sametime web audio-visual plugin package on an alternate update site and have a newer version to deploy, update the package on the alternate server and update the Web AV Settings on the server.

About this task

Follow these steps to copy the upgraded plugin package files to the alternate HTTP server and update the Web AV Settings on the Proxy Server to reflect the new version.

Procedure

1. Log in to the computer where the HTTP server is installed.
2. Navigate to the HTTP server directory where the plugin package is hosted.
3. Back up the original plugin package to a backup folder.
4. Copy the upgraded plugin package to the folder.
5. Log in to the Sametime System Console.
7. In the Proxy Servers list, click the server with the configuration that you want to change.
8. In the Web AV Settings tab, provide the following details:
   - URL
     The URL remains the same; for example:
     http://Host_name:HTTP_port/directory
   - WebPlayer Version
     Specify the value of the WebPlayer Version in the VersionInfo.txt file included with the Web Meeting Room client package.
   - Softphone Plugin Version
     Specify the value of the Plugin Version in the VersionInfo.txt file included with the Web Meeting Room client package.
9. Click Apply, then click OK.
10. Click System administration > Save changes to master repository.
11. Select Synchronize changes with Nodes. Click Save.
12. Restart the Proxy Server.
   - If the Sametime Proxy Server’s primary node is federated to the Sametime System Console deployment manager, then restart the System Console deployment manager, Proxy Server primary node agent, and Proxy Server.
   - If the Sametime Proxy Server is installed as a Cell profile, then restart the Proxy Server’s own deployment manager, node agent, and server.

Migrating older user IDs to a unique directory attribute

If you are using an older release, you can migrate user IDs to a unique ID, so you do not need to run the name change utility when a person’s name changes in the directory. Having a constant user ID attribute eliminates the need to change a user ID when a name changes.
About this task

Sametime provides RESOLVE mode, which lets you run the name conversion utility one time only, in a way that eliminates the need for additional conversions in the future. The Sametime Community server stores contact and privacy lists in the \texttt{vpuserinfo.nsf} file. RESOLVE mode migrates the \texttt{VpUserInfo.nsf} database, from the old user ID to the new user ID.

If you change the Sametime LDAP configuration to map the user ID to a directory attribute in the person entry that is not likely to change, you eliminate the need to run the Name Change tool when a user’s name changes.

Note: The old name still appears in the contact list for users who have previously added them.

Preparing user IDs for RESOLVE mode

Before you use the name conversion utility in RESOLVE mode, you must make LDAP directory changes (if needed) and IBM Sametime configuration changes.

About this task

If your LDAP directory does not contain an attribute with a unique value in the person entry, then you must change to the schema to provide one. See the documentation provided by your specific LDAP vendor. See also RFC 4530 (http://www.ietf.org/rfc/rfc4530.txt) which introduces the entryUUID attribute in LDAP directories. The value of this attribute is constant by definition, which makes it suitable for the user ID mapping in Sametime. If your LDAP directory does not support this attribute, consider extending the directory schema to support it. If you prefer to use an existing attribute instead of modifying the schema, choose an attribute that is not likely to change when users change their name or relocate. Here are examples of stable attributes in some well-known LDAP servers:

- IBM Directory Server: \texttt{ibm-entryUUID}
- Domino LDAP: \texttt{dominounid}
- Novell Directory Server (NDS): \texttt{guid}
- SunOne: \texttt{nsuniqueid}
- Active Directory: \texttt{objectGUID}

Unlike the ID name conversion mode, which expects a table of oldName and newName entries as input, the RESOLVE mode does not expect any input from the administrator. When the name conversion is run in this mode, it looks up each user ID in the database against the directory, and replaces the old user ID with the directory user ID. The tool accomplishes this by using the StResolve service to look up each person. This requires the administrator to make the LDAP configuration change to use the new user ID mapping before running the tool on every Sametime server in the organization.

Creating a comma-separated value file for RESOLVE mode

A comma-separated value (CSV) file created in a text editor provides the name conversion utility with the information for migrating the old user ID to a new user ID that uses a directory attribute that is not likely to change.

Procedure

1. Use a text editor to create a comma-separated file.
2. Since the RESOLVE mode does not require any additional information, the CSV file is very simple. The content of the CSV file is a single line: RESOLVE.

   **Note:** Create a CSV for only one type of change: RESOLVE. You cannot mix name change types in the same CSV.

3. Name and save the file with an extension of .csv in a directory accessible by the Sametime server.

### Creating a Name Change task for mapping user IDs

Create a name change task on the IBM Sametime Community server.

#### Before you begin

Before you create a name change task, create a comma-separated value (CSV) file of the name changes in the Sametime Community Server directory.

#### About this task

A name change task is not actually a scheduled program; its timestamp merely indicates when the task was created and not when it will be run. The list of tasks is ignored until you run the **stnamechange.cmd** program, which then operates on all of the tasks in the list, using the .CSV files specified in the **Name Change** page.

Follow the steps below to create a name change task.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server where you want to add a name change task. If you want to create a task to run on multiple servers, then click the deployment name of any of the servers on which you want to run the task.
4. Click the **Name Change** tab.
5. Click **New**.

   **Note:** If you only want to edit a task, you can click the name of the scheduled task to edit it.
6. Enter a name in the **Name of Task** field. The name is at your discretion. By default, the name is the date the task is created.
7. Optional: Enter a description for the task.
8. Browse for the CSV file you want to use, and then click **OK**.
9. The name change task appears in the list of scheduled tasks.

   All tasks listed here run when the **stnamechange.cmd** is run.

#### Results

After you have completed these steps on one Sametime Community server, it is necessary to repeat this process on other servers in distributed environment.
When you are finished configuring the task, name changes are saved to the stnamechange.nsf file. For a clustered environment, create this task on one server per cluster. All other servers receive the changes through the cluster replication process.

Lotus Domino picks up all valid name change tasks in the stnamechange.nsf file. You choose the servers or cluster on which the name change task runs on a regular basis using general scheduling tools. The application does not run by default; you must run the task manually.

To Delete a name change task, on the Name Change page, select the task, and then click **Delete**. If any name changes are entered incorrectly, you can import a new CSV file.

### Running the name conversion utility in RESOLVE mode

Running the name conversion utility in RESOLVE mode updates user contact and privacy lists with the new Sametime user ID.

#### Before you begin

The IBM Sametime Community Server must be running. Name change in RESOLVE mode differs from running other name conversion modes, because in RESOLVE mode, the Sametime Community server must be running, so that the name change utility can access **StResolve**. IBM recommends running the name conversion utility at off-peak hours.

Complete all the previous steps outlined in the parent topic, "Migrating older user IDs to a unique directory attribute:

1. Prepare user IDs for RESOLVE mode. The LDAP directory contains a unique and constant attribute in each person entry. The attribute needs to be added to the directory schema if it does not exist, and needs to be populated with a unique value in each person entry. The value needs to be set with a string that will not change when the person’s name changes.
2. Create a CSV file with the RESOLVE mode indicated.
3. Create a name change task.

#### About this task

Running the name conversion utility in RESOLVE mode migrates the old user ID to a new user ID that is a directory attribute that is not likely to change. The tool looks up every user ID in the database against the directory and replaces the old user ID with the directory user ID.

Run the name change task on all the servers in the community. In a clustered environment, run the task for only one server per cluster. The task should run once on the selected server and then replicated to other servers in the cluster.

#### Procedure

1. Change your Sametime Community Server configuration to use a unique user ID, so you run the name change utility in RESOLVE mode. This is controlled in the LDAPServer document in the StConfig.nsf file. See ""Change your Sametime Community Server user ID” on page 781."
2. Gather diagnostic trace information during the task in case it is necessary for future verification. See "Gathering Sametime Community Server name change utility diagnostic data" on page 1205.


4. Follow these steps to run the name conversion utility in RESOLVE mode for your operating system:
   - "Running the name change utility in Resolve mode on Windows"
   - "Running the name change utility in RESOLVE mode on UNIX" on page 786
   - Running the name change utility in RESOLVE mode on IBM i

5. Disable diagnostic traces that you set in step 2.

6. Restart Sametime Community Server.

7. Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well. Restart the Sametime Proxy server as needed.

**Running the name change utility in Resolve mode on Windows**

Follow these steps to run the name conversion utility in RESOLVE mode on Windows.

**Procedure**

1. Disable the Sametime Community Server multiplexor service Sametime Polling service on all servers in the cluster.
   Open the `sametime_installation_directory/STCommLaunch.dep` file in an editor and comment out the following lines by putting a number sign # in front of them:
   
   ```
   #SERVERAPP ST Mux,ST Community,SOFT
   #SERVERAPP ST Polling,ST Mux,SOFT
   ```

2. Restart the Sametime Community Server.

3. Open a command prompt, change to the Domino directory, and then type the following command to run the name conversion utility:
   ```
   stnamechange.cmd
   ```

4. Use the Sametime Administration Tool to change the Sametime Community Server LDAP configuration. See "Change your Sametime Community Server LDAP configuration" on page 782.

5. Enable the Sametime Community Server multiplexer and Sametime Polling services.
   Open the `sametime_installation_directory/STCommLaunch.dep` file in an editor and remove the number sign # from the following lines:
   ```
   SERVERAPP ST Mux,ST Community,SOFT
   SERVERAPP ST Polling,ST Mux,SOFT
   ```

**Change your Sametime Community Server user ID:**

Configure the Sametime Community Server user ID to a directory attribute that is not likely to change.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers.**

3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.

4. Click the **Community Services** tab.

5. Under LDAP Attributes, enter the name of the field within the LDAP person entries that contains the unique value used for logging in. This attribute is used for determining the internal user ID field. This is the value you prepared in "Preparing user IDs for RESOLVE mode".

6. Click **OK**.

**Related tasks**

“Preparing user IDs for RESOLVE mode” on page 778

Before you use the name conversion utility in RESOLVE mode, you must make LDAP directory changes (if needed) and IBM Sametime configuration changes.

**Change your Sametime Community Server LDAP configuration:**

Change your IBM Sametime Community Server LDAP configuration to match the new user ID attribute.

**About this task**

Use the Sametime Administration Tool to change the Sametime Community Server LDAP configuration.

**Procedure**

1. **Open a browser and navigate to the Sametime Community Server.**
   
   Type the following address:
   
   http://host_name/servlet/auth/admin
   
   where **host_name** is the fully qualified host name of the server; for example:
   
   http://commsvr1.acme.com/servlet/auth/admin
   
2. **Enter the administrator name and password specified during the Sametime Community server installation.**

3. **On the Sametime home page, click **Administer the Server.**

4. **Extend the Sametime Community Server LDAP authentication filter.** Skip this step if you are using a Novell LDAP configuration, and see “Creating a customized class for your Sametime Community Server Novell LDAP filters” on page 783.

   a. **Click **LDAP directory > Authentication.**

   b. Append the unique Sametime user ID attribute to the authentication filter. For example if the old filter was:

   ```
   (&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)))
   ```

   and the Sametime user Id is ibm-entryUUID, and the new authentication filter is:

   ```
   (&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(ibm-entryUUID=%s)))
   ```

   c. **Click **Update.**

5. **Extend the Sametime Community Server LDAP search filter to include the new user ID.** Skip this step if you are using a Novell LDAP configuration, and see “Creating a customized class for your Sametime Community Server Novell LDAP filters” on page 783.
a. Click LDAP directory > Searching.
b. Append the chosen Sametime user ID attribute to the **Search filter for resolving person names** filter.

   **Note:** An asterisk should not be added to the Sametime user Id attribute while it should be added to the other attributes.

   For example if the old filter was:
   
   `(&(objectclass=organizationalPerson)(|(cn=%s*)(givenname=%s*)(sn=%s*)))`

   and the Sametime user ID is `ibm-entryUUID`, the new authentication filter is:
   
   `(&(objectclass=organizationalPerson)(|(cn=%s*)(givenname=%s*)(sn=%s*)(ibm-entryUUID=%s)))`

c. Click **Update**.

6. Define the Sametime Community Server LDAP attribute used to distinguish between two similar person names.

   a. Click LDAP directory > Basics.
   b. Set the **Attribute used to distinguish between two similar person names** to **DN** or leave it empty.
   c. Click **Update**.

**Creating a customized class for your Sametime Community Server Novell LDAP filters:**

The resolve and the authentication filters need to be customized Java filters.

**About this task**

The Java code should check whether the string passed by the Sametime Connect client is an escaped binary value. The string contains a backslash followed by 2 hexadecimal digits. In this case only, the GUID attribute should be included in the filter returned by the Java code. Otherwise a regular filter should return from the Java code. This filter should not include the GUID attribute.

For additional information about customized Java filters refer see “Creating custom Java classes for searching the LDAP” on page 332.

```java
public class CustomSearchUUID {

    /**
     * String representing an escaped forward slash sign '/'
     */
    private final static String SLASH_SIGN_CONVERTED = '\\5c';

    /**
     * String representing an escaped * sign '*'
     */
    private final static String STAR_SIGN_CONVERTED = '\\2a';

    /**
     * String representing an escaped opening bracket sign '('
     */
    private final static String OPENING_BRACKET_SIGN_CONVERTED = '\\28';

    /**
     * String representing an escaped closing bracket sign ')
     */
    private final static String CLOSING_BRACKET_SIGN_CONVERTED = '\\29';

    /**
     * String representing an escaped open bracket sign '['
     */
    private final static String OPENING_BRACKET_SIGN_CONVERTED = '\\2b';

    /**
     * String representing an escaped close bracket sign ']
     */
    private final static String CLOSING_BRACKET_SIGN_CONVERTED = '\\2d';

    /**
     * String representing an escaped = sign '='
     */
    private final static String EQUAL_SIGN_CONVERTED = '\\3d';

    /**
     * String representing an escaped = sign '='
     */
    private final static Stringorrar;\n
    public static String convert(String input) {
        if (input == null) {
            return null;
        }

        int length = input.length();
        StringBuilder converted = new StringBuilder();

        for (int i = 0; i < length; i++) {
            char c = input.charAt(i);
            if (c == '\') {
                int escaped = i + 2;
                if (escaped < length) {
                    String escapedString = input.substring(i, escaped);
                    String convertedString = convert(escapedString);
                    if (convertedString == null) {
                        return null;
                    }
                    converted.append(convertedString);
                    i = escaped;
                    continue;
                }
            }

            converted.append(c);
        }

        return converted.toString();
    }

}```
private static String escape(String name)
{
    StringBuffer escapedName = new StringBuffer();
    for (int i=0; i< name.length(); ){
        switch(name.charAt(i)){
        case '\':
            // if the next 2 chars are hex we don't need to escape
            if((i< name.length()-2) && isHex(name.charAt(i+1)) &&
            isHex(name.charAt(i+2))){
                escapedName.append('\');
                escapedName.append(name.charAt(++i));
                escapedName.append(name.charAt(++i));
            }else{
                escapedName.append(SLASH_SIGN_CONVERTED);
            }
            i++;
            break;
        case '*':
            escapedName.append(STAR_SIGN_CONVERTED);
            i++;
            break;
        case '(':
            escapedName.append(OPENING_BRACKET_SIGN_CONVERTED);
            i++;
            break;
        case ')':
            escapedName.append(CLOSING_BRACKET_SIGN_CONVERTED);
            i++;
            break;
        default:
            escapedName.append(name.charAt(i));
            i++;
            break;
        }
    }
    return escapedName.toString();
}

/**
 * Verifies whether this char is a hex char
 * @param c
 * @return
 */
private static boolean isHex(char c){
    boolean hex = true;
    hex = !{( Character.digit(c, 16) == -1);}
    return hex;
}

/**
 * Verifies whether name is a regular text string or an escaped binary value
 * @param name String to be checked
 * @return true if name is an escaped binary value, false otherwise
 */
public static boolean isEscapedBinaryValue(String name)
```java
int index = 0;
int length = name.length();

while ( (index < length - 2) && (name.charAt(index) == '\') )
{
    if ( ( Character.digit(name.charAt(++index),16) == -1 ) ||
        ( Character.digit(name.charAt(++index),16) == -1 ) )
    {
        break;
    }
    index++;
}

if (index == length)
{
    // Reached the end of the string, so name is an escaped binary value.
    return true;
}
else
{
    // name is a regular text string
    return false;
}

public static String authenticationFilter(String name)
{
    String filter = null;
    if (isEscapedBinaryValue(name))
    {
        // name is an escaped binary value, search for UUID only
        filter = "(&objectclass=organizationalPerson)(guid=" + name + ")";
    }
    else
    {
        // name is a regular text string, use the regular filter
        String escapedName = escape(name); //first escape according to LDAP standard
        filter = "(&objectclass=organizationalPerson)(|((cn=" + escapedName + ")((givenname=" + escapedName + ")|(sn=" + escapedName + "))mail=" + escapedName + ")";
    }
    return filter;
}

public static String personResolveFilter(String name)
{
    String filter = null;
    if (isEscapedBinaryValue(name))
    {
        // name is an escaped binary value, search for UUID only
        filter = "(&objectclass=organizationalPerson)(guid=" + name + ")";
    }
    else
    {
        // name is a regular text string, use the regular filter
        String escapedName = escape(name); //first escape according to LDAP standard
        filter = "(&objectclass=organizationalPerson)(|((cn=" + escapedName + ")((givenname=" + escapedName + "))(sn=" + escapedName + "))mail=" + escapedName + "")";
    }
    return filter;
}

public static String groupResolveFilter(String name)
{
    String filter = null;
    if (isEscapedBinaryValue(name))
    {
        // name is an escaped binary value, search for UUID only
        filter = "(&objectclass=organizationalPerson)(guid=" + name + ")";
    }
    else
    {
        // name is a regular text string, use the regular filter
        String escapedName = escape(name); //first escape according to LDAP standard
        filter = "(&objectclass=organizationalPerson)(|((cn=" + escapedName + ")((givenname=" + escapedName + ")|(sn=" + escapedName + "))mail=" + escapedName + ")";
    }
    return filter;
}
```

Chapter 12. Migrating and upgrading 785
// name is an escaped binary value, search for UUID only
filter = "(&(objectclass=groupOfNames)(guid=" + name + "));"
}
else
{
    // name is a regular text string, use the regular filter
    String escapedName = escape(name); //first escape according to LDAP standard
    filter = "(&(objectclass=groupOfNames)(cn=" + escapedName + "));"
}
return filter;
}

Running the name change utility in RESOLVE mode on UNIX
Follow these steps to run the name conversion utility in RESOLVE mode on UNIX.

Procedure
1. Disable the Sametime Community Server multiplexor service on all servers in the cluster.
   a. Stop the IBM Sametime Community Server.
   b. Open a shell and edit the data-directory/STCommLaunch.dep file and comment out the following line by putting a number sign # in front of it:
   
   #SERVERAPP stmux_launcher.sh,stserver,SOFT
   #SERVERAPP stpolling,stserver,SOFT
   
   c. Restart the Sametime Community Server. This starts the server without running Sametime Community Server multiplexer service. Name change in RESOLVE mode differs from running other name conversion modes, because in the RESOLVE mode the Sametime Community server should be running, so that the name change utility can access StResolve

2. Restart the Sametime Community Server.

3. Open a shell and change to the Domino data directory. Type the following command:

   ./stnamechange.sh <domino_bin_directory> <domino_data_directory>

   For example:

   . /stnamechange.sh /domino/opt/lotus/notes/80020/linux /domino/notesdata

4. Use the Sametime Administration Tool to change the Sametime Community Server LDAP configuration. See “Change your Sametime Community Server LDAP configuration” on page 782

5. Enable the Sametime Community Server multiplexor service on all the servers in the cluster.
   a. Stop the IBM Sametime Community Server.
   b. Open a shell and edit the data-directory/stcommLaunch.dep file and remove the number sign # from the following line:
   
   SERVERAPP stmux_launcher.sh,stserver,SOFT
   SERVERAPP stpolling,stserver,SOFT
Chapter 13. Configuring

After setting up your initial IBM Sametime environment, you may want to make additional changes, such as setting client preferences, configuring connections to other servers, enabling SSL or single sign-on.

This section contains information about enlarging and securing your Sametime environment.

Configuring security

After setting up your initial IBM Sametime environment, you may want to make additional changes to safeguard information at your site, including limiting user access to certain features, using encryption, and modifying default security settings.

This section contains information about securing your Sametime servers running on Domino and WebSphere Application Server.

Important: For security, IBM recommends that you configure an HTTPS environment using SSL encryption for all Sametime Meeting Server deployments.

Working with Sametime servers that are enabled for SSL

Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

Configuring Sametime Community Server to use SSL encryption

Configure IBM Sametime Community Server to use SSL (Secure Socket Layer) for its services; and configure HTTPS when communicating with Web clients or enable LDAPS (LDAP over SSL) with LDAP server.

About this task

You can encrypt communications for Sametime Services and the communication between Sametime and web browsers. You can also encrypt communications between an LDAP server and the Sametime server with the LDAPS protocol.

You can set up either, or both, of these protocols independently. If you are upgrading from a previous release, take steps to upgrade the GSKit and iKeyMan utility as described in the related topic.

Related tasks

“Preparing for SSL encryption after upgrading” on page 630

If SSL is enabled, upgrade the GSKit environment to work with this release of IBM Sametime.

Enabling encryption for Sametime Services, and between Sametime and web browsers:

Configure SSL encryption for IBM Sametime Services and enable HTTPS for Web browsers.
About this task

Enabling SSL encryption with the HTTPS (browser-based) protocol involves the following tasks:

Preparing Lotus Domino to use SSL:

Because IBM Sametime resides on an IBM Lotus Domino server, you must enable the Lotus Domino server's HTTP component to support Secure Socket Layer (SSL) before you can configure the Sametime server to encrypt communications.

About this task

Follow these steps in the Lotus Domino Administrator information center to set up a Lotus Domino server to support SSL for HTTP connections:

Setting up SSL on a Domino server

Preparing Sametime to use SSL:

Set up SSL encryption on the IBM Sametime server by importing the SSL certificate used by IBM Lotus Domino and configuring the Sametime server to use it.

About this task

Install the GSKit and use the IKeyMan program to create a keystore on the Sametime server before you import the Lotus Domino server's SSL certificate and complete configuration changes to enable support for SSL. Complete the following tasks in the sequence shown:

Setting up a keystore for the SSL certificate used by Lotus Domino:

Install the IBM GSKit with the IBM IKeyMan utility and then create a keystore file to hold the IBM Lotus Domino server's SSL certificate.

About this task

Sametime on IBM i already includes a keystore file called stkeys.jks, so you can skip this procedure and proceed directly to obtain and import a copy of the SSL certificate from the Lotus Domino server into the Sametime server.

On IBM AIX, Linux, Solaris, and Microsoft Windows, you must create the keystore file yourself by completing the following tasks:

Installing GSKit on the Sametime Community Server:

To configure the server for SSL, you must install the most recent release of GSKit provided with IBM Sametime. Install GSKit on the IBM Sametime Community Server.

Installing GSKit on a Sametime Community Server (AIX):

Install GSKit on a server that runs on IBM AIX.
About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on AIX, follow the steps below:

Procedure
1. Log on to the server as the root user.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.
   
   Open this release’s Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
4. Expand the GSKit package.
5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Change to the directory into which you expanded the package.
   b. Uncompress the .tar files by using the following commands:
      
      zcat gskcrypt32-version_number.aix.ppc.tar.Z | tar -xf -
      zcat gskssl32-version_number.aix.ppc.tar.Z | tar -xf -
      
      The string version_number represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.
   c. Install GSKit v8 by using the following command:
      
      inutoc /tmp/gsk8
      installp -acgw -d /tmp/MQ/gsk8 GSKit8.gskcrypt32.ppc.rte \
      GSKit8.gskssl32.ppc.rte \
      GSKit8.gscrypt32.ppc.rte \
      GSKit8.gskssl32.ppc.rte
      
      /tmp represents the directory into which you expanded the package.
6. Set the JAVA_HOME environment variable to the java VM installed under the Sametime binaries directory:
   
   JAVA_HOME=/opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/

Installing GSKit on a Sametime Community Server (Linux):

Install GSKit on a server that runs on Linux.

About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on Linux, follow the steps below:

Procedure
1. Log on to the server as the root user.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.
   
   Open this release’s Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
4. Expand the GSKit package into a temporary directory.
5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Change to the temporary directory where you expanded the GSKit package.
   b. Install the packages into the `usr/lib` directory by using the following command:
      ```
      rpm -Uv -ivh /usr/lib gskcrypt32-version_number.linux.arch.rpm gskssl32-version_number.linux.arch.rpm
      ```
      The string `version_number` represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.
      The string `arch` represents your system architecture, for example x86.

6. Set the `JAVA_HOME` environment variable to the Java VM installed under the Sametime binaries directory:
   ```
   JAVA_HOME=/opt/ibm/lotus/notes/latest/linux/ibm-jre/jre export JAVA_HOME
   ```

   **Installing GSKit on a Sametime Community Server (Solaris):**

   Install GSKit on a server that runs on Solaris.

   **About this task**

   IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

   To install GSKit on Solaris, follow the steps below:

   **Procedure**
   1. Log on to the server as the root user.
   2. Stop the Lotus Domino and Sametime server.
   3. Download the GSKit package to a temporary location on the server.
      Open this release's Download document at the following web address:
      https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   4. Expand the GSKit package.
   5. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
      a. Change to the directory into which you expanded the package.
      b. Uncompress the .tar files by using the following commands:
         ```
         zcat gskcrypt32-version_number.sun.sparc.tar.Z | tar -xf -
         zcat gskssl32-version_number.sun.sparc.tar.Z | tar -xf -
         ```
         The string `version_number` represents the version number of GSKit being installed, such as 8.0.14.6, and can vary as new modifications of GSKit are released.
      c. Install GSKit v8 by using the following command:
         ```
         pkgadd -d gsk8cry32 gsk8ss32 gsk8cry64 gsk8ss64
         ```
   6. Set the `JAVA_HOME` environment variable to the java VM installed under the Sametime binaries directory:
      ```
      JAVA_HOME=/opt/ibm/lotus/notes/latest/sunspa/ibm-jre/export JAVA_HOME
      ```

   **Installing GSKit on a Sametime Community Server (Windows):**

   Install the GSKit on a server that runs on Windows.
About this task

IBM Lotus Domino also ships with a version of GSKit, but for this task you must use the version included with Sametime.

To install GSKit on Microsoft Windows, follow the steps below:

Procedure
1. Log on to the server as the Windows administrator.
2. Stop the Lotus Domino and Sametime server.
3. Download the GSKit directory to a temporary location on the server.
   Open this release's Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
4. Extract the GSKit package to a temporary directory.
5. Open a command prompt and navigate to the path of the temporary directory.
6. Install GSKit to the relevant operating system (32-bit or 64-bit) as follows:
   a. Double-click the gsk8crupt32.exe file and follow the installation prompts,
      and progress through the wizard following the prompts until the product is
      successfully installed.
   b. Repeat for the gsk8ssl32.exe file.
7. Set the JAVA_HOME environment variable to the Java VM installed under the
   Sametime binaries directory:
   a. From the Windows desktop, right click on the My Computer icon and select
      System Properties.
   b. In the "System Properties" dialog box, select the Advanced tab.
   c. Click the Environment Variables button.
   d. In the "New System Variable" dialog box, click the New button under the
      "System Variables" list, and enter the following information:

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Variable value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVA_HOME</td>
<td>Sametime_install_root\ibm-jre\jre</td>
</tr>
</tbody>
</table>

   e. Click OK to close the "New System Variable" dialog box.
   f. Click OK to close the "Environment Variables" dialog box.
   g. Click OK to close the "System Properties" dialog box.

Updating the .jar files for the iKeyMan utility:

The iKeyMan utility on the IBM Sametime Community Server requires a specific
version of the Java runtime environment and updated .jar and java security files
for this release.

Procedure
1. On the Sametime Community Server, download and Install Java 1.6 SR 3 from
   the Java web site into a java6sr3 directory.
2. Navigate to the Sametime_install_root\ibm-jre\lib\ext directory.
3. Find gskikm.jar and ibmcmsprovider.jar, back them up in a different folder,
   but with the same names. Then remove them from the ext directory.
4. Copy gskikm.jar and ibmcmsprovider.jar from java6sr3\jre\lib\ext to the Sametime_install_root\ibm-jre\jre\lib\ext directory.

5. Use a text editor to add com.ibm.security.cmskeystore.CMSProvider to the list of providers in the java.security file as follows:
   a. Navigate to the Sametime_install_root\ibm-jre\jre\lib\security directory. For example:
      AIX
      /opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/lib/security
      Linux
      /opt/ibm/lotus/notes/latest/linux/ibm-jre/jre/lib/security/
      Solaris
      /opt/ibm/lotus/notes/latest/sunspa/ibm-jre/jre/lib/security/
      Windows
      C:\Program Files\Lotus\Domino\ibm-jre\jre\lib\security
   b. Open the java.security file.
   c. In the java.security file, and add the following statement to the list of security providers as shown, where number is the last sequence number in the list.
      security.provider.number=com.ibm.security.cmskeystore.CMSProvider
      The example below illustrates this line added to the java.security file (notice that the preference numbers must be in sequence):
      ## List of providers and their preference orders (see above)##
      security.provider.1=com.ibm.jsse.IBMJSSEProvider
      security.provider.2=com.ibm.crypto.provider.IBMJCE
      security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
      security.provider.4=com.ibm.security.cert.IBMCertPath
      security.provider.5=com.ibm.security.cmskeystore.CMSProvider
      #
   d. Close and save the file.

Creating a keystore file for the Domino server’s SSL certificate:

Use the IBM IKeyMan utility and to create a keystore .jks file on the IBM Sametime Community Server, which will be used for storing a copy of the IBM Lotus Domino server’s SSL certificate.

About this task

On IBM AIX, Linux, and Solaris, create a keystore file is called keys.jks; on Microsoft Windows, call it stkeys.jks.

Note: On IBM i, the keystore already exists; skip this procedure.

Follow these steps to create a keystore file on the Sametime Community Server:

Procedure

1. Open a command prompt and navigate to the Sametime_install_root\ibm-jre\jre\bin directory. For example:
   AIX
   /opt/ibm/lotus/notes/latest/ibmpow/ibm-jre/jre/bin
   Linux
   /opt/ibm/lotus/notes/latest/linux/ibm-jre/jre/bin
2. Start the IKeyMan program by running the following command:
   - AIX, Linux, and Solaris
     ```
     java com.ibm.gsk.ikeyman.Ikeyman
     ```
   - Windows
     ```
     ikeyman.exe
     ```
3. Click **Key Database File > New**.
4. In the "New" dialog box, complete these fields and then click **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key database type</td>
<td>Accept the default of jks.</td>
</tr>
</tbody>
</table>
   | File name       | Enter a file name for the key database:
   |                 | • AIX, Linux, Solaris: keys.jks
   |                 | • Windows: stkeys.jks |
   | Location        | Choose the directory in which the 'stkeys.jks' file will be stored. The examples in this documentation assume the file is stored in the `Sametime_install_root/jvm/bin` directory. |

5. In the "Password" dialog box, complete these fields and then click **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Type the password that you will use to access the keystore. You will need this password later in the procedure.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the password again to confirm it.</td>
</tr>
</tbody>
</table>
   | Set expiration time? | Click this option to enable it and type the number of days for which the password will remain valid.
   |                 | If you do not want the password to expire, leave this option disabled. |

*Obtaining a copy of the SSL certificate used by Lotus Domino:*

When the IBM Lotus Domino server is configured to use SSL, an SSL server certificate is received from a Certification Authority (CA) and merged into the Lotus Domino Server Certificate Admin database. When you configure SSL for IBM Sametime, you import a copy of this certificate to the Sametime server.

*About this task*

There are two versions of the SSL certificate that you can use:

*Obtaining the SSL certificate directly from the Lotus Domino server:*

When configuring SSL for IBM Sametime, you can import a copy of the SSL certificate directly from the IBM Lotus Domino server.
About this task

When the Lotus Domino server was configured to use SSL, an SSL server certificate was received from a Certification Authority (CA) and merged into the Lotus Domino Server Certificate Admin (certsrv.nsf) database. In this procedure, you export a copy of that certificate and save it as a file so that you can import it into Sametime in a later task.

Procedure

1. Open a browser and navigate to the Lotus Domino server where you enabled SSL.

   **Note:** The steps below use the Microsoft Internet Explorer browser; steps for your own browser may differ.

   You can locate the Lotus Domino server by navigating to the Sametime server that is hosted on the same computer, using an address similar to the following (replace Sametime.acme.com with your fully qualified Internet host name):

   https://Sametime.acme.com

2. Install the SSL certificate in Microsoft Internet Explorer to ensure it is available for export:

   a. When prompted to “select the certificate to use when connecting,” click **OK**.
   b. At the "Security Alert" dialog box, click **View Certificate**.
   c. At the "Certificate" dialog box, click **Install Certificate**.
   d. At the "Certificate Manager Import Wizard" screen, click **Next**.
   e. Click the **Automatically select the certificate store based on the type of certificate** option, and then click **Next**.
   f. Back at the "Certificate Manager Import Wizard" screen, click **Finish**.
   g. When the message indicating that the SSL server certificate was imported successfully appears, click **OK** repeatedly until you have closed all of the dialog boxes.

3. Now export the SSL certificate from Internet Explorer and save it as a file.

   a. From the browser, click **Tools > Internet Options**.
   b. Click the **Contents** tab.
   c. Click the **Certificates** button.
   d. Click the **Other People** tab.
   e. Scroll down the list of certificates and select the server certificate that you imported earlier in this procedure.

      The certificate name should provide some indication that the certificate is associated with the Domino server from which it was imported. For example, if the certificate was imported from a server named Sametime.acme.com, the certificate might be issued to "Sametime" or to "Example."
   f. Click the **Export** button.
   g. At the "Certificate Manager Export Wizard" screen, click Next.
   h. At the "Certificate Export File" screen, select **Base64 encoded X.509 (.CER)**, and then click **Next**.
   i. At the "Export File Name" screen, provide a name for the file, select the Sametime server's data directory as the location where you want to store the file, and then click **Next**.
For example, on Windows, you might enter SSLservercertificate.cer as the file name, and select C:\Lotus\Domino\data as the location.

Note: On IBM i, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation and transfer it to your IBM i server later.

j. When the message appears indicating the export was successful, click OK.

Obtaining a copy of the trusted root certificate:

If you are unable to obtain a copy of the IBM Lotus Domino server’s SSL certificate, you can request a trusted root certificate from a CA or export a trusted root certificate from your web browser.

About this task

If you need to obtain a trusted root certificate, you must obtain the same trusted root certificate that is used by the Domino server to sign the Domino SSL server certificate. For example, if the VeriSign Class 4 Public Primary Certification Authority trusted root certificate is used to sign the Domino SSL server certificate, you must either export this certificate from your web browser or request a VeriSign Class 4 Public Primary Certification Authority trusted root certificate from VeriSign.

There are two ways to obtain a copy of the trusted root certificate:

Obtaining a trusted root certificate from the web browser:

When configuring SSL for the IBM Sametime server, you can import a copy of the trusted root certificate that was used for signing the IBM Lotus Domino server’s own SSL certificate from a web browser, and then import it in the Sametime server’s key store.

About this task

Rather than obtaining a copy of the Lotus Domino server’s own SSL certificate, you may choose to obtain a copy of the trusted root certificate that was used for signing the Lotus Domino server’s certificate. The easiest way to obtain a trusted root certificate is to export one from your web browser.

Web browsers include many different SSL trusted root certificates by default. If your Web browser contains a trusted root certificate that corresponds with the Lotus Domino server’s trusted root certificate that was used to sign the Lotus Domino SSL server certificate, you can export it from the browser and save it as a file.

Note: You must use the same trusted root that signed the Lotus Domino server’s own SSL certificate.

The procedure below illustrates how you can export a trusted root certificate from a Microsoft Internet Explorer web browser:

Procedure

1. From the browser, click Tools > Internet Options.
2. Click the Contents tab.
3. Click the **Certificates** button.
4. Select the **Trusted Root Certification Authorities** tab.
5. Select the appropriate trusted root certificate from the list.
6. Click the **Export** button.
7. At the “Certificate Manager Export Wizard” screen, click **Next**.
8. At the “Certificate Export File” screen, select **Base64 encoded X.509 (.CER)**, and then click **Next**.
9. At the “Export File Name” screen, provide a name for the file, select the Sametime server’s data directory as the location where you want to store the file, and then click **Next**.

   For example, on Windows, you might enter `SSLservercertificate.cer` as the file name and select `C:\Lotus\Domino\data` as the location.

   **Note:** On IBM i, save the file directly to your server if you have mapped to the server drive. Otherwise, save the file on your client workstation and transfer it to your IBM i server later.
10. When the message appears indicating that the export was successful, click **OK**.

---

**Obtaining a trusted root certificate from the Certification Authority:**

When configuring SSL for the IBM Sametime server, you can obtain a copy of the trusted root certificate used for signing the IBM Lotus Domino server’s SSL certificate from the original Certificate Authority.

**About this task**

If you are unable to obtain a copy of the Lotus Domino server’s SSL server certificate, you can request a copy of the trusted root certificate from a CA.

Normally, you request a certificate from a CA by browsing to the CA’s website. For example, follow these steps to request a certificate from VeriSign:

**Procedure**

1. Open a browser and navigate to the VeriSign site:
   
   `www.verisign.com`
2. Follow the instructions on the website to request a certificate.
   
   Once the certificate request is approved, you will receive an email explaining how to pick up the certificate.
3. Pick up the certificate as instructed (for example, by browsing to the website and copying it from a field on the specified page).
   
   You can provide a file name for the certificate when receiving it from the CA and then store it in the Sametime server’s data directory.

**Importing the Lotus Domino server’s SSL certificate into the keystore:**

After you obtain a copy of either the IBM Lotus Domino server’s own SSL certificate, or the trusted root certificate that was used to sign it, import your copy into the IBM Sametime server’s keystore.
About this task

The procedure for importing the SSL certificate depends on your operating system:

Importing an SSL certificate on AIX, Linux, Solaris:

To enable SSL between IBM Sametime running on IBM AIX, Linux, or Solaris, import the IBM Lotus Domino server's SSL certificate into the keystore.

Before you begin

Make sure you have copied one of the following certificates from the server into the Sametime server's data directory:
- CA.txt (the trusted root certificate)
- Server.txt (the SSL server certificate)

About this task

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

Procedure

1. Verify that the `ikeyman.sh` file's SAMETIME_HOME variable specifies the correct path for your server's installation directory, modifying it as needed.
   The default installation directories for Sametime are as follows:
   - AIX: `/opt/ibm/lotus/notes/latest/ibmpow`
   - Linux: `/opt/ibm/lotus/notes/latest/linux`
   - Solaris: `/opt/ibm/lotus/notes/latest/sunspa`

2. Make sure the `ikeyman.sh` file has execute privileges.

3. Start the `ikeyman.sh` utility.
   The `ikeyman.sh` utility requires a graphical interface. If you run it in a text-only terminal, be sure to redirect the display to an x-windows session.

4. Click the Add button.

5. In the "Add CAs certificate from a File" dialog box, do the following:
   a. Verify that Base64-encoded ASCII data is selected as the "Data type".
   b. Set the Certificate file name to the name of the text file (for example, CA.txt) into which you copied the certificate.
   c. Set the Location to the location to which you transferred the CA.txt file in the previous procedure (for example, /local/notes/data).
   d. Click OK.

6. Close IKeyMan after the file is imported successfully.

Importing an SSL certificate on IBM i:

To enable SSL between IBM Sametime running on IBM i, import the IBM Lotus Domino server’s SSL certificate into the keystore.

Before you begin

Make sure you have copied one of the following certificates from the server into the Sametime server's data directory:
- CA.txt (the trusted root certificate)
About this task

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

Procedure
1. From an IBM i command line, run the following command to start qshell:
   ```
   strqsh
   ```
2. From qshell, run the following keytool command:
   ```
   keytool -import -alias certificate_name
   -file certificate_filename
   -storepass keystore_password
   -keystore keystore_path_and_filename
   ```
   Where:
   - `certificate_name` is `CA.txt`
   - `certificate_filename` is also `CA.txt`
   - `keystore_password` is "sametime."
   
   Note: On IBM i versions of Sametime, `stkeys.jks` is provided by default and uses "sametime" as the default password
   - `keystore_path_and_filename` is `stserver/data/stkeys.jks`
   
   Example:
   ```
   keytool -import -alias stserver1cert
   -file /stserver/data/CA.txt
   -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```
3. After you have imported the certificate, use the following command to view the list of certificates in the `stkeys.jks` file and verify that the certificate was imported successfully:
   ```
   keytool -list -storepass keystore_password
   -keystore keystore_path_and_filename
   ```
   Example:
   ```
   keytool -list -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```
4. Press F3 to exit qshell.

Importing an SSL certificate on Windows:

To enable SSL between IBM Sametime running on Microsoft Windows, import the IBM Lotus Domino server's SSL certificate into the keystore.

Before you begin

Make sure you have copied one of the following certificates from the server into the Sametime server's data directory:
- CA.txt (the trusted root certificate)
- Server.txt (the SSL server certificate)
About this task

Follow the steps below to import the SSL certificate into the keystore on the Sametime server:

Procedure

1. Open a command prompt and navigate to the `Sametime_install_root\ibm-jre\jre\bin` directory.
   The default installation path for Sametime is `C:\Lotus\Domino`.
2. Start the IKeyMan utility by running the `ikeyman.exe` program.
3. Browse to and select the `stkeys.jks` key store file.
4. Enter the password required to access this file.
5. In the "Key database content" area, select Signer certificates.
6. Click the Add button.
7. In the "Add CAs certificate from a File" dialog box, do the following:
   a. Verify that Base64-encoded ASCII data is selected as the "Data type"
   b. Browse to and select the SSL certificate you want to import.
   c. Click OK.
8. In the "Enter a Label" dialog box, do the following:
   a. Type a label for the certificate.
      This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program.
   b. Click OK.
      The new certificate's label appears in the list of Signer Certificates.
10. Close the IKeyMan utility.

Modifying the Sametime server configuration for SSL:

Modify the configuration of the IBM Sametime server to encrypt connections.

About this task

Modify the Sametime server's configuration by making changes to the `sametime.ini` file. The necessary changes vary with your operating system:

Modifying the Sametime configuration on AIX, Linux, Solaris:

Modify the IBM Sametime server's `sametime.ini` file on IBM AIX, Linux, or Solaris to support Secure Socket Layer (SSL) encryption.

About this task

To modify the Sametime configuration, complete the following steps:

Procedure

1. Stop the Sametime server.
2. Use a text editor to open the `sametime.ini` file.
   This is located in the Sametime installation directory.
3. Locate the `ConfigurationPort=` setting. Make sure that it specifies the port on which the Lotus Domino HTTP server listens for SSL connections (by default, this is port 443), modifying the setting if necessary.

For example:
```plaintext
ConfigurationPort=443
```

4. If these settings are not present in the `[Config]` section at the bottom of the `sametime.ini` file, manually type them in:

```plaintext
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=/local/notesdata/key.jks
javax.net.ssl.trustStore=/local/notesdata/key.jks
javax.net.ssl.keyStorePassword=keystore_password
javax.net.ssl.trustStorePassword=truststore_password
```

**Note:** Specify the complete path name of the `key.jks` file for both the `javax.net.ssl.keyStore` and the `javax.net.ssl.trustStore` settings. Specify the password that you provided for `key.jks` when you created it for both the `javax.net.ssl.keyStorePassword` and `javax.net.ssl.trustStorePassword` settings.

5. If these two lines appear in the `sametime.ini` file, remove them:
```plaintext
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.keyStoreType=JKS
```

6. Save and close the `sametime.ini` file.

7. Restart the Sametime Community Server.

*Modifying the Sametime Configuration on IBM i:*

Modify the IBM Sametime server's `sametime.ini` file on IBM i to support Secure Socket Layer (SSL) encryption.

**About this task**

To modify the Sametime configuration for IBM i, complete the following steps:

**Procedure**

1. Stop the Sametime server.
2. Use a text editor to open the `sametime.ini` file.
   
   This is located in the Sametime server's data directory.
3. Locate the `ConfigurationPort=` setting. Make sure that it specifies the port on which the Lotus Domino HTTP server listens for SSL connections (by default, this is port 443), modifying the setting if necessary.
   
   For example:
   ```plaintext
   ConfigurationPort=443
   ```

4. If these settings are not present in the `[Config]` section at the bottom of the `sametime.ini` file, manually type them in:

   ```plaintext
   [Config]
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=stkeys.jks
   javax.net.ssl.trustStore=stkeys.jks
   javax.net.ssl.keyStorePassword=sametime
   javax.net.ssl.trustStorePassword=sametime
   ```

   **Note:** By default, the password for the `stkeys.jks` file is "sametime." If you change the password for `stkeys.jks`, you must change the setting of both
javax.net.ssl.keyStorePassword and javax.net.ssl.trustStorePassword to match the new password. The full path for the stkeys.jks file is not needed for the IBM i version of Sametime.

5. Save the sametime.ini file.
6. Restart the Sametime server.

Modifying the Sametime configuration on Windows:

Modify the IBM Sametime server's sametime.ini file on Microsoft Windows to support Secure Socket Layer (SSL) encryption.

About this task
To modify the Sametime configuration for Windows, complete the following steps:

Procedure
1. Stop the Sametime server.
2. Use a text editor to open the sametime.ini file, which is located in the Sametime server installation directory (for example: C:\Program Files\lotus\domino).
3. Verify that the "ConfigurationPort=" setting specifies the port on which the Lotus Domino HTTP server listens for SSL connections (default port is 443).
   For example:
   \n   ConfigurationPort=443
4. Verify that the [Config] section contains the following settings (or modify as needed):

   [Config]
   ConfigurationSSLEnabled=true
   javax.net.ssl.keyStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
   javax.net.ssl.trustStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
   javax.net.ssl.keyStorePassword=passw0rd
   javax.net.ssl.trustStorePassword=passw0rd
   
   Where:
   • For the javax.net.ssl.keyStore and the javax.net.ssl.trustStore settings, you specify the complete path name for the stkeys.jks file.
   • For the javax.net.ssl.keyStorePassword and the javax.net.ssl.trustStorePassword settings, you specify the password that you provided for the stkeys.jks file when you created it.
5. Save and close the sametime.ini file.
6. Start the Sametime server.

Tunneling through the firewall when SSL is enabled:

Configure an IBM Sametime server to allow clients to tunnel through a firewall when SSL is enabled.

Before you begin

Sametime Connect clients communicate with the Sametime server by directing messages to the HTTP server, which listens on port 80. When SSL is enabled, port 443 is normally used for sending encrypted messages; however, the Lotus Domino server (which hosts Sametime) is already listening on port 443 for encrypted Web-based communications. If Sametime Connect clients also send messages to the HTTP server on port 443, a conflict arises.
You can work around this conflict by configuring clients to access the Sametime server by tunneling to its Community Services multiplexer with an HTTPS proxy. In this type of configuration, both the Sametime Community Server and the Lotus Domino server listen for connections on port 443 – but they use different addresses to avoid conflicts. You set up this type of connection by assigning an additional IP address to the Sametime server, and then configuring both the Community Services multiplexer and your clients to use that address when communicating on port 443.

The following picture shows an example of this type of connection:

![Diagram of a connection](image)

**Restriction:** This connection is not encrypted. In addition, clients using this connection will not have access to the Meeting Server and the web server, so Meeting services, as well as audio and video services, are not supported in this configuration.

**About this task**

If you want to allow clients to tunnel to the Community Services multiplexer on port 443 when SSL is enabled, complete the following tasks:

*Binding the base DNS to the HTTP server:*

Before assigning an additional IP address to an IBM Sametime server, avoid potential conflicts by binding the server's base DNS to the HTTP server where it listens for communications. This ensures that the IBM Lotus Domino server hosting Sametime (and using this HTTP server) still receives all communications intended for it.

**About this task**

Bind the server's base DNS to the HTTP server by completing the following steps:

**Procedure**

1. On the Sametime server, open the Sametime Administration Tool.
2. Click **Configuration > Connectivity > Networks and Ports.**
3. On the 'Networks and Ports' page, click **Configure HTTP services on a web page in its own window.**
   The "HTTP" section of the Lotus Domino Directory's Server document opens in a separate window.
4. Locate the **Host name** field.
5. Under the "Basics" heading, type the base DNS for the HTTP server (for example: sametime1.acme.com).

6. Still in the same field, type a comma and the following IP address: 127.0.0.1 so it looks like this: sametime1.acme.com,127.0.0.1
   This additional entry is required for enabling the Sametime Administration Tool to operate in this configuration.

7. Click the **Save & Close** button at the top of the Server document.


---

**Adding a new IP address to the Sametime server:**

Assign an additional IP address to an IBM Sametime server.

**Before you begin**

To add a new IP address to a Sametime server, you can either install an additional Network Interface Card (NIC) or assign multiple IP addresses to a single NIC. For additional information, see IBM Tech Note #1181387, "Forcing a Sametime server with multiple NICs to bind to the correct IP address," at: www.ibm.com/support/docview.wss?rs=899&uid=swg21181387

**About this task**

To assign multiple IP addresses to a single NIC on server running Microsoft Windows:

**Procedure**

1. Open the Windows Control Panel.
2. Click the **Protocols** tab.
3. Click **TCP/IP Protocols** > **Properties** > **Specify an IP Address**.
4. Click the **Advanced** tab.
5. Use the "Advanced IP Addressing" page to assign multiple IP addresses to a single NIC.
6. Save your changes and close all of the dialog boxes.

**Mapping the IP address and DNS for Community Services:**

Configure an IBM Sametime server to map an IP address to the specific DNS and port used by Sametime Community Services.

**Before you begin**

You must have already assigned the IP address to the Sametime server.

**Procedure**

Set up your DNS server to map the new IP address to a new DNS name for the Sametime server's Community Services. To avoid confusion, it is recommended that your new DNS for the Community...
Services use the old DNS name plus “community-” as a prefix. For example, if your base DNS for the server is sametime1.example.com, use the following name for the new DNS:

```
community-sametime1.example.com
```

**Configuring HTTPS tunneling settings for clients using port 443:**

Configure the IBM Sametime Community Services to listen for client communications using the new DNS and port 443.

**Before you begin**

You must have already assigned an additional IP address to the Sametime server, then mapped a new DNS to it for use by the Community Services.

**Procedure**

1. On the Sametime server, open the Sametime Administration Tool.
2. Click **Configuration > Connectivity > Networks and Ports**.
3. On the "Networks and Ports" page, click **Community Services Network > Address for HTTPS-tunneled client connections** and fill in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>community-base_DNS</td>
</tr>
<tr>
<td></td>
<td>For example, if your base DNS for the server is sametime1.example.com, type the following name for the new DNS: community-sametime1.example.com</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
</tbody>
</table>

4. Restart the Sametime and Lotus Domino servers.
5. Close the Sametime Administration Tool.

**Results**

With this configuration, the Sametime Community Services multiplexer will listen for HTTPS-tunneled connections using host name community-sametime1.example.com on port 443.

**Connecting clients to the new Community Services DNS:**

Configure an IBM Sametime Connect client to communicate with a Sametime server that is listening for HTTPS connections using the host name (DNS) and port that you specified in the HTTPS tunneling settings for the server.

**About this task**

Every Sametime Connect client located outside of the firewall requires this configuration to tunnel through the firewall to the Sametime Community Services.

**Procedure**

For each Sametime Connect client, configure the following settings in the "Sametime Connectivity" tab:
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Type the new DNS that you mapped to the IP address that will be used for the Community Server. For example, if your base DNS for the server is <code>sametime1.example.com</code>, it was recommended that you use the following name for the new DNS: <code>community-sametime1.example.com</code>. That is the name you should type here.</td>
</tr>
<tr>
<td>Community port</td>
<td>443</td>
</tr>
<tr>
<td>Use proxy</td>
<td>Select this setting.</td>
</tr>
<tr>
<td>Use HTTPS proxy</td>
<td>Select this setting and enter the host name (<code>community-sametime1.example.com</code>) and port (443) on which the Sametime Connect clients connect to the HTTPS proxy.</td>
</tr>
</tbody>
</table>

### Enabling encryption between Sametime and the LDAP server:

Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

**About this task**

When you enable this protocol, you can choose whether to encrypt only the data used for authenticating users in Sametime, or to encrypt all data that is transmitted between the two servers.

**Note:** If you are using an IBM Lotus Domino Directory and it is not configured as an LDAP directory, this section does not apply to you. You can skip these procedures.

Enabling SSL encryption for an LDAP server involves the following tasks:

*Enabling SSL on the LDAP server:*

You must enable SSL on your LDAP server before you can configure the IBM Sametime server to encrypt its communications with the LDAP directory.

**About this task**

**Note:** If you are using a Domino Directory and Sametime is not configured with an LDAP directory, this section does not apply to you and you should skip these procedures.

The procedure for enabling SSL depend on the LDAP directory that you use:

*Setting up a Lotus Domino LDAP directory to use SSL:*

You must enable the IBM Lotus Domino server’s LDAP component to support SSL before you can configure the IBM Sametime server to encrypt its communications with the Lotus Domino LDAP Server.
About this task

Follow these steps in the Lotus Domino Administrator information center to set up a Lotus Domino server to support SSL for LDAP connections:

Setting up SSL on a Domino server

Enabling IBM Tivoli Directory Servers to use SSL:

You must enable the LDAP server to support SSL before you can configure the IBM Sametime server to encrypt communications to the LDAP directory hosted on the IBM Tivoli Directory Server.

About this task

Refer to the documentation provided by IBM Tivoli Directory Server for instructions on enabling SSL. The server must be running GSKit 7.0.4.29 or later. If it is not, you must upgrade to a later version.

Related tasks

“Installing a supported release of GSKit on Tivoli Directory Server” on page 810
You should install the latest version of GSKit available on the IBM Tivoli Directory Server web site. At a minimum, you must upgrade to 7.0.4.28.

Related information

Secure Sockets Layer (Tivoli Directory Server)

Enabling third-party LDAP servers to use SSL:

You must enable the LDAP server to support SSL before you can configure the IBM Sametime server to encrypt communications to the LDAP directory hosted on that server.

About this task

Refer to the documentation provided by the LDAP directory's vendor for instructions on enabling SSL.

Using SSL to encrypt connections between the Sametime and LDAP servers:

When Sametime is configured to connect to an LDAP server, the Sametime Community Server makes five separate connections to the LDAP server.

About this task

The Sametime Community Server makes a separate connection to the LDAP server to perform each of these five tasks:

- Authenticate users
- Resolve a user name to a distinguished name as part of the login procedure
- Resolve user and group names (for example, as a response to an "Add Person or Group" request from a Sametime Connect client)
- Browse the directory
- Get the content of public groups
The Sametime Community Server and LDAP servers exchange directory information, including user names and passwords, over these connections. To ensure this information is secure, the administrator can use SSL to encrypt the data that passes over these connections. The administrator should consider the level of protection required before enabling SSL. Using SSL to encrypt these connections can slow the server performance. The administrator has the following options when using SSL to encrypt the data transmitted between the Sametime and LDAP servers:

- **Encrypt all data** - This option encrypts all directory information (both user names and passwords) that is transmitted between the Sametime Community Server and the LDAP server. If you encrypt all data, all five connections between the Sametime Community Server and LDAP server are encrypted with SSL. This option provides the most security but also has the greatest affect on server performance.

- **Encrypt only user passwords** - This option encrypts passwords but not other directory information (such as user names) passing over the connections between the Sametime Community Server and LDAP servers. If you encrypt only user passwords, only the "authenticating users" connection between the Sametime server and the LDAP server is encrypted with SSL. This option provides an intermediate level of security and has less affect on server performance than encrypting all of the data.

- **Encrypt no data** - This option allows all directory information and passwords to pass unencrypted between the Sametime and LDAP servers. This option does not affect server performance and should be used if the administrator feels there is no chance that an unauthorized user can intercept information transmitted over the connections between the Sametime and LDAP servers.

- **Using SSL to encrypt connections between the Sametime servlet and LDAP**
- **Ensuring the Sametime Community Server trusts the LDAP server certificate on Windows and AIX/Solaris/Linux servers**

**Note:** If you are encrypting connections between an AIX version of the Sametime server and an LDAP directory, x1C.aix50.rte must be 6.0.0.3 (or higher).

**Setting up a keystore for the SSL certificate used by the LDAP server:**

On IBM AIX, Linux, Microsoft Windows, and Sun Solaris, install the GSKit program and the IBM IKeyMan utility so you can store a copy of the LDAP server's SSL certificate. On IBM i, Sametime Community Server comes with the IKeyMan utility already installed, but you must install DCM software instead; the instructions are in this section.

**About this task**

The Sametime server must store a copy of LDAP Server's SSL trusted certificate to complete the SSL handshake when making an SSL connection to that LDAP server. Before you can import the SSL certificate from the LDAP Server, you will use the GSKit program and IKeyMan utility (the DCM program on IBM i) to create a keystore file on the Sametime server for storing the certificate.

**Note:** You only need to install these programs once. If you have already installed these programs during an earlier procedure, you can skip this task.

The instructions for installing GSKit and IKeyMan, or DCM, vary according to your server's operating system. Use the instructions in the appropriate topic.
Installing and setting up Digital Certificate Manager on IBM i:

Install and set up the DCM (Digital Certificate Manager) program on an IBM i server hosting IBM Sametime, and ensure that Sametime trusts the LDAP server’s SSL certificate.

About this task

Set up DCM and ensure that Sametime trusts the LDAP server by completing the following tasks:

Installing Digital Certificate Manager:

Install the DCM (Digital Certificate Manager) program on an IBM i server that hosts IBM Sametime.

About this task

On IBM i, SSL certificates are managed using the integrated DCM program. You must install and set up DCM before you can establish SSL encryption for communications between the IBM i server’s LDAP client and the deployment’s LDAP server. All of the following software must be installed on the IBM i server where your Sametime server is located:

- 5722-SS1 Option 34, Digital Certificate Manager
- 5722-DG1, IBM HTTP Server
- 5722-AC3, Crypto Access Provider 128-bit

If you need more detailed information about setting up and using DCM in order to complete the steps in this section, see the IBM i information center at:

www.ibm.com/as400/infocenter

After selecting the appropriate IBM i release and your preferred language, select the “Digital Certificate Manager” topic in the “Security” section.

Ensuring that the LDAP client trusts the LDAP server’s certificate:

Ensure that the IBM i LDAP client trusts the SSL certificate used by the LDAP server with which it communicates.

About this task

IBM Sametime for IBM i uses the LDAP client included with the IBM Directory Server that is installed as part of the IBM i operating system. Enable the LDAP client to trust the LDAP server by importing the server’s SSL certificate into the store on the client (the IBM i server) and then adding the Certificate Authority to the trust list.

Procedure

1. Use the DCM (Digital Certificate Manager) program to determine whether the CA Certificate that signed the LDAP directory server’s certificate is already included in the DCM *SYSTEM certificate store.
   Well-known public Internet Certificate Authorities (CA) that most web browsers can recognize readily, such as VeriSign, are already included in the DCM. If the appropriate CA is included in the certificate store, you have finished this task; skip the remaining steps.
If the CA used by your LDAP server’s certificate does not appear in the DCM *SYSTEM certificate store, import it now by completing the remaining steps in this procedure.

2. Import the LDAP directory server’s certificate into the DCM *SYSTEM certificate store.

3. Use DCM to add the CA Certificate to the trust list of the IBM Directory Server LDAP client application.
   The application ID is QIBM_GLD_DIRSRV_CLIENT.

Ensuring that Sametime has access to the *SYSTEM certificate store:

Assign IBM Sametime access to the IBM i *SYSTEM certificate store.

About this task

Sametime must be able to access certificates located in the DCM *SYSTEM certificate store when connecting to an LDAP server using SSL. The DCM *SYSTEM certificate store is located in the /qibm/userdata/icss/cert/server directory on an IBM i server.

QNOTES is an IBM i user profile created by IBM Lotus Domino and used by Sametime. By default, the QNOTES user profile does not have access to the DCM *SYSTEM certificate store or the /qibm/userdata/icss/cert/server directory, although the higher level directories usually have *PUBLIC *RX authority which allows QNOTES to access those directories.

Provide Sametime with access to the *SYSTEM certificate store by completing the following step:

Procedure

1. Run the following command from any IBM i command line to view the contents of the /qibm/userdata/icss/cert/server directory and verify the name of the certificate store:
   
   By default, the certificate store is named default.kdb and uses "sametime" as the password.

   WRKLNK '/QIBM/USERDATA/ICSS/CERT/Server/*'

2. Run the following commands from any IBM i command line to ensure QNOTES has the necessary authority to the DCM *SYSTEM certificate store and associated directory:

   CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server') USER(QNOTES) DTAAUT(*RX)
   CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.RDB') USER(QNOTES) DTAAUT(*RX)
   CHGAUT OBJ('/QIBM/USERDATA/ICSS/CERT/Server/DEFAULT.KDB') USER(QNOTES) DTAAUT(*RX)

   In this example:
   • QNOTES is the user receiving access
   • default.kdb is the name of the certificate store

Setting up GSKit, IKeyMan, and the key database on AIX, Linux, Solaris, Windows:

Install the GSKit program and the IBM IKeyMan utility on IBM AIX, Linux, Microsoft Windows, or Solaris and then use IKeyMan to create a key database for storing the LDAP server’s SSL certificate.
About this task

Install the programs and create the key database by completing the following tasks:

*Installing a supported release of GSKit on Tivoli Directory Server:*

You should install the latest version of GSKit available on the IBM Tivoli Directory Server web site. At a minimum, you must upgrade to 7.0.4.28.

*About this task*

Tivoli Global Security Kit (GSKit) is an optional software package included with Tivoli Directory Server. You can enable the SSL feature by installing the IBM GSKit package. For instructions about installing GSKit 8, see the Tivoli Directory Server 6.3 information center.

*Creating a keystore database for the LDAP server’s SSL certificate:*

The Sametime Community Server must store a copy of the IBM Lotus Domino server’s SSL trusted root certificate to complete the SSL handshake when making an SSL connection to a browser-based client. Before you can import the SSL certificate from the Lotus Domino server, use the GSKit and IKeyMan utility to create a keystore file on the Sametime Community Server for storing the certificate. This procedure applies to IBM AIX, Linux, Microsoft Windows, or Sun Solaris, but does not apply to IBM i. The keystore database is not used by Sametime on IBM i.

*Before you begin*

Update the iKeyMan utility and add com.ibm.spi.IBMCMSProvider to the java.security file before you begin this procedure to enable the required CMS key database type used in this procedure.

*About this task*

Use the IBM iKeyMan utility to create a keystore database of type "cms" on the IBM Sametime Community Server. The keystore database that you create for storing the LDAP server’s SSL certificate is different from the keystore file used for storing the Lotus Domino server’s SSL certificate and must use a different file name. Create the keystore database by completing the following steps:

*Procedure*

1. Start the IBM IKeyMan utility:
   a. Open a command prompt and navigate to the Sametime_install_root/ibmjre/jre/bin directory.
      The default installation path for Sametime is as follows:
      - *AIX*: /local/notesdata
      - *Linux*: /local/notesdata
      - *Solaris*: /local/notesdata
      - *Windows*: C:\Program Files\IBM\Lotus\Domino
      - *64-bit Windows*: C:\Program Files (x86)\IBM\Lotus\Domino
      You can check the
   b. Run the ikeyman.sh or ikeyman.exe program.
2. From the iKeyMan utility’s menu, click **Key Database > File > New**.

3. In the "New" dialog box, fill in the following fields and click **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key database type</td>
<td>CMS key database file</td>
</tr>
<tr>
<td>File name</td>
<td>key.kdb</td>
</tr>
<tr>
<td>Note: If you enabled the HTTPS protocol, make sure that this keystore database's file name is different from that file name, to avoid conflicts.</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Enter the path to the directory where the sametime.ini file is stored. For example:</td>
</tr>
<tr>
<td></td>
<td>• AIX: /local/notesdata</td>
</tr>
<tr>
<td></td>
<td>• Linux: /local/notesdata</td>
</tr>
<tr>
<td></td>
<td>• Solaris: /local/notesdata</td>
</tr>
<tr>
<td></td>
<td>• Windows: C:\Program Files\IBM\Lotus\Domino</td>
</tr>
<tr>
<td></td>
<td>• 64-bit Windows: C:\Program Files (x86)\IBM\Lotus\Domino</td>
</tr>
</tbody>
</table>

4. In the "Password" dialog box, fill in the following fields and click **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter the password you will use for accessing this keystore database.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Confirm the password by typing it again.</td>
</tr>
<tr>
<td>Stash the password to a file?</td>
<td>You must click this option to enable it.</td>
</tr>
</tbody>
</table>

Results

The following key files are created in the Sametime directory: key.kdb, key.sth, and key.rdb.

*Importing a copy of the LDAP server’s trusted root certificate:*

Import a copy of the LDAP server’s trusted root SSL certificate into the keystore database on the IBM Sametime server to encrypt communications between Sametime and the LDAP server.

**Before you begin**

When the key.kdb database is created, it contains several trusted root (or "signer") certificates by default. If a trusted root certificate used by the LDAP server exists in the key.kdb database by default, then you can skip this procedure.

If the key.kdb database does not contain an appropriate trusted root certificate by default, you must obtain a trusted root certificate from the appropriate CA and add it to the key.kdb database.

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime server’s data directory. The data type should be **Base64-encoded ASCII**. The file format can be .CER, .p12 or .txt.
About this task

The procedure for importing the trusted root certificate depends on your operating system:

*Importing a trusted root certificate on AIX, Linux, Solaris:*

To enable SSL between IBM Sametime running on IBM AIX, Linux, or Solaris and an LDAP server, import the server's trusted root certificate into the key database.

**Before you begin**

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime Community Server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be .CER, .p12 or .txt. You use this file in the following procedure.

About this task

Follow the steps below to import the SSL certificate into the key database on the Sametime server:

**Procedure**

1. Verify that the `ikeyman.sh` file's `SAMETIME_HOME` variable specifies the correct path for your server's installation directory, modifying it as needed.
   The default installation directories for Sametime are as follows:
   - **AIX**: `/local/notes/data`
   - **Linux**: `/local/notes/data`
   - **Solaris**: `/local/notes/data`
2. Make sure the `ikeyman.sh` file has execute privileges.
3. Start the `ikeyman.sh` utility.
   The `ikeyman.sh` utility requires a graphical interface. If you run it in a text-only terminal, be sure to redirect the display to an x-windows session.
4. Open the key.kdb file.
5. Click the Add button.
6. In the "Open" dialog box, do the following:
   a. Browse to and select the file into which you copied the SSL certificate in the last procedure (for example, CA.txt).
   b. Click OK.
7. In the "Enter a Label" dialog box, do the following:
   a. Type a label for the certificate.
      This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program.
   b. Click OK.
      The new certificate's label appears in the list of Signer Certificates.
8. Close the keystore file.
9. Close the IKeyMan utility.

*Importing a trusted root certificate on IBM i:*
To enable SSL between IBM Sametime running on IBM i and an LDAP server, import the server's trusted root certificate into the keystore file.

Before you begin

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime server's data directory. The data type should be **Base64-encoded ASCII**. The file format can be `.CER`, `.p12` or `.txt`.

About this task

Follow the steps below to import the SSL certificate into the keystore file on the Sametime server:

Procedure

1. From an IBM i command line, run the following command to start qshell:
   
   ```sh
   strqsh
   ```

2. From qshell, run the following keytool command:
   
   ```sh
   keytool -import -alias certificate_name
   -file certificate_filename
   -storepass keystore_password
   -keystore keystore_path_and_filename
   ```

   Where:
   
   - `certificate_name` is `CA.txt`
   - `certificate_filename` is also `CA.txt`
   - `keystore_password` is "sametime."

   **Note:** On IBM i versions of Sametime, the keystore is called "stkeys.jks" and uses "sametime" as the default password

   - `keystore_path_and_filename` is `stserver/data/stkeys.jks`

   Example:
   
   ```sh
   keytool -import -alias stserver1cert
   -file /stserver/data/CA.txt
   -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```

3. After you have imported the certificate, use the following command to view the list of certificates in the `stkeys.jks` file and verify that the certificate was imported successfully:
   
   ```sh
   keytool -list -storepass keystore_password
   -keystore keystore_path_and_filename
   ```

   Example:
   
   ```sh
   keytool -list -storepass sametime
   -keystore /stserver/data/stkeys.jks
   ```

4. Press F3 to exit qshell.

Importing a trusted root certificate on Windows:

To enable SSL between IBM Sametime running on Microsoft Windows and an LDAP server, import the server's trusted root certificate into the key database.

Before you begin

Make sure you have copied the trusted root certificate from the LDAP server into the Sametime Community Server's data directory. The data type should be
**Base64-encoded ASCII.** The file format can be .CER, .p12 or .txt. You use this file in the following procedure.

**About this task**

Follow the steps below to import the SSL certificate into the key database on the Sametime server:

**Procedure**

1. Open a command prompt and navigate to the Sametime_install_root\ibm-jre\jre\bin directory.
   
   The default installation directories for Sametime are as follows:
   
   - **Windows:** C:\Program Files\IBM\Lotus\Domino
   
   - **64-bit Windows:** C:\Program Files (x86)\IBM\Lotus\Domino

2. Start the IKeyMan utility by running the ikeyman.exe program.
3. Browse to and select the key.kdb key database.
4. Enter the password required to access this file.
5. In the "Key database content" area, select Signer certificates.
6. Click the Add button.
7. In the "Open" dialog box, do the following:
   a. Browse to and select the file into which you copied the SSL certificate in the last procedure (for example, CA.txt).
   b. Click OK.
8. In the "Enter a Label" dialog box, do the following:
   a. Type a label for the certificate.
   This label identifies the certificate in the Signer Certificates list of the IBM IKeyMan program.
   b. Click OK.
   The new certificate's label appears in the list of Signer Certificates.
10. Close the IKeyMan utility.

**Configuring Directory Assistance for SSL:**

Modifying the IBM Lotus Domino Directory Assistance document is required when you use SSL to encrypt data transmitted between the IBM Sametime and the LDAP server.

**About this task**

In this procedure, you modify the Directory Assistance document for the LDAP server to ensure that the connection between the Sametime server and the LDAP server is encrypted using SSL.

**Procedure**

   a. Click File > Database > Open.
   b. For the Server, select Local.
   d. Click Open.
2. In the Directory Assistance database, double-click the Directory Assistance document for the LDAP server to open the document.

3. Click Edit Directory Assistance.
4. Next, click the Basics tab.
5. In the Make this domain available to: field, select Notes Clients & Internet Authentication/Authorization.
6. Now click the LDAP tab.
7. Fill in the following fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel encryption</td>
<td>Select SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the same port that appears in the LDAP SSL port field of the &quot;LDAP Directory - Connectivity&quot; options in the Sametime Administration Tool. This port is the one on which the LDAP server listens for SSL connections; the default is port 636.</td>
</tr>
<tr>
<td>Accept expired SSL certificates</td>
<td>Select Yes (the default setting) to accept a certificate from the LDAP directory server, even if the certificate has expired. For tighter security, select No to require the Sametime server to check certificate expiration dates. If the certificate presented by the LDAP server has expired, the connection is terminated.</td>
</tr>
</tbody>
</table>
| SSL protocol version        | Select the version number of the SSL protocol to use. The choices are:  

  - V2.0 only - This setting allows only SSL 2.0 connections.  
  - V3.0 handshake - This setting attempts an SSL 3.0 connection. If this connection attempt fails but Sametime detects that SSL 2.0 is available on the LDAP server, Sametime attempts the connection using SSL 2.0.  
  - V3.0 only - This setting allows only SSL 3.0 connections.  
  - V3.0 and V2.0 handshake - This setting attempts an SSL 3.0 connection, but starts with an SSL 2.0 handshake that displays relevant error messages. This setting is used to receive V2.0 error messages when trying to connect to the LDAP server. These error messages might provide information about any compatibility problems found during the connection.  
  - Negotiated - This setting allows SSL to determine the handshake and protocol version required. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify server name with remote server's certificate</td>
<td>Select Enabled (the default setting) to verify the server name with the remote server's certificate. If Enabled is selected, the Sametime server verifies the name of the LDAP server with the remote server's certificate. If the names do not match, the connection is terminated. For more relaxed security, select Disabled (the server name is not verified with the certificate).</td>
</tr>
</tbody>
</table>

8. Click **Save and Close** to close the Directory Assistance document.

*Connecting Sametime to the LDAP server:*

Enable SSL encryption for connections between IBM Sametime and the LDAP server.

**Before you begin**

The Sametime Community server must be running.

**Procedure**

1. Configure LDAP connectivity settings in the Sametime Administration Tool as follows:
   a. From the Sametime server's home page, click the [Administer the Server](link) link to open the Sametime Administration Tool.
   b. Click [LDAP Directory] > [Connectivity].
   c. In the Host name or IP address of the LDAP server list, select the name of the LDAP server.
   d. Click the option called [Use SSL to authenticate and encrypt the connection between the Sametime server and the LDAP server](option).
   e. In the LDAP SSL port field, specify the port on which the LDAP server is listening for SSL LDAP connections (the default is port 636).
   f. Click [Update].
   g. Close the Sametime Administration Tool.

At this point, you have enabled SSL encryption for all data that is transmitted between the Sametime server and the LDAP server.

2. (Optional) To improve performance, you may choose to loosen security and encrypt only user credentials as follows:
   a. Open the sametime.ini file (located in the Sametime installation directory).
   b. Locate the [Directory] section within the file.
   c. Add the following setting:
      ```
      ST_DB_LDAP_SSL_ONLY_FOR_PASSWORDS=1
      ```
   d. Save and close the file.

3. Restart the Sametime server

*Modifying the LDAP server configuration for SSL:*
Modify the configuration of the IBM Sametime server to encrypt connections between the LDAP server and the Sametime Community Server.

About this task

Modify the Sametime server's configuration by making the following changes to the `sametime.ini` file.

Procedure

1. Open the `sametime.ini` file in a text editor.
2. If these settings are not present in the `[Config]` section at the bottom of the `sametime.ini` file, manually type them in. Follow the instructions for your operating system.

AIX, Linux, and Solaris

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=/local/notesdata/key.jks
javax.net.ssl.trustStore=/local/notesdata/key.jks
javax.net.ssl.keyStorePassword=keystore_password
javax.net.ssl.trustStorePassword=truststore_password
```

Note: Specify the complete path name of the `key.jks` file for both the `javax.net.ssl.keyStore` and the `javax.net.ssl.trustStore` settings. Specify the password that you provided for `key.jks` when you created it for both the `javax.net.ssl.keyStorePassword` and `javax.net.ssl.trustStorePassword` settings.

IBM i

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=stkeys.jks
javax.net.ssl.trustStore=stkeys.jks
javax.net.ssl.keyStorePassword=sametime
javax.net.ssl.trustStorePassword=sametime
```

Note: By default, the password for the `stkeys.jks` file is "sametime." If you change the password for `stkeys.jks`, you must change the setting of both `javax.net.ssl.keyStorePassword` and `javax.net.ssl.trustStorePassword` to match the new password. The full path for the `stkeys.jks` file is not needed for the IBM i version of Sametime.

Windows

```
[Config]
ConfigurationSSLEnabled=true
javax.net.ssl.keyStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
javax.net.ssl.trustStore=c:\program files\lotus\domino\jvm\bin\stkeys.jks
javax.net.ssl.keyStorePassword=passw0rd
javax.net.ssl.trustStorePassword=passw0rd
```

Where:
- For the `javax.net.ssl.keyStore` and the `javax.net.ssl.trustStore` settings, you specify the complete path name for the `stkeys.jks` file.
- For the `javax.net.ssl.keyStorePassword` and the `javax.net.ssl.trustStorePassword` settings, you specify the password that you provided for the `stkeys.jks` file when you created it.

3. If these two lines appear in the `sametime.ini` file, remove them:

```
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.keyStoreType=JKS
```
4. Save and close the sametime.ini file.
5. Restart the Sametime Community Server.

Encrypting the UserInfo servlet:

If your IBM Sametime deployment uses SSL encryption when communicating with
the LDAP server, you can additionally choose to encrypt the UserInfo servlet.

Before you begin

You must have created a keystore .jks file on the IBM Sametime Community
Server, which stores a copy of the IBM Lotus Domino server's SSL certificate.

About this task

This configuration is necessary to enable the Business Card feature when you have
chosen to encrypt all data transmitted between the Sametime server and the LDAP
server, where the Business Card data is stored.

Procedure

1. Open a command prompt and navigate to the following directory:
   - IBM AIX, IBM i, Linux, Solaris: the Sametime server's data directory
   - Windows: the Sametime server's installation directory
2. Open the UserInfoConfig.xml file in an editor and make the following changes:
   a. Locate the <ReadStConfigUpdates> tag and set to value="true". If this
      statement is not in the file, you do not need to add it.
      The statement should look like this:
      `<ReadStConfigUpdates value="true"/>
   b. Locate the <StorageDetails> tag and set the following values:
      `<SslEnabled="true"
      <SslPort="636"
      Use the value of the port that your LDAP server listens on for SSL
      communications (the default is port 636).
   c. In the <SslProperties> tag, set the following values:
      `<SslProperties KeyStorePath="D:\IBM\Lotus\Domino\jvm\bin\key.jks OR_stkeys.jks"
      KeyStorePassword="mypwd"/>
      Where:
      • KeyStorePath indicates the path to where the keystore database is stored.
        On Windows and IBM i, the file is named stkeys.jks; on AIX, Linux, and
        Solaris, the file is named keys.jks.
      • KeyStorePassword indicates the password you created for accessing the
        keystore database.
3. Save and close the file
4. Restart the Sametime Community Server.
Related tasks
“Creating a keystore file for the Domino server’s SSL certificate” on page 792
Use the IBM IKeyMan utility and to create a keystore .jks file on the IBM
Sametime Community Server, which will be used for storing a copy of the IBM
Lotus Domino server’s SSL certificate.

Configuring Transport Layer security for the Sametime Media
Manager
Configuring the IBM Media Manager SIP Proxy and Registrar component to use
SIP authentication and authorization requires some additional steps.

About this task
Follow the instructions in this section to configure Transport Layer Security (TLS)
if you chose it as the encryption protocol and to set up user authentication.

Configuring ports for Transport Layer encryption on an upgraded Sametime
Media Manager:
After upgrading an IBM Sametime Media Manager, edit settings in the
stavconfig.xml file to specify secure ports for TLS encryption. Do this only if all
clients are running 8.5.1 or later; otherwise older clients cannot connect to the
upgraded Media Manager.

Before you begin
Make a note of the values you need to transfer to stavconfig.xml from the
SIP/Proxy Registrar, Conference Manager, and Packet Switcher servers. Open the
WebSphere Application Server Integrated Solutions Console for each server and
click Application servers > STMediaServer > Ports.

Find the values for a non-clustered or clustered environment.

Non-clustered environment
• SIP/Proxy Registrar
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE
• Conference Manager
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
• Packet Switcher
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port

Clustered environment
• SIP/Proxy Registrar
  SIP_ProxyRegHOST/SIP_ProxyRegSECURE
  (Clustered node) WebSphere Application Server proxy host
  (Clustered node) WebSphere Application Server proxy secure port
• Conference Manager
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
  (Clustered node) WebSphere Application Server proxy host
  (Clustered node) WebSphere Application Server proxy secure port
• Packet Switcher
  SIP_DEFAULTHOST/SIP_DEFAULTHOST_SECURE port
About this task

The default settings in the stavconfig.xml file specify non-secure ports and must be modified for use with TLS encryption. Edit the stavconfig.xml files on the Conference Manager and Packet Switcher to reflect this update by changing the non-secure ports to secure ports. Follow these steps on both machines. This file is not used by the SIP Proxy and Registrar.

Follow these steps to update the stavconfig.xml file for every instance of the Media Manager components. When multiple profiles are installed on the same computer, each profile uses its own copy of the file and requires the updates.

Procedure

1. Log in to the Integrated Solutions Console for the machine.
2. On the server hosting the Conference Manager, Packet Switcher, or SIP Proxy and Registrar, navigate to the following directory:
   
   \dm_install_root\config\cells\cell_name\nodes\node_name\servers\server_name

3. In a text editor, open the stavconfig.xml file.
4. Modify the following settings:
   - The ConferenceServerPort setting should contain the SIP_DEFAULTHOST_SECURE port value from the Conference Manager server.
   - The SIPProxyServerPort setting should contain the SIP_ProxyRegSECURE port value from the SIP Proxy/Registrar server.
   - The port setting in the [packetswitches] section should contain the SIP_DEFAULTHOST_SECURE port value from the Packet Switcher server.
   - Clustered environment only: Change the SIPProxyServerTransport Protocol setting value to TLS.
5. (Packet Switcher only) Add these three attributes if they are missing.
   
   <configuration lastUpdated="1226425838277" name="IsEncryptedConferenceEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="AudioRTCPEnabled" value="false"/>
   <configuration lastUpdated="1226425838277" name="VideoRTCPEnabled" value="true"/>

   **Note:** If you have Sametime 8.5.0 clients in your environment, set the third attribute for "VideoRTCPEnabled" to "false" instead.
6. (Clustered environment only)

   Make these additional changes in the file if you are configuring on a clustered node server.

   **Conference Manager node**
   - SIPProxyServerHost field
     
     SIP Proxy/Registrar WAS proxy host
   - SIPProxyServerPort field
     
     SIP Proxy/Registrar WAS proxy secure port

   **Packet Switcher node**
   - SIPProxyServerHost field
     
     SIP Proxy/Registrar WebSphere Application Server proxy host
   - SIPProxyServerPort field
     
     SIP Proxy/Registrar WebSphere Application Server proxy secure port
   - ConferenceServerHost field
Conference Manager WebSphere Application Server proxy host

- ConferenceServerPort field

Conference Manager WebSphere Application Server proxy secure port

7. Close and save the updated file.
8. Synchronize all nodes in the Deployment Manager that manages the component.
   a. In the Deployment Manager's Integrated Solutions Console, click System Administration > Nodes.
   b. Click Full Resynchronize.

Results

Communications will now take place over the secure ports. If you later switch back to (nonencrypted) TCP or UDP transport protocol, you must change the port settings back to their original values. For SIP transport, you should use either TLS or TCP transport protocols.

Distributing certificates for Transport Layer encryption to all Media Manager components:

If you installed Media Manager components on separate machines or as separate cell profiles, you must extract the signed security certificate from the SIP Proxy and Registrar server. Then add the certificate to all Conference Manager and Packet Switcher servers. This step does not apply if you installed all components of the media manager on the same cell profile.

Before you begin

Extract the certificate used by the SIP Proxy and Registrar and copy it to a location from which each Media Manager component can copy the file.
1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the SIP Proxy and Registrar certificate.
2. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   • In a non-clustered environment, the certificate is on the same machine as the SIP Proxy and Registrar component.
   • In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the SIP Proxy and Registrar.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the Media Manager component can retrieve the file.

About this task

Follow these steps to add a signed certificate to each Media Manager component.

Procedure

1. Log in to the Media Manager component's Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
Note: If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.

3. Click Add.

4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.

5. In the File name field, type the path to the certificate file; for example: c:sip-pr.cer

6. Click OK.

7. Click Save.

8. Restart the server.

9. Repeat these steps for each Media Manager component.

Distributing certificates for Transport Layer encryption to the SIP Proxy and Registrar:

If you installed the SIP Proxy and Registrar on separate machines or as a separate cell profile from the other IBM Sametime Media Manager components, you must extract the signed security certificate from the Conference Manager and Packet Switcher components and add the certificates to the SIP Proxy and Registrar. This step does not apply if you installed all components of the Sametime Media Manager and SIP Proxy and Registrar on the same cell profile.

Before you begin

Extract the certificate used by each Conference Manager and Packet Switcher component and copy it to a location from which the SIP Proxy and Registrar can copy the file.

1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Manager certificate.

2. Click Security > SSL Certificates and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.

   • In a non-clustered environment, the certificate is on the same machine as the Sametime Media Manager component (Conference Manager or Packet Switcher)

   • In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.

   Note: The Packet Switcher does not run in a cluster.

3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.

4. Type a unique file name for the signed certificate.

5. Copy the extracted certificate to a location from which the SIP Proxy and Registrar component can retrieve the file.

6. Repeat this procedure for the Packet Switcher.

About this task

Follow these steps to add from the Conference Manager and Packet Switcher components the signed certificates to the SIP Proxy and Registrar.
Procedure
1. Log in to the SIP Proxy and Registrar component's Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.

   **Note:** If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.
3. Click Add.
4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.
5. In the File name field, type the path to the certificate file; for example: c:\cm-pr.cer or c:\ps-pr.cer
6. Click OK.
7. Click Save.
8. Restart the server.
9. Repeat these steps for each Media Manager component.

Exchanging certificates between the Packet Switcher and the Conference Manager:

The Packet Switcher component of the IBM Sametime Media Manager opens a TLS connection to the Conference Manager, so you need to exchange certificates between the Packet Switcher and the Conference Manager. You must extract the certificate used by the Conference Manager and then add this certificate to the Packet Switcher.

**Before you begin**

Extract the certificate used by the Conference Manager component and copy it to a location from which the Packet Switcher component can copy the file.
1. Log in to the IBM WebSphere Application Server Integrated Solutions Console on the server that has the Conference Focus certificate.
2. Click Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
   • In a non-clustered environment, the certificate is on the same machine as the Conference Manager component.
   • In a clustered environment, the certificate is on the WebSphere Application Server proxy used by the Conference Manager.
3. Select the Alias default if you used a self-signed certificate or select the appropriate signed certificate you want to share and click Extract.
4. Type a unique file name for the signed certificate.
5. Copy the extracted certificate to a location from which the Packet Switcher component can retrieve the file.

**About this task**

Follow these steps to add a signed certificate to the Packet Switcher.

**Procedure**
1. Log in to the Packet Switcher component’s Integrated Solutions Console.
2. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.

Note: If CellDefaultTrustStore is not in the table then choose NodeDefaultTrustStore.

3. Click Add.

4. In the Alias field, type a description for the certificate. Include information about what kind of certificate it is, such as an internal self-signed certificate, a public self-signed certificate or a public Certificate Authority.

5. In the File name field, type the path to the certificate file; for example: c:\conf-focus.cer

6. Click OK.

7. Click Save.

8. Restart the server.

Adding trusted IP addresses to the Media Manager SIP Proxy and Registrar:

The Sametime SIP Proxy and Registrar accepts connections from the Sametime Media Manager components – Conference Manager and Packet Switcher. To ensure that the SIP Proxy and Registrar trusts these components when they establish a connection, you must add a custom SIP container property that uses the IP address or fully qualified domain name for these trusted components as its value.

About this task

Complete these steps for each server in a Sametime SIP Proxy and Registrar cluster or for every SIP Proxy/Registrar in a multiple-server deployment.

Procedure

1. Log in to the Sametime Media Manager's Integrated Solutions Console.
   If you installed the SIP Proxy/Registrar component on a separate server, log in to the SIP Proxy and Registrar's Integrated Solutions Console.

2. Click Servers > Server Types > WebSphere Application Servers.

3. Click the name of the Media Manager server.
   In a clustered environment, click the name of a cluster member.

4. Under Container settings, click SIP Container Settings > SIP container.

5. Click Custom Properties.

6. Add this new property if it does not exist:
   com.ibm.ws.sip.security.trusted.iplist

7. Add the Conference Manager and Packet Switcher as trusted IP addresses.
   Use commas to separate multiple values if you are using multiple servers.
   In a non-clustered environment, use the servers' IP addresses or fully qualified domain names.

   Note: If the Conference Manager operates in a cluster, use the IP address or fully qualified domain name for the WebSphere Application Server proxy used by the Conference Manager cluster instead.

8. Click OK.

9. Click Save.

10. Restart the Sip Proxy and Registrar server.
Configuring secure access to an LDAP repository:

Configure secure access to a Lightweight Directory Access Protocol (LDAP) repository used by the IBM Sametime SIP Proxy and Registrar server.

Before you begin

Ensure that the enterprise LDAP server is running.

About this task

If the LDAP server is using a public certificate, then you need to obtain the public root CA and import it. If your LDAP server is using a self-signed certificate, then you simply import the self-signed certificate.

Procedure

1. Import the certificate:
   a. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
   b. Select Security > SSL Certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
   c. Click Add.
   d. In the Alias field, type a description for the certificate, whether it’s self-signed or a public CA.
   e. In the File name field, type the path to the certificate file. For example, c:\ldap.cer.
   f. Click Apply and then Save.
   g. Restart all WebSphere Application Server processes for the change to take effect.

2. Enable SSL between the SIP Proxy and Registrar server and the LDAP repository.
   a. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
   b. Select Security > Global security.
   c. Click Configure.
   d. In Repositories in the realm table select the LDAP server identifier.
   e. In the Port field type 636. For some LDAP servers, you can specify a different port for a SSL connection.
   f. Click Require SSL communications.
   g. Click Apply and then Save.
   h. Restart the SIP Proxy and Registrar server for the change to take effect.

Configuring Transport Layer security for the Sametime Bandwidth Manager

If the IBM Sametime Media Manager is configured to use Transport Layer Security (TLS), you must also configure TLS on the server hosting IBM Sametime Bandwidth Manager.

Configuring the stand-alone Bandwidth Manager to use TLS encryption:

If the IBM Sametime Media Manager is configured to use Transport Layer Security (TLS), you must also configure TLS on the server hosting IBM Sametime Bandwidth Manager.
About this task

Sametime Bandwidth Manager can use TLS (Transport Layer Security) encryption for security. In IBM WebSphere Application Server, the TLS functionality requires a certificate. This certificate can be a self-signed for testing or demonstration environment purposes, but IBM recommends using a certificate issued by a valid Certificate Authority (CA) for any production environment.

Because the Bandwidth Manager exchanges information with the Sametime Media Manager, you must import a copy of the certificate to the Media Manager cell's cell default trust store to ensure it will accept communications from the Bandwidth Manager.

Procedure

1. Import the Bandwidth Manager security certificate into the Media Manager's SIP Proxy and Registrar:
   a. On the server hosting the Media Manager's SIP Proxy and Registrar component (if that component is clustered, use the server hosting its deployment manager), open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
   b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.
   c. Click CellDefaultTrustStore.
   d. Click Signer certificates.
   e. Click Retrieve from port and enter the Bandwidth Manager's host name and TLS port.
   f. Save the retrieved signer certificate.

2. Import the Media Manager's SIP Proxy and Registrar security certificate into the Bandwidth Manager:
   a. On the server hosting the Bandwidth Manager, open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
   b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.
   c. Select the correct trust store:
      For a stand-alone Bandwidth Manager server, click NodeDefaultTrustStore.
      For a clustered Bandwidth Manager server, click CellDefaultTrustStore.
   d. Click Signer certificates.
   e. Click Retrieve from port and enter the SIP Proxy and Registrar's host name and TLS port.
   f. Save the retrieved signer certificate.

3. Locate the secure port value:
   a. From the Bandwidth Manager's WebSphere Integrated Solutions Console, return to the navigation tree and click Servers > Server types > WebSphere application servers.
   b. On the Application servers page, navigate to the servers table and click the name of your Bandwidth Manager server.
   c. On the Configuration page, navigate to the Container Settings section and click SIP Container Settings > SIP container transport chains.
   d. In the Transport Chains table, locate the Port value in the SIPCInboundDefaultSecure row.
This is the secure port value, which you will need in the next step.

4. Configure the Bandwidth Manager to use the secure port:
   a. Back on the navigation tree, click Sametime Servers > Bandwidth Manager.
   b. On the Status page, click the Configuration tab.
   c. On the Configuration page, click the SipFrontend component listed in the table at the bottom of the page.
   d. On the General Properties page for the SipFrontend component, edit the SIP URI field, typing the value of the secure port that you obtained earlier from the value of SIPCInboundDefaultSecure in the Transport Chains table.
   e. Cluster only: If you are setting up a cluster, also change the Cluster SIP URI field to use that same secure port.
   f. Click Apply and then click the Save link in the "Messages" box at the top of the page.

5. Restart the server or cluster:
   • For a stand-alone server, restart it now as follows:
     a. On the server’s Configuration page, click the Status tab.
     b. On the Status page, click the Start/Restart button at the top of the table.
     c. Click the Refresh button and verify that all components are active.
   • For a clustered server, synchronize nodes and restart the cluster as follows:
     a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
     b. Select all nodes in the cluster
     c. Click Full Resynchronize.
     d. Back in the navigator, click System Administration > Node agents.
     e. Click a node agent, and then click Restart; repeat for each node agent.

Configuring the Bandwidth Manager node to use TLS encryption:

If the IBM Sametime Media Manager is configured to use Transport Layer Security (TLS), you must also configure TLS on the server hosting IBM Sametime Bandwidth Manager.

About this task

Sametime Bandwidth Manager can use TLS (Transport Layer Security) encryption for security. In IBM WebSphere Application Server, the TLS functionality requires a certificate. This certificate can be a self-signed for testing or demonstration environment purposes, but IBM recommends using a certificate issued by a valid Certificate Authority (CA) for any production environment.

Because the Bandwidth Manager exchanges information with the Sametime Media Manager, you must import a copy of the certificate to the Media Manager cell’s cell default trust store to ensure it will accept communications from the Bandwidth Manager.

Procedure

1. Import the Bandwidth Manager security certificate into the Media Manager’s SIP Proxy and Registrar:
   a. On the server hosting the Media Manager’s SIP Proxy and Registrar component (if that component is clustered, use the server hosting its
deployment manager), open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.

b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.

c. Click CellDefaultTrustStore.

d. Click Signer certificates.

e. Click Retrieve from port and enter the Bandwidth Manager's host name and TLS port.

f. Save the retrieved signer certificate.

2. Import the Media Manager's SIP Proxy and Registrar security certificate into the Bandwidth Manager:

a. On the server hosting the Bandwidth Manager, open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.

b. On the navigation tree, click Security > SSL certificate and key management > Key stores and certificates.

c. Select the correct trust store:
   For a stand-alone Bandwidth Manager server, click NodeDefaultTrustStore.
   For a clustered Bandwidth Manager server, click CellDefaultTrustStore.

d. Click Signer certificates.

e. Click Retrieve from port and enter the SIP Proxy and Registrar's host name and TLS port.

f. Save the retrieved signer certificate.

3. Locate the secure port value:

a. From the Bandwidth Manager's WebSphere Integrated Solutions Console, return to the navigation tree and click Servers > Server types > WebSphere application servers.

b. On the Application servers page, navigate to the servers table and click the name of your Bandwidth Manager server.

c. On the Configuration page, navigate to the Container Settings section and click SIP Container Settings > SIP container transport chains.

d. In the Transport Chains table, locate the Port value in the SIPCInboundDefaultSecure row.
   This is the secure port value, which you will need in the next step.

4. Configure the Bandwidth Manager to use the secure port:

a. Back on the navigation tree, click Sametime Servers > Bandwidth Manager.

b. On the Status page, click the Configuration tab.

c. On the Configuration page, click the SipFrontend component listed in the table at the bottom of the page.

d. On the General Properties page for the SipFrontend component, edit the SIP URI field, typing the value of the secure port that you obtained earlier from the value of SIPCInboundDefaultSecure in the Transport Chains table.

e. Cluster only: If you are setting up a cluster, also change the Cluster SIP URI field to use that same secure port.

f. Click Apply and then click the Save link in the "Messages" box at the top of the page.

5. Restart the server or cluster:

   • For a stand-alone server, restart it now as follows:
     a. On the server’s Configuration page, click the Status tab.
b. On the Status page, click the **Start/Restart** button at the top of the table.
c. Click the **Refresh** button and verify that all components are active.
• For a clustered server, synchronize nodes and restart the cluster as follows:
  a. In the Deployment Manager’s Integrated Solutions Console, click **System Administration > Nodes.**
  b. Select all nodes in the cluster
  c. Click **Full Resynchronize.**
  d. Back in the navigator, click **System Administration > Node agents.**
  e. Click a node agent, and then click **Restart;** repeat for each node agent.

### Configuring Sametime Meeting Server for secure access to an LDAP repository

Configure secure access to a Lightweight Directory Access Protocol (LDAP) repository used by the IBM Sametime Meeting Server.

#### Before you begin

Ensure that the enterprise LDAP server is running.

#### About this task

If the LDAP server is using a public certificate, then you need to obtain the public root CA and import it. If your LDAP server is using a self-signed certificate, then you simply import the self-signed certificate.

#### Procedure

1. Import the certificate:
   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Select **Security > SSL Certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.**
   c. Click **Add.**
   d. In the **Alias** field, type a description for the certificate, whether it's self-signed or a public CA.
   e. In the **File name** field, type the path to the certificate file. For example, `c:\ldap.cer`.
   f. Click **Apply** and then **Save.**
   g. Restart all WebSphere Application Server processes for the change to take effect.

2. Enable SSL between the Sametime Meeting Server and the LDAP repository.
   a. Log in to the Integrated Solutions Console for the Sametime Meeting Server.
   b. Select **Security > Global security.**
   c. Click **Configure.**
   d. In Repositories in the realm table select the LDAP server identifier.
   e. In the **Port** field type 636. For some LDAP servers, you can specify a different port for a SSL connection.
   f. Click **Require SSL communications.**
   g. Click **Apply** and then **Save.**
   h. Restart the Sametime Meeting Server for the change to take effect.
Replacing the default IBM self-signed certificate with another certificate
The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, using a self-signed certificate from IBM. If you want to use a different certificate, you can import it into the keystore yourself.

About this task
The following Sametime servers install with SSL already enabled, using a self-signed certificate provided by IBM:

- Sametime Proxy Server
- Sametime Meeting Server
- Sametime Media Manager
  - If you install the Media Manager components on separate servers, each is installed with SSL enabled.
- Sametime Advanced

Note: The Sametime Gateway server does not install with SSL enabled; the configuration instructions in this information center explain how to enable SSL and import a certificate for Sametime Gateway servers.

If you want to modify your deployment to use a different SSL certificate, follow the instructions in the WebSphere information center topic, Import certificate from a key file or managed keystore.

Adding a Sametime server SSL certificate to the Sametime System Console
If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

About this task
To enable SSL, you must extract the certificate from the Sametime product server and add it to the trust store of the Sametime System Console. The Sametime product servers include:

- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Gateway Server
- SIP Proxy and Registrar

Follow these instructions. See the WebSphere Application Server information center for more information on extracting and adding certificates.

Procedure
1. Log in to the Integrated Solutions Console for the Sametime product server.
2. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
3. Select the alias named root, and click Extract.
4. Enter the name of the .cer file, and select **Base64** as the type for storing the process server signer certificate.

5. Log in to the Integrated Solutions Console for the Sametime System Console.

6. Click **Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates**

7. Click **Add**.

8. Enter an alias.

9. Enter the file name where you stored the extracted process server signer certificate from the product server.

10. Click **Apply**.

11. Restart the Sametime System Console deployment manager.

**Related tasks**

“Updating Sametime Proxy Server connection properties on the console” on page 1143

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Proxy Server.

“Updating Sametime Media Manager connection properties on the console” on page 1144

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Media Manager.

“Updating Sametime Meeting Server connection properties on the console” on page 1161

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Meeting Server.

**Importing an SSL certificate from Sametime Unified Telephony**

If you plan to configure telephony services in your deployment using IBM Sametime Unified Telephony, import the Telephony Application Server's SSL certificate into the Sametime Proxy Server's truststore.

**Before you begin**

Secure Socket Layer (SSL) encryption is required for telephony services. You must import the telephony server's SSL certificate into the Sametime Proxy Server’s truststore before you enable SSL between Sametime Proxy Server and Sametime Unified Telephony.

**Procedure**

1. Copy the SSL certificate from Sametime Unified Telephony:
   a. On the Telephony Application Server, log in to the IBM WebSphere Application Server Integrated Solutions Console as the WebSphere administrator.
   b. Click **Security > SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates**.
   c. Select the Alias default_signer or the appropriate one, if you customized, and click **Extract**.
   d. Type a file name for storing the signer certificate. The Telephony Application Server WebSphere Application Server console displays the location of the extracted certificate. For example: `/opt/IBM/WebSphere/AppServer/profiles/<AppSrvxx>/etc/<file>`
Note this location because you need to copy the file to the live names proxy server in the following step.

2. Move the file from the previous step to the etc/ directory under the Deployment Manager for the Live Names Proxy cell. For example:
   /opt/IBM/WebSphere/AppServer/profiles/<xxxxSTPDMProfile>/etc/<file>

3. Now import the SSL certificate into the Sametime Proxy Server's truststore:
   a. On the Sametime Proxy Server, log in to the WebSphere Application Server Integrated Solutions Console as the WebSphere administrator.
   b. Click Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
   c. Click Add.
   d. Type an alias for the certificate; for example, "SUT".
   e. Type the name of the file where you stored the SSL certificate.
   f. Click Apply.
   g. Save the imported certificate by clicking Save in the "Messages" box at the top of the page.
   h. Restart the Sametime Proxy Server.

Configuring TLS/SSL for Sametime Gateway

Transport Layer Security (TLS) and Secure Sockets Later (SSL) provide encrypted SIP communications between Sametime Gateway and the external instant messaging communities such as AOL, Office Communications Server, and Sametime communities, but only if the other Sametime community requires SSL. TLS/SSL also provides encrypted XMPP communications for XMPP communities. The TLS/SSL protocols allow Sametime messages to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. Use these steps to set up SSL with a certificate signed by a Certificate Authority and exchange trusted certificates with external communities.

About this task

Messages that flow between Sametime Gateway and AOL and Office Communications Server always require a TLS/SSL connection. Sametime and XMPP communities may or may not require a TLS/SSL connection, depending whether the external community requires a CA-signed certificate. Google Talk does not work over TLS/SSL.

This section provides steps for a single Sametime Gateway server or cluster of Sametime Gateway servers. In addition, this section provides steps needed to set up SSL on a Sametime 6.5.1 or later server in an external community. You can provide these steps as a courtesy to an external community or refer them to the Sametime documentation.

SSL can encrypt sensitive information for SIP and XMPP communications, and provides authenticity and data signing to ensure a secure connection between the local Sametime Gateway community and an external instant messaging community. The foundation technology for SSL is public key cryptography, which guarantees that when an entity encrypts data using its private key, only entities with the corresponding public key can decrypt that data.

SSL is required for connections to the following communities:

- External community using AOL Instant Messenger
- External community using Office Communications Server
• AOL clearinghouse community

SSL is not required but it is recommended for connections to XMPP or Sametime communities.

You cannot use SSL between Sametime Gateway and Google Talk communities.

SSL is not needed between Sametime Gateway and the local Sametime community because the connection uses the Virtual Places (VP) protocol over TCP and includes built-in encryption.

Setting up SSL on a single server:

These procedures describe how to set up Secure Sockets Layer (SSL) on a single Sametime Gateway server for both SIP and XMPP communications.

Before you begin

Before you begin, make sure the Sametime Gateway server is running.

About this task

To have a secure network connection, you will create a key for secure network communications and receive a certificate from a certificate authority (CA) that is designated as a trusted CA on your server.

WebSphere Application Server uses the certificates that reside in keystores to establish trust for a SSL connection. WebSphere Application Server creates the key.p12 default keystore file and the trust.p12 default truststore file during profile creation.

A default, self-signed certificate is also created in the key.p12 file at this time. Do not use this self-signed or other self-signed certificate to connect to external communities.

Note: Ensure that the SSL certificate contains the Basic Constraints extension. Do not use a non-SSLv3-compliant self-signed CA. WebSphere Application Server 6.1 uses the IBM JDK 1.5.0 JSSE2 which checks for the presence of the Basic Constraints extension. If the extension is not set, WebSphere Application Server assumes that the CA is not a valid CA but a user certificate, which in returns doesn't allow to validate a server certificate as valid, because the issuing CA is not found.

Trial certificates are not publicly trusted and so cannot be used to test against public instant messaging providers such as AOL Instant Messenger.

The following procedures describe how to:

1. Import the certificate authorities’ public certificate used by each of the public or private external communities your Sametime Gateway server will be communicating with.

2. Request a CA-signed certificate, and then import the signed certificate that the CA provided in response. Before performing this step you might have to import intermediary certificates.

3. Configure the WebSphere environment to make use of the imported keys.
A complete technical reference of how to setup up SSL on the WebSphere Application Server can be found in the WebSphere Application Server information center.

*Adding trust for certificate authorities used by external communities:*

External communities certificates are signed by a specific certificate authority - probably a different authority from the CA used to sign your Sametime Gateway certificate. In order for the Sametime Gateway to trust a certificate presented by an external community, the CA that issued this certificate would have to be configured to be trusted in advance.

**About this task**

This topic explains what CA certificate needs to be downloaded and imported into the WebSphere Application Server trust store.

- Steps 1-4 explain how to obtain the required CA certificate.
- Steps 5-7 explain how to import the obtained CA certificates into the WebSphere Application Server.

**Procedure**

1. To connect to AOL, download the following CA certificate. Navigate to [http://www.geotrust.com/resources/root_certificates/index.asp](http://www.geotrust.com/resources/root_certificates/index.asp) and download the Equifax Secure Certificate Authority:
   - Download - Equifax Secure Certificate Authority (Base-64 encoded X.509)

2. To connect to AOL, you are also required to download the following additional certificates:
   - Navigate to [https://pki-info.aol.com/AOL/](https://pki-info.aol.com/AOL/) and download both certificates titled: "America Online Root CA 1 certificate" and the "America Online Root CA 2 certificate."
   - Navigate to [https://pki-info.aol.com/AOLMSPKI/index.html](https://pki-info.aol.com/AOLMSPKI/index.html) and download the certificate titled: "AOL Member CA certificate"

3. To connect to an external Sametime-based IM community over SSL you will need to obtain the CA certificate used by external community
   - a. Check with the external community administrator to determine which trusted certificate authority they are using.
   - b. Obtain the CA certificate.

4. To connect to an external XMPP-based IM community over SSL. Note that the Google talk public community does not use SSL you need to obtain the CA certificate used by external community.
   - a. Check with the external community administrator to determine which trusted certificate authority they are using.
   - b. Obtain the CA certificate.

5. In case the received certificate is stored in any type of a certificate file database (a file with a suffix of .db or .p12, for example), you have to extract the certificate to an independent file, before you can import it to WebSphere Application Server.

6. Complete the following tasks in the Integrated Solutions Console: Click Security > SSL Certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer Certificate.

7. Click Add.
a. Type an alias to identify the Certificate Authority in the Alias field. This is a 
freeform value used to identify the certificate inside WebSphere, a good idea 
would be to set the alias to the certificate’s CN (common name) field value.
b. Type in the full path to the file name containing the Certificate Authority’s 
public key. For example: c:\certificates\acme_external_community.arm.
c. Select the data type.

Note: Attention: For IBM i, you must select binary as the data type.
d. Click OK.

Note: For IBM i only, Certificates are automatically downloaded with the .CER 
file extension, so you must manually rename them to the .DER file extension

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere 
Application Server administrative console.

Requesting a certificate signed by a Certificate Authority:

To ensure Secure Sockets Layer (SSL) communication, servers require a personal 
certificate that is signed by a certificate authority (CA). You must first create a 
personal certificate request to obtain a certificate that is signed by a CA.

Before you begin

The keystore that contains a personal certificate request must already exist. In 
WebSphere Application Server, the keystore file key.p12 exists.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Related items > Key 
stores and certificates > NodeDefaultKeyStore.
4. Click New.
5. In the File for certificate request field, type the full path where the certificate 
request is to be stored, plus a file name.
   For example: c:\servercertreq.arm (for a Windows machine).
6. Type an alias name in the Key label field.
   The alias is the name you use to identify the certificate request in the keystore.
   For example: stgwcertificate
7. Type a common name (CN) value.
   The CN must be your external visible DNS address to which the external 
community (AOL for example) would be opening a TCP connection to. The 
CN value does not have to be identical to any of the email domains 
associated with your community.
   You should decide on the CN value in advance primarily by consulting your 
network administrator
8. Type an organization name in the Organization field.
   This value is the "organization" value in the certificate’s distinguished name.
9. In the Organization unit field, type the “organization unit” portion of the 
distinguished name.
10. In the **Locality** field, type the "locality" portion of the distinguished name.

11. In the **State or Province** field, type the "state" portion of the distinguished name.

12. In the **Zip Code** field, type the "zip code" portion of the distinguished name.

13. In the **Country or region** drop down list, select the two-letter "country code" portion of the distinguished name.

14. Click **Apply and Save**.

   The certificate request is created in the specified file location in the keystore. The request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore.

   **Note:** Key store tools (such as iKeyman and keyTool) cannot receive signed certificates that are generated by certificate requests from WebSphere Application Server. Similarly, WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.

15. Send the certification request arm file to a Certificate Authority for signing.

   For more information, see List of supported Certificate Authorities.

16. Stop the Sametime Gateway server.

17. Make a backup copy of your keystore file. Make this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is **WebAS**. The Integrated Solutions Console has the path information for the keystore's location.

   The path to the **NodeDefaultKeyStore** is listed in the Integrated Solutions Console as:

   ```
   stgw_profile_root\config\cells\cell_name\nodes\node_name\key.p12
   ```

18. Start the Sametime Gateway server.

**Related tasks**

“Starting the Sametime System Console” on page 482

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Importing any intermediate CA certificates into the keystore:**

If your server certificate is issued by an intermediary CA, then complete the steps that follow.

**Before you begin**

You have received the signed certificate from the certificate authority, but before importing the signed certificate into the keystore, you have to determine if the received certificate had been signed by a root Certificate Authority (CA), or by a intermediary Certificate Authority. If the certificate was signed by a root CA you could skip this topic completely and continue straight to "Importing a signed certificate into the keystore". If the certificate was signed by an intermediary CA you will need to import the intermediary signer certificates as described in this topic.

**About this task**

IBM WebSphere Application Server creates a certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Therefore, it is important to
import all intermediate certificates as signer certificates into the keystore before receiving the Certificate Authority-signed certificate. When you purchase a server certificate for Sametime Gateway, the certificate is issued by a Certificate Authority (CA). The CA can either be a root CA or an intermediary CA.

**Procedure**

1. The following steps describe how to tell if your certificate was signed by a root CA or an intermediary CA (example given is on the Windows operating system)
   a. Save the signed certificate to a text file with a `.cer` extension. For example: `signed-certificate.cer`. Include the Begin Certificate and End Certificate lines when you save the file. For example:

```
-----BEGIN CERTIFICATE-----
ZZZZ3zCAlgAwIBAgIBMASEG0E nghĩa ngừ
```

b. Double-click the new file that you created and a Certificate dialog box opens.

c. Click the **Certification Path** tab.

d. Look at the tree-like structure representing the full certificate chain. The top of the chain is referred to as the root Certificate Authority (CA). The bottom of the chain represents your server's certificate. If your server is not listed one-level below the root CA, then your certificate was issued by an intermediary CA. However, if your server is listed one-level below the root CA, then the certificate was issued by the root CA. For example, the following screen capture shows a certificate chain where an intermediary CA, VeriSign Class 3 Secure Server CA, issued a certificate for

```
-----END CERTIFICATE-----
```
If the server certificate is not issued by an intermediary CA, stop here and click Next topic at the bottom of this topic.

2. One you determine that the certificate is an intermediate certificate, you must export the certificate from the chain into its own certificate file:
   a. Double-click the server's certificate (i.e. server.cer) file and a Certificate dialog box opens.
   b. Click Certification Path tab.
   c. Highlight an entry of the certificate chain.
   d. Click View Certificate.
   e. In the Certificate dialog window, click the Details tab.
   f. Click Copy to File...
   g. In the Certificate Export Wizard that appears, click Next.
   h. Select Base-64 encoded X.509 (.CER), and click Next.
   i. Type in a unique name for the certificate you are exporting and click Next. For example, "VS-intermediary-CA" for VeriSign's intermediary certificate authority.
   j. Click Finish.
   k. Click OK in the dialog box that displays the following message: The export was successful.
1. Repeat the preceding sub steps for each intermediate certificate in the chain. Note that there is no need to repeat these steps for the bottom entry of the chain because the server’s certificate already exists. When you are done, you will have a certificate file (.cer) for each entry of the chain. In our example, there are three certificate files:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Name</th>
<th>Certificate file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>VeriSign Class 3 Public Primary CA</td>
<td>VS-root-CA.cer</td>
</tr>
<tr>
<td>Intermediary</td>
<td>VeriSign Class 3 Secure Server CA</td>
<td>VS-intermediary-CA.cer</td>
</tr>
<tr>
<td>Server</td>
<td>stgw.lotus.com</td>
<td>stgw.cer</td>
</tr>
</tbody>
</table>

3. Finally, import the intermediary CA certificate into the keystore by completing the following steps:
   a. Using the Integrated Solutions Console, click Security > SSL Certificate and key management.
   b. Click Key stores and certificates.
   c. Click NodeDefaultKeyStore.
   d. Click Signer certificates.
   e. Click Add.
   f. In the Alias field, type a short descriptive name for the certificate. For example, “Verisign Intermediary CA.”
   g. In the File name field, type the path to the certificate file of the intermediary CA. For example, C:\certs\VS-intermediary-CA.cer.
   h. Accept the default file data type.
   i. Click Apply and Save.
   j. Repeat the preceding steps for each intermediary CA that is part of the certificate chain. In most cases, only one intermediary CA exists.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Importing a signed certificate issued into the keystore:

Before you begin

You have received the signed certificate from the certificate authority. You have determined whether the certificate is signed by a root CA or an intermediate CA, if the certificate was signed by an intermediate CA, then you have imported into the keystore all intermediate CA certificates. Now you are ready to import the signed certificate itself into the keystore.

About this task

WebSphere Application Server can receive only those certificates that are generated by a WebSphere Application Server certificate request. It cannot receive certificates that are created with certificate requests from other keystore tools, such as iKeyman and keyTool. The keystore must contain the certificate request that was created and sent to the CA. This means that you cannot import a certificate to the keystore if the keystore does not contain the original certificate request.
Make sure the certificate file you have received does not contain any text lines before the "-----BEGIN CERTIFICATE-----" line appears on top. These lines can cause the certificate import process to fail, and therefore you must delete these lines if they are present in the certificate file.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Related items > Key stores and certificates > NodeDefaultKeyStore.
4. Click Receive a certificate from a certificate authority.
5. Type the full path and name of the certificate file. For example on windows: c:\mycertificate.cer
6. Do not change the default data type on the list (Base64-encoded ASCII Data).
7. Click Apply and Save.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Setting up Sametime Gateway to use a new certificate:

Set up IBM Sametime Gateway server to use the new certificates.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Security > SSL certificate and key management > Configuration settings > Manage endpoint security configurations.
3. Expand the Inbound node, and then expand all levels below Nodes.
4. In the tree view, click the Sametime Gateway server.
5. On the configuration panel, under Specific SSL configuration for this endpoint, select Override inherited values if this option is available.
6. Select NodeDefaultSSLSettings in the SSL configuration drop down.
7. Click Update certificate alias list.
8. Select the certificate alias from the Certificate alias in key store drop down that you specified when you received the certificates from the CA.
9. Click Apply and then Save.
10. Important: Repeat the preceding steps on the Outbound node of the local topology tree.
11. Restart the Sametime Gateway server.
    For a standalone: the single Java process.
    For a cluster configuration: restart the DMGR, STGW servers, XMPP proxies, SIP Proxies.
    You do not need to restart the node agents.

Related tasks
“Starting the Sametime System Console” on page 482
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Setting up SSL on a cluster:
These procedures describe how to set up Secure Sockets Layer (SSL) on a cluster of Sametime Gateway servers.

Before you begin

You must first install Sametime Gateway on each node, including a Deployment Manager node, create the cluster, and create a SIP proxy server for the cluster.

About this task

To have a secure network connection, create a key for secure network communications and receive a certificate from a certificate authority (CA) that is designated as a trusted CA on your server.

WebSphere Application Server uses the certificates that reside in keystores to establish trust for a SSL connection. WebSphere Application Server creates the key.p12 default keystore file and the trust.p12 default truststore file during profile creation. A default, self-signed certificate is also created in the key.p12 file at this time.

**Note:** If you use a certificate other than the default self-signed certificate provided, ensure that the SSL certificate contains the **Basic Constraints** extension. Do not use a non-SSLv3-compliant self-signed CA. WebSphere Application Server 6.1 uses the IBM JDK 1.5.0 JSSE2 which checks for the presence of the **Basic Constraints** extension. If the extension is not set, WebSphere Application Server assumes that the CA is not a valid CA but a user certificate, which in returns doesn't allow to validate a server certificate as valid, because the issuing CA is not found.

Trial certificates are not publicly trusted and so cannot be used to test against public instant messaging providers such as AOL Instant Messenger.

The following procedure describes how to request a Certificate Authority-signed certificate, receive the request, then extract the certificate to the keystore.

For complete details for setting up SSL in WebSphere Application Server, see the WebSphere Application Server information center.

**Purchasing a certificate from a Certificate Authority:**

Purchase a Certificate Authority-signed certificate for secure connections between Sametime Gateway and other instant messaging providers.

About this task

The CA certificate installed on Sametime Gateway must conform to RFC 3280 certificate standards. The CA certificate can be a root certificate or an intermediary certificate. When requesting a certificate, check with the vendor to make sure that the certificate supports both TLS Web Server Authentication and TLS Web Client Authentication. Some certificate authorities provide certificates that support server authentication only or client authentication only. Certificates must include both server and client authentication EKU flags. Thawte certificates meet these standards. It is your responsibility to make sure that the certificate supports both.

Procedure

1. Review the list of Certificate Authorities recognized by AOL and XMPP.
   For more information, see List of supported Certificate Authorities.
2. Purchase a certificate that supports both client and server authentication.

Creating a new keystore:

The keystore file is a key database file that contains both public keys and private keys. Public keys are stored as signer certificates while private keys are stored in the personal certificates. A Secure Sockets Layer (SSL) configuration references keystore configurations during WebSphere Application Server runtime. Whether a keystore file was created by another keystore tool or saved from a previous configuration, the file must be part of a keystore configuration object. You can create a keystore configuration for the existing keystore object.

Before you begin

Expected state: the Deployment Manager, node agents, and servers are started.

Procedure

1. Stop all Sametime Gateway servers, but leave the Deployment Manager and node agents running.
2. Using the Integrated Solutions Console, click Security > SSL certificate and key management > Key stores and certificates.
3. Click New.
4. Type a name in the Name field that specifies the unique name to identify the key store; for example: STGWKS.
5. In the Path field, specify this location for the keystore file:
   
   \${CONFIG_ROOT}/STGWKS.p12.
6. Type a password in the Password field. The password is used to protect the keystore.
7. Type the keystore password again in the Confirm Password field to confirm the password.
8. Select PKCS12 from the list. The type that you select is for the keystore file that you specified in the Path field.
9. Click Apply and Save.
10. Ensure that all of the nodes in the cluster are started.
    a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Node agents.
    b. Start any node agent that is not running.
11. Synchronize all the nodes.
    a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
    b. Select all available nodes and click Full Resynchronize.

Creating a certificate request:

To ensure Secure Sockets Layer (SSL) communication, servers require a personal certificate that is signed by a certificate authority (CA). You must first create a personal certificate request to obtain a certificate that is signed by a CA.

Before you begin

The keystore that contains a personal certificate request must already exist. In WebSphere Application Server, the keystore file p12 exists.
About this task

Complete the following tasks in the WebSphere Integrated Solutions Console.

Expected state: the Deployment Manager and node agents are started. The servers are stopped.

Procedure

1. Click Security > SSL certificate and key management > Key stores and certificates.
2. Click the keystore that you created in the previous step.
3. Click Personal certificate requests, then click New.
4. In the File for certificate request field, specify the fully qualified file name from which the certificate request is exported. This portion of the certificate request can be given to the certificate authority to generate the real certificate. For example: c:\servercertreq.arm (for a Windows machine).
5. Type an alias name in the Key label field. The alias is the name you give to identify the certificate request in the keystore.
6. Type a common name (CN) value in the Common Name field. The common name must be the Fully qualified domain host name of your proxy server node machine. The CN of the certificate must match the domain name of your community. For example, if your Sametime community is us.acme.com, then the CN of the SSL certificate that you create for your community must be us.acme.com.
7. Type an organization name in the Organization field. This value is the organization value in the certificate distinguished name.
8. In the Organization unit field, type the organization unit portion of the distinguished name.
9. In the Locality field, type the locality portion of the distinguished name.
10. In the State or Province field, type the state portion of the distinguished name.
11. In the Zip Code field, type the zip code portion of the distinguished name.
12. In the Country or region drop down list, select the two-letter country code portion of the distinguished name.
13. Click Apply and Save. The certificate request is created in the specified file location in the keystore. The request functions as a temporary placeholder for the signed certificate until you manually receive the certificate in the keystore. **Note:** Key store tools (such as iKeyman and keyTool) cannot receive signed certificates that are generated by certificate requests from WebSphere Application Server. Similarly, WebSphere Application Server cannot accept certificates that are generated by certificate requests from other keystore utilities.
14. Synchronize your changes to all nodes in the cluster. Click System Administration > Nodes
15. Select all nodes in the cluster, then click Full Resynchronize.
16. Stop the Sametime Gateway server.
17. Make a backup copy of your keystore file. Make this backup before receiving the CA-signed certificate into the keystore. The default password for the keystore is WebAS. The Integrated Solutions Console has the path information for the keystore’s location. The path to the CellDefaultKeyStore is listed in the Integrated Solutions Console as: 
   stgw_profile_root\config\cells\cell_name\key.p12
18. Now start the Sametime Gateway server.

What to do next

After you receive the certificate back from the Certificate authority, you are ready to proceed to the next step.

Importing intermediate CA certificates into the keystore:

IBM WebSphere Application Server creates a certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Therefore, it is important to import all intermediate certificates as signer certificates into the keystore before receiving the Certificate Authority-signed certificate. When you purchase a server certificate for Sametime Gateway, the certificate is issued by a Certificate Authority (CA). The CA can either be a root CA or an intermediary CA.

About this task

If your server certificate is issued by an intermediary CA, then complete the steps that follow, otherwise skip these steps and click Next topic at the bottom of this topic.

Procedure

1. Before you import an intermediate CA, first determine if your server's certificate was issued by an intermediary CA:
   a. Save the signed certificate to a text file with a .cer extension. For example: signed-certificate.cer. Include the Begin Certificate and End Certificate lines when you save the file. For example:

      -----BEGIN CERTIFICATE-----
      ZZZZZzCCAkigAwIgAgIDB5iRMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
      MRAYQGZQKEdwFcyxZmF4MS50KwZDYVQlEyRFCCQjZmF41FIY3yZSBDBXZJ0
      awZPy2FDZBBdXRZZZZzdpHhW0hNMDwJgJE4MTQwMD13WQhNMDQwMjJE4MTQwMD13
      WjJ8mQxwCQYDVQQGEwJVUZZZzGA1UECBMVVG5nYXRlM2EuZXRlc3QwCAYDMwQ0
      bjEMMMAoA1UECjEUMG4wJwYDVQQLEwNNbS5mb3JjY2RlZ29yZSBBdXRZ
      YXRRlMxvqHhlJhTbCnzaNBZZZzG59wDBAQEA0AoBjAQwYkCgYEAE1a77136t1
      obqRiUy0u4wJrRvZf7vBskrF5Q04uQ4wJkQwFV0WIK0U2g
      OP1rCpY8oY1Z5R7f1f/t5MFUJHhYw7k6z9jflufa2Bn3e+jzm7ivS5dcE2
      Gm3ajjYqgwjCJbfDh7P9F1EIdWN2Z2ZZzWCCwEAAo8BnjCqAoBQVHQQB8AFBE
      BACMBPAwHQQYDVR0BBYEFMhrhr2oiTGBcBH7591mRZZZzYNVSMDoGA1uHwc2MDIw
      L6AtuoGWh0dHA6Ly9jcmwuZ2VvdHJ1c3QuY29tLTNybHlMc2VjdDJyZEuY3Js
      MB8BAEweWQYMBaAEFjaMPkrBoky10fi1Y5Q0ZyYkO/zZZgG2uiUJQ0xMBCQCCsG
      AQUFBwM8BgrByEFBoCDAJANBZZZzA1GWBAQQUA0B9qBz81UVJJ/DOPu5bL/nn
      IGRR10tB/Y1z5cZzzzz1ge0L0mzZj1dRkbaoH04N9zq2Zw5s2hJZj3ewvijkJX
      FeRH5fY5zZZZzHh1++WeZq/f/PjxjhVlKwsikFaGhJS5y2P31tMG0S6an0zzuE4L
      wpZZZzSpMnvPI3U24w76bqyVg==
      -----END CERTIFICATE-----

   b. Double-click on the new file that you created and a Certificate dialog box opens.
   c. Click on the Certification Path tab.
   d. Look at the tree-like structure representing the full certificate chain. The top of the chain is referred to as the root Certificate Authority (CA). The bottom of the chain represents your server's certificate. If your server is not listed one-level below the root CA, then your certificate was issued by an intermediary CA. However, if your server is listed one-level below the root CA, then the certificate was issued by the root CA. For example, the following screen capture shows a certificate chain where an intermediary

2. One you determine that the certificate is an intermediate certificate, you must export the certificate from the chain into its own certificate file:
   a. Double-click the server's certificate (i.e. server.cer) file and a Certificate dialog box opens.
   b. Click Certification Path tab.
   c. Highlight an entry of the certificate chain.
   d. Click View Certificate.
   e. In the Certificate dialog window, click the Details tab.
   f. Click Copy to File...
   g. In the Certificate Export Wizard that appears, click Next.
   h. Select Base-64 encoded X.509 (.CER), and click Next.
   i. Type in a unique name for the certificate you are exporting and click Next. For example, "VS-intermediary-CA" for VeriSign's intermediary certificate authority.
   j. Click Finish.
   k. Click OK in the dialog box that displays the following message: The export was successful.
   l. Repeat the preceding sub steps for each intermediate certificate in the chain. Note that there is no need to repeat these steps for the bottom entry of the chain because the server's certificate already exists. When you are done, you will have a certificate file (.cer) for each entry of the chain. In our example, there are three certificate files:
<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Name</th>
<th>Certificate file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>VeriSign Class 3 Public</td>
<td>VS-root-CA.cer</td>
</tr>
<tr>
<td></td>
<td>Primary CA</td>
<td></td>
</tr>
<tr>
<td>Intermediary</td>
<td>VeriSign Class 3 Secure</td>
<td>VS-intermediary-CA.cer</td>
</tr>
<tr>
<td></td>
<td>Server CA</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>stgw.lotus.com</td>
<td>stgw.cer</td>
</tr>
</tbody>
</table>

3. Finally, import the intermediary CA certificate into the keystore by completing the following steps:
   a. Using the Integrated Solutions Console, click **Security > SSL Certificate and key management**.
   b. Click **Key stores and certificates**.
   c. Click **CellDefaultKeyStore**.
   d. Click **Signer certificates**.
   e. Click **Add**.
   f. In the **Alias** field, type a short descriptive name for the certificate. For example, "Verisign Intermediary CA."
   g. In the **File name** field, type the path to the certificate file of the intermediary CA. For example, `C:\certs\VS-intermediary-CA.cer`.
   h. Accept the default file data type.
   i. Click **Apply** and **Save**.
   j. Repeat the preceding steps for each intermediary CA that is part of the certificate chain. In most cases, only one intermediary CA exists.

*Receiving a signed certificate:*

A Certificate Authority (CA) creates a certificate from a certificate request. WebSphere Application Server keystore receives the certificate from the CA and generates a CA-signed personal certificate that your Sametime Gateway cluster can use for Secure Sockets Layer (SSL) security.

**Before you begin**

The keystore must contain the certificate request that was created and sent to the Certificate Authority. Also, the keystore must be able to access the certificate that is returned by the Certificate Authority.

Expected state: the Deployment Manager and the node agents are started. The servers are stopped.

**Note:** WebSphere Application Server creates the certificate chain when the signed certificate is received. The chain is constructed from the signer certificates that are in the keystore at the time the certificate is received. Be sure to import all intermediate certificates as signer certificates into the keystore before receiving the CA-signed certificate.

**Procedure**

1. Click **Security > SSL certificate and key management > Key stores and certificates**.
2. Click the **keystore** that you created previously.
3. Click **Personal certificates**.
4. Click **Receive a certificate from a certificate authority**.
5. Type the full path and name of the certificate file generated by the CA.
6. Select the appropriate data from the list.
7. Click **Apply** and **Save**.

**What to do next**

Now you are ready to define a new SSL configuration.

**Defining the SSL configuration for a cluster:**

Complete these steps to create a new SSL configuration for a cluster of Sametime Gateway servers.

**About this task**

Secure Sockets Layer (SSL) configurations contain the attributes that you need to control the behavior of client and server SSL endpoints. You create a single SSL configuration to be used on the inbound and outbound trees in the configuration topology.

Expected state: the Deployment Manager and node agents are started. The servers are stopped.

**Procedure**

1. Using the Integrated Solutions Console, click **Security > SSL certificate and key management > SSL Configurations**.
2. Click **New** to display the SSL configuration panel.
3. Type name in the **Name** field for your SSL configuration.
4. In the Trust store name drop-down list, replace the default CellDefaultKeyStore value with **CellDefaultTrustStore**. The truststore name refers to a specific truststore that holds signer certificates that validate the trust of certificates sent by remote connections during an SSL handshake.
5. Select the **keystore** that you created from the **Keystore name** drop-down list. A keystore contains the personal certificates that represent a signer identity and the private key that WebSphere Application Server uses to encrypt and sign data.
6. Click **Get certificate aliases**.
7. Select your certificate alias as the default server certificate alias.
8. Select your certificate alias as the default client certificate alias.
9. Click **Apply**, and then **Save**.
10. Synchronize your changes to all nodes in the cluster. Click **System Administration > Nodes**.
11. Select all nodes in the cluster, then click **Full Resynchronize**.

**Obtaining the root certificate:**

Download a certificate authority’s (CA) root certificate. After you download the certificate, you must add it to the WebSphere Application Server truststore. For connections to AOL, download the Equifax Secure CA because this certificate is used by both communities. For connections to XMPP communities, you must determine what root certificate, if any, is being used, and then check to see if
WebSphere Application Server already recognizes the certificate, and, if necessary, download and add the certificate to your truststore.

About this task

XMPP communities are free to use either a TLS/SSL or TCP connection, so a certificate may not be needed. If the XMPP community is using TLS/SSL, the root certificate CA may already be in the WebSphere Application Server truststore. If not, you must obtain it.

Procedure

1. To obtain the same certificate used by AOL:
   b. In the list of certificates, navigate to the following:
      All other SSL certificates except for Quick SSL:
      Equifax Secure Certificate Authority
   c. Select the following download:
      Download - Equifax Secure Certificate Authority (Base-64 encoded X.509)
   d. Add this root CA to your WebSphere Application Server truststore (see next step in setting up SSL).
2. AOL users require additional certificates:
   a. Navigate to https://pki-info.aol.com/AOL/ and download both the “America Online Root CA 1” certificate and the “America Online Root CA 2” certificate.
   b. Navigate to https://pki-info.aol.com/AOLMSPKI/index.html and download the “AOL Member CA” certificate.
3. To obtain a root certificate used by a XMPP community:
   a. Check with the XMPP community to determine which trusted certificate authority they are using.
   b. Determine if WebSphere Application Server supports the certificate.
   c. If the certificate is recognized, there’s nothing more to do on this step.
   d. If the certificate is not recognized, obtain the certificate from the CA and add it to your truststore (see next step in setting up SSL).

What to do next

If for any reason the root certificate authority for an instant messaging community changes or you add an additional instant messaging community to your Sametime Gateway, you must explicitly add the new root CA to your WebSphere Application Server truststore.

Adding a trusted CA certificate to the keystore:

Add your new Certificate Authority certificate to the keystore to establish the trust relationship in SSL communication.

Before you begin

The keystore that you want to add the CA certificate to must already exist.

Expected state: the Deployment Manager and node agents are started. The servers are stopped.
Procedure

1. In the Integrated Solutions Console, click **Security > SSL certificates and key management**.
2. Click **Key stores and certificates > CellDefaultTrustStore > Signer certificates**.
3. Click **Add**.
4. Type a certificate alias in the **Alias** field. The alias is how the certificate is referenced in the keystore.
5. In the **File name** field, type the file name and path to where the certificate is located.
6. Select the appropriate file data type.
7. Click **Apply** and then **Save**.
8. Synchronize your changes to all nodes in the cluster. Click **System Administration > Nodes**.
9. Select all nodes in the cluster, then click **Full Resynchronize**.
10. Open a command window.
11. In the command window, stop the Deployment Manager and wait for the command to finish, and then restart the Deployment Manager. Use the user name and password that you provided when you enabled administrative security to stop the Deployment Manager. Open a command window and navigate to the \stgw_profile_root\bin directory and use the following commands:

   **AIX, Linux, and Solaris**
   ```
   ./stopManager.sh -username username -password password
   ./startManager.sh
   ```

   **Windows**
   ```
   stopManager.bat -username username -password password
   startManager.bat
   ```

   **IBM i**
   ```
   stopManager -username username -password password
   startManager
   ```
12. Restart the node agents.
   b. Click **System Administration > Node agents**.
   c. Select all node agents, and then click **Restart**.
13. Choose **Servers > Clusters**.
14. Select the Sametime Gateway cluster and click **Start**.
15. Click **Servers > Proxy servers**. Note that if you are not connecting to any instant messaging service over SIP, it’s not necessary to start the SIP proxy server.
16. Select the SIP proxy server or servers and click **Start**.
17. Choose **Server > Application servers**.
18. Select the XMPP proxy server and click **Start**. Note that if you are not connecting to any instant messaging service over XMPP, it’s not necessary to start the XMPP proxy server.

*Configuring the SIP proxy server to use SSL:*

Apply the new SSL definition to the SIP proxy server.
Before you begin

Expected state: the Deployment Manager, node agents, and all servers in the cluster are started.

Procedure

1. In the Integrated Solutions Console, click Security > SSL certificate and key management > Manage endpoint security configurations.
2. Expand the Inbound node on the local topology tree.
   a. Expand cell with sip proxy.
   b. Expand nodes.
   c. Expand node with sip proxy.
   d. Expand servers.
3. Select sip proxy server from the tree.
4. On the configuration panel, select Override inherited values.
5. Select the SSL configuration that you defined from the SSL configuration drop-down list.
6. Click Update certificate alias list.
7. Select your certificate alias from the Certificate alias in key store drop-down list.
8. Click Apply.
9. Repeat the preceding steps on the Outbound node of the local topology tree.
10. Change the SSL configuration on the SIP proxy server:
    a. Click Servers > Proxy Servers > name of your SIP proxy server > SIP Proxy Server Settings > SIP proxy server transports > SIPS PROXY CHANNEL > SSL inbound channel (SSL_4).
    b. Under SSL Configuration, select Centrally Managed.
    c. Click OK, and then Save.
11. Synchronize your changes to all nodes in the cluster. Click System Administration > Nodes.
12. Select all nodes in the cluster, then click Full Resynchronize.
13. Open a command window.
14. In the command window, stop the Deployment Manager and wait for the command to finish, and then restart the Deployment Manager. Use the user name and password that you provided when you enabled administrative security to stop the Deployment Manager. Open a command window and navigate to the stgw_profile_root\bin directory and use the following commands:
    AIX, Linux, and Solaris
    ./stopManager.sh -username username -password password
    ./startManager.sh
    Windows
    stopManager.bat -username username -password password
    startManager.bat
    IBM i
    stopManager -username username -password password
    startManager
15. Restart the node agents.
b. Click **System Administration** > **Node agents**.
c. Select all node agents, and then click **Restart**.

16. Click **Servers** > **Clusters**.
17. Select the Sametime Gateway cluster, and click **Stop**, and wait for the cluster to stop.
18. Click **Servers** > **Clusters**.
19. Select the Sametime Gateway cluster, and click **Start**.
20. Click **Servers** > **Proxy servers**.
21. Select the SIP proxy server and click **Start**.

**What to do next**

Now you can exchange signer certificates with other server communities.

**Configuring the XMPP proxy server to use SSL:**

Apply the new SSL definition to the XMPP proxy server.

**Before you begin**

Expected state: the Deployment Manager, node agents, and all servers in the cluster are started.

**Procedure**

1. In the Integrated Solutions Console, click **Security** > **SSL certificate and key management** > **Manage endpoint security configurations**.
2. Expand the **Inbound** node on the local topology tree.
   a. Expand **cell with XMPP proxy**.
   b. Expand **nodes**.
   c. Select the node with the XMPP proxy.
3. On the configuration panel, select **Override inherited values**.
4. Make sure **NodeDefaultSSLSettings** is selected in the **SSL configuration** drop-down list.
5. Click **Update certificate alias list**.
6. Select your certificate alias from the **Certificate alias in key store** drop-down list.
7. Click **Apply**.
8. Repeat the preceding steps on the **Outbound** node of the local topology tree.
9. Click **OK** and **Save**.

**What to do next**

Now you can exchange signer certificates with other server communities.

**List of supported Certificate Authorities:**

Certificate authorities (CAs) can issue public key certificates which state that the CA attests that the public key contained in the certificate belongs to you. You then
use your CA-signed certificate to exchange certificates with AOL and XMPP to provide for the secure exchange of instant messages.

Certificate vendors sometimes change the product names of their offerings without changing the underlying CA certificate. AOL and XMPP cannot keep track of all the product-naming conventions of each certificate vendor.

**Attention:** Server certificate installed on Sametime Gateway must conform to RFC 3280 certificate standards. When requesting a certificate, make sure the certificate supports both server and client authentication. Some certificate authorities provide certificates that support server authentication only or client authentication only. Certificates must include both server and client authentication EKU flags. Thawte certificates in the following list meet these standards. It is your responsibility to make sure that the certificate supports both.

As part of a public key infrastructure (PKI), a CA checks with a registration authority to verify information provided by your digital certificate. If the registration authority verifies your information, the CA can then issue a certificate to you.

For the current list of Certificate Authorities and accepted by Sametime Gateway and AOL and XMPP, see the IBM FAQ Tech Note #1372445, "List of Certificate Authorities (CAs) accepted by Sametime Gateway" at: www.ibm.com/support/docview.wss?&uid=swg21372445

### Setting up email notifications for certificate expiration:

This optional procedure allows the Sametime Gateway administrator to receive email notifications about SSL certificates that are about to expire soon.

**About this task**

Follow these steps to create a list of people who need to be notified of SSL certificate expirations.

**Procedure**

1. On the Sametime Gateway, log in to the Integrated Solutions Console.
2. Click **Security > SSL Certificate and key management > Manage certificate expiration**.
3. Click **NotificationsMessageLog**.
4. Select **Email sent to notification list**.
5. In the **Email address to add** field, add the administrator's email address.
6. In the **Outgoing mail (SMTP) server**, provide your organization's outgoing SMTP server host name.
7. Click to add the email address to the list of email addresses.
8. Repeat Steps 4 - 6 for additional email addresses you want to add.
9. Click **OK**.
10. Click **Save**.

**Setting up compliance for FIPS 140-2**

IBM Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2). If your Sametime deployment must maintain FIPS 140-compliance
for all data exchanged between clients and Sametime Community Servers, you
must install the FIPS Server on the Sametime Proxy Server to accept data on behalf
of Sametime Community Servers.

Installing the FIPS administration portlet
To administer the FIPS Server from the Sametime System Console, you must install
the FIPS administration portlet before you install the FIPS Server.

Procedure

Install the FIPS administration portlet into the Sametime System Console of the
Integrated Solutions Console. Go to WebSphere\STSCServerCell\optionalConsoleApps\fips.proxyadmin and install the portlet using the instructions
in the readme.txt.

Results

Note: After you install the FIPS server on the Sametime Proxy server, you can
make configuration changes. Always restart the Sametime Proxy Server if you
make any configuration changes using the administration portlet. Currently, you
cannot administer the per-node configuration or vertical clustering of FIPS on the
Sametime System Console. The administrative portlet only administers and
therefore shows registered cell deployments or horizontal cluster deployments. It
will not show individual primary or secondary nodes of the cluster.

Installing the FIPS Server
IBM Sametime supports the U.S. government-defined security requirements for
cryptographic modules known as FIPS 140-2 (Federal Information Processing
Standard 140-2). Installing the FIPS Server is only necessary if your Sametime
deployment must be FIPS-compliant; otherwise, it is optional.

Before you begin

You should have already installed the IBM Sametime System Console and the
Sametime Proxy Server. If you want to administer the FIPS Server from the
Sametime System Console, you should have already installed the FIPS
administration portlet.

If you did not install the FIPS administration portlet, you can manage the FIPS
Server using information in FIPS Support for IBM Sametime 8.

About this task

The FIPS administration portlet can connect to the FIPS Server only if the server is
installed on the Sametime Proxy Server. You cannot have multiple FIPS Servers
running on the same machine.

Note: Currently, you cannot administer the per-node configuration or vertical
clustering of FIPS on the Sametime System Console. The administrative portlet
only administers and therefore shows registered cell deployments or horizontal
cluster deployments. It will not show individual primary or secondary nodes of
the cluster.
Procedure

1. On the server where you will install the FIPS server, enable FIPS on the WebSphere Application Server by following the procedure in Configuring Federal Information Processing Standard Java Secure Socket Extension files.

2. Copy `sametimefipsproxy.war` from `setup\STIPLaunchpad\disk1\FIPSProxy` on the image disk to your local drive.

3. Log in to the Integrated Solutions Console on the machine where you are installing the FIPS Server.

4. Click Applications > Application Types > Websphere Enterprise Applications.

5. On the Enterprise Applications page, click Install.

6. Under Path to the new application, browse to the `sametimefipsproxy.war` file. Keep the default settings to install the server, and then click Next.

7. Enter the context root that you want for the FIPS Server, for example, `/fipsProxy`.

8. Click Finish and save the configuration.

9. Restart the Sametime Proxy Server to automatically start the FIPS Server.

10. Log in to the Integrated Solutions Console.

11. Click Sametime System Console > Sametime Servers > FIPS Proxy Servers. You can only edit data for FIPS if the FIPS war is running on the installed server. Make sure that your FIPS Server is running in order to administer it.

12. Click the FIPS Server that you installed.

13. Enter a fully qualified inbound host name and port and an outbound host name and port to which FIPS connects.

   If you are using the FIPS administration portlet, also replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server. Click OK.

14. Restart the Sametime Proxy Server again to automatically start the FIPS Server.

15. In a text editor, open the `sametimeProxy.xml` file. This file defines the port routing so the TLS connections can use the proxy to access the Sametime server.

   The file is located in the `\WebSphere\AppServer\profiles\profile_name\installedApps\cell_name\sametimefipsproxy_ear\sametimefipsproxy.war` directory.

16. If you are using the FIPS administration portlet, skip to the next step.

   If you are not using the FIPS administration portlet, edit the SametimeProxyChannel properties in the `sametimeProxy.xml` file. Replace the serverAddress entries with entries for the Sametime Community server that is connected to the Sametime Proxy Server.

   In the following entries, replace "temp.sametimeserver.com" with your Sametime server name, for example, "yourserver.yourdomain.com".

   ```xml
   <channel name="SametimeProxyChannel" factory="com.ibm.sametime.proxy.channel.impl.SametimeProxyChannelFactory" sequence="2" weight="1">
   ...
   <property name="serverAddress1" value="temp.sametimeserver.com:8081" />
   <property name="clientAddress2" value="*:1533" />
   <property name="serverAddress2" value="temp.sametimeserver.com:1533" />
   <property name="clientAddress3" value="*:554" />
   <property name="serverAddress3" value="temp.sametimeserver.com:554" />
   ...
   </channel>
   ```

17. Edit the TLSInboundChannel properties in the `sametimeProxy.xml` file:
• For the com.ibm.ssl.keyStore property, replace the wccmDefault value of DummyServerKeyFile.jks with the actual keyFileName and location for the keystore on this WebSphere Application Server. Replace the file:///c: designation with the operating system’s absolute path to the file.

• For the com.ibm.ssl.trustStore property, replace the wccmDefault value of DummyServerTrustFile.jks with the actual trustFileName and location for the keystore on this WebSphere Application Server. Replace the file:///c: designation with the operating system’s absolute path to the file.

<channel name="TLSInboundChannel" factory="com.ibm.ws.ssl.channel.impl.SSLChannelFactory" sequence="2" weight="1">

• For the com.ibm.ssl.protocol property, replace the SSLv3 value with TLSv1.

18. Close and save the file.
19. Restart the Sametime Proxy Server again to put the configuration changes into effect.

Results

Sametime Connect clients use the "Direct connection using TLS" Connection option when setting up the server community connected to the FIPS-enabled server.

Setting up single sign-on (SSO) for Sametime clients

Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Preparing servers running on WebSphere Application Server for single sign-on

Prepare for single sign-on (SSO) by exporting a LTPA key from the servers running on WebSphere Application Server. This step applies to the Sametime Media Manager SIP Proxy and Registrar server, the Sametime Meeting server, and Sametime Advanced. If you plan to enable the Click to Call feature, it also applies to the Sametime Unified Telephony Application Server. The Sametime Proxy Server does not need to be set up for single sign-on.

Before you begin

Servers using SSO must use the same LDAP directory that the Sametime Community Server uses.

About this task

The Sametime Community Server installation creates a Domino SSO key. You must replace the Domino SSO key with a WebSphere LTPA key to allow the Sametime Community server running on Domino and the other servers running on WebSphere Application Server to have an identical key for token validation and generation. If Sametime servers running on WebSphere Application Server are managed by different Sametime System Console, you must export the LTPA key.
from one of the servers (the Media Manager SIP Proxy and Registrar, Meeting Server, or Advanced server).

**Procedure**

1. Log in to the Integrated Solutions Console for the Sametime server.
3. Make sure that the Domain name matches the Sametime Server domain.

   **Note:** Verify that Interoperability Mode is selected if you allow LTPAv1 tokens (used by Sametime servers running releases earlier than Sametime 8.5). Do not select Interoperability Mode if the Sametime Community Servers are running Sametime 8.5 or later.
4. Click OK and save the master configuration.
6. Under Authentication, click LTPA.
7. In the LTPA timeout section, set the timeout value to a value larger than the default to minimize the potential for an LTPA token to expire during an active meeting. A value that covers a period somewhat longer than a typical work day, such as 600 minutes, is recommended.
8. Under Cross Cell single sign-on, enter a Password, confirm the password, and specify a file name to store the key. Click Export keys. Make a note of the location of the file created. You need to know its location when you import the file to the Sametime Community Server.
9. Navigate to the directory where you exported the LTPA key.
10. Copy the LTPA key to a location where you can access the file from the Sametime Community Server.

**Configuring the Sametime Community Server for single sign-on**

After creating LTPA keys for Sametime servers, configure the Sametime Community Server for single sign-on.

**Before you begin**

Make sure all servers use the same LDAP directory.

**About this task**

By default the Sametime installation creates a Domino SSO key. This key should be replaced by the WebSphere LTPA key you exported in the previous section, Preparing servers running WebSphere Application Server for single sign-on. Follow these steps to import the LTPA key from WebSphere to Domino.

**Procedure**

1. Import the LTPA keys used by Sametime servers in the same DNS domain.
   b. Click Configuration > Web Web Configurations view.
   c. Open the Web SSO Configuration for LtpaToken document.
   d. Click Edit SSO Configuration.
   e. Click Keys > Import WebSphere LTPA keys.
f. Type in the exact file location of the key file you created on the Sametime SIP Proxy and Registrar server.

g. Enter the password you created on the server when you enabled single sign-on.

h. Click OK.

The message "Successfully imported WebSphere LTPA keys" appears after the key has been imported.

2. For Domino 8.0 and higher:

   Note: Sametime 8.5 requires Lotus Domino 8.0 and higher; if you are maintaining an older Sametime server it may be running a version of Lotus Domino prior to R8.

   In the Token Format field of the WebSphere Information section, select the LTPA token formats to be supported by Domino.
   - LtpaToken - LTPAv1 only
   - LtpaToken2 - LTPAv2 only
   - LtpaToken and LtpaToken2 - both LTPAv1 and LTPAv2 formats are supported

   With this last option selected, both tokens are created, but the token returned to the client is determined by the TOKEN_TYPE_TO_RETURN flag under the AuthToken section of sametime.ini. The default value is LTPA, which returns the LTPAv1 token. Changing the value to LTPA2 results in the LTPAv2 token being returned instead.

3. Click Save and Close.

4. Configure the Sametime Community Server so that LtpaToken gets set by the Sametime Proxy web client instead of the Sametime token:
   a. Log in to the Sametime System Console as the Sametime administrator.
   b. Click Sametime Servers > Sametime Community Servers.
   c. In the list of Community Servers, click the name of a Sametime Community Server to open its Configuration page.
   d. Click the Community Services tab.
   e. Under the "General" section, select the authentication type that users can use while logging into the community server: LTPA only.

5. Restart the Lotus Domino server to put your changes into effect.

Importing a shared LTPA key to enable SSO for a server in a different cell

If you set up SSO between IBM Sametime servers running on WebSphere Application Server that are in different cells, import the shared LTPA key you exported as described in “Preparing servers running on WebSphere Application Server for single sign-on” into each Media Manager SIP Proxy and Registrar server, Sametime Meeting Server, and Advanced server that is part of the same SSO environment. If the servers are managed by one Sametime System Console, you do not need to perform this step because they already share the same LTPA key.

Procedure
   1. From the Integrated Solutions Console of the Sametime server, click Global security > LTPA.
   2. Scroll down to "Cross-cell single sign-on."
3. In the Password and Confirm password fields, enter the password that is used to decrypt the LTPA keys. This password must match the password that was used in the cell from which you are importing the keys.

4. Enter the fully qualified key file name, and click Import.

5. Click Apply and then Save.

6. Restart the Sametime server to put your changes into effect.

7. Repeat these steps for every Sametime server that belongs to a different cell.

**What to do next**

From the Deployment Manager's Integrated Solutions Console, select all nodes in the environment and select Full Resynchronize. Then start or restart all node agents.

**Verifying that servers have the same single sign-on settings**

Confirm that the IBM Sametime Meeting Server and the Media Manager SIP Proxy and Registrar server use the same SSO settings.

**About this task**

Check the settings first on the Meeting Server first, then on Media Manager SIP Proxy and Registrar server and verify that they are the same.

**Procedure**

1. Log in to the server’s Integrated Solutions Console.

2. 


4. Make a note of the domain name and Interoperability mode.

**Results**

Both servers must have the same settings for single sign-on to work.

**Configuring single sign-on with Microsoft Windows Active Directory**

The Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) replaces Microsoft Windows Single Sign-On, which is no longer supported by Sametime. If the Sametime Community Server uses a Microsoft Windows Active Directory, you must integrate all server components to allow Sametime users to log in and authenticate only once at their desktop and thereafter automatically authenticate with the Sametime server.

**About this task**

This white paper on the developerWorks site explains the procedure:

Integrating SPNEGO with IBM Sametime components using IBM WebSphere Application Server 7.0

**Configuring security for the Sametime Community Server**

The IBM Sametime server uses the Internet and intranet security features of the Domino server on which it is installed to authenticate web browser users who access Domino databases on the server.
About this task

Follow the instructions in this section to set up SSL, HTTP tunneling, and user authentication.

Authentication by token using LTPA and Sametime tokens

Sametime uses authentication by token to authenticate connections that occur after a user has authenticated to Domino once using password authentication.

Authentication by token prevents a user from having to re-enter authentication credentials when accessing different servers or using Sametime web clients or Domino applications that connect to a Sametime server.

The Sametime server includes two separate security features capable of generating the authentication token used by Sametime:

- Domino Single Sign-On (SSO) authentication feature - The Domino SSO feature must be enabled on a Sametime server.

  If the Domino SSO feature is not enabled on the Domino server when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, you might need to alter the default SSO configuration provided by the Sametime installation. For more information, see Altering the Domino Web SSO configuration following the Sametime server installation.

  The user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meetings.example.com) in the web browser URL locator when accessing the Sametime server to authenticate successfully using SSO.

- If your Sametime environment includes only Sametime 3.0 (or higher) servers, and you do not use Sametime TeamRoom or Discussion databases that were available with earlier Sametime server releases, only the Domino SSO feature is required to support authentication by token.

  If your Sametime environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0, both the Domino SSO feature and the Secrets and Tokens databases must be supported on the Sametime server to enforce authentication by token.

  Sametime includes a custom logon form for the SSO feature. This custom logon form can be used in place of the default SSO logon form. The custom logon form is presented to the user the first time the user accesses a database on the server that requires basic password authentication.

Note: If the Sametime Server is configured to use Internet Sites, the Notes client integration with Sametime (and therefore SSO with Sametime) has been supported only since Sametime 8.5.1 and Notes client 8.5. When configuring the Sametime Server to use Internet Sites the following settings must be configured under the [AuthToken] section of the sametime.ini file:

- ST_TOKEN_TYPE must contain the name of the Web SSO document used by the Sametime Community server. The default value is LtpaToken.

- ST_ORG_NAME must contain the organization name that is set in the Web SSO document used by Sametime Community server. The default value is an empty organization name.

For additional information about the Domino Internet Sites configuration see Domino documentation.
Secrets and Tokens authentication databases - Sametime server releases earlier than Sametime 3.0 used only the Secrets and Tokens authentication databases to create authentication tokens. When Sametime 8.x operates in environments that include servers from Sametime releases earlier than Sametime 3.0, the Sametime 8.x server supports both the Domino SSO feature and the Secrets and Tokens authentication databases.

A Sametime 8.x server supports Secrets and Tokens authentication by default. The following are required to support Secrets and Tokens authentication:

- The Secrets and Tokens databases must be present on the server following a Sametime server installation.
- The "Allow users to authenticate using either LTPA token or Sametime Token (stauths.nsf and stautht.nsf)" option must be selected in the Configuration-Community Services-General settings of the Sametime Administration Tool.

Both conditions above exist on a Sametime server following the server installation, so no additional procedures are required to support Secrets and Tokens authentication following the installation. However, if you have enhanced security by enabling the SametimeSecretsGenerator agent in one Secrets database on one Sametime server in your community, you must ensure that this Secrets database is replicated to all Sametime servers in the community. For more information, see Replicating the Secrets database (optional).

Authentication by token using the Domino Single Sign-On (SSO) feature:

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. This feature creates Lightweight Third Party Authentication (LTPA) tokens that enable web browser users to log in a single time to access multiple Sametime, Domino, or IBM WebSphere servers that are in the same DNS domain. This capability is called "single sign-on."

Sametime also uses LTPA tokens to authenticate connections from Sametime clients to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services on the Sametime server. These clients are Java applets and include the Meeting Room client, and Recorded Meeting client.

Sametime supports two versions of LTPA tokens: LTPAv1 and LTPAv2. Sametime allows authenticating by a single LTPA token or by a list of LTPA tokens. For example, a client can send an LTPAv1 token and LTPAv2 token in the same authentication request to authenticate a user. The Domino configuration determines which token is validated.

The LTPA token types supported by Domino are configured in the Web SSO document in names.nsf. When using a Domino SSO key, only LTPAv1 tokens are supported. When importing a WebSphere LTPA key, both LTPAv1 and LTPAv2 tokens are supported by Domino. The supported formats are defined in the Token Format field under the WebSphere Information section of the Web SSO document.

Sametime can generate a single LTPA token or a list of LTPA tokens depending on the SSO key that is configured in Domino and the Token Format field in the case of WebSphere LTPA keys.

Note: Sametime also requires users to present an authentication token when attending an instant meeting. Client applications generate this token from the user's home Sametime server. Users with Sametime 2.5 (or earlier) home Sametime servers will present Sametime tokens (generated from the Secrets and Tokens databases).
databases) when connecting to instant meetings started on a Sametime 8.x server. For this reason, Sametime 8.x servers operating in Sametime environments that include Sametime servers from previous releases must also support the Secrets and Tokens databases for authentication by token.

Authentication by LTPA token occurs after a user has already authenticated once using password authentication. For example, authentication by token on a Sametime server might occur as follows:

1. A user accesses a Sametime Meeting Center database that requires authentication or clicks the "Log onto Sametime" link in the Sametime Meeting Center.
   
   **Note** To successfully authenticate, the user must enter the fully qualified domain name of the Sametime server (for example, sametimeserver.meeting.acme.com) in the web browser URL locator when accessing the Sametime server.

2. An SSO logon form appears, and the user enters a valid user name and password from the Domino Directory (or LDAP directory) to authenticate.
   
   **Note** Sametime provides a custom Sametime SSO logon form that can be enabled by the administrator. If the custom logon form is not enabled, the standard Domino SSO logon form displays to the user.

3. After a successful authentication, the Domino Single Sign-On (SSO) feature generates an LTPA token containing the user's authentication information and passes the token to the user's web browser in a cookie.
   
   The user's web browser must have cookies enabled to accept the LTPA token.

4. The user attends a meeting, and the Meeting Room client loads in the user's web browser.

5. The Meeting Room client connects to the Meeting Services and Community Services and passes the LTPA token to Sametime. The Meeting Services and Community Services connections are authenticated using the LTPA token. The user is not required to re-enter authentication credentials to authenticate these connections.

The same LTPA token described above can be used to authenticate the user when the user accesses other Sametime, Domino, or WebSphere servers in the same DNS domain during a single web browser session. The other Sametime, Domino, or WebSphere servers must also support the SSO feature (that is, the servers must accept LTPA tokens).

If the Domino SSO feature is not enabled when you install Sametime, the Sametime installation automatically enables and configures the Domino SSO feature. In some environments, it may be necessary to alter the SSO configuration following the Sametime server installation. For more information, see Altering the Domino Web SSO configuration following the Sametime server installation.

**Related concepts**

Authentication by token using Secrets and Tokens databases

To authenticate by token, the Sametime server can accept an authentication token created by the Secrets and Tokens authentication databases, the Domino Single Sign-On (SSO) feature, or both. The Sametime server can also generate tokens using the Secrets and Tokens authentication databases or the Domino SSO feature.

*Altering the Domino Web SSO configuration following the Sametime server installation:*
The IBM Sametime installation automatically enables and configures the Domino SSO feature on the Domino server. In some cases, it may be necessary to alter the default configuration of the Domino SSO feature following the Sametime server installation.

This topic discusses the following issues pertaining to the Sametime installation and the Domino SSO feature:

- **SSO configurations performed by the Sametime installation** - This section explains how the Sametime installation configures the Domino Web SSO feature. You can use this information to determine if it is necessary to alter the default SSO configuration following a Sametime server installation.

- **Altering the SSO configuration** - This section explains the most common reasons for altering the SSO configuration following the Sametime server installation. In multiple Sametime server environments, it is frequently necessary to add the Domino server names of Sametime servers to the Domino Web SSO Configuration document.

- **Viewing and editing the Domino Web SSO configuration document** - This section explains how to edit the Domino Web SSO configuration document in the Domino Directory. This document contains the parameters for the Web SSO configuration that you may need to change.

- **Sametime includes a custom SSO logon form. See Using the Sametime custom logon form for SSO for information about enabling this form following the Sametime server installation.**

**Note:** If for some reason it is necessary to manually enable the Domino SSO feature, you can use the procedures described in Manually enabling the Domino SSO feature. You can also review these procedures to understand all configurations that are required to support SSO for the Sametime server.

**SSO configurations performed by the Sametime installation**

The Sametime installation enables the Domino SSO feature and performs the SSO configurations described below. The Sametime installation:

- Creates a Web SSO Configuration document named LtpaToken. This document contains the SSO configuration needed for generation and validation of LTPA tokens. The following fields are populated into this document:
  - DNS Domain - To populate the DNS Domain field, the installation determines the fully-qualified domain name of the Sametime server machine and then subtracts the hostname value from the fully-qualified domain name.
    For example, if the installation determines the fully qualified name of the Sametime server is "Sametimeserver.east.acme.com," the installation writes ".east.acme.com" in the DNS Domain field.
    The LTPA token is then valid for the servers that belong to the DNS domain specified in the DNS Domain field.
  - Expiration (minutes) - This field specifies the length of time for which the LTPA token is valid. This value is 30 minutes by default. You may want to provide a longer value for the token expiration. Lotus software recommends a setting of 120 minutes.
  - Domino Server Names: Each Domino/Sametime server that can accept the SSO token must be listed in the Domino Server Names field. By default, the installation writes only the name of the Domino server on which Sametime is installed in this field. It may be necessary to add the names of all other
Domino/Sametime servers in the community to this field. For more information, see Altering the SSO configuration.

- Alters the Sametime/Domino server Server document. The installation changes the Internet Protocols-Domino Web Engine-Session authentication field in the Server document to the value "Multiple servers (SSO)." The Server authentication field must have the "Multiple servers (SSO)" value even if your Sametime community uses only one Sametime server. If the "Multiple server (SSO)" value is not selected, the SSO feature will not function properly for Sametime.

- Automatically configures the Sametime server to use the Sametime custom logon form for SSO. To enable the custom logon form, the Sametime installation:
  - Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server.
    *Note:* If a domcfg.nsf database already exists on the Domino server when Sametime is installed, the Sametime installation overwrites the existing domcfg.nsf database.
  - Creates a "Mapping a Login Form" document in the domcfg.nsf database.
  - Populates the following fields in the Mapping a Login Form document:
    - Target database filename - This field is set to the value "stcenter.nsf."
    - Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named "STLogonForm.nsf" displays to users when users authenticate with the server.

### Altering the SSO configuration

The default configuration outlined above meets the basic requirements necessary for a Sametime server to support SSO. In some cases, it may be necessary for the administrator to alter the "DNS Domain" field or the "Domino Server Names" field of the Domino Web SSO Configuration document following the Sametime server installation.

- **Altering the DNS Domain field** - The Sametime installation may not always accurately detect the fully-qualified domain name of the Sametime server machine. If this problem occurs, the DNS Domain field may not specify the appropriate DNS domain. The administrator might need to manually edit the Domino web SSO Configuration document to add the appropriate entry in the DNS Domain field of the Domino web SSO Configuration document. Follow the instructions in "Viewing and editing the Domino Web SSO Configuration document" below to manually edit the document.

- **Altering the Domino Server Names field** - If the Sametime community consists of multiple Sametime/Domino servers, the Domino server names of all of the Sametime/Domino servers in the Sametime community must exist in the "Domino Server Names" field of the Domino Web SSO Configuration document. By default, the installation writes only the name of the Domino server on which Sametime is installed to this field. If you have multiple Sametime servers, it may be necessary to manually open the Domino Web SSO configuration document and enter the names of the Domino/Sametime servers in the "Domino Server Names" field.

For example, if you have Sametimeserver1/East/Example and Sametimeserver2/East/Example in your Sametime community, and you install Sametimeserver3/East/Example, only Sametimeserver3/East/Example is written to the Domino Server Names field during the Sametime installation. The administrator may need to open the Domino Web SSO Configuration document and manually enter the names Sametimeserver1/East/Example and Sametimeserver2/East/Example in the "Domino Server Names" field on the
Domino Web SSO Configuration document on Sametimeserver3/East/Example to ensure that all servers in the community are entered in this field. To manually open the Domino Web SSO Configuration document, see "Viewing and editing the Domino Web SSO Configuration document" below.

Note that in multiple server environments, the Domino Directory may already be replicated to the Domino server at the time the Sametime server is installed. If the Domino Directory already exists on the server and contains a Domino Web SSO configuration document, the Sametime installation will not attempt to alter the existing configuration in any way. In this case, the existing Domino Web SSO configuration document may already contain the names of the existing servers in the community and it may be necessary to add the name of the newly installed Sametime server to the Domino Web SSO configuration document.

For example, the names Sametimeserver1/East/Example and Sametimeserver2/East/Example may already exist in the Domino Web SSO configuration document in the Domino Directory on the server reserved for the Sametimeserver3/East/Example installation. Since the Sametimeserver3/East/Example installation does not alter an existing SSO configuration, that server name will not appear in the Domino Web SSO Configuration document following the Sametime server installation. In this scenario, it is necessary to open the Domino Web SSO configuration document in the Domino Directory on Sametimeserver3/East/Example and manually enter "Sametimeserver3/East/Example" in the "Domino Server Names" field. All other parameters in the existing Web SSO Configuration document should be valid for the newly-added server.

Altering the SSO key

By default the Sametime installation creates a Domino SSO key. If WebSphere is participating in SSO, this key should be replaced by the WebSphere LTPA key to allow both Domino and WebSphere to have an identical key for token validation and generation. Do this by importing the LTPA key from WebSphere to Domino. For more information, see Setting up single sign-on for Sametime browser clients.

Viewing and editing the Domino Web SSO Configuration document

To view or edit the Web SSO configuration document that is created by the Sametime installation, do the following:

1. From a Lotus Notes client, open the Domino Directory on the Sametime server.
2. Choose the Configuration > Web > Web Configurations view.
3. In the right-hand pane, select the twistie to display the document under "Web SSO Configurations."
5. Click Edit to put the document in edit mode.
6. Edit the appropriate field (for example, the DNS Domain or Domino Server Names field).
7. Click Save and Close after editing the document.

In some cases the name of the Web SSO configuration document can be different than LtpaToken, and the Organization field in the document might not be empty. This is mainly relevant for Internet Sites configuration. In this case the following settings must be set under the [AuthToken] section of the sametime.ini file:
• **ST_TOKEN_TYPE** must contain the name of the Web SSO document used by the Sametime Community server. The default value is *LtpaToken*.

• **ST_ORG_NAME** must contain the organization name that is set in the Web SSO document used by Sametime Community server. The default value is an empty organization name.

**Manually enabling the Domino SSO feature:**

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**About this task**

This procedure is identical to the procedure used to enable the SSO feature on a Domino server. After manually enabling the feature, you can configure the server to use the Sametime custom SSO logon form.

Generally, the Domino SSO feature will be enabled by default during the Sametime installation and it is not necessary to manually enable the feature. For more information, see Altering the Domino Web SSO feature following the Sametime server installation.

To enable the Domino SSO feature on the Sametime server:

**What to do next**

After enabling the Domino SSO feature, follow the procedure described in Using the custom Sametime SSO logon page to use the custom Sametime SSO logon form.

*Create the Web SSO Configuration document in the Domino Directory:*

Create a Web SSO document that specifies the servers participating in the shared authentication, the time-out value for the cookie containing the LTPA access token, and the encrypted secret used to create the cookie.

**Procedure**

2. Select Configuration > Servers > All Server Documents.
3. Select the Web button on the taskbar.
4. Select Create Web SSO Configuration.
5. In the document, select the Keys pull-down menu button.
6. The default value for the **Configuration Name** field is *LtpaToken*. This is the preferred value and usually it should not be changed. In case another value is configured as the Web SSO document name, the **ST_TOKEN_TYPE** setting under the [AuthToken] section of the *sametime.ini* file must contain the same value.
7. Select Create Domino SSO Key.

*Note* The Import WebSphere LTPA Keys option is usually used to enable a WebSphere server to communicate with a Domino server. To enable a WebSphere server to communicate with a Domino server, you must export the
8. Configure the Token Expiration field. Note that a token does not expire based on inactivity; it is valid only for the number of minutes specified from the time of issue. The token is also valid only for a single browser session.

**Note** Set the expiration value to a value somewhat longer than a typical work day, such as 600 minutes, to minimize the potential for an LTPA token to expire during an active meeting. Setting a higher value may create a security risk. If the LTPA token is intercepted by an attacker, the attacker may use the token to illegally gain access to the Sametime server until the token expires. Setting up the Domino server to support SSL for web browser connections provides the highest level of security against attempts to intercept LTPA tokens.

9. In the DNS Domain field, enter the DNS domain (for example, .lotus.com or .meetings.acme.com.) for which the tokens will be generated. The servers enabled for SSO must all belong to the same DNS domain. This field is required and the DNS domain must start with a comma.

When users access the Sametime server, they must enter the fully qualified domain name of the Sametime server for authentication to be successful (for example, sametimeserver/meetings/acme/com).

10. In the Server Names field, enter the servers that will be participating in SSO. Generally, this field should contain the Domino hierarchical names of all Sametime servers in your environment. You can browse and select the server names from the Domino Directory.

**Note** Groups and wildcards are not allowed in the field.

11. The Organization field should usually stay empty. In case it has a value, which is mandatory only for Internet Sites configuration, the ST_ORG_NAME field setting under the [AuthToken] section of the sametime.ini file must contain a similar value. For additional information about Internet Sites see the Domino documentation.

12. Select **Save & Close** to save the Web SSO Configuration document. The document will appear in the Web Configurations view. This document will be encrypted for the creator of the document, the members of the Owners and Administrators fields, and the servers specified in the Server Names field.

**Related tasks**
Manually enabling the Domino SSO feature
If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**Enable SSO and “Name & Password” authentication in the Server document:**

Use this procedure to enable SSO and "Name & Password" authentication in the Server document of the Sametime server for which you are enabling the Domino SSO feature.

**About this task**
This procedure is the second of three required to manually enable the Domino SSO authentication feature on a Sametime server.
Procedure
1. In the Configuration - Servers - All Server Documents view of the Domino Directory, double-click the name of the Sametime server to open the Server document.
2. Select Edit Server to put the Server document in edit mode.
3. Select the Ports tab.
4. Select the Internet Ports tab.
5. Select the Web tab (if it is not displayed by default).
6. For the HTTP TCP/IP port Authentication Options, select Yes in the "Name & Password" field.
7. Select the Internet Protocols tab.
8. Select the Domino Web Engine tab.
9. In the "HTTP Sessions" section, select "Multiple server (SSO)" in the "Session authentication" field.
   Note You must select the "Multiple server (SSO)" value even if your environment includes only a single Sametime server.
10. Click Save and Close to save the Server document.

What to do next
Start (or restart) the HTTP task on the SSO-enabled server

Related tasks
Manually enabling the Domino SSO feature
If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

Start (or restart) the HTTP task on the SSO-enabled server:
Use the Domino console to start or stop the HTTP server.

About this task
This procedure is required to manually enable the Domino SSO authentication feature on a Sametime server.

To start the HTTP task on the SSO-enabled server:

Procedure
1. Open the Domino console.
2. Start the HTTP server, or stop and restart the HTTP server if it is already running.
   • Use the Tell HTTP Quit command to stop the HTTP server.
   • Use the Load HTTP command to start the HTTP server.
3. On the Domino console, the following message should appear:
   HTTP: Successfully loaded Web SSO Configuration
4. If a server enabled for SSO cannot find a Web SSO Configuration document or is not included in the Server Names field (and thus cannot decrypt the document), then the following message should appear on your server's console.
HTTP: Error Loading Web SSO configuration. Reverting to single server session authentication.

What to do next

Lotus software recommends using the custom Sametime SSO logon form. If you do not use this logon form, users will see the default Domino SSO logon form the first time they access a database on the server that requires authentication.

Note: Authentication by token does not occur if you allow anonymous access to the Sametime server and all its databases.

To configure the Sametime server to use the custom Sametime SSO logon form, see Using the Sametime custom logon form for SSO.

Using the Sametime custom logon form for SSO:

The IBM Sametime installation automatically configures the Sametime server to use the Sametime custom logon form for SSO.

The Sametime installation performs the following configurations to enable the custom logon form:

1. Creates a Domino Configuration database named domcfg.nsf in the root data directory of the Domino server on which Sametime is installed. This database is created from the domcfg5.ntf template available with the Domino server.


3. Populates the following fields in the Mapping a Login Form document:
   - Target database filename - This field is set to the value "stcenter.nsf."
   - Target form name - This field is set to STLogonForm.nsf.

The configurations described above ensure that the custom logon form named "STLogonForm.nsf" displays to users when users authenticate with the server.

If a database named domcfg.nsf exists on the Sametime server when Sametime is installed, the administrator must manually enable the custom logon form. This procedure is described below.

Manually enabling the custom logon form

Follow the procedure below to manually enable the Sametime custom logon form for SSO. The custom logon form displays when the user accesses the first database on the server that requires authentication or selects the "Log on to Sametime" link in the Sametime Meeting Center.

Note: The custom logon form exists in the Sametime server home page database (stcenter.nsf). If you want to require users to authenticate when accessing the server, you should allow anonymous access to the Sametime server home page (stcenter.nsf) and require authentication to the Sametime Meeting Center database (stconf.nsf). With this arrangement, users access the server home page anonymously and are presented with the SSO logon form when attempting to create or attend a meeting.

To use the Sametime custom logon form for SSO, you must configure settings in the Domino Configuration database (domcfg.nsf) provided with the Domino server on which Sametime is installed.
To use the Sametime custom logon form for SSO:

1. Verify that the Sametime server has a Domino Configuration database named domcfg.nsf.

   **Note** If your server includes an existing domcfg.nsf database, but you do not want to use that database you can delete the existing domcfg.nsf database and create a new one. To create a new domcfg.nsf database, use the Domino Configuration (R5) template (domcfg5.ntf) available with a Domino server. When creating the new database, you must select the “Show advanced templates” option to access the domcfg5.ntf template.

2. If necessary, copy the domcfg.nsf Domino Configuration database to the root data directory of the Domino server on which Sametime is installed (for example C:\Lotus\Domino\Data directory).

3. From a Lotus Notes client, open the Domino Configuration database.

4. Choose **Add Mapping**.

5. Under Site Information, accept the default of All Websites/Entire Server.

6. In the "Target database filename" field, enter stcenter.nsf.

7. In the "Target form name" field, enter STLogonForm.

**Required ACL settings for the Sametime Center database (stcenter.nsf)**

The Sametime Center database (stcenter.nsf) must meet the following ACL requirements for the custom logon form to operate properly.

- In the Advanced options of the stcenter.nsf ACL settings, the “Maximum Internet name & password” field must allow at least Reader access. If either Depositor or No Access are selected, the logon form will not appear.

- In the Basics options of the stcenter.nsf ACL settings, anonymous users must have an access level of Reader or higher. If the access level provided for anonymous users is less than Reader, the logon form will not appear. The "Write public documents" and "Read public documents" options should also be selected.

**Related tasks**

Manually enabling the Domino SSO feature

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

**Authentication by token using Secrets and Tokens databases:**

To authenticate by token, the Sametime server can accept an authentication token created by the Secrets and Tokens authentication databases, the Domino Single Sign-On (SSO) feature, or both. The Sametime server can also generate tokens using the Secrets and Tokens authentication databases or the Domino SSO feature.

If the Sametime server is operating in an environment that includes Sametime servers from releases earlier than Sametime 3.0, or if Domino databases enabled with Sametime technology (such as the Sametime Discussion and TeamRoom databases that were available with earlier releases) are used in your environment, the Sametime server must support both the Secrets and Tokens authentication databases and the Domino SSO authentication feature.

The Sametime server is set up to support Secrets and Tokens authentication by default. The basic requirements for this authentication system are:
• The Secrets (stauths.nsf) and Tokens (stautht.nsf) databases must exist on the
  Sametime server. These databases are created during the Sametime server
  installation.

• The "Allow users to authenticate using either LTPA or Sametime Tokens
  (stauths.nsf and stautht.nsf)" option must be selected in the Sametime
  Administration Tool. (This option is selected by default.)

Note that previous releases of Sametime allowed an administrator to enhance the
level of security provided by the Secrets and Tokens databases by enabling the
SametimeSecretsGenerator agent in one Sametime Secrets database (stauths.nsf) on
one Sametime server in the Sametime community. If you enable the
SametimeSecretsGenerator agent on one Secrets database on one Sametime server,
that Secrets database must be replicated to all Sametime servers in the community.
If your environment includes Sametime servers from previous releases and you are
currently replicating a Secrets database to all of the servers in your environment,
you must also replicate that Secrets database to the Sametime servers.

There are two procedures associated with ensuring the Secrets and Tokens
authentication databases on the Sametime server are functioning properly:

1. If necessary, select the "Allow users to authenticate using either LTPA or
   Sametime Tokens (stauths.nsf and stautht.nsf)" option in the Sametime
   Administration Tool. (This option is selected by default.)

2. Replicating the Secrets and Tokens databases (optional) - This step is necessary
   only if you have deployed Domino databases enabled with Sametime
   technology (such as Sametime TeamRoom and Discussion databases) or if you
   have enhanced security by enabling the SametimeSecretsGenerator agent in the
   Secrets database.

Selecting the "Allow users to authenticate using either LTPA or Sametime Tokens
(stauths.nsf and stautht.nsf)" option:

The "Allow users to authenticate using either LTPA or Sametime Tokens
(stauths.nsf and stautht.nsf)" setting must be enabled in the Sametime
Administration Tool to enable the Sametime server to accept both the LTPA and
Sametime Tokens. This setting must be set consistently on all Sametime 8.x, 7.x,
6.5.1, 3.x servers in your environment.

About this task

Note: This procedure might not be necessary as the "Allow users to authenticate
using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" setting is
enabled by default following the server installation.

If you enable this setting on one Sametime server, you must enable it on all
Sametime servers in your environment. If you disable it on one Sametime server,
you must disable it on all Sametime servers in the environment.

To enable this setting:

Procedure

1. From the Sametime server home page, click Administer the server to open the
   Sametime Administration Tool.

2. Choose Configuration.

3. Choose Community Services.
4. Select the "Allow users to authenticate using either LTPA or Sametime Tokens (stauths.nsf and stautht.nsf)" option.
5. Click Update.
6. Restart the server for the setting to take effect.

Results

You have the option of replicating the Secrets database to enhance security.

Related tasks

Manually enabling the Domino SSO feature

If your environment requires you to manually enable the Domino SSO feature instead of using the default configuration provided by the IBM Sametime installation, you can use the steps in this section to manually enable the Domino SSO feature.

Replicating the Secrets and Tokens databases (optional):

If you have installed multiple Sametime servers, you can enable the SametimeSecretsGenerator agent in the Secrets database. Enabling the SametimeSecretsGenerator agent is an optional procedure that increases security against outside attacks.

About this task

This topic discusses the second of two procedures associated with setting up the Secrets and Tokens authentication system on a Sametime server.

The Secrets and Tokens databases exist on every Sametime server.

If you enable the SametimeSecretsGenerator agent, only one Secrets database should be used for all Sametime servers in the environment. You should replicate the Sametime Secrets database in which you have enabled the SametimeSecretsGenerator agent to all Sametime servers in the environment.

Create a replication schedule for the Secrets database in which you have enabled the SametimeSecretsGenerator agent to ensure it replicates at regular intervals.

Delete all other copies of the Secrets database from all Sametime servers in the environment. For more information, see Integrating a Sametime server into an existing Sametime community.

Do not replicate the Tokens database to the other Sametime servers. The replicated Secrets database can work with the Tokens database that exists on each Sametime server by default following the server installation.

If you do not enable the SametimeSecretsGenerator agent in any Secrets database on any Sametime server, it is not necessary to replicate the Secrets database. If you do not enable the SametimeSecretsGenerator agent, administration is simpler because no replications or replication schedules are required, but the security level is not as high.

Working with Sametime security

The IBM Sametime server uses the Internet and intranet security features of the Domino server on which it is installed to authenticate web browser users who access Domino databases on the server. These databases include the Sametime Center database (stcenter.nsf), which contains the Sametime server home page, and the Sametime Meeting Center database (stconf.nsf).
Sametime also uses authentication-by-token features to authenticate connections from Sametime clients to the Sametime server. The authentication-by-token features include the Secrets and Tokens databases supported by all previous Sametime releases and the Domino Single Sign-On (SSO) authentication feature that is supported by Sametime 3.0 and higher-version servers.

Sametime also provides security features that enable users to encrypt meetings and specify meeting-specific passwords. The Security section includes the following topics:

Getting started with Sametime security:

This section includes basic security information to help you get started with IBM Sametime security.

The required fully-qualified server name:

The user must enter the fully qualified DNS name of the IBM Sametime server (for example, sometimeserver.meetings.acme.com) in the web browser URL locator when accessing the Sametime server to authenticate with a Sametime server.

The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. The Domino SSO feature requires the user to enter the fully qualified DNS name of the server for a successful authentication. For more information, see Authentication by token using LTPA and Sametime tokens.

Basic password authentication and authentication by token:

IBM Sametime uses two types of authentication: Basic password authentication and authentication by token.

Basic password authentication

Sametime uses basic password authentication to authenticate web browser connections and Sametime Connect client connections. Sametime uses the same Internet and intranet security features as a Domino server to authenticate the web browser connections. These features include Domino database Access Control Lists (ACLs) and security settings in the Server document of the Domino server on which Sametime is installed.

The Domino security features also allow you to configure databases for anonymous access. When a database is configured for anonymous access, the user is not authenticated when accessing the database.

The following topics in this section discuss basic password authentication:

- User requirements for basic password authentication
- Using database ACLs for identification and authentication
- Basic password authentication and database ACLs
- Setting up basic password authentication in a database Access Control List (ACL)

Authentication by token

After a web browser user authenticates using basic password authentication, Sametime Java applet clients (such as the Meeting Room client, Recorded Meeting
client, and Sametime Connect for browsers client) load in a user's web browser. These Sametime clients make connections to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services when a user attends a meeting. Sametime uses "authentication by token" to authenticate the connections from these Sametime clients to the Sametime services.

**Note:** Connections from the Sametime clients to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services are authenticated only if the Sametime Meeting Center database (stconf.nsf) requires basic password authentication. If the Sametime Meeting Center allows anonymous access, these connections are not authenticated.

When the Sametime Meeting Center requires basic password authentication, authentication by token is supported on the Sametime server using the Domino Single Sign-On (SSO) authentication feature.

If your environment includes only Sametime 3.0 (or higher) servers, it is only necessary to enable the Domino SSO feature on the Sametime servers.

**Note:** Sametime TeamRoom and Discussion databases were available with previous Sametime releases but are no longer included in the Sametime product.

The Sametime server must support both the Domino SSO feature and the Secrets and Tokens database authentication system if your environment includes Sametime 3.0 (or higher) servers that interoperate with Sametime servers from releases earlier than Sametime 3.0.

The following topics discuss authentication by token:
- Authentication by token
- Authentication by token using the Domino Single Sign-On (SSO) feature
- Authentication by token using Secrets and Tokens databases

**User requirements for basic password authentication:**

When accessing the Sametime server with a Web browser, a user must enter a user name and Internet password to access any protected database on the Sametime server.

A protected database is a database that has its Access Control List (ACL) set to require basic password authentication. If the ACL settings of a database allow anonymous access, the user is not authenticated (prompted for a user name and Internet password) when accessing the database.

**Note:** It is important for a user to enter a name when accessing a Sametime database so that the user's name can be displayed in any presence list within the database. If the ACL settings of a database allow anonymous access, a user is not prompted for a name unless the "Users of Sametime applications can specify a display name so that they do not appear online as anonymous" setting is selected in the Configuration-Community Services-Anonymous Access settings of the Sametime Administration Tool. When this option is selected, it forces a name entry prompt to appear when an anonymous user attends a scheduled meeting. From this name entry prompt, the user can enter a name for display purposes in a presence list. The server accepts any name entered by the user at the name entry prompt; the user is not authenticated.
A Sametime Connect user must also be authenticated each time the user starts the Sametime Connect client and connects to the Community Services on the Sametime server. Sametime Connect users must enter the user name and Internet password from the Person document in the Domino Directory when logging on to Sametime Connect.

**Note:** If you have configured Sametime to operate with an LDAP directory, Sametime authenticates users based on the user names and passwords stored in the person entries of the LDAP directory.

**Person document, User names, and Internet passwords in the Domino Directory**

This section discusses the requirements for basic password authentication when Sametime is installed to operate with a Domino Directory. You must choose either the Domino Directory or an LDAP directory during the Sametime installation.

Each member of the Sametime community must have a Person document in the Domino Directory to authenticate with the Sametime server. The names and password that a user can enter when accessing a Sametime server are maintained in the Basics tab of a Person document in the Domino Directory.

To access a Person document, open the Sametime Administration Tool and select **Domino Directory > Domino > Manage People.** Double-click a person’s name to open that user’s Person document.

The table below shows a sample entry in the Basics section of a user’s Person document. The text that follows the table explains how these entries are used in the web browser and Sametime Connect client password authentication processes.

**Sample settings in the Basics section of a Person document**

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Gary</td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Middle initial</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Last name</td>
<td>Ollerman</td>
<td>This field is required.</td>
</tr>
<tr>
<td>User name</td>
<td>Gary Ollerman/Community/GOllerman</td>
<td>This field is required.</td>
</tr>
<tr>
<td>Alternate name</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Short name/UserID</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Generational qualifier</td>
<td></td>
<td>This field is optional.</td>
</tr>
<tr>
<td>Internet password</td>
<td>(FCF5F3960B0A289D3)</td>
<td>This field is required.</td>
</tr>
</tbody>
</table>
The following fields on the Person document are used by the authentication process:

- **First name** - This field is optional.

  *Web browser* - If an entry exists in the "First name" field in the Basics tab of the Person document, the user can enter just this name at the User Name prompt that appears when accessing a protected database on the Sametime server with a web browser. The user must also enter the Internet password to access the database. (A protected database is a database that has its ACL set to require basic password authentication.)

  *Sametime Connect* - The first name is not a valid entry at the User Name prompt that appears when logging on to the Sametime Connect client.

- **Last name** - This field is required. An entry must exist in the "Last name" field of the Basics tab of a Person document.

  The last name can be entered in the User Name prompt that appears when accessing a protected database on the Sametime server with a Web browser. The last name can also be used when logging on from the Sametime Connect client. A user must also enter the Internet password to complete the authentication process.

  **Note:** If both the "First name" and "Last name" fields contain entries, the user can enter the first and last names at the User Name prompt that appears when accessing the Sametime server.

- **User name** - This field is required. An entry must exist in the "User name" field in the Basics tab of a Person document.

  Generally, it is good practice to use a user's first and last name in the "User name" field. The "User name" field can contain multiple entries. In our example, the User name field contains both Gary Ollerman/Community and GOllerman. (Each entry must be separated by a semicolon or a carriage return in the "User name" field of the Person document.)

  A user can enter any name that appears in the "User name" field of the Person document when logging on to the Sametime server from the Sametime Connect client or a web browser. For example, the user could enter Gary Ollerman/Community or GOllerman at a Sametime Connect or web browser User Name prompt. The name entered by the user is resolved to the topmost name (Gary Ollerman/Community in the example) in the "User name" field. The topmost name in the "User name" field is the name that is displayed in the presence lists of all Sametime clients.

  **Note:** If you want a user's email address to display in presence lists, enter the user's email address as the topmost name in the "User name" field of the Person document. If the email address is included in the User name field, the user can also enter the email address at the "User name" prompt when logging in from a Sametime Connect client or web browser.

  Sametime uses the topmost name in the "User name" field to validate a user in a database ACL. If you require basic password authentication for a database and you enter the names of individual users in the ACL of a database, enter the topmost name that appears in the "User name" field of the Person document in the database ACL. Although the user can enter "GOllerman" when logging on, Sametime uses "Gary Ollerman/Community" to validate the user in the database ACL. Therefore, "Gary Ollerman/Community" must be the name that appears for this user in database ACLs.

- **Internet password** - This field is required. Users must enter the Internet password to authenticate with the Sametime server using a Web browser or the
Sametime Connect client. In the example, the Internet password is "sametime." The password displays as a series of random characters because Internet passwords are encrypted on the Person document.

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

: \ } ' = &

**Self-registration**

If you are using the self-registration feature of the Sametime server, a Person document containing a last name, user name, and Internet password is automatically created for a user in the Domino Directory on the Sametime server at the time the user self-registers. Agents in the Self-Registration database (streg.nsf) access the Domino Directory to create these Person documents. The signers of these agents must have the proper access levels and permissions in the Domino Directory for self-registration to work properly. If you allow self registration, you might need to add these signers to the Domino Directory ACL.

The Sametime self-registration feature cannot be used if you have configured the Sametime server to operate with an LDAP directory on a third-party server (such as a Microsoft Exchange or Netscape Directory Server).

**LDAP**

If you have configured the Sametime server to operate with an LDAP directory on a third-party server, the authentication process uses the user names and passwords stored in the LDAP directory. It is not necessary to create Person documents containing separate user names and passwords in the Domino Directory on the Sametime server.

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

: \ } ' = &
Related concepts
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Related tasks
Changing a user's password
When accessing the IBM Sametime server from any Sametime client, the user might be prompted for a user name and password. The password is specified in the Internet password field on the user's Person document in the Domino Directory on the Sametime server.

Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

Changing a user’s password:

When accessing the IBM Sametime server from any Sametime client, the user might be prompted for a user name and password. The password is specified in the Internet password field on the user's Person document in the Domino Directory on the Sametime server.

About this task
To change a user's password, open the user's Person document and enter a new password in the "Internet password" field.

Note: If you have configured the Sametime server to operate with an LDAP directory on an LDAP server, the authentication process uses the passwords specified in the LDAP directory. Use the administrative tools provided with the third-party LDAP server to access the LDAP directory and make password changes for individual users. You cannot change passwords stored in an LDAP directory from the Sametime Administration Tool.

To change a user's Internet password in the Domino Directory on the Sametime server:

Procedure
1. From the Sametime server home page, open the Sametime Administration Tool.
2. Select Domino Directory.
3. Select Domino.
4. Select Manage People.
5. Double-click the name of the user whose password you want to change.
6. Click Edit Person.
7. Enter the new password in the "Internet password" field of the Person document. You might want to write the new password down before closing and saving the Person document. After you close and save the Person document, the Internet password is encrypted and you cannot view it.

Password character restrictions
In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
Ensuring Sametime servlet access when Domino requires SSL for all connections:

An IBM Sametime server installs on a Domino server and relies on the Domino HTTP server to handle all HTTP traffic to the Sametime server. To encrypt web browser access to the Sametime Meeting Center with SSL, the administrator must configure the Domino HTTP server to support SSL.

About this task

When setting up a Domino HTTP server to support SSL, the administrator can force all connections to the Domino server to use SSL. The administrator forces all HTTP connections to use SSL by performing either of the following configurations in the Ports-Internet Ports-Web section of the Domino Server document during the Domino HTTP server SSL set up procedure:

- Setting the Web HTTP "TCP IP port status" setting to "Disabled" and setting the Web HTTP "SSL port status" to "Enabled."
- Setting the Web HTTP "TCP IP port status" to "Redirect to SSL."

If you force all HTTP connections to use SSL, you must also configure the Sametime server to support SSL for HTTP connections to its servlets. If you do not configure the Sametime server to support SSL for connections to its servlets, users will be unable to access the Sametime server.

To ensure access to the Sametime servlets when Domino requires SSL for all connections, complete the following steps:

Procedure

1. Set up the Domino server to support SSL
2. Import the SSL trusted room or SSL server certificate into the key store database on the Sametime server
3. Modify the Sametime configuration for SSL

Results

You can use these procedures regardless of whether your Sametime server operates on the Windows, AIX, Solaris, Linux or IBM i operating system.

Note: It is possible to configure a Domino server to allow unencrypted HTTP connections on port 80 and simultaneously allow SSL-encrypted HTTP (or HTTPS) connections on port 443. This configuration enables you to encrypt connections to databases containing sensitive data while allowing unencrypted connections to databases that do not contain sensitive data. Since the Domino server on which Sametime is installed is dedicated to supporting only Sametime, it is unlikely that such a configuration would be implemented on a Domino/Sametime server.

Domino security and the web browser connection:

To attend a meeting on the Sametime server, a user first connects to the Sametime HTTP server with a web browser. By default, the user is not authenticated when accessing the Sametime server over this port and is able to access the Sametime server home page database (stcenter.nsf) without entering a user name and password.
By using the Access Control List (ACL) settings of individual databases, the Sametime administrator can force users to authenticate using basic password authentication when they attempt to access the databases on the server.

Generally, the first database that a user accesses when connecting to the Sametime server is the Domino database that contains the Sametime server home page (stcenter.nsf). By default, the ACL settings of the stcenter.nsf database allow anonymous access so users can access the Sametime server home page without being authenticated (entering a user name and password that is verified against entries in a directory).

After accessing the home page, a user selects links to access other databases on the Sametime server. Most users will access the Sametime Meeting Center (stconf.nsf). The Sametime Administrator can alter the ACLs of these databases to force users to authenticate at the time they select the link that accesses the database.

The databases on the Sametime server that are accessible from the Sametime server home page include:

- **Self-Registration (streg.nsf)** - An administrator controls whether self-registration is available on the server. The administrator controls self-registration by selecting or clearing the "Allow people to register themselves in the Directory" check box available from the Domino Directory - Domino option in the Sametime Administration Tool. The self-registration database (streg.nsf) should always allow anonymous access to enable anonymous users to self-register when the administrator allows self-registration.

- **Server Administration** - You must add users to the ACLs of several Sametime databases when allowing other users to have administrative privileges on the Sametime server. For more information about controlling access to the Sametime Administration Tool, see Adding a new Sametime administrator

**Note:** By default, the connection from a web browser to the Sametime server is neither authenticated nor encrypted. The authentication occurs at the time a user accesses an individual database on the Sametime server. You can configure Sametime so that all HTTP traffic (including passwords and authentication tokens) that passes over the connection between the web browser and the HTTP server is encrypted using the Secure Sockets Layer (SSL).

**Note:** References to the Sametime Meeting Center and to the web browser connection do not apply to Sametime Entry servers.
Related concepts
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

Anonymous access and database ACLs
You can set a database ACL to allow anonymous access.

Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Related tasks
Setting up anonymous access in a database Access Control List (ACL)
To allow anonymous access to a database, you can add the Anonymous entry to the ACL and assign an access level to the Anonymous entry.

Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

Using database ACLs for identification and authentication:

Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

For each database on the server, you can set the ACL to allow:

- Anonymous access
  or
- Basic password authentication

The settings in the database ACLs work together with the "Maximum Internet name & password" setting for each database to control the level of access that web browser users have to a database on the Sametime server.

Using database ACLs

The database ACL defines user access to the content of the database. Before you set up basic password authentication or anonymous access to a database, you should be familiar with how to add users to a database ACL and the available settings within the ACL. For more information, see:

- Adding a name to a database ACL
- Database ACL settings

Maximum Internet name & password setting

The "Maximum Internet name & password" setting on the Advanced panel of each database ACL specifies the maximum level of access to the database that is allowed for web browser clients. This setting overrides individual levels set in the ACL.

Generally, administrators should not need to change the "Maximum Internet name & password" settings for databases on the Sametime server. The default settings should function adequately in most cases.

Adding a name to a database Access Control List (ACL):
Use the Sametime Administration Tool to add a name to a database Access Control List.

Procedure
1. From the Sametime server home page, click **Administer the Server** to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select **LDAP Directory**.
3. Select **Access Control**.
4. Select a database from the list.
5. Click **Access**. The database ACL displays.
6. Click **Add**.
7. In the dialog box, type the exact user name from a Person document or the group name from a Group document. Click **OK**.
   When entering a user name for a user with a Person document in the Domino Directory on the Sametime server, type the name exactly as it appears in the topmost entry of the "User name" field in the user's Person document.
   When entering the names of users or groups registered in an LDAP directory in a Sametime database ACL, use the fully qualified Distinguished Name, but use forward slashes (/) as delimiters instead of commas. For example, if the Distinguished Name for the user in the LDAP directory is:
   - uid = Joe Waters, ou=West, o=Example
   enter the name in the Sametime database ACL as follows:
   - uid = Joe Waters/ou=West/o=Example
   You can also use asterisks for wildcards when entering names from an LDAP directory or a Domino Directory in an ACL. For example, entering */ou=West/o=Example* is equivalent to entering all users in the ou=West/o=Example branch of the directory to the ACL.
   **Note** It is possible to enter entities other than user and group names in an ACL. For more information about the types of entries that can exist in an ACL, see User type - ACL settings.
8. Click the name entered in the previous step so that the name is selected (highlighted).
9. In the User Type box, select the type of user (Unspecified, Person, Server, Person Group, Server Group, or Mixed Group). For more information, see User type - ACL settings.
10. In the Access Box, assign an access level for the user (Manager, Designer, Editor, Author, Reader, Depositor, or No Access). For more information, see Access level - ACL settings.
11. Edit the privileges if necessary. For more information, see Privileges - ACL settings.
12. Click **Submit**.
Related concepts
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.
Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Database ACL settings:
A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

For each user in the database ACL, you can specify the following ACL settings:

Related concepts
Using database ACLs for identification and authentication
Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.
Basic password authentication and database ACLs
You can set a database ACL to require basic password authentication.

Related tasks
Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

User type - ACL settings:
When you add a user or group to an ACL, you specify a user type for the entry in the ACL. A user type identifies whether a name in the ACL is for a person, server, group, or other entity. You assign a user type to a name to specify the type of ID required for accessing the database with that name.

You can designate an entry in the ACL as any of the following user types:

Unspecified
Select the Unspecified user type if you want to enable the name you are entering to access the database with any type of ID (Person, Server, or Group). The Default entry in an ACL is always assigned the Unspecified user type. IDs used to sign agents, such as Sametime Development/Lotus Notes Companion Products, are also assigned the Unspecified user type when entered in a database ACL.

Person
Select the Person user type if the name you are entering belongs to a user who has a Person document containing a user name and Internet password in the Directory on the Sametime server or if the user has a Person entry in an LDAP directory on a third-party server.

Server
Select the Server user type if the name you are entering belongs to another server in the Domino domain. When multiple servers are installed in a Domino environment, it might be necessary for a server to access data within the database or to replicate a database. Server names are frequently added to the pre-existing LocalDomainServers and OtherDomainServers server groups. The Server user type is generally used only if you have
installed Sametime in a Domino environment. This user type performs the same function as it does on a Domino server.

**Mixed Group**
Select the Mixed Group user type if the name you are entering belongs to a group that consists of both Server and Person names.

**Person Group**
Select the Person Group user type if you are entering the name of a group that contains only people. You can enter a group from the Directory on the Sametime server, or you can enter a group stored in an LDAP directory on a third-party server in the ACL of a database.

**Server Group**
Select the Server Group user type if the name you are entering belongs to a group that consists of only servers.

**Access level - ACL settings:**
Access levels are the database ACL settings that control the type of actions a user can perform on the contents of a database and on the database itself.

Access levels range from No Access, which prevents a user from opening a database, to Manager, which lets a user read, create, and edit the ACL and all documents in the database.

Users that are listed both individually and in one or more groups in the ACL might be assigned different levels of access. The access level granted in an individual entry takes precedence over the access level granted through a group entry. If a user is in multiple groups, the user is granted the access level of the group with the highest level of access.

If a user or group has one level of access in the ACL and another level of access in a database component (such as a Read or View access list), the database component access level takes precedence over the user or group access level.

The following access levels are listed from lowest to highest. A higher access level has all the privileges granted to lower access levels. For example, Authors can perform all of the functions of a Depositor and a Reader.

**No Access**
No Access prevents a user from accessing the database. For example, if you assign No Access as the Default access for a database, only a user who has a Person document in the Address Book and is listed in the ACL can access the database.

**Depositor**
Depositor access allows a user to create documents but not view any documents in the database, including the documents created by the user. This access level is not generally used for Sametime databases. This ACL type is most frequently used for automatic agents to write documents into a database for Domino workflow applications.

**Reader**
Reader access allows a user to read documents in a database, but not create or edit documents. For example, you can assign Reader access in the Meeting Center (stconf.nsf) ACL to users who are allowed to attend but not start meetings.
Note: If you assign a user the Reader access level in the Meeting Center (stconf.nsf), the user can attend listed meetings but cannot attend unlisted meetings in the Meeting Center. To enable a user with Reader access to also attend unlisted meetings, you must select the "Write public documents" check box for that user in the ACL.

Author

Author access allows a user to create and edit documents. Users with Author access can edit documents they have created themselves, but they cannot edit documents created by other users.

Assign Author access in the Meeting Center ACL to allow users to create meetings in the Sametime Meeting Center. Meeting Center users with Author access can modify the meetings they create, but they cannot modify meetings created by other users. To create a meeting, the user must have Author access and the Write Public Documents privilege selected.

Editor

Editor access allows users to read, create, and edit all documents in the database, including those created by other users.

Assign Editor access in the Meeting Center ACL to users who are allowed to modify meetings they create and meetings that are created by other users. Editors can also start meetings in the Meeting Center. To create meetings, the user must also have the Write Public Documents privilege selected.

Designer

Designer access allows a user to create full-text indexes, modify all database design elements, and read, create, and edit all documents in the database. This access level is primarily for programmers and database developers.

Manager

Manager access allows a user to read, create, and edit the ACL and all documents in a database, modify ACL settings, and delete the database. Modifying the ACL and deleting databases are tasks permitted by no other access level. This access level is usually assigned to Sametime administrators and is not recommended for general users.

Each database must have at least one Manager. Generally, the Manager access level is provided in each database to the person specified as the administrator during the Sametime installation and setup procedure. You should assign Manager access to two people in case one manager is unavailable. For information about granting other users administrative privileges, see Allowing others to use the Sametime Administration Tool.

Privileges - ACL settings:

The database Access Control List (ACL) defines privileges for users.

Depending on the access level assigned to a user, some ACL permissions are granted, denied, or optional. Privileges listed in the ACL are:

Create documents

This privilege allows users to create documents in a database. This privilege is:

- Permanently granted to Managers, Designers, Editors, and Depositors
- Permanently denied to Readers
- Optionally granted to Authors
Delete documents
This privilege allows users to delete documents from a database. This privilege is:

- Permanently denied to Readers and Depositors
- Optionally granted to Managers, Designers, Editors, and Authors

Create personal agents
This privilege allows an Lotus Notes developer or user to create agents that perform automated procedures in a database. This privilege is:

- Permanently granted to Managers and Designers
- Optionally granted to Editors, Authors, and Readers

Clear this option on server databases to prevent certain users from creating personal agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running personal agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Create personal folders/views
This privilege is:

- Permanently granted to Managers and Designers
- Permanently denied to Depositors
- Optionally granted to Editors, Authors, and Readers

Personal folders and views created on a server are more secure and are available on multiple servers. Also, administrative agents can operate only on folders and views stored on a server. If this permission is not selected, users can still create personal folders and views that are stored on their local workstations. Clear this option to save disk space on a server.

Create shared folders/views
This privilege is:

- Permanently granted to Managers and Designers
- Permanently denied to Authors, Readers, and Depositors
- Optionally granted to Editors

Deny this privilege to Editors to save disk space on a server and maintain tighter control over database design.

Create LotusScript®
This privilege is:

- Permanently granted to Managers
- Permanently denied to Depositors
- Optionally granted to Designers, Editors, Authors, and Readers

Clear this option on server databases to prevent certain users from running restricted and unrestricted LotusScript agents that take up server disk space and processing time. Use the Agent Restrictions settings in the Security tab of the Server document in the Directory to prevent users from running restricted and unrestricted LotusScript agents on a server, even if the “Create personal agents” permission in a server database ACL is selected.

Read Public Documents
This privilege is:
- Permanently granted to Managers, Designers, Editors, Authors, and Readers
- Optionally granted to Depositors

Write Public Documents

This privilege is:
- Permanently granted to Managers, Designers, and Editors
- Optionally granted to Authors, Readers, and Depositors

Public documents, such as the meeting details document in the Sametime Meeting Center, are designed to be accessed by a wide audience. Users with the Write Public Documents permission can read, create, edit, and delete public documents from a database. To create a meeting in the Sametime Meeting Center, a user must have the Author access level with the Write Public Documents privilege selected.

A user must also have the Write Public Documents privilege selected to attend unlisted meetings on the Sametime server.

Users without the Write Public Documents privilege are prompted for a password when accessing a database with public documents. After entering the user name and Internet password, the user is given the Default access level to the database.

Roles - ACL settings:

Database Access Control List (ACL) roles grant access to individual database components, such as forms or views.

You can use ACL roles to delegate authority for managing specific documents in a database. You can create up to 75 roles in a database. For example, you can assign the roles of UserCreator and UserModifier in the Directory (Address Book) ACL to the administrator who has the responsibility for creating and maintaining Person documents.

ACL roles are optional in most databases. You can choose to rely on a broader access level and not use roles.

For more information on roles available in important Sametime databases, see Roles in Sametime databases ACLs.

Anonymous access and database ACLs:

You can set a database ACL to allow anonymous access.

Anonymous access has the following characteristics:
- Users are not identified or authenticated when they access databases and applications on the server.
- Data sent between the user and the Sametime server is not encrypted.
- Anonymous users are not identified in the maintenance log files. All anonymous user activity is recorded under the name "Anonymous."

The anonymous access level requires the least maintenance from the administrator, but it is the least secure. You should only allow anonymous access when you do not need to know the identity of users accessing your server. For example, use
anonymous access if the Sametime server is behind your firewall and you plan to allow only trusted intranet users to access it.

Setting up anonymous access in a database Access Control List (ACL):

To allow anonymous access to a database, you can add the Anonymous entry to the ACL and assign an access level to the Anonymous entry.

About this task

Note: Alternatively, you can remove the Anonymous entry from the ACL and assign an access level to the Default entry in the ACL. When the Anonymous entry is removed from the ACL, anonymous users receive the access level and privileges assigned to the Default entry in the database ACL.

Use the following procedure to allow anonymous users to access a database:

Procedure
1. From the Sametime server home page, click the "Administer the Server" link to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click the Advanced button.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.
   Note: The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author, and assign Editor access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager, and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.
7. Click the Access button.
   If the Anonymous entry exists in the ACL, select the Anonymous entry and assign an access level (for example, Author). Edit the default privileges if necessary.
   If the Anonymous entry does not exist in the ACL, users who access the database anonymously receive the access level and privileges assigned to the Default entry in the ACL.
   Note: If the Anonymous entry does not exist in the ACL, the administrator also has the option to create an Anonymous entry and assign an access level and privileges. In this case, users receive the access level associated with the Anonymous entry instead of the Default entry.
8. Click Submit.
What to do next

If you set the ACL of the Sametime Meeting Center database to allow anonymous access, you should ensure that users are required to enter a display name when accessing the database. To ensure that users will be required to enter a display name to appear in the Participant List of the Sametime Meeting Room during a scheduled meeting, make sure that the "Users of Sametime or Sametime applications can specify a display name so that they do not appear online as "anonymous"" setting is selected in the Sametime Servers > Sametime Community Servers > deployment_name > Anonymous setting of the Sametime System Console.

Basic password authentication and database ACLs:

You can set a database ACL to require basic password authentication.

Basic password authentication has the following characteristics:

- Users are identified or authenticated when they access databases and applications on the server.
- A web browser user must have a user name and an Internet password stored in the user's Person document to access databases. Only users with these credentials can access a database that requires basic password authentication.
- Data transmitted between the user and the Sametime server (including the name and password) is not encrypted.
- Users are identified in the maintenance log files.

Basic password authentication identifies users, but it does not prevent unauthorized users from listening to network transmissions or gaining server access by guessing passwords. For information on using Secure Sockets Layer (SSL) to encrypt the data that passes over the web browser connection to the IBM Sametime server, see Configuring Sametime to use SSL encryption.

Using the Default entry or individual names in database ACLs

When basic password authentication is enabled for a database, browser clients are authenticated when they attempt to open a database. For example, a web browser user might be authenticated when selecting the "Attend a Meeting" link from the Sametime server home page to access the Sametime Meeting Center database (stconf.nsf).

The Sametime server challenges the user to supply a valid name and password and then verifies that the user's response matches the information stored in the user's Person document in the Domino Directory (or LDAP directory if you have configured Sametime to operate with an LDAP directory). Authentication succeeds if the user name and password provided by the user matches the user name and password in the directory and:

- The user is listed individually or as a member of a group in the database ACL.
- The Anonymous entry is set to No Access while an access level is specified for the Default entry in the ACL. Using this method allows you to require users to authenticate but prevents you from having to add individual entries for every user and group in the ACL.
When the Anonymous entry in the database ACL is set to No Access, users are presented with a logon prompt when they attempt to access the database.

Users must enter the user name and Internet password at the logon prompt. Users that are successfully authenticated are then provided with the access level that is specified for the Default entry in the database ACL.

If both the Anonymous entry and the Default entry in the database ACL are set to No Access, a user must be listed in the ACL individually or as part of a group to access the database. Setting the Anonymous and Default entries to No Access provides the strictest control over access to the database because only users and groups that are listed in the ACL are allowed to access the database.

An individual name receives precedence over the Default entry. If a user's name is entered in a database ACL and provided with an access level, the user receives the access level assigned to the user name entry in the database. Only users who are not listed individually in the database ACL receive the Default access level.

Note: If the Anonymous entry does not exist in the database ACL, the Default entry in the ACL must be set to "No access" to require basic password authentication to the database. When the Anonymous entry does not exist in the database ACL, anonymous users can access the database and receive the access level assigned to the Default entry in the database. If the Anonymous entry exists in the ACL and is assigned the "No access" access level, users are authenticated when accessing the database and receive the access level specified for the Default entry in the ACL.

Related concepts
Database ACL settings
A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

Related tasks
Setting up basic password authentication in a database Access Control List (ACL)
You can require users to specify a valid name and password when accessing a database on the Sametime server.

Setting up basic password authentication in a database Access Control List (ACL):
You can require users to specify a valid name and password when accessing a database on the Sametime server.

About this task
Follow these steps to set up basic password authentication for a database.

Procedure
1. From the Sametime server home page, click Administer the Server to open the Sametime Administration Tool.
2. If you are using a Domino Directory with the Sametime server, select Domino Directory > Domino. If you are using an LDAP directory with the Sametime server, select LDAP Directory.
4. Select a database from the list.
5. Click Advanced.
6. Set the "Maximum Internet name & password" access to Manager, which is the maximum access level.
   
   **Note** The "Maximum Internet name & password" setting on the advanced panel of each database Access Control List (ACL) specifies the maximum database access level granted to web browser clients. This setting overrides higher individual access levels set in the ACL. For example, if you set the "Maximum Internet name & password" to Author and assign Manager access to the Anonymous entry in the database ACL, anonymous users will only have Author access to the database. Alternatively, if you set the "Maximum Internet name & password" to Manager and assign Reader access to the Anonymous entry in the database ACL, anonymous users will only have Reader access to the database.

7. Click Access.

8. Select the Anonymous entry, and then select No Access in the Access box.
   
   If the Anonymous entry does not exist, you must create it. Use the following procedure to create an Anonymous entry and assign the No Access level to the entry:
   - Click Add.
   - Type Anonymous in the dialog box and click OK.
   - Select the Anonymous entry, and then select No Access in the Access box.

9. Select the Default entry. You can either set an access level for the Default entry, or set the Default entry to No Access.
   - If you specify an access level for the Default entry other than No Access, all users are required to authenticate when accessing the database. Each authenticated user receives the access level you have specified for the Default entry. It is not necessary to enter individual names or groups in the ACL. After selecting an access level for the Default entry, click Submit. You have finished the procedure required to set up basic password authentication in a database ACL. Skip the remaining steps.
   - If you select No Access for the Default entry, you must enter individual user names or group names in the ACL. Only the names and groups you enter can access the database. Complete steps 10 and 11 to add users to the ACL.

10. Click Add to add user names or group names to the ACL. Click OK after adding each name.

11. Click Submit.

**Related concepts**

**Using database ACLs for identification and authentication**

Identification and authentication is the process of determining the name of a user and verifying that users are who they say they are. You can use database Access Control Lists (ACLs) to control access to individual databases on the server.

**Basic password authentication and database ACLs**

You can set a database ACL to require basic password authentication.

**Database ACL settings**

A database Access Control List (ACL) contains a list of users and defines user access to the contents of the database.

**Setting up single sign on authentication:**

IBM Sametime single sign-on (SSO) authentication allows web users to log in once to a Domino or WebSphere server, and then access any other Domino or WebSphere server in the same DNS domain that is enabled for single sign-on (SSO).
without having to log in again. In a multiple server environment, it is possible that one or more servers in your Domino domain are already configured for Domino SSO, and the Domino Directory already contains a Domino Web SSO configuration document. When you install Sametime, it creates a Web SSO configuration document called LtpaToken unless one already exists in the Domino Directory. If an LtpaToken configuration document already exists, Sametime does not attempt to alter it.

**About this task**

In some cases, it may be necessary to alter the default configuration of the Domino SSO feature following the Sametime server installation. For instructions, see “Altering the Domino Web SSO configuration following the Sametime server installation” on page 861.

**Configuring the Domino Server for Web SSO**

Complete the steps in this section if your Domino server is not configured for Web SSO, and you want to use the Web SSO document that Sametime creates to configure it.

**Procedure**

1. From the Domino Administrator or a Lotus Notes client, click **File > Database > Open**. Browse to the Domino server and type names.nsf in the Filename field. Click **Open**.

   **Note:** If you attempt to open this document from Domino Administrator Configurations tab, Web - web Configurations view, the Web SSO Configuration document will not display.

2. Expand the list of Web SSO Configurations.

3. Double click the "Web SSO Configuration for LtpaToken" document to open it in edit mode.

4. Update these fields as necessary:
   - Configuration name -- Enter LtpaToken.
   - DNS Domain -- make sure this is the fully qualified domain suffix of the Sametime server. For example, if the server's fully qualified name is server.domain.com, the .domain.com should be entered in this field. Ensure that the leading period (.) is present in front of the domain suffix.
   - Organization -- Leave this field blank.
   - Participating servers -- Add the Sametime server and other servers that belong to the SSO realm to the list.

5. After entering the information, select **Keys** and do one of the following:
   - Create a Domino SSO Key
   - If WebSphere is participating in SSO, the Domino SSO key created by the install program should be replaced by the WebSphere LTPA key to allow both Domino and WebSphere to have an identical key for token validation and generation. Do this by importing the LTPA key from WebSphere to Domino. For more information, see Setting up single sign-on for Sametime browser clients.

   **Note:** When adding servers to the Participating servers field, click the arrow and choose the name from an Address Book when possible. If this is not
possible, make sure that you use the full hierarchical name when you add a server (for example, Server1/Example where CN=Server/O=Org).

Configuring a Sametime Community Server

This section describes how to configure an IBM Sametime Community Server.

Related tasks

“Working with Sametime servers that are enabled for SSL” on page 787
Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

“Setting up single sign-on (SSO) for Sametime clients” on page 855
Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

“Configuring security for the Sametime Community Server” on page 858
The IBM Sametime server uses the Internet and intranet security features of the Domino server on which it is installed to authenticate web browser users who access Domino databases on the server.

Do I need to restart the Sametime server?

Use this table to determine which changes in server settings require you to restart the server.

<table>
<thead>
<tr>
<th>Main Function in Admin</th>
<th>Sub-Function</th>
<th>Details - Setting</th>
<th>Switches</th>
<th>Required restart</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Settings</td>
<td>General</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable logging to a Domino database. (STLog.nsf)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remove history after (days).</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable logging to a text file. Path to log text file</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Sametime Statistics</td>
<td></td>
<td></td>
<td>Write statistics to the log every 60 minutes. This includes Community Services logging of people and chats, and Meeting Services logging of meeting, duration, and participants</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Community Server Events to Log</td>
<td></td>
<td></td>
<td>Successful logins Failed logins Community server events and activities</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Meeting Server Events to Log</td>
<td></td>
<td></td>
<td>Failed meeting authentications Meeting Client Connections Connections to other meeting servers in this community Meeting Events Meeting server events and activities</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Logging</td>
<td>Settings</td>
<td>Capacity Warnings - Sharing in Instant Meetings</td>
<td>Number of active screen sharing/whiteboard meetings exceeds</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number of people in all screen sharing/whiteboard meetings exceeds</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number of people in one active screen sharing/whiteboard meeting exceeds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td>Domino/ LDAP</td>
<td>User Registration</td>
<td>Allow people to register themselves in the Domino Directory</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin Config.</td>
<td>Sub - Function Connectivity</td>
<td>Details - Setting HTTP Services</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>Config.</td>
<td>Connectivity</td>
<td>Community services network</td>
<td>Address for server connections</td>
<td>Yes</td>
<td>It belongs to Domino feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for client connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 1533)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for HTTPS tunneled client connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for HTTP tunneled client connections</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8082 or 80)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Meeting Services network</td>
<td></td>
<td>Address for server connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for client connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 1503)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for HTTPS tunneled client connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8081)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>---------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Address for HTTP tunneled client connections</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8081 or 80)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Event server port (default 9092)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Broadcast Services</td>
<td></td>
<td></td>
<td>Token server port (default 9094)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interactive Audio/Video Network</td>
<td></td>
<td></td>
<td>TCP tunneling address for client connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8084)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multimedia Processor (MMP) UDP port numbers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>start at :49252</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia Processor (MMP) UDP port numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>end at :65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multimedia control address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 9093)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reverse Proxy Support</td>
<td>Enable Reverse Proxy Discovery on the client</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Server Alias (this is what the Reverse Proxy is using to forward HTTP(S) messages to this server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connectivity</td>
<td>Connecting Meeting Servers</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connecting Meeting Servers</td>
<td>To allow meeting participants to attend a meeting on more than one server, you must create a connection record from each source server to each destination server. Once you do that, the destination servers are automatically included in a meeting when users schedule a meeting and click the appropriate check boxes on the Location tab.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Community services</td>
<td></td>
<td>General</td>
<td>Number of entries on each page in dialog boxes that show names in the Directory: (100)</td>
<td>Yes</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>How often to poll for new names added to the Sametime Community Directory (minutes): (60)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>How often to poll for new servers added to the Sametime Community (minutes): (60)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum user and server connections to the Community server: (20000)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General</td>
<td>Allow users to authenticate using either LTPA or Sametime Token (stauths.nsf and stauthl.nsf). The server uses LTPA if this item is unchecked. (The item is unchecked by default.)</td>
<td>Yes</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Display the &quot;Launch Sametime Connect for the desktop&quot; link on the Sametime Home page.</td>
<td>No</td>
<td>.</td>
</tr>
</tbody>
</table>

900 Sametime Advanced: Installation and Administration Guide
<table>
<thead>
<tr>
<th>Main Function in Admin</th>
<th>Sub - Function</th>
<th>Details - Setting</th>
<th>Switches</th>
<th>Required restart</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow users to transfer files to each other.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum file size allowed (KB):1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow users to send announcements (unencrypted one-way messages).</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow Connect users to save their user name, password, and proxy information (automatic login).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Display the &quot;Launch Sametime Connect for browsers&quot; link on the Sametime Home page (stcenter.nsf).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Display Name</td>
<td></td>
<td>Settings for Anonymous Access to Meetings or other Virtual Places</td>
<td>Anonymous users can participate in meetings or enter virtual places. Their name appears as user1, user2, and so on. Users of Sametime applications (databases such as stconf.nsf or websites) can specify a display name so that they do not appear online as &quot;anonymous.&quot; This does not authenticate users. (Databases must also allow anonymous access in the ACL.)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Community Services</td>
<td>Directory</td>
<td>Searching and Browsing</td>
<td>Users cannot browse or search the Directory.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Users can type names (resolve users and groups) to add them to an awareness list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Users can browse the directory (see a list of names) or type names (resolve users and groups).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Users can browse the directory to see group content and names, or type names (resolve user and groups).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meeting services</td>
<td>General</td>
<td></td>
<td>Automatically extend meetings beyond scheduled end time when there are still people in the meeting.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>After a meeting, add the names of participants to the meeting document</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>When people start or schedule a meeting</td>
<td>Allow people to choose the Screen Sharing tool in meetings:</td>
<td>Participants can share their screen, view a shared screen, or control a shared screen if the moderator permits.</td>
<td>No</td>
<td>Force Screen Sharing to use 8-bit color.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Allow people to view the shared screen only.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allow people to share their screen if the moderator permits or view a shared screen.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Allow people to enable the “Send Web Page” tool in meetings</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Allow people to save whiteboard annotations as attachments to the meeting.</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow people to choose the Polling tool in meetings</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow people to record meetings for later playback (scheduled meetings only).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Save recorded meetings in the following location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Stop recording when this much disk space is left (MBytes) (an error is written to the log): 300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When People Start an Instant Meeting or Schedule a Meeting</td>
<td></td>
<td></td>
<td>Allow people to schedule Recorded Meeting Broadcast meetings</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td>Encrypt all SameTime meetings</td>
<td>No</td>
<td>It does work in Meeting center, but doesn’t affect the instant meeting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Require all scheduled meetings to have a password</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>---------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Meeting Services</td>
<td></td>
<td>Connection Speed Settings</td>
<td>Meetings with modem users</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Meetings with LAN/WAN users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio/video</td>
<td></td>
<td>When People Schedule a Meeting</td>
<td>Allow people to choose Sametime IP Audio (in addition to or instead of telephone) in meetings.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow people to choose Sametime IP Video in meetings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switching</td>
<td>Time to wait for silence before switching to next speaker (100 - 500 ms): 250</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Time to wait before switching to next video (500 - 4000 ms): 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recorded Meeting Broadcast Meetings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection Speed Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Switches</td>
<td>Required restart</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>----------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Usage Limits and Denied Entry for Instant Meetings</td>
<td></td>
<td></td>
<td>Set a maximum number of interactive audio connections for all instant meetings on this server. :100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Set a maximum number of interactive video connections for all instant meetings on this server. Each video connection requires an audio connection. Ensure that there are at least as many audio connections allowed as video.:100</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Set a maximum number of interactive audio connections for all instant meetings on this server.:100</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Using reverse proxy or portal servers with the Sametime server

The manipulation of IBM Sametime data by a reverse proxy server imposes specific requirements and limitations, discussed in this section.

An IBM Sametime server can be deployed behind a reverse proxy server or a portal server. This section discusses issues related to using reverse HTTP proxy servers with a Sametime server. The issues discussed in this section also apply to deploying a Sametime server behind a portal server.

When a Sametime server is deployed on an internal network behind a reverse proxy server, the reverse proxy server operates as an intermediary between the Sametime server and the Sametime clients. All Sametime data flowing between the Sametime server and its clients passes through the reverse proxy server.

To accomplish its security objectives, a reverse proxy server manipulates the data that passes through it. The table below shows the client-side proxy types through which clients can connect to the Sametime server.

<table>
<thead>
<tr>
<th>Sametime client</th>
<th>SOCKS 4 proxy</th>
<th>SOCKS 5 proxy</th>
<th>HTTP proxy</th>
<th>HTTPS proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Connect</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
</tr>
</tbody>
</table>
This section includes topics related to the use of reverse HTTP proxy servers with the Sametime server.

Note: If you are configuring the Sametime server to operate behind a Tivoli Access Manager WebSEAL reverse proxy server, refer to the Sametime Server Release Notes for additional configuration information.

What is a reverse proxy server?
A reverse proxy server is a security device that is usually deployed in a network DMZ to protect HTTP servers (or IBM Sametime servers) on a corporate intranet by performing security functions that protect the internal servers from attacks by users on the Internet.

The reverse proxy server protects internal HTTP servers by providing a single point of access to the internal network. Providing a single point of access to all HTTP servers on an internal network offers these specific security advantages and network access characteristics:

- The administrator can use the authentication and access control features of the reverse proxy server to control who can access the internal servers and control which servers each individual user can access. When a reverse proxy is deployed, the authentication process and access rights to multiple internal servers can be controlled from a single machine, which simplifies the security configuration.

- All traffic to your intranet servers appears to be destined for a single network address (the address of the reverse proxy server).

When a reverse proxy server is deployed, only URLs that are associated with the reverse proxy server are made public to web browser users. Users from the Internet use these URLs to access the reverse proxy server. The reverse proxy server handles these requests from Internet users and redirects these requests to the appropriate internal HTTP server.

<table>
<thead>
<tr>
<th>Sametime client</th>
<th>SOCKS 4 proxy</th>
<th>SOCKS 5 proxy</th>
<th>HTTP proxy</th>
<th>HTTPS proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Mobile</td>
<td>not supported</td>
<td>not supported</td>
<td>supported</td>
<td>supported</td>
</tr>
<tr>
<td>Sametime Meeting Room</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
<td>not supported</td>
</tr>
<tr>
<td>screen-sharing/whiteboard components</td>
<td>supported</td>
<td>not supported</td>
<td>supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Sametime Meeting Room</td>
<td>supported</td>
<td>not supported</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>participant list/chat components</td>
<td>supported</td>
<td>not supported</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Sametime Meeting Room</td>
<td>supported</td>
<td>not supported</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>interactive audio/video components</td>
<td>supported</td>
<td>not supported</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>Sametime Recorded Meeting client</td>
<td>supported</td>
<td>not supported</td>
<td>supported</td>
<td>not supported</td>
</tr>
</tbody>
</table>
The administrator performs URL mapping configurations on the reverse proxy server that make this redirection possible. When configuring the reverse proxy server, the administrator maps the URLs that are used to access the reverse proxy server to the real URLs of the internal HTTP servers. When an Internet user sends a URL to the reverse proxy server, the reverse proxy server examines the URL and uses these mapping configurations (or rules) to rewrite the URL.

The reverse proxy server rewrites the URL by replacing the server address provided by the Internet user (a reverse proxy address) with the real address of the internal server. The HTTP request is then sent on the internal network from the reverse proxy server to the internal server.

- All traffic sent to Internet users from your internal servers appears to originate from a single network address.

When an internal HTTP server (or Sametime server) responds to a request from an Internet user, the internal server sends the response to the reverse proxy server and the reverse proxy server sends the response to the Internet user. The response sent on the Internet to the Internet user contains the address of the reverse proxy server, not the address of the internal HTTP server.

Starting with Release 7.5, Sametime is designed to enable Sametime clients to establish and maintain connectivity with a Sametime server when these clients connect to the Sametime server through a reverse proxy server.

The security functionality of reverse proxy servers described above imposes specific requirements and limitations on the use of reverse proxy servers with Sametime. See any of the following topics for specific information about using reverse proxy servers with a Sametime server.

- Requirements and limitations associated with using a reverse proxy server with the Sametime server
- Configuring mapping rules on a reverse proxy server to support Sametime
- Configuring a Sametime server to operate with a reverse proxy server
- Sametime client connectivity and reverse proxy servers

**Requirements and limitations of Sametime reverse proxy support**

Using a reverse proxy server with IBM Sametime is subject to some limitations as described in this topic.

The requirements and limitations associated with using a reverse proxy server with Sametime include:

- Reverse proxy server requirements
- Sametime client limitations and requirements
- Sametime server limitations
- Secure Sockets Layer (SSL) issues and requirements
- Client certificate authentication issues
- IBM Sametime Enterprise Meeting Server (WCMS) restrictions

Each of these topics is discussed under a separate heading below.

**Reverse proxy server requirements**

This section lists the requirements and issues that are specific to the reverse proxy server.
- **URL specification requirement (affinity-id requirement)** - Only reverse proxy servers that use the following URL specification to access protected internal servers can be used with Sametime:

  \[\text{Http[s]}://\text{hostname}:\text{port}/\text{affinity-id/}\]

  The "affinity-id" is an administrator-defined alias for an internal Sametime server. This affinity-id must be present in the URLs sent from web browsers to the reverse proxy server to enable web browser users to access the Sametime server through the reverse proxy. For detailed information on this mandatory requirement of the reverse proxy server, see Configuring mapping rules on a reverse proxy server.

- **Multiple reverse proxy servers must use the same DNS name and mapping configurations** - If you have deployed multiple reverse proxy servers in your network environment, and you expect users to access your Sametime server(s) through multiple reverse proxy servers, each of the reverse proxy servers must have the same DNS name and the same mapping configurations as noted below:

  - **DNS name** - All reverse proxy servers must use the same DNS name. For example, if one reverse proxy server is named reverseproxy.ibm.com all other reverse proxy servers must be named reverseproxy.ibm.com. If the reverse proxy servers have different DNS names, the Sametime clients will be unable to maintain communications with a Sametime server deployed behind the reverse proxy servers.

  **Note:** If a network environment includes multiple reverse proxy servers that have the same DNS names, a connection dispatching device (such as an IBM WebSphere EdgeServer) is usually used to distribute connections from web browsers to the multiple reverse proxy servers. These devices are frequently used to load balance connections to multiple machines.

  - **Mapping configurations** - Each reverse proxy server must use identical mapping rules and configurations to govern the translation of URLs sent by web browsers to the reverse proxy server for the purpose of accessing an internal Sametime server. If the translation of these URLs to the URLs of the internal Sametime servers does not occur in exactly the same way on each of the reverse proxy servers, the Sametime clients will be unable to maintain communications with a Sametime server deployed behind the reverse proxy server.

  **Note:** Each Sametime server must be represented by the same "affinity-id" in the mapping rules on each of the reverse proxy servers.

  For more information about the affinity-id and mapping rules, see Configuring mapping rules on a reverse proxy server.

- **The reverse proxy server must use cookies for authentication** - When an user uses a web browser to access and authenticate with the reverse proxy server, the reverse proxy server must send an authentication cookie to the web browser. All subsequent HTTP requests from a Sametime client will then pick up this cookie and use it for automatic authentication with the reverse proxy server. Reverse proxy servers that rewrite URLs for authentication purposes are not supported. Some reverse proxy servers append authentication and session information to the end of URLs embedded in HTML that passes through the proxy back to the client. The client will include this appended data on subsequent requests to the reverse proxy server. When the reverse proxy server receives these subsequent requests from the client, the reverse proxy server strips the authentication data and rewrites the URL to accomplish the internal routing of requests. A Sametime server cannot operate behind a reverse proxy server that handles authentication data in this way.
A lengthy timeout value should be specified for the authentication cookies -
The administrator should specify a lengthy timeout value for authentication
cookies generated by the reverse proxy server.

If the authentication cookie expires when the user is attending a meeting, the
user is disconnected from the meeting. To re-enter the meeting, the user must go
through the inconvenient process of reconnecting to the reverse proxy,
reauthenticating with the reverse proxy, and waiting for the Java applets to be
reloaded to the web browser.

Setting a lengthy timeout value for authentication cookies can prevent
unexpected user disconnections due to an authentication cookie expiration.
Generally, the authentication cookie should be valid for the entire length of the
longest meetings that are routinely conducted on the Sametime server deployed
behind the reverse proxy server.

**Sametime client/Web browser limitations and JVM requirements**

The following Sametime clients can communicate with Sametime servers through a
reverse proxy server:
- Sametime Meeting Room client
- Sametime Recorded Meeting client
- Sametime Connect for browsers (the Java version of Sametime Connect)
- Sametime Connect for the desktop (the Microsoft Windows version of Sametime
  Connect)
- Sametime Links applications built with Sametime developer toolkits

On UNIX and IBM AIX servers, the Meeting start-up log contains the Sametime
server name when the Sametime server is configured behind a proxy server.

The Sametime Meeting Room client and the Sametime Recorded Meeting client can communicate with a Sametime server through a reverse proxy server when
running with the following Web browsers and Java Virtual Machines (JVMs):
- A Microsoft Internet Explorer 6 browser that operates with the Microsoft native
  VM or the Sun Microsystems JVM 1.4.2 (and associated Java Plug-in).
- A Netscape 7 browser that operates with the Sun Microsystems JVM 1.4.2 (and
  associated Java Plug-in).

The Sametime Connect for browsers client and Sametime Links applications can communicate with a Sametime server through a reverse proxy server when
running in an Internet Explorer 6 or Netscape 7 browser that operates with the Sun
JVM 1.4.2. These clients may not function appropriately with other JVMs, including
the native Microsoft VM provided for Internet Explorer.

**Sametime server limitations**

The following limitations apply to Sametime server features when the Sametime
server is deployed behind a reverse proxy server.

- **Audio/video is not available** - Audio/video streams cannot be transmitted to
  Sametime clients that access the Sametime server through a reverse proxy server.

- **Access to the Sametime Administration Tool is not available** - A user that
  connects to the Sametime server through a reverse proxy server cannot access
  the Sametime Administration Tool. The user can open a web browser that is
  installed on the Sametime server to access the Sametime Administration Tool.
  The user can also connect to the Sametime server from an internal network
location that does not route HTTP traffic through the reverse proxy server to access the Sametime Administration Tool.

**Secure Sockets Layer (SSL) issues and requirements**

Note the following about SSL and Sametime in a reverse proxy environment:

- Secure Sockets Layer (SSL) can be used to encrypt data transmitted between the Sametime clients and the reverse proxy server.
- SSL cannot be used to encrypt data transmitted between the Sametime servers and the reverse proxy server.

If SSL is used to encrypt data transmitted between web browsers and the reverse proxy server, the administrator must perform the mapping configurations on the Sametime server necessary to map the HTTPS data received from the web browser to the HTTP required by the Sametime server.

The reverse proxy must also be configured to translate the HTTP data received from the Sametime server to the HTTPS data required by the client.

When a reverse proxy server is configured to support SSL, the reverse proxy server sends an SSL server certificate to the web browser during the SSL connection handshake. The Java 1.4.2 Plug-in used by the web browser must have access to a Signer certificate that is signed by the same Certificate Authority (CA) as the server certificate that is sent by the reverse proxy.

By default, the Java Plug-in has access to several different Signer certificates that can be used for this purpose. To view the Signer certificates that are available to the Java Plug-in 1.4.2, use the Java Plug-in Control Panel as described in “Viewing the Signer certificates.”

**Client certificate authentication issues**

If the reverse proxy server is configured to require client certificate authentication, the client certificate for an individual user must be imported into the Java Plug-in 1.4.2 Control Panel on that user’s machine as described in “Importing the client certificate” on page 914.

**Enterprise Meeting Server restrictions**

The IBM Sametime Enterprise Meeting Server that operates with Sametime servers cannot be deployed behind a reverse proxy server.

**Viewing the Signer certificates:**

The Java Plug-in has access to several different Signer certificates that can be used for reverse proxy support.

**About this task**

To view the Signer certificates that are available to the Java Plug-in 1.4.2, use the Java Plug-in Control Panel:

**Procedure**

1. From the Windows desktop, open the Control Panel by clicking Start > Settings > Control Panel.
2. Double-click on the Java Plug-in 1.4.2 icon to open the Java Plug-in Control Panel.
3. Click Certificates.
4. Click Signer CA.

Results
The server certificate sent by the reverse proxy server to the client web browser must be signed by one of the CAs that appears in the signer CA list for the SSL connection handshake to succeed.

Importing the client certificate:
If the reverse proxy server is configured to require client certificate authentication, the client certificate for an individual user must be imported into the Java Plug-in 1.4.2 Control Panel on that user's machine.

About this task
You can use the Certificates tab of the Java Plug-in Control Panel to import the client certificate into the Java Plug-in key store:

Procedure
1. From the Windows desktop, open the Control Panel by clicking Start > Settings > Control Panel.
2. Double-click on the Java Plug-in 1.4.2 icon to open the Java Plug-in Control Panel.
3. Click Certificates.
4. In the Certificates column, click Secure Site.
5. Click Import to import the client certificate.

Configuring mapping rules on a reverse proxy server to support Sametime
When an IBM Sametime server is deployed behind a reverse proxy server, the Sametime administrator must configure mapping rules on the reverse proxy server.

The mapping rules enable the reverse proxy server to translate (or rewrite) a URL associated with the reverse proxy server to the URL of an internal Sametime server. This section discusses how mapping rules are configured on a reverse proxy server to accomplish the translation (or rewriting) of URLs when the reverse proxy operates with Sametime. This section includes the following topics:

Affinity-id (server alias) requirement of the reverse proxy server:
Only reverse proxy servers that support the use of an affinity-id (or server alias) in the URLs that are associated with internal servers can be used with IBM Sametime.

Specifically, the reverse proxy server must support the following URL specification to access protected internal servers:
Http[s]://hostname:port/affinity-id/

where hostname represents the DNS name of the reverse proxy server and the affinity-id is an alias for an internal server that is protected by the reverse proxy server. A specific example of this URL format is:
Http[s]://reverseproxy.ibm.com/st01/stcenter.nsf

where the text string "st01" is the affinity-id. The affinity-id is an alias for a specific Sametime server (such as sametime.ibm.com) that is protected by the reverse proxy server. The affinity-id is used by the reverse proxy server to direct incoming requests to the specific internal Sametime server.

For example, if the incoming URL from the Web browser is:
Http[s]://reverseproxy.ibm.com/st01/stcenter.nsf

and the mapping rules on the reverse proxy server map the "st01" affinity-id to the Sametime server named "sametime.ibm.com," the affinity-id ensures the reverse proxy server rewrites the incoming URL to:
Http[s]://sametime.ibm.com/stcenter.nsf

Essentially, the affinity-id is an administrator-defined alias for an internal Sametime server. The affinity-id is defined in the mapping rules of the reverse proxy server. If you have multiple Sametime servers deployed behind a reverse proxy server, each Sametime server must have an individual affinity-id as indicated below:

<table>
<thead>
<tr>
<th>Mapping rule for client-provided URL:</th>
<th>Routed to internal server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>/st01/*</td>
<td><a href="http://sametime1.ibm.com/">http://sametime1.ibm.com/</a>*</td>
</tr>
<tr>
<td>/st02/*</td>
<td><a href="http://sametime2.ibm.com/">http://sametime2.ibm.com/</a>*</td>
</tr>
</tbody>
</table>

It is mandatory that any reverse proxy server that operates with a Sametime server support the affinity-id (or server alias) in URLs.

For additional information about configuring mapping rules on reverse proxy server, see Example of URL mapping configurations on the reverse proxy server.

**Important:** The Sametime Administration Tool on a Sametime server contains a "Server Alias" setting. This Server Alias setting must specify the same affinity-id that is used to represent the Sametime server in the mapping rules on the reverse proxy server. For more information, see Configuring a Sametime server to operate with a reverse proxy server.

**Example of URL mapping configurations on the reverse proxy server:**

Here are some examples of how an administrator might configure URL mapping configurations for a reverse proxy server deployed in front of an IBM Sametime server.

When a user connects to a Sametime server through a reverse proxy server, the reverse proxy server must be configured to support the following actions that enable Sametime users to attend meetings and participate in chat sessions:

- The user must be able to click on links in the Sametime server home page and navigate to the various HTML pages of the UI. This capability requires the reverse proxy server to rewrite the URLs of the HTML pages that comprise the Sametime UI.
- The Sametime Java applet clients that load in a user’s web browser must be able to connect to the services on the Sametime server. Since these connections must occur through the reverse proxy server, the reverse proxy server must also be able to rewrite the URLs required to establish these connections to the services on the Sametime server.
The following sections provide examples of the mapping configurations required to accomplish the two tasks above.

Reverse proxy mapping configurations that enable a web browser user to navigate the Sametime user interface

The example below illustrates how an administrator can configure the reverse proxy server to enable users to navigate the HTML pages of the Sametime user interface. This example assumes the following:
- The Sametime server name is "sametime.ibm.com."
- The URL required to access the reverse proxy server is "reverseproxy.ibm.com."
- The affinity-id chosen by the administrator for the Sametime server is "st01."

Listed below are two entities of the Sametime server user interface and the URLs required to access these entities on a Sametime server with the server name "sametime.ibm.com."
- **Active Meeting page** - The Sametime server URL for the Active Meeting page is http://sametime.ibm.com/stconf.nsf/vwWebActiveMeetings?OpenView.

Example 1 - Translating the URL of the server home page

To access the Sametime server home page through a reverse proxy server, the web browser would send the following URL to the reverse proxy server:
http[s]://reverseproxy.ibm.com/st01/stcenter.nsf

The reverse proxy server must contain a mapping rule that translates this URL into the following URL required to access the Sametime server home page:
http[s]://sametime.ibm.com/stcenter.nsf

Example 2 - Translating the URL of the Active Meeting page

If the user selects the Attend a Meeting link in the Sametime user interface to view the list of active meetings, the web browser would send the following URL to the reverse proxy server:
http[s]://reverseproxy.ibm.com/st01/stconf.nsf/vwWebActiveMeetings?OpenView

The reverse proxy server must contain a mapping rule that translates this URL into the following URL required to access the Sametime server Active Meetings page:
http[s]://sametime.ibm.com/stconf.nsf/vwWebActiveMeetings?OpenView

A single mapping rule can be used to translate all URLs associated with the Sametime server user interface

Through the use of wildcards, the administrator can create a single mapping rule on the reverse proxy server to translate all URLs associated with the Sametime server interface. Following the examples above, the administrator can create a mapping rule that translates the following URL from the web browser:
http[s]://reverseproxy.ibm.com/st01/*

To this Sametime server URL:
http[s]://sametime.ibm.com/*
A single mapping rule that accomplishes this type of URL translation should enable users to access all entities of the Sametime user interface through a reverse proxy server.

**Note:** It is not mandatory to configure the mapping rules as described above. The actual configuration of the mapping rules on the reverse proxy server is at the discretion of the administrator. When configuring the mapping rules note that the URL for any entity of the Sametime server user interface will begin with the Sametime server name (sametime.ibm.com in this example).

**Reverse proxy mapping configurations that enable Sametime Java applet connectivity through the reverse proxy server**

The following example URL mappings enable the Sametime Java applet clients running in a user's Web browser to connect to the Community Services, Meeting Services, and Recorded Meeting Broadcast Services on the Sametime server through the reverse proxy server:

**Example 1 - Mapping configuration for Community Services connectivity**

This example illustrates the mapping configurations that enable a Java applet client to connect to the Community Services:

If the incoming URLs from the Java applet are:

```
Http[s]://proxy.ibm.com/st01/communityCBR
```

The mapping rules on the reverse proxy must translate these URLs to:

```
http://sametime.ibm.com:8082/communityCBR
```

**Note:** The mapping configuration for the Community Services connectivity should contain two case-sensitive mapping rules as indicated above. Some pieces of the Java code contain the lowercase "c" in "communityCBR" and some pieces of the Java code use the uppercase "C" in "CommunityCBR." This difference may prevent connections if the proxy is case-sensitive.

**Example 2 - Mapping configuration for Meeting Services connectivity**

This example illustrates the mapping configurations that enable a Java applet client to connect to the Meeting Services:

If the incoming URL from the Java applet is:

```
Http[s]://proxy.ibm.com/st01/MeetingCBR
```

The mapping rule on the reverse proxy must translate this URL to:

```
Http://sametime.ibm.com:8081/MeetingCBR
```

**Example 3 - Mapping configuration for Recorded Meeting Broadcast Services connectivity**

This example illustrates the mapping configurations that enable a Java applet client to connect to the Recorded Meeting Broadcast Services:

If the incoming URL from the Java applet is:

```
Http[s]://proxy.ibm.com/st01/BroadcastCBR
```
The mapping rule on the reverse proxy must translate this URL to:
Http://sametime.ibm.com:554/BroadcastCBR

Information about the Java applet connectivity mapping rule examples

During a Sametime server installation, the administrator has the option of allowing or not allowing HTTP tunneling on port 80.

If the administrator does not allow HTTP tunneling on port 80 during the Sametime server installation, it is necessary to configure separate mapping rules for each of the three Sametime services (Community Services, Meeting Services, and Recorded Meeting Broadcast Services).

**Note:** Four mapping rules are required: two for the Community Services, one for the Meeting Services, and one for the Recorded Meeting Broadcast Services as shown in the three examples above.

When the administrator does not allow HTTP tunneling on port 80, each of the Sametime services listens for HTTP connections on a different port:

- The Community Services listen for HTTP connections on port 8082. Port 8082 is reflected in the mapping rule for Community Services connections above. You can view or change this port setting from the Community Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

- The Meeting Services listen for HTTP connections on port 8081. Port 8081 is reflected in the mapping rule for Meeting Services connections above. You can view or change this port setting from the Meeting Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

- The Recorded Meeting Broadcast Services listen for HTTP connections on port 554. Port 554 is reflected in the mapping rule for Recorded Meeting Broadcast Services connections above. You can view or change this port setting from the Recorded Meeting Broadcast Services Network - Address for HTTP-tunneled client connections option in the Networks and Ports tab of the Sametime Administration Tool.

Because each of these Sametime services listens for a connection on a separate port, separate mapping rules must be established for each of the services. The mapping rule must specify the port on which each of the services is listening for connections.

**Note:** If you change the HTTP-tunneling port number for a specific service in the Sametime Administration Tool, the mapping rules you configure on the reverse proxy server must reflect the new port number.

If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the Sametime clients connect to all of the services on a single port. With this configuration, the single mapping rule that enables users to navigate the Sametime server user interface will also enable the Sametime clients to make connections to the Sametime services.

When HTTP tunneling on port 80 is allowed, the Community Services multiplexer on the Sametime server listens for HTTP connections on behalf of the HTTP Services, Community Services, Meeting Services, and Recorded Meeting Broadcast Services.
Services on the Sametime server. The Community Services multiplexer listens for connections to all of these services on a single port (port 80).

**Note:** When operating in this mode, the Community Services multiplexer on the Sametime server can distinguish between HTTP requests destined for the HTTP Services, Community Services, Meeting Services, and Recorded Meeting Broadcast Services and establish intraserver connections to each of the services. For example, if the Community Services multiplexer receives an HTTP request for the Meeting Services on port 80, the Community Services handles the request and creates an intraserver connection to the Meeting Services. The Community Services multiplexer then forwards the request to the Meeting Services. The ability of the Community Services multiplexer to handle requests for multiple services in this way is sometimes referred to as "single port mode."

When the administrator allows HTTP tunneling on port 80 (that is, when the Sametime server is operating in single port mode), the mapping rules for Java applet connectivity are much simpler. Since all connections from the Sametime Java applet clients occur on the same port, it is not necessary to specify individual ports for each service in the mapping rules.

In this scenario, the administrator would only need to ensure that this incoming URL from the Sametime Java applets:

```
Http[s]://proxy.ibm.com/st01/*
```

Is translated to this URL by the mapping rules on the reverse proxy server:

```
Http://sametime.ibm.com/*
```

Note that server performance is not as efficient when the Sametime server is configured to support HTTP tunneling on port 80 because of the connectivity burden placed on the Community Services multiplexer.

**Configuring a Sametime server to operate with a reverse proxy server**

Use the IBM Sametime Administration Tool (hosted on the Sametime server) to configure a Sametime server to operate with a reverse proxy server.

**About this task**

There are two settings the administrator must configure in the Configuration-Connectivity-Networks and Ports tab of the Sametime Administration Tool to enable a Sametime server to operate with a reverse proxy server. These settings include:

- **Enable Reverse Proxy Discovery on the client** - Selecting this setting allows the administrator to enable or disable the reverse proxy support. This setting enables the logic in the Sametime clients that enables them to connect to a Sametime server through the reverse proxy server. This setting is disabled by default.

**Note:** Enabling this setting does **not** require that all users on your corporate intranet access the Sametime server through the reverse proxy server. Users on your corporate intranet that are not required to route connections through the reverse proxy servers can still establish connections with the Sametime server using the standard Sametime client connection processes. For more information, see Connecting to a Sametime server without going through the reverse proxy server.
**Server Alias** - The Server Alias setting must specify the affinity-id that the administrator uses to represent this Sametime server in the mapping rules on the reverse proxy server.

**Note:** The term "Server Alias" is synonymous with affinity-id.

For example, if the administrator uses the text string "st01" as the affinity-id that represents the Sametime server in the mapping rules on the reverse proxy server, the administrator must also enter "st01" as the value for the Server Alias setting in the Sametime Administration Tool.

Following a Sametime server installation, the Server Alias setting defaults to the Sametime server name that is extracted from the fully-qualified DNS name of the Sametime server. For example, if the fully-qualified DNS name of the Sametime server is "sametime.ibm.com," the default value for the Server Alias is "sametime."

**Note:** An administrator may want to change the default Server Alias setting to avoid using the real Sametime server name as the affinity-id in the mapping rules on the reverse proxy server. If the real Sametime server name is used as the affinity-id on the reverse proxy server, the real server name will appear in URLs transmitted on the Internet.

For more information about the affinity-id, see Configuring mapping rules on a reverse proxy server to support Sametime.

To enable reverse proxy support on a Sametime server:

**Procedure**
1. From the Sametime server home page, click **Administer the Server** to open the Sametime Administration Tool.
2. Click **Configuration**.
3. Click **Connectivity**.
4. If necessary, click **Networks and Ports**.
5. At the bottom of the **Networks and Ports** tab, click **Enable Reverse Proxy Discovery on the client**.
6. In the **Server Alias** text box, type the text string that is used as the affinity-id that represents this Sametime server in the mapping configurations on the reverse proxy server (for example, type **st01**).
7. Click **Update**.
8. Restart the Sametime server for the changes to take effect.

**Configuring Sametime Community Server to work behind WebSEAL reverse proxy**

If you are deploying the IBM Sametime Community Server behind a Tivoli WebSEAL reverse proxy server, there are some specific procedures and configurations you must employ to ensure the Lotus Sametime Community Server can operate behind the WebSEAL reverse proxy server.

**Procedure**
1. Follow the instructions below to enable HTTP tunneling on port 80 using the Sametime Administration Tool.
   a. From the Sametime home page, select **Administer the server** to open the Sametime Administration Tool.
   b. Select **Configuration > Connectivity > Networks and Ports**.
c. Ensure that the Community Services Network > Enable the Meeting Room client to try HTTP tunneling to the Community Server after trying other options setting is enabled.

d. In the Community Services Network > Address for HTTP tunneled client connections settings:
   - If your Sametime Community Server operates on a Microsoft Windows server, you can leave the Host name field blank.
   - In the HTTP tunneling Port number field, delete port number 8082 and enter port number 80.

e. Click Update and then restart the server for the change to take effect.

2. You must open the stlinks.js file on the Sametime Community Server and modify the following two lines to point to your WebSEAL reverse proxy server and WebSEAL junction. The WebSEAL junction is st in the example:

   ```javascript
   varII_RProxyName="https://ampc0.support.tivlab.austin.ibm.com"
   varII_AffinityID="st"
   
   Note: The WebSEAL reverse proxy server must be listening on the default ports of 80 and 443 for the changes above to work.
   
3. Enable reverse proxy support and specify the WebSEAL junction in the Sametime Administration Tool on the Sametime Community Server.
   a. Open the Sametime Administration Tool.
   b. Click Configuration > Connectivity.
   c. In the "Reverse Proxy Support" section, click Enable Reverse Proxy Discovery on the client to enable the reverse proxy support.
   d. Enter the WebSEAL junction name in the Server Alias field. In this example, st is the WebSEAL junction name.

4. Create the Tivoli Access Manager WebSEAL junction. Issue the command as one line:

   ```bash
   
   You cannot use the -w parameter for this setup. Some requests generated by Sametime are not allowed through the junction if the -w exists. You must also ensure that the LTPA key used in the junction is the same LTPA key that the Sametime Community Server uses in its Web SSO Configuration document.

What to do next

After performing this configuration, you should be able to log in to https://webseal/stjunction and be prompted by WebSEAL for authentication. Once authenticated, SSO between WebSEAL and the Sametime Community Server should work and all requests for Sametime will route through WebSEAL.

Using multiple non-clustered Sametime Community Servers

Install multiple IBM Sametime Community Servers to support a large or geographically distributed user community and synchronize the servers to operate as a single Sametime community.

Some reasons to install multiple Sametime servers include:
   - Spreading the load of a large user population among multiple servers.
   - Reducing network usage and improve server performance when you have significant user populations in remote or distributed locations.
This section discusses the issues associated with deploying multiple Sametime servers, including:

**Integrating a Sametime server into an existing Sametime community**
This topic provides an overview of the tasks involved in integrating a new IBM Sametime server into an existing Sametime community.

These are the basic processes and issues involved with integrating a new Sametime server into an existing Sametime community.

**Configuring client connectivity to the multiplexer:**

After you have configured the Community Server multiplexer, give users the DNS name of the multiplexer and instruct them to set up their Sametime Connect preferences to connect to the multiplexer instead of the Sametime Community Server.

**About this task**

Each user must update the Sametime Connect client with the DNS name of the multiplexer. If you have deployed multiple Community Server multiplexers, distribute users evenly among the machines. For example, with two multiplexers, direct half of your users to use multiplexer 1 and the other half to use multiplexer 2.

**Procedure**

1. Open Sametime Connect.
2. Choose **File > Preferences > Server Communities**.
3. In the Server Community field, type the DNS name of the Community Server multiplexer machine, such as messaging.example.com, as instructed by the administrator.

**Configuring ports for server-to-server connections:**

When multiple IBM Sametime servers are installed in an IBM Lotus Domino environment, the Sametime servers must be able to communicate on specific ports.

**Ports required for communication between Sametime servers**

**Note:** Ports for Meetings do not apply to Sametime Entry, Sametime Limited Use, or versions of Sametime that do not support web conferencing.

The table below lists the ports on which Sametime servers communicate with each other. When these ports are open, Community Services and Meeting Services data can pass between the two servers, and one Sametime server can invite the other to a meeting.
<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1503</td>
<td>Port 1503 is the default &quot;Meeting Server port for server connections.&quot; This port is configurable from the Configuration - Connectivity - Network and Port Settings - Meeting Services Network options in the Sametime Administration Tool. The &quot;Meeting Server port for server connections&quot; setting must be set to the same port number for the Sametime servers. The servers must communicate on TCP/IP port 1503 to exchange Meeting Services data.</td>
</tr>
<tr>
<td>Port 1516</td>
<td>The Community Services listen for direct TCP/IP connections from the Community Services of other Sametime servers on this port. If you have installed multiple Sametime servers, this port must be open for presence, chat, and other Community Services data to pass between the servers. The communications that occur on this port also enable one Sametime server to start a meeting on another server (or &quot;invite&quot; the other server to the meeting).</td>
</tr>
<tr>
<td>Port 1352</td>
<td>The servers must be able to communicate on port 1352 for replication to occur between the Sametime servers. This is the port used for Notes and Domino Remote Procedure Calls (RPCs).</td>
</tr>
</tbody>
</table>

**About invited servers, audio/video, and client connectivity**

When one Sametime server invites another Sametime server to a meeting that includes interactive audio/video, the audio/video data is not transmitted between the two Sametime servers. Instead, the user must connect to the Sametime server on which a meeting was started and receive the audio/video streams directly from that host server. For example, assume a meeting that includes chat, screen sharing, and audio/video is started on Sametime server A and Sametime server A invites Sametime server B to the meeting. A user can attend the meeting on Sametime server B (the invited server) and receive the chat and screen sharing data from Sametime server B. However, the user is redirected to Sametime server A for the audio/video data.

**Next step:**

Next, perform the procedures described in Synchronize the Sametime server with other Sametime servers deployed in the environment.
**Related concepts**

“Integrating a Sametime server into an existing Sametime community” on page 922
This topic provides an overview of the tasks involved in integrating a new IBM
Sametime server into an existing Sametime community.

**Related reference**

“Ports used by the Sametime Community Server” on page 323
IBM Sametime uses a number of ports on the server. This topic lists the default
ports and their uses.

**Synchronizing the Sametime server with other Sametime servers:**

When multiple Sametime servers are installed, you must synchronize the Sametime
servers to operate as a single community.

**Related concepts**

“Integrating a Sametime server into an existing Sametime community” on page 922
This topic provides an overview of the tasks involved in integrating a new IBM
Sametime server into an existing Sametime community.

**Domino Directory management for multiple Sametime servers:**

This topic discusses managing IBM Lotus Domino Directories for multiple IBM
Sametime servers.

After you have installed a new Sametime server, the administrator should
determine how to manage the Directory for the Sametime community.

Use these recommendations to manage Domino Directories in multiple Sametime
server environments:

- If the Sametime server is installed into a Domino environment that uses only a
  single Domino Directory, the Directory in which all Sametime servers are
  registered must be replicated to each Sametime server.

- If the Sametime server is installed into a Domino environment that uses multiple
  Domino Directories, the primary Domino Directory (the Directory in which the
  Sametime server is registered) should be replicated to the Sametime server.
  Directory Assistance should be set up on the Sametime server to access the other
  Domino Directories of interest in the environment. The Sametime server can use
  Domino Directory Assistance to obtain all needed Directory information from
  the other Directories used in the environment. Ideally, the Directory Assistance
database should point to a Directory server that is dedicated to providing
Directory services. However, it is not a requirement that Directory servers be
used in a Sametime community that includes multiple Sametime servers.
  For information on setting up Directory Assistance on the Sametime server, see
  your Domino server Administration documentation. Use the same procedures to
  set up Directory Assistance on a Sametime server that you use to set up
  Directory Assistance on a Domino server. The Domino Administration
documentation is available from the Documentation Library at the following
Internet location: http://www.lotus.com/ldd/doc (and also in the Help
subdirectory of the Domino server on which Sametime is installed).

- Optionally, in a Domino environment that uses multiple Domino Directories, an
  Extended Server Directory Catalog can be set up on the Sametime server to
  enable the server to access Directory information from all directories of interest
  in the environment. For more information on setting up an Extended Server
  Directory Catalog for use with Sametime, see Alternate ways to share Directory
  information across domains.
For more information about the Directory issues relevant to extending a single Sametime community across multiple Domino domains, see Extending a single Sametime community across multiple Domino domains.

Related concepts
“Integrating a Sametime server into an existing Sametime community” on page 922
This topic provides an overview of the tasks involved in integrating a new IBM Sametime server into an existing Sametime community.

**Extending a single Sametime community across multiple Domino domains**
This section provides instructions and suggestions on how to link different IBM Lotus Domino domains into a single IBM Sametime community. When separate Domino domains are linked into a single Sametime community, users in each domain can share presence and chat capabilities and participate in Sametime meetings with users in the other domain.

Related concepts
“Alternate ways to share Directory information across domains” on page 931
This topic discusses the Directory information that is shared between IBM Sametime servers and describes some alternate, more efficient ways to share Directory information when connecting Sametime communities across multiple IBM Lotus Domino domains.

**Example of extending a single Sametime community across two Domino domains:**

This topic provides an example of how to connect an IBM Sametime server in an IBM Lotus Domino domain with another Sametime server within a different Domino domain.

About this task

The procedure below provides an example of how one Sametime server in a Domino domain can be linked with a different Sametime server operating in a different Domino domain. Linking the two Sametime servers extends a single Sametime community to both Domino domains.

When a single Sametime community is extended to both Domino domains:

- Users in one Domino domain can add users from the other Domino domain to presence lists in Sametime clients and engage in Sametime communications with users in the other domain.
- Users in the Sametime community can authenticate on either of the domains to participate in Sametime meetings and communications.
- The Sametime server in one Domino domain can invite the Sametime server in the other Domino domain to a meeting so that a single Sametime meeting can be attended by users in both Domino domains.

Follow the procedures below to link two Sametime servers that operate in different Domino domains:

Setting up the environment by cross-certifying servers:

You can extend a single IBM Sametime community across multiple IBM Lotus Domino domains by cross-certifying the servers.
About this task

The example below describes the simplest way to cross-certify the two Sametime servers. In this example, the two Sametime servers are Sametimeserver1/East and Sametimeserver2/West. To cross-certify these servers, the West organization certifier (/West) must obtain a cross-certificate for the East organization certifier (/East) and the East organization certifier must obtain a cross-certificate for the West organization certifier. These cross-certificates are stored in the Domino Directories on the respective Sametime servers.

For more information about cross-certification, see the Domino Administration Help database, available in the Help directory of any Domino server. Domino administration documentation is also available from the Documentation Library at www.lotus.com/ldd/doc.

Procedure

1. On Sametimeserver1/East, open the IBM Lotus Notes client. From the Microsoft Windows desktop click Start > Run and browse to C:\Sametime\nlnotes.exe before clicking OK.
2. Click File > Database > Open and specify the Sametimeserver2/West server.
3. When prompted for a cross-certificate, select OK.
4. Repeat steps 1 through 3, but this time use the Notes client on Sametimeserver2/West to access Sametimeserver1/East, and accept the cross-certificate from the Sametimeserver2/West server.

What to do next

Now that the servers are cross-certified, connect the communities.

Connecting the communities:

You can extend a single IBM Sametime community across two IBM Lotus Domino domains by sharing Directory information between domains.

About this task

In this procedure, the administrator connects the Sametime communities by ensuring that Directory information is shared between the two Domino domains by following these steps:

Procedure

1. Replicating the Directories
2. Setting up Directory Assistance

Results

In this example, the two Sametime servers that operate in different domains are Sametimeserver1/East and Sametimeserver2/West.

Note: This example describes replicating the entire Directories of both domains. There are more efficient ways to share Directory information between two Domino domains when connecting the communities. For more information on alternate methods for sharing the Directory information, see Alternate ways to share Directory information across domains.
Step 1 - Replicating the Directories:

About this task

This procedure provides an example of replicating Directories between two Sametime servers (Sametimeserver1/East and Sametimeserver2/West) operating in different Domino domains.

Procedure

1. Using the IBM Lotus Notes client on Sametimeserver1/East, open the Directory (names.nsf) on Sametime server2/West.
2. Click File > Replication > New Replica.
3. Specify Local for the Server and change the filename (names.nsf) to something different, such as sametimeserver2west.nsf.
4. Select Create: Immediately to ensure that the database is created immediately, and then click OK.
5. Repeat steps 1 through 4, except this time create a replica of the Directory existing on Sametimeserver1/East on the Sametimeserver2/West server.

What to do next

After you have created replicas of the Directories on each Sametime server, you must create Connection Documents to ensure the Directories replicate at regular intervals. When creating the Connection Documents:

- For Connection Type, select Local Area Network.
- Complete the Destination Server, Source Domain, Destination Domain, and Optional Network Address fields.
- For Replication Type, select Pull Push.
- In the Files/Directories to Replicate field, enter names.nsf.
- In the Schedule field, select Enabled.

Note: Be sure to create a Connection Document on each server. One Connection Document should enable the names.nsf file on Sametimeserver1/East to replicate to the Sametimeserver1east.nsf file on the Sametimeserver2/West server. The other Connection Document should enable the names.nsf file on Sametimeserver2/West to replicate to the sametimeserver2west.nsf file on the Sametimeserver1/East server.

After creating the Connection Documents, set up Directory Assistance on each of the Sametime servers to ensure that each Sametime server can locate the Directories you have just replicated.

Step 2 - Setting up Directory Assistance:

About this task

The procedures required for setting up Directory Assistance on each of the Sametime servers are summarized below. For more information on Directory Assistance, see the Domino Server Administration Help, available in the Help directory on every Domino server, as well as at www.lotus.com/ldd/doc.

To set up Directory Assistance you must:

- Ensure that a Directory Assistance database is available on the Sametime server.
• Identify the Directory Assistance database on the Sametime server.
• Create a Directory Assistance Document within the Directory Assistance
database that points to the appropriate Directory.

Follow the procedures below to set up Directory Assistance:

Ensure that a Directory Assistance database is available on each Sametime server:

About this task

To ensure that a Directory Assistance database is available on each Sametime
server, you can either replicate an existing Directory Assistance database to the
Sametime server or create a new Directory Assistance database on the Sametime
server.

If a Directory Assistance database is already in use on Domino servers in the
domain, you can replicate the existing Directory Assistance database to the
Sametime server. To replicate an existing Directory Assistance database, follow the
normal Domino procedure for replicating a database. First create a new replica of
the Directory Assistance database on the Sametime server and then create a
Connection Document to schedule replication of the database. See the Domino
server Administration Help for more information on these procedures.

To create a new Directory Assistance database on each Sametime server:

Procedure
1. Start the Lotus Notes client.
2. Click File > Database > New.
3. Create the Directory Assistance database as you would any other Domino
database.
   • Create the database on the Sametimeserver1/East server
   • Provide a database name and filename for the Directory Assistance database
   • Use the Directory Assistance template (da50.ntf) when creating the database
4. Repeat steps 1 through 3 to create a Directory Assistance database on the
   Sametime server in the other domain (Sametimeserver2/West in this example).
5. Perform the procedure below to identify the Directory Assistance database on
   each Sametime server.

Identify the Directory Assistance database on each Sametime server:

About this task

After replicating or creating the Directory Assistance databases on the Sametime
servers, you must identify the Directory Assistance databases on each server.

To identify a Directory Assistance database on each Sametime server:

Procedure
1. Start the Lotus Notes client.
2. Click Configuration > Server > All Server Documents.
3. Double-click the name of the Sametime server (Sametimeserver1/East) to open
   the Server document.
4. If necessary, select the Basics tab of the Server document.
5. Click **Edit Server**.
6. In the **Directory Assistance database name** field, enter the filename (for example, **da.nsf**) of the Directory Assistance database.
7. Click **Save and Close**.
8. Repeat this procedure to identify the Directory Assistance database on the Sametime server in the other domain (Sametimeserver2/West in this example).
9. Perform the procedure below to create a Directory Assistance Document in each Directory Assistance database.

**Create a Directory Assistance Document in each Directory Assistance database:**

**About this task**

You must create a Directory Assistance Document in each Directory Assistance database on each Sametime server so that each Sametime server can access the new Directory information that has been replicated to it.

To create a Directory Assistance document in the Directory Assistance database on each Sametime server:

**Procedure**

1. From the Notes client:
   - Click **File > Database > Open**.
   - Select the Sametimeserver1/East server.
   - Select the Directory Assistance database (default name is da.nsf).
   - Click **Open**.
2. Click **Add Directory Assistance**.

   In the **Basics** tab, enter these settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type</td>
<td>Click <strong>Notes</strong>.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter the name of the Domino domain associated with the secondary Directory (or Directory that was replicated from the other domain to this Sametime server). The domain name must be different from the primary Notes domain and from all other domain names configured in Directory Assistance.</td>
</tr>
<tr>
<td>Company name</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Search order</td>
<td>A number representing the order in which this directory is searched, relative to other directories in the Directory Assistance database.</td>
</tr>
<tr>
<td>Group expansion</td>
<td>The suggested setting is <strong>Yes</strong>. This setting enables Directory Assistance to examine the contents of groups in the LDAP directory. This capability is necessary if you enter the name of a group defined in the LDAP directory in the ACL of a database on the Sametime server.</td>
</tr>
</tbody>
</table>
Setting Value
Nested group expansion
The suggested setting is Yes. This setting enables Directory Assistance to examine the content of an LDAP directory group that is a member of another LDAP directory group. This capability is also used when an LDAP directory group name is entered in the ACL of a database on the Sametime server.
Enabled
Set to Yes to enable Directory Assistance for the LDAP Directory.

3. Select the Rules tab and enter these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule #</td>
<td>One or more rules that describe the names in the directory. By default, the first rule contains all asterisks, indicating all names in the Directory.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Choose one:</td>
</tr>
<tr>
<td></td>
<td>• No to disable a specific rule.</td>
</tr>
<tr>
<td></td>
<td>• Yes to enable a specific rule.</td>
</tr>
<tr>
<td>Trusted for Credentials</td>
<td>Choose Yes to allow Domino to use this Directory to authenticate web clients.</td>
</tr>
</tbody>
</table>

4. Select the Replicas tab and do the following:
5. You must repeat this procedure to create a Directory Assistance document in the Directory Assistance database on the Sametime server in the other domain (Sametimeserver2/West in this example).

Alternate ways to share Directory information across domains:

This topic discusses the Directory information that is shared between IBM Sametime servers and describes some alternate, more efficient ways to share Directory information when connecting Sametime communities across multiple IBM Lotus Domino domains.

The example procedure for extending a single Sametime community across two Domino domains earlier in this section explains how you can share Directory information to connect two Sametime communities.

When extending a single Sametime community across multiple Domino domains, each Sametime server that is part of the community must have access to the following Directory information for the other domain(s):

- Person documents
- Group documents
- Server documents - The following fields in the Server document are needed for each Sametime server to support online presence (or awareness) between servers:
  - **Server name** - This field in the Basics tab of the Server document must contain the name of the Sametime server.
**Is this a Sametime server?** - This field in the Basics tab of the Server document must be set to Yes to indicate that the Server document describes a Sametime server.

**Port** - This field in the Ports > Notes Network Ports tab of the Server document must be set to TCPIP.

**Net Address** - This field in the Ports > Notes Network Ports tab must contain the TCP/IP address (for example, sametime.example.com) of the Sametime server.

To share this Directory information, each domain must replicate the information to the other domains that comprise the Sametime community. In the example scenario described in Example of extending a single Sametime community across two Domino domains, the entire Directories of two separate Domino domains are replicated between the two Sametime servers. The Domino components of Sametime provide features that you can use to replicate the Directory information in a more efficient manner. You can use either of the following alternate techniques to share Directory information across Domino domains.

- Selective replication of Directory information across domains
- Set up Extended Directory Catalogs to share Directory information across domains

Each technique is discussed briefly below.

**Selective replication of Directory information across domains**

Instead of replicating the entire Domino Directory between domains, you can use selective replication to replicate only the Person, Group, and Server documents. For example, you can open the Directory database to be replicated to the other domain and use the Replication Settings to replicate a subset of the documents contained in the database. Use a selection formula, such as (Type="Person") | (Type="Group") | (Type="Server" and Sametime="1") to ensure that only the Person, Group, and Server documents (for which the **Is this a Sametime server?** field is set to Yes) are replicated.

For more information on selective replication, see the Domino Server Administration Help, available in the Help directory on every Domino server as well as in the Documentation Library at www.lotus.com/ldd.

**Using Extended Directory Catalogs to share Directory information across domains**

An Extended Directory Catalog is another Domino feature that can be used to share Directory information when a Sametime community is extended across multiple Domino domains. The Extended Directory Catalog feature allows you to aggregate directory information from several different Domino directories, including directories for different Domino domains, into a single directory catalog. The servers are then configured to access the Extended Server Directory catalog for directory information.

Before using this feature, the administrator should read the documentation in Domino Server Administration Help that explains the function and set up of Extended Server Directory Catalogs. This documentation is available in the Help directory on every Domino server as well as in the Documentation Library at www.lotus.com/ldd.
You can follow the procedures in the Domino administration documentation to set up an Extended Server Directory Catalog on the Sametime server. When setting up the Extended Server Directory Catalog to be used by Sametime, note the following when creating the Configuration document for the Extended Server Directory Catalog:

- The Configuration document contains an **Additional fields to include** list in the **Basics** tab. The following field name entries must exist in the **Additional fields to include** list to ensure that all information needed by Sametime is available in the Extended Server Directory Catalog:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>Server name field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>ServerTitle</td>
<td>Server title field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain name field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>ServerBuildNumber</td>
<td>Server build number field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Administrator field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>ServerPlatformDisplay</td>
<td>Operating system field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>Sametime</td>
<td><strong>Is this a Sametime server?</strong> field in the <strong>Basics</strong> section of the Server document.</td>
</tr>
<tr>
<td>Port_0 - Port_7</td>
<td><strong>Ports</strong> fields in the <strong>Ports &gt; Notes Network Ports</strong> section of the Server document. For completeness it is recommended that you list seven <strong>Ports</strong> fields (for example Port_0, Port_1, Port_2, Port_3, Port_4, Port_5, Port_6, and Port_7).</td>
</tr>
<tr>
<td>Protocol_0 - Protocol_7</td>
<td><strong>Protocol</strong> fields in the <strong>Ports &gt; Notes Network Ports</strong> section of the Server document. For completeness, it is recommended that you list seven <strong>Protocol</strong> fields (for example, Protocol_0, Protocol_1, Protocol_2 and so on).</td>
</tr>
<tr>
<td>NetName_0 - NetName_7</td>
<td><strong>Notes Network</strong> fields in the <strong>Ports &gt; Notes Network Ports</strong> section of the Server document. For completeness, it is recommended that you list seven <strong>Notes Network</strong> fields (for example, NetName_0, NetName_1, NetName_2, and so on.</td>
</tr>
<tr>
<td>NetAddr_0 - NetAddr_7</td>
<td><strong>Net Address</strong> fields in the <strong>Ports &gt; Notes Network Ports</strong> section of the Server document. The NetAddr_0 field is required. For completeness, it is recommended that you list seven <strong>Net Address</strong> fields.</td>
</tr>
<tr>
<td>Enabled_0 - Enabled_7</td>
<td><strong>Enabled</strong> fields in the <strong>Ports &gt; Notes Network Ports</strong> section of the Server document. The Enabled_0 field is required. For completeness, it is recommended that you list seven <strong>Enabled</strong> fields.</td>
</tr>
</tbody>
</table>
The **Advanced** tab of the Configuration document provides a **Selection formula**
(do not include form) setting that enables you to specify a selection formula to
ensure that only the Directory documents required by Sametime are used when
the "Dircat" task creates the Directory Catalog. The selection formula for
selecting only the documents required by Sametime is:

\[
(Type = "Person") \lor (Type = "Group") \lor (Type = "Server" \land Sametime = "1")
\]

### Configuring SiteMinder for the Sametime server

This section describes how to configure CA eTrust SiteMinder for the IBM
Sametime server.

#### About this task

When you configure SiteMinder to work the Sametime server, you create a new
agent object, agent configuration object, Host configuration object, realm, and
sub-realms.

#### Creating configuration objects for Sametime

Follow these steps to create configuration objects for IBM Sametime 8 on the CA
eTrust SiteMinder Policy server.

#### Before you begin

Open the SiteMinder Policy Server console.

#### Procedure

1. To create an Agent object, follow these steps.
   a. Click the **System** tab.
   b. Under System Configuration, right-click the Agents icon.
   c. In the SiteMinder Agent Dialog, type a unique value not used previously
   for an existing agent in the **Name** field.
   d. Optional: Type a description such as "Sametime Agent."
   e. Under Agent Type, select **SiteMinder** and select **Web Agent** from the
drop-down list.
   f. Click **OK**.
2. Create a duplicate of the existing DominoDefaultSettings Agent Conf Object on
   the SiteMinder Policy Server and modify the duplicate as appropriate. To create
   an Agent Conf object for your HTTP Server:
   a. Under System Configuration, click the Agent Conf Objects icon.
   b. Right-click the **DominoDefaultSettings Agent Conf** object in the Agent
   Conf Object List on the right side of the console, and select **Duplicate
   Configuration Object**.
   c. In the SiteMinder Agent Configuration Object Dialog, type a unique value
   not used previously for an existing agent in the **Name** field.
   d. Optional: Type a description such as "Domino Configuration Agent."
e. In the Configuration Values list, set the following parameters to the values indicated or to the appropriate values for your server. Clicking each parameter, and select the Edit:
   • DefaultAgentName - Name given to agent created in step c.
   • AllowLocalConfig - Yes
   •CssChecking - No
   •BadUrlChars - remove // and /, %00-%1f, %7f-%ff,%25 from the default list of Bad Url Characters
   •SkipDominoAuth - No. All other parameters can be left at their default settings.

f. Click OK.

3. IBM recommends that you create a duplicate of the existing DefaultHostSettings Host Conf Object on the SiteMinder Policy Server and modify the duplicate as appropriate. To create a Host Conf object for your HTTP Server:
   a. Under System Configuration, click the Host Conf Objects icon.
   b. Right-click the DefaultHostSettings object in the Host Conf Object List on the right side of the console, and select Duplicate Configuration Object.
   c. In the SiteMinder Host Configuration Object Dialog, type a unique value in the *Name field.
   d. Optional: Type a description such as "Sametime Advanced Host."
   e. In the Configuration Values list, edit the #Policy Server value by removing the # from in front of the parameter name and enter the IP address of your SiteMinder Policy Server in the appropriate place in the value field.
   f. Click OK.

Configuring realms for Sametime
Follow these steps to configure the realms for IBM Sametime 8 on the CA eTrust SiteMinder Policy Server.

Procedure
1. Open the SiteMinder Policy Server console.
2. Define the realm definition for the Web Agent domain:
   a. Click the Domains tab in the left side of the SiteMinder Policy Console.
   b. Right-click the Web Agent domain that you previously created.
   c. Click Create Realm.
   d. In the SiteMinder Realm Dialog, type a unique value in the *Name field, for example, Sametime.
   e. Optional: Type a description.
   f. Click the Resource tab.
   g. In the Agent field, type the name of the agent that you created for the Web Agent for Sametime 8. You can also select it using Lookup.
   h. Type the Resource Filter as /
   i. In Authentication Scheme drop-down list, select Basic.
   j. Under Default Resource Protection, select Protected. Leave all the other fields on the Resource, Session and Advanced tabs as their default values.
   k. Click OK.
3. Create sub-realms under the realm you just created.
   a. Click the Domains tab in the left side of the SiteMinder Policy Console..
b. Right-click the realm that you created in step 2.

c. Click **Create Realm**.

d. Create the following sub-realms for your configuration, with the values indicated in each dialog:

<table>
<thead>
<tr>
<th>Name</th>
<th>Resource Filter</th>
<th>Authentication Scheme</th>
<th>Default Resource Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST Test</td>
<td>stlinks</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST AdminConfig</td>
<td>servlet/auth/scs</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST AdminPage</td>
<td>servlet/auth/admin</td>
<td>Basic</td>
<td>Protected</td>
</tr>
<tr>
<td>ST Src</td>
<td>stsrc.nsf/join</td>
<td>Basic</td>
<td>Protected</td>
</tr>
<tr>
<td>ST Domino</td>
<td>STDomino.nsf</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Applets</td>
<td>sametime/applets</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Applet</td>
<td>Sametime/Applet</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>IMI Sametime</td>
<td>sametime/hostAddress.xml</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST MMAPI</td>
<td>servlet/auth/mmapi</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST Admin CGI</td>
<td>cgi-bin/StAdminAct.exe</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
<tr>
<td>ST UserInfoServlet</td>
<td>servlet/UserInfoServlet</td>
<td>Basic</td>
<td>Unprotected</td>
</tr>
</tbody>
</table>

4. Create rules for the protected realm (Sametime) and the two protected sub-realms (ST AdminPage and ST Src).

   a. Right-click the realm that was created for the Web Agent domain (for example Sametime), and select **Create Rule under Realm**.

   b. Use the SiteMinder Rule dialog to create the following rules named Rule 1 and Rule 2:

   **Rule 1 properties**
   - *Name* - GetPost Rule
   - *Realm* - Sametime
   - Resource: *
   - Web Agent actions - Get,Post,
   - When this Rule fires - Allow Access
   - Enable or Disable this Rule - Enabled

   **Rule 2 properties**
   - *Name* - OnAuthAccept
   - *Realm* - Sametime
   - Resource: *
   - Authentication events - OnAuthAccept
   - When this Rule fires - Allow Access
   - Enable or Disable this Rule - Enabled

c. Right-click the ST AdminPage sub-realm, and select **Create Rule under Realm**.

d. Use the SiteMinder Rule dialog to create the following rule named Rule 1:

   **Rule 1 properties**
   - *Name* - GetPost Rule
• Realm - Sametime.ST AdminPage
• Resource: *
• Web Agent actions - Get, Post,
• When this Rule fires - Allow Access
• Enable or Disable this Rule - Enabled

e. Right-click the ST Src sub-realm, and select Create Rule under Realm.
f. Use the SiteMinder Rule dialog to create the following rules named Rule 1 and Rule 2:

   **Rule 1 properties**
   • *Name - GetPost Rule
   • Realm - Sametime.ST Src
   • Resource: *
   • Web Agent actions - Get, Post,
   • When this Rule fires - Allow Access
   • Enable or Disable this Rule - Enabled

   **Rule 2 properties**
   • *Name - OnAuthAccept
   • Realm - Sametime.ST Src
   • Resource: *
   • Authentication events - OnAuthAccept
   • When this Rule fires - Allow Access
   • Enable or Disable this Rule - Enabled

5. Add the rules to the SiteMinder policy that you created for Sametime Advanced.
a. Double-click the policy you created for Sametime Advanced, for example, STADVWAPolicy.
b. Click the Rules tab, and then click Add/Remove Rules. Add all the rules you created previously for the realm and sub-realms to the current members list. Click OK.

### Installing and configuring the SiteMinder Web Agent

IBM recommends that you install the latest available version of the CA eTrust SiteMinder Web Agent as well as the latest available hot fix that is certified by Computer Associates to work with the version of the HTTP server that you are using.

#### Before you begin

Before you begin, you must download the SiteMinder V6-QMR5 W32 Web Agent installation files from the SiteMinder support site at http://support.netegrity.com.

#### About this task

Refer to the SiteMinder platform support matrices for more details. These matrices can be obtained from the SiteMinder support site. You can also refer to the SiteMinder WebAgent Installation Guide for details about configuring the Web Agent to work with the HTTP server that you are using. The application agent for IBM Sametime Advanced should be v6.0 CR005 or later to ensure support of IBM WebSphere Application Server 6.1.
Note: To install the SiteMinder Web Agent on platforms other than Microsoft Windows, you can use the relevant Win32 instructions as a reference document. The same configuration information needs to be provided, regardless of platform. There are also additional instructions included with the Web Agent installation files that indicate platform-specific steps that are required for installing and configuring the Web Agent on a specific platform.

Follow these steps to install and configure the Win32 6x Web Agent for your HTTP server.

Procedure

1. If necessary, extract all the files from the ZIP file provided by SiteMinder.
2. Start the Web Agent executable. The format is nete-wa-6qmrX-platform.exe. For example:
   nete-wa-6qmr5-win32.exe

   The CA SiteMinder Web Agent Introduction screen appears.
3. Click Next.
4. On the License Agreement screen, scroll down and select I accept the terms of the License Agreement, and click Next.
5. Click Next on the Important Information screen.
6. On the Choose Install Location screen, accept the default location for installing the Web Agent or click Choose to select a different location, then click Next.
7. Click Next on the Choose Shortcut Folder screen.
8. Click Install on the Pre-Installation Summary screen.
9. On the Install Complete screen, accept the defaults selection and click Done. Your system restarts.
10. Click Start > Programs > Siteminder > Web Agent Configuration Wizard to start the Web Agent Configuration Wizard.
11. On the Host Registration screen, select Yes, I would like to do Host Registration now, but do not select the Enable PKCS11 DLL Cryptographic Hardware check box. Click Next.
12. On the Admin Registration screen, type the SiteMinder administrator name and password provided by your SiteMinder contact. Do not select the Enable Shared Secret Rollover check box. Click Next.
13. On the Trusted Host Name and Configuration Object screen, type the trusted hostname and Host Conf Object provided by your SiteMinder contact. Click Next.
14. On the Policy Server IP Address screen, type the SiteMinder Policy Server IP address provided by your SiteMinder contact and click Add. Click Next.
15. On the Host Configuration file location screen, accept the default file name and location and click Next.
16. On the Select Web Server(s) screen, select the check box next to the http server that you wish to configure with the Web Agent, and then click Next.
17. On the Agent Configuration Object screen, enter the Agent Conf Object provided by the SiteMinder contact and click Next.
18. On the Web Server Configuration Summary screen, click Install. The Web Agent configuration process starts, and then the Configuration Complete screen appears.
19. Click Done to complete the configuration process.
Note: You can ignore messages indicating that some warnings occurred during the installation. These warnings appear by default and do not affect the functionality of the Web Agent.

What to do next

There are additional steps that must be completed to enable the Web Agent to function properly for your server. Follow the additional instructions that are provided by your SiteMinder contact in order to complete this setup.

Add the DSAPI filter file name to the Domino Directory

Your IBM Sametime server will run on a Lotus Domino server. When you integrate IBM Sametime with CA eTrust SiteMinder, the SiteMinder Web Agent is implemented as a Domino Web Server Application Programming Interface (DSAPI) filter file.

About this task

Follow these steps to add the DSAPI filter file name to the Domino Directory.

Procedure

2. Edit the server document for the Domino server as follows:
   a. Click the Internet Protocols tab, then click the HTTP tab. In the DSAPI filter file names field, type the full path and name of the SiteMinder Web Agent (typically c:\Program Files\Netegrity\Siteminder Web Agent\bin\dominowebagent.dll)
   b. Click the Domino Web Engine tab, then set the Session authentication field to Disabled.
3. Save and close the server document.

Enabling SiteMinder for Sametime

Follow these steps to enable the CA eTrust SiteMinder Web Agent for the IBM Sametime server.

Procedure

1. Locate the local Web Agent configuration file for the SiteMinder Web Agent that has been configured with your HTTP server. For example:
   C:\Program Files\IBM\HTTPServer\conf\WebAgent.conf
2. Use a text editor to open the file and set the EnableWebAgent parameter to YES.
3. Restart your HTTP and Lotus Domino Servers. When you start or stop the Domino server, you are starting and stopping the Sametime server as well.

Configuring the Sametime client

This section describes how to configure IBM Sametime clients.

Connecting the Sametime Connect client to the Sametime Community Server

The Sametime Connect client uses Server Communities preferences to connect to the Sametime Community Server for presence and chat features.
The client finds a Sametime Community server using the server community's Host server and Server community ports specified in Preferences > Server Communities. The client connects most efficiently when the Host server matches the home Sametime server defined in the user's Person document. The corresponding Connectivity settings for the Sametime Community Server must contain the correct IP addresses or DNS names and ports for clients to connect successfully.

The client uses the connection method selected in the Global connection settings for all Server Communities unless the server community's Connection tab specifies an alternate method. This section explains how to configure the different types of connections.

Related tasks
- “Assigning users to a home Sametime Community Server” on page 338
  A user's home Sametime Community Server saves the user's preferences and data. Each user connects to the home server for online presence (or awareness) and chat functionality.

Defining the host server and port for connecting to a Sametime Community server

The Sametime Connect client uses the Host and Server community port preferences to determine the host name and port it should use when attempting a connection to the Sametime Community server.

Before you begin

Verify the Connectivity settings for client connections set for the Sametime Community Server. The client's successful connection depends on defining the correct host name, port, and connection method for the server.

- Under Client Connections, type the fully qualified Host Name and Port from which Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients.
- Under HTTP Tunneled Client Connections, type the fully qualified Host Name and Port from which Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default.
- Under HTTPS Tunneled Client Connections, type the fully qualified Host Name and Port from which the Community Services clients attempt HTTPS connections when accessing the Sametime Community Server through an HTTPS proxy server.

About this task

Follow these instructions to define the host server and port for a server community.

Procedure
1. From the Sametime Connect client, click File > Preferences.
2. Click Server Communities.
3. Do one of the following:
   - To add a new server connection, click Add New Server Community.
   - To change an existing server connection, expand the Server Community list and select the community name.
4. For an existing community, proceed to the next step. For a new community, provide a community name and Log in information.

5. Click the Connection tab.

6. Provide a Host server and port. The method chosen for connecting to the server may also affect the Host server and port you use here.
   - Host server
     The client connects most efficiently when the Host server matches the home Sametime server defined in the user's Person document.
     If you have set up a rotating DNS system for load balancing, specify the DNS name (for example, sametime.cscluster.com) of the rotating DNS system in this field.
     If you have set up a WebSphere® Edge Server to perform load balancing, users must enter the IP address or DNS name of the WebSphere Edge Server machine in this field.
   - Server community port
     The method you choose for connecting to the server also affects the port setting. For example, if you choose Direct connection using HTTP protocol and the client that operates behind a firewall that only allows outbound connections on port 80, you must change the default port from 1533 to port 80.

7. For an existing community, click OK to close the Preferences window.
   For a new community, click OK to save and then OK to close the Preferences window.

Related concepts
“Choosing a method for connecting to the Sametime Community Server”
The Sametime Connect client uses the connection method specified in Server Communities preferences. The Global connection settings apply to all connections unless a specific server community uses an alternate connection method as defined on its Connection tab in the Preferences window.

Related tasks
“Configuring Sametime Community Server connectivity” on page 321
Define the host names and ports for Community Services on the IBM Sametime Community Server.

Choosing a method for connecting to the Sametime Community Server
The Sametime Connect client uses the connection method specified in Server Communities preferences. The Global connection settings apply to all connections unless a specific server community uses an alternate connection method as defined on its Connection tab in the Preferences window.

This section explains how to configure the different types of connections.

Connecting the client through a direct connection over TCP/IP:

When a user starts the Sametime Connect client with a Direct connection preference, the client connects to the Sametime Community server using a unique Sametime protocol over TCP/IP. By default, the Community Server listens for this connection on port 1533. Use this preference when the connection does not need to occur through a proxy server, and the network does not block TCP/IP connections on the port used by the client.
Before you begin

A successful connection depends on these prerequisites.

- The client’s preferences for the server community must contain a valid Host server and Server community port for a TCP/IP connection.
- The Sametime Community Server Connection Settings for Client connections, as defined in the Sametime System Console, must match the Host server and Server community port specified in the client. The default port is 1533.

The connection can fail if it must pass through a proxy server or network that prevents direct TCP/IP connections on the specified port.

About this task

Follow these steps to select the Direct connection method for the client.

Procedure

1. From the Sametime Connect client, click File > Preferences.
2. Do one of the following:
   - To select this connection method for all server communities, click Server Communities. Under Global connection settings, click Direct connection and click OK.
   - To select this connection method for only one server community, click Server Communities, select the server community name, and open the Connection tab. Uncheck Use global connection settings, then click Direct connection and click OK. Click OK to close the Preferences window.

Results

This connection is the same as the Use my Internet Explorer HTTP settings preference for a user who has no proxy selected in Internet Explorer.

Related tasks

“Connecting the client through Internet Explorer HTTP settings” on page 944

When a user starts the Sametime Connect client with the Use my Internet Explorer HTTP settings preference, the client examines the Internet Explorer Connection settings to determine how to connect to the Sametime Community server. If no proxy server is selected, the HTTP request goes to the Sametime Community server in a direct connection. If a proxy server is selected, the client connects through the appropriate SOCKS or HTTP proxy server.

“Configuring Sametime Community Server connectivity” on page 321

Define the host names and ports for Community Services on the IBM Sametime Community Server.

Connecting the client through a TLS connection:

When a user starts the Sametime Connect client with a Direct connection using TLS preference, the client connects to the Sametime Community server using the Transport Layer Security (TLS) protocol. Use this preference for clients that must connect through a FIPS proxy server.

Before you begin

A successful connection depends on these prerequisites.
The client’s preferences for the server community must contain a valid Host server and Server community port for a TLS connection.

A Sametime Proxy Server with an associated FIPs proxy server must be installed and connected to the Sametime Community Server.

The Sametime Community Server Connection Settings for Client connections, as defined in the Sametime System Console, must match the Host server and Server community port specified in the client.

About this task

Follow these steps to select the Direct connection using TLS method for the client.

Procedure

1. From the Sametime Connect client, click **File > Preferences**.
2. Do one of the following:
   - To select this connection method for all server communities, click **Server Communities**. Under Global connection settings, click Direct connection using TLS and click OK.
   - To select this connection method for only one server community, click **Server Communities**, select the server community name, and open the **Connection** tab. Uncheck Use global connection settings, then click Direct connection using TLS and click OK. Click OK to close the Preferences window.

Related tasks

“Installing a Sametime Proxy Server” on page 346
The IBM Sametime Proxy Server enables browser-based clients to participate in Sametime instant messaging and online meetings. In addition, the Sametime Proxy Server works with Sametime Community Server or Connections to enable the business card feature in Sametime, and with Sametime Unified Telephony or other TCSPI-enabled products to enable the Sametime click-to-call feature. The Sametime Proxy Server also provides live names awareness, and can replace the Links Toolkit used in earlier releases of Sametime.

“Installing the FIPS Server” on page 853
IBM Sametime supports the U.S. government-defined security requirements for cryptographic modules known as FIPS 140-2 (Federal Information Processing Standard 140-2). Installing the FIPS Server is only necessary if your Sametime deployment must be FIPS-compliant; otherwise, it is optional.

“Configuring Sametime Community Server connectivity” on page 321
Define the host names and ports for Community Services on the IBM Sametime Community Server.

Connecting the client through an HTTP connection:

When a user starts the Sametime Connect client with the Direct connection using HTTP protocol preference, the client encases the standard Sametime protocol connection information within an HTTP request in a process known as HTTP tunneling. Use this preference in the absence of proxy servers to allow clients operating behind restrictive firewalls to connect to a Sametime Community server that is also available to Internet users.

Before you begin

A successful connection depends on these prerequisites.
The client's preferences for the server community must contain a valid Host server and Server community port. If the firewall allows HTTP connections on port 80 and the client's firewall or network environment does not include an HTTP proxy server, change the port from the default of 1533 to 80.

If you are not using a multiplexer, the Sametime Community Server Connection Settings for **Client connections**, as defined in the Sametime System Console, must match the Host server and Server community port specified in the client. The default port is 1533.

If you are using a multiplexer, the Sametime Community Server Connection Settings for **HTTP Tunneled Client connections**, as defined in the Sametime System Console, must match the Host server and Server community port specified in the client. Clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the Community Services multiplexer listens for HTTP-tunneled connections on port 80.

If the HTTP port is to be changed manually, so must the port be changed in the `stconvservices.properties` file. This is a limitation in that the server does not pull the port from the server document.

**About this task**

**Procedure**

1. From the Sametime Connect client, click **File > Preferences**.
2. Do one of the following:
   - To select this connection method for all server communities, click **Server Communities**. Under Global connection settings, click **Direct connection using HTTP protocol** and click **OK**.
   - To select this connection method for only one server community, click **Server Communities**, select the server community name, and open the **Connection** tab. Uncheck **Use global connection settings**, then click **Direct connection using HTTP protocol** and click **OK**. Click **OK** to close the Preferences window.

**Results**

When the Sametime Connect client starts, it attempts the more efficient direct connection through TCP/IP and if unsuccessful, attempts the HTTP-tunneled connection. This connection is the same as the **Use my Internet Explorer HTTP settings** preference who has an HTTP proxy server selected in Internet Explorer.

**Related tasks**

“Connecting the client through Internet Explorer HTTP settings”

When a user starts the Sametime Connect client with the **Use my Internet Explorer HTTP settings** preference, the client examines the Internet Explorer Connection settings to determine how to connect to the Sametime Community server. If no proxy server is selected, the HTTP request goes to the Sametime Community server in a direct connection. If a proxy server is selected, the client connects through the appropriate SOCKS or HTTP proxy server.

“Configuring Sametime Community Server connectivity” on page 321

Define the host names and ports for Community Services on the IBM Sametime Community Server.

**Connecting the client through Internet Explorer HTTP settings:**
When a user starts the Sametime Connect client with the Under my Internet Explorer
HTTP settings preference, the client examines the Internet Explorer Connection
settings to determine how to connect to the Sametime Community server. If no
proxy server is selected, the HTTP request goes to the Sametime Community
server in a direct connection. If a proxy server is selected, the client connects
through the appropriate SOCKS or HTTP proxy server.

Before you begin

A successful connection depends on these prerequisites.
- The client's preferences for the server community must contain a valid Host
  server and Server community port that matches the browser's connection
  settings.
- The Sametime Community Server Connection Settings, as defined in the
  Sametime System Console, must be correct for the type of connection set up in
  Internet Explorer.

About this task

Follow these steps to select the Under my Internet Explorer HTTP settings
connection method for the client.

Procedure
1. From the Sametime Connect client, click File > Preferences.
2. Do one of the following:
   - To select this connection method for all server communities, click Server
     Communities. Under Global connection settings, click Use my Internet
     Explorer HTTP settings and click OK.
   - To select this connection method for only one server community, click Server
     Communities, select the server community name, and open the Connection
     tab. Uncheck Use global connection settings, then click Use my Internet
     Explorer HTTP settings and click OK. Click OK to close the Preferences
     window.

Results

If the connection does not succeed, Sametime Connect displays an error message.

Related tasks

“Configuring Sametime Community Server connectivity” on page 321
Define the host names and ports for Community Services on the IBM Sametime
Community Server.

Connecting the client through a proxy connection:

When a user starts the Sametime Connect client with a Use proxy preference, the
client connects to the Sametime Community server through a SOCKS, HTTP, or
HTTPS proxy server.

Before you begin

For this connection to succeed, the port specified as the Community port setting in
the Sametime Connect client's Sametime Connectivity settings must match a port
number specified in one of these settings in the Sametime System Console.
• Under **Client Connections**, type the fully qualified **Host Name** and **Port** from which Community Services listen for direct TCP/IP connections and HTTP-tunneled connections from the Community Services clients. A direct TCP/IP connection occurs when the Sametime client uses a unique Sametime protocol over TCP/IP to establish a connection with the Community Services.

• Under **HTTP Tunneled Client Connections**, type the fully qualified **Host Name** and **Port** from which Community Services clients can make HTTP-tunneled connections to the Community Services multiplexer. Community Services clients can make HTTP-tunneled connections on both ports 80 and 8082 by default. Port 8082 ensures compatibility with previous Sametime releases. In previous releases, Sametime clients made HTTP-tunneled connections to the Community Services only on port 8082. If a Sametime Connect client from a previous Sametime release attempts an HTTP-tunneled connection to a Sametime server, the client might attempt this connection on port 8082.

**Note:** If the administrator allows HTTP tunneling on port 80 during the Sametime server installation, the **Community Services > Client connections** > **Port number** setting default to port 1533, and the **Community Services > HTTP tunneled client connections** > **Port number** settings are ports 80 and 8082. In this configuration, the Sametime Connect client can complete an HTTP-tunneled connection to the Community Services multiplexer using either port 1533, 80, or 8082.

• Under **HTTPS Tunneled Client Connections**, type the fully qualified Host Name and Port from which the Community Services clients attempt HTTPS connections when accessing the Sametime Community Server through an HTTPS proxy server. If a Community Services client connects to the Sametime Community server using HTTPS, the HTTPS connection method is used, but the data passed on this connection is not encrypted.

**About this task**

The connection methods for the **Use proxy** option differ in the types of proxy servers they use for connecting.

• **SOCKS4 or SOCKS5 proxy**
  The client uses the **Standard Sametime protocol** over TCP/IP for this connection. The connection from the SOCKS proxy to the Community Services occurs on the "Community port" (default 1533) specified in the Sametime Connect client Sametime Connectivity settings. This connection is the same as the **Use my Internet Explorer HTTP settings** preference for a user who has a SOCKS proxy server selected in Internet Explorer.

• **Reverse proxy**
  This selection allows the Sametime Connect client to connect to a Sametime server over the Internet through a reverse proxy server. The reverse proxy server protects internal HTTP servers by providing a single point of access to the internal network. For information about using reverse proxy servers with Sametime servers, see the following topics:
  – Configuring mapping rules on a reverse proxy server to support Sametime
  – Configuring a Sametime server to operate with a reverse proxy server

• **HTTP Proxy**
  The client encases the standard Sametime protocol connection information within an HTTP request. Sametime Connect connects to the HTTP proxy, and the HTTP proxy server connects to the Community Services multiplexer on the Sametime server on behalf of the Sametime Connect client. The HTTP
connection to the Community Services multiplexer occurs on the "Community port" (default 1533) specified in the Sametime Connect client Sametime Connectivity settings.

The Community Services multiplexer on the Sametime server listens for HTTP connections on all ports specified in the Port number field under Client connections in the Community Services settings of the Sametime System Console and HTTP tunneled client connections in the Community Services settings of the Sametime System Console.

Follow these steps to select the Use proxy method for the client.

**Procedure**

1. From the Sametime Connect client, click **File > Preferences**.
2. Do one of the following:
   - To select this connection method for all server communities, click **Server Communities**. Under Global connection settings, click **Use proxy**.
   - To select this connection method for only one server community, click **Server Communities**, select the server community name, and open the **Connection** tab. Uncheck **Use global connection settings**, then click **Use proxy**.
3. Select the appropriate **Proxy type**.
   - **Use SOCKS4 proxy**
   - **Use SOCKS5 proxy**
   - **Use reverse proxy**
   - **Use HTTP proxy**
4. Fill in the additional values for the proxy type you selected.
   - **Use SOCKS4 proxy**
     a. Provide the **Host name** (DNS name or IP address) of the SOCKS proxy server and the port required to connect to the SOCKS proxy server.
   - **Use SOCKS5 proxy**
     a. Provide the **Host name** (DNS name or IP address) of the SOCKS proxy server and the port required to connect to the SOCKS proxy server.
     b. Specify the user name and password required for SOCKS5 authentication.
     c. Select the **Resolve server name locally** option to have the client resolve the Sametime Community server name by calling a local DNS server and passing the IP address to the SOCKS proxy server. If your organization, for security reasons, prohibits internal DNS servers from resolving the names of external servers, do not select the **Resolve server name locally** option. The SOCKS proxy resolves the external server name by calling a different DNS server instead, one that is not available on the internal network.
   - **Use reverse proxy**
     a. Specify the **URL** of the reverse proxy server. The clients uses this URL to access the reverse proxy server. The reverse proxy server handles requests from the client and redirects the request to the Sametime server
     b. Specify the **User name** and **Password** for authenticating with the reverse proxy server.
   - **Use HTTP proxy**
     a. Specify the **Host name** (DNS name or IP address) of the HTTP proxy server and the port required to connect to the HTTP proxy server
b. Specify the user name and password required for authentication to the HTTP proxy server if they are required.

5. Click **OK** to close the Preferences window.

**Related tasks**

“Connecting the client through Internet Explorer HTTP settings” on page 944

When a user starts the Sametime Connect client with the **Use my Internet Explorer HTTP settings** preference, the client examines the Internet Explorer Connection settings to determine how to connect to the Sametime Community server. If no proxy server is selected, the HTTP request goes to the Sametime Community server in a direct connection. If a proxy server is selected, the client connects through the appropriate SOCKS or HTTP proxy server.

“Configuring Sametime Community Server connectivity” on page 321

Define the host names and ports for Community Services on the IBM Sametime Community Server.

**Sametime client connectivity and reverse proxy servers:**

This section briefly discusses IBM Sametime client connectivity issues when the Sametime Meeting Room client, Sametime Recorded Meeting client, and Sametime Connect client operate with a reverse proxy server.

Client connectivity issues for reverse proxy servers are discussed in the following topics:

**Connecting to a Sametime server without using the reverse proxy server:**

When an IBM Sametime server is configured to operate with a reverse proxy server, users on the corporate intranet that are not required to route connections through the reverse proxy server can still connect using the standard Sametime client connection processes.

**Note:** In this scenario, both intranet and Internet users connect to the same Sametime server. Connections from Internet users are routed through the reverse proxy server while connections from intranet users are not routed through the reverse proxy server.

To configure a Sametime server to operate with a reverse proxy server, the administrator must select the **Enable Reverse Proxy Discovery on the client** setting in the Sametime Administration Tool. Selecting this setting:

- Enables the additional logic in the Meeting Room client, Recorded Meeting client, and Sametime Connect for browsers client that the clients use to connect to a Sametime server through a reverse proxy server.
- Does **not** disable the existing connectivity logic in these Sametime clients.

Enabling this setting enhances the existing logic in the Sametime clients by adding the reverse proxy connection logic to the existing logic. This design enables clients that do not connect to the Sametime server through the reverse proxy server to follow the standard Sametime client connection processes when connecting to the Sametime server.

To illustrate this point, the Meeting Room client connection process that occurs when the **Enable Reverse Proxy Discovery on the client** setting is selected is summarized below.

1. Upon loading in a user's web browser, the Sametime Meeting Room client attempts a direct TCP/IP connection to the Sametime server.
If the direct TCP/IP connection attempt fails, the Meeting Room client continues with the connection process as described below.

**Note:** Step 1 is part of the standard Sametime client connection process.

2. If the user’s web browser detects the existence of a forward SOCKS proxy server, the Meeting Room client will attempt the TCP/IP connection through the forward SOCKS proxy server to the Sametime server.

   If the TCP/IP connection through the SOCKS proxy server is not successful, the Meeting Room client continues with the connection process as described below.

   **Note:** Step 2 is part of the standard Sametime client connection process.

3. If the TCP/IP connection attempt is not successful, the Meeting Room client attempts to detect the reverse proxy server.

   If the reverse proxy server is detected, the Meeting Room client attempts to connect to the Sametime server through the reverse proxy server using HTTP tunneling. The client programatically detects the address of the reverse proxy server. No client-side configurations are required to enable the Sametime client to detect the reverse proxy server.

   **Note:** Step 3 represents the major difference in the connection process that occurs when the "Enable Reverse Proxy Discovery on the client" setting is selected.

4. If the reverse proxy server is not detected, the Sametime clients will still attempt to connect to the Sametime server using HTTP tunneling but the connection attempts will not be made to the reverse proxy server.

   **Note:** These HTTP-tunneled connection attempts are part of the standard Sametime client connection processes. These connection attempts enable Sametime clients that do not connect to the Sametime server through the reverse proxy server to establish HTTP-tunneled connections to the Sametime server.

**Understanding Sametime client connectivity through a reverse proxy server:**

This section provides additional notes about IBM Sametime client connectivity through a reverse proxy server.

Generally, there are no client-side configurations required to enable a Sametime Meeting Room client, Sametime Recorded Meeting client, or Sametime Connect for browsers client to connect to a Sametime server through a reverse proxy server.

If the administrator has selected the "Enable reverse proxy discovery on client" setting and specified the "Affinity ID" setting in the Sametime Administration Tool on the Sametime server, the Sametime clients should be able to programatically detect the presence of the reverse proxy server and connect to the Sametime server through the reverse proxy server.

If these clients must connect to the reverse proxy server through a forward (or client-side) HTTP or SOCKS proxy server, the connectivity settings (address and port) of the forward proxy server should be specified in the locations noted below:

- If the Sametime client runs in a web browser that operates with the Sun Microsystems Java Virtual Machine (1.4.2), the forward proxy server address and port are specified in the Sun Microsystems Java Plug-in Control Panel on the user’s machine. (The Java Plug-in Control Panel is available from the user’s Windows Control Panel).
• If the Sametime client runs in a web browser that operates with the native Microsoft Virtual Machine (VM), the forward proxy server address and port are specified in the proxy configuration settings of the web browser.

Note the following about using Sametime Connect for browsers with a reverse proxy server:
• The Sametime Connect for browsers client loads in the user's web browser with either the "Use my Java Plug-in settings" option or the "Use my Internet Explorer Browser settings" option selected by default in the Options-Preferences-Sametime Connectivity tab. User's should not change this default setting when operating with a reverse proxy server. These connectivity settings ensure the client will make either a direct connection to the Sametime server or connect through a forward proxy server if one is defined in the web browser connectivity settings or Java Plug-in as noted above.
• The Sametime Connect for browsers client includes a "Host name" and "Port" setting in the Options-Preferences-Sametime Connectivity tab. The values in these settings are ignored when the Sametime server is configured to operate with a reverse proxy server. (In a normal Sametime deployment, these settings specify the Host name of the Sametime server to which the client should connect and the port number on which the Sametime server listens for connections from Sametime Connect clients).

Setting client preferences
The following topics describe the different methods for setting preferences for the Sametime Connect client and the Sametime embedded client for Lotus Notes.

Selecting preferences in the client
In the Preferences dialog of the IBM Sametime Connect client and the Lotus Notes client, users can choose any Sametime preferences that have not been locked by the administrator.

About this task
Any preferences set using this method can be overwritten by Sametime policies. Preferences set using this method are stored in the end-user's profile directory either within an XML document or a .pref file.

Procedure
1. Log in to the client.
2. Click File > Preferences.
3. Click a feature in the list on the left.
4. Select the preferred behavior for that feature, and then click Apply.
5. Click OK.

Configuring client preferences using policies
You can use policies to configure and force IBM Sametime Connect client preferences. A client preference determined by a policy cannot be changed by the user and takes precedence over any other method used to set client preferences.

About this task
When a user authenticates, Sametime applies a policy for that user. You can create new policies that grant or limit access to features, and assign users to these policies. You can use the Sametime System Console to configure and manage
policies. For more information on Sametime policies, see Managing users with policies.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. Specify the features that you want to enable or disable for the users or groups that you will assign to this policy.

**Configuring Sametime Connect client preferences with the Expeditor managed settings framework**

You can configure and manage user preferences for IBM Sametime Connect clients using the Expeditor managed settings framework.

**About this task**

The Expeditor managed settings framework lets you set preference values on Sametime Connect clients. The Expeditor managed settings framework pulls preference settings from an associated back-end management system and pushes the settings to Sametime Connect clients. The framework also lets you designate read-only settings and schedule update intervals. When a setting is set as read-only, the user is prevented from changing the setting on the Sametime preference user interface.

The following topics explain how to configure and update settings using the Expeditor managed settings framework.

**Automatically updating client preferences with the managed-settings.xml file:**

When you use the Expeditor managed settings framework to create a managed-settings.xml file and post it to an update site, clients receive new or updated preferences automatically. The managed-settings.xml file is policy-based, so you can define different sets of preferences for different users. This method applies only to Sametime Connect clients. Settings for Sametime embedded clients for Lotus Notes are managed through the Domino desktop policy settings document instead.

**About this task**

Use a managed-settings.xml file to centrally manage and define preferences. At login time, the client receives policies then checks for the existence of the managed-settings.xml file according to the "Sametime update site URL" policy. For example, if the administration update site URL is http://example.com/updates, the client looks for updated preferences in http://example.com/updates/managed-settings.xml.

The managed-settings.xml file can override and control any client preference, including hidden configuration preferences and preferences in the client user interface. Many preferences can also be set as read-only by specifying a locked="true" attribute for the preference.

Follow these steps to create and post a managed-settings.xml file.
**Procedure**

1. Create a settings XML file and save it as `managed-settings.xml`.
3. Post the file to the policy-configured administration update site URL.

**Results**

Changes take effect the next time the user starts Sametime. Settings found in the `managed-settings.xml` take precedence over matching settings in the `plugin_customization.ini` file.

**What to do next**

To test changes in a `managed-settings.xml` file, create a policy set that includes the administration update site URL and place the .xml file in the location specified by the update site URL. Apply the policy to yourself and log in to the client to verify the preferences.

You can also enable logging of the managed settings to help debug problems. To enable logging for the handling of the remote `managed-settings.xml` file, set the following log level in the `user.home/Lotus/Sametime/.config/rcpinstall.properties` file:

```
com.ibm.collaboration.realtime.policy.sametime.managedsettings.level=FINEST
```

**Related concepts**

“Logging and tracing on Sametime Connect” on page 1185

IBM Sametime Connect users can enable tracing on their clients.

**Related tasks**

“Configuring preferences for the Sametime embedded client for Lotus Notes” on page 956

To configure preferences for clients running the Sametime embedded client for Lotus Notes, you may use the Domino desktop policy settings document.

**Defining preferences in the settings XML file:**

Follow these instructions to define preferences in a settings file that will be posted to an update site or included in a `plugin_customization.ini` file.

**Procedure**

Format the XML file using these parameters:

- It must contain a `<ManagedSettings>` element that contains one or more `<settingGroup>` elements. Each `<settingGroup>` element must contain one or more `<setting>` elements.
- Each `<settingGroup>` tag must have the following attributes:
  - `name` – Use the same name as the qualifier (typically plugin name, but it can be anything) that its settings are associated with.
  - `lastModDate` – Optional timestamp specifying the date using the `java.text.SimpleDateFormat` format. The syntax is `YYYYMMDDThhmmssZ`, where `YYYY=year, MM=month, DD=day, hh=hours, mm=minutes, ss=seconds`. The values following the `T` are optional. If used, every change to a setting group must be accompanied by a change to the `lastModDate` attribute or the new...
values will not be updated. If no lastModDate is specified, the values are always updated, even if they are not new.

- Each `<setting>` tag must have the following attributes:
  - `name` – Use a name that identifies what the setting does.
  - `value` – Provide a default value for the setting.

- Each `<setting>` tag can have the following optional attributes:
  - `isLocked` – Boolean. The default value is true. If true, the setting is read-only and any changes that a user or application make to the value set by you, the administrator, are prevented or later overwritten. If this attribute is set to false, the administrator's setting is treated as a default value that can be changed.
  - `overwriteUnlocked` - Boolean. The default value is false. By default, a setting that is specified as being unlocked will be treated as a default and will not overwrite any existing value on the client. This is to avoid undoing changes that the user might have legitimately made. However, if this setting is set to true, the unlocked value will be overwritten with this new value even if it means clearing the user's existing value.
  - `restartRequired` - Boolean. The default value is false. This attribute applies only when you automatically update client preferences with the managed-settings.xml file. Setting this to true creates a user prompt to restart the client as soon as the managed setting is applied. Use this optional attribute only if a restart of the client is required to activate the preference. The restart occurs only if the setting that includes this attribute is updated.

Example

Here is an example of a formatted XML file:

```xml
<ManagedSettings>
  <settingGroup name="com.ibm.collaboration.realtime.chat.logging">
    <setting name="logging.enabled" value="false" isLocked="false"/>
    <setting name="logging.service" value="7" isLocked="false"/>
    <setting name="root.location" value="C:\work" isLocked="true"/>
    <setting name="save.file.location" value="C:\temp" isLocked="true"/>
  </settingGroup>
</ManagedSettings>
```

Related tasks

“Automatically updating client preferences with the managed-settings.xml file” on page 951

When you use the Expeditor managed settings framework to create a managed-settings.xml file and post it to an update site, clients receive new or updated preferences automatically. The managed-settings.xml file is policy-based, so you can define different sets of preferences for different users. This method applies only to Sametime Connect clients. Settings for Sametime embedded clients for Lotus Notes are managed through the Domino desktop policy settings document instead.

“Configuring Sametime Connect client preferences in the plugin_customization.ini file” on page 955

Defining a settings file in the plugin_customization.ini file is an alternate method for distributing preferences to Sametime Connect clients. Unlike the managed-settings.xml file posted on an update site, this method does not provide any policy-based distribution of preferences.

Changing the update interval for managed preferences:
If you want to change the update interval for managed preferences, you can update the existing settings XML file.

**About this task**

By default, managed settings are updated every 720 minutes (12 hours) and whenever the Sametime Connect client is started. To change the update interval, edit the settings XML file to add a new setting group.

**Procedure**

Update the existing XML file with a new setting group that contains an `UpdateIntervalInMinutes` setting.

```xml
<settingGroup name="com.ibm.rcp.managedsettings">
  <setting name="UpdateIntervalInMinutes" value="1" isLocked="false"/>
</settingGroup>
```

**Results**

Updating settings has the following results:

- All unlocked settings can be modified by the user. Once a setting is modified by the user, any subsequent update to the same setting will not apply unless the setting is changed to `isLocked=true` on the settings XML file. This behavior is consistent with settings changed with the `plugin_customization.ini` file. User-modified preferences take precedence over settings from the `plugin_customization.ini` file and settings XML file. However, if the user's workspace is cleaned, the administrator's values will apply.

- Any settings or setting groups removed from the settings XML file (for example, to unmanage those settings) will remain on the client, and if the setting was previously locked, it will be automatically set to unlocked.

- All unmanaged settings will automatically be managed as standard preferences.

**Discontinuing managed preferences:**

To stop setting preferences through the Expeditor managed settings framework, remove the reference to the settings XML file and unlock any previously read-only settings.

**About this task**

Discontinue use of the settings.xml file based on the method you used to distribute managed preferences.

**Managed-settings.xml file and an administration update site URL**

Remove the managed-settings.xml file from the update site location.

**Settings.xml file and a plugin_customization.ini file**

Remove the `com.ibm.rcp.managedsettings.provider.file/URL` setting from the `plugin_customization.ini` file and provision the updated file to clients.

**Note:** Managed settings that were previously pushed to the clients as read-only will continue to be managed this way unless the managed settings are removed from the client.
Procedure

Unlock all managed settings by editing the XML file:
1. Change all "isLocked=true" instances to "isLocked=false".
2. If the lastModDate attribute was used previously, change the lastModDate attribute to a newer timestamp for all group settings. Otherwise, skip this step.
3. Provision the updated XML file to the client.

Configuring Sametime Connect client preferences in the plugin_customization.ini file:

Defining a settings file in the plugin_customization.ini file is an alternate method for distributing preferences to Sametime Connect clients. Unlike the managed-settings.xml file posted on an update site, this method does not provide any policy-based distribution of preferences.

About this task

Follow these steps to create a settings XML file and define it in the plugin_customization.ini file.

Procedure

1. Create a settings XML file with a name such as settings.xml or mysettings.xml.
3. Copy the settings XML file to the location where it will be called from the plugin_customization.ini file.
4. You can update the plugin_customization.ini file in the install/deploy/ directory on a CD-structure or provision the setting using the method described in TechNote 1261055.
5. Add a key that defines the Expeditor Managed settings framework com.ibm.rcp.managedsettings.provider.file/URL and the name and location of the settings XML file to be used. For example:
   or
   com.ibm.rcp.managedsettings.provider.file/URL=file://c:/data/mysettings.xml
6. Save the file and make it available to clients.

Results

Every time the client starts, the plugin_customization.ini preferences are read.
Related tasks

“Defining preferences in the settings XML file” on page 952
Follow these instructions to define preferences in a settings file that will be posted to an update site or included in a plugin_customization.ini file.
“Changing the update interval for managed preferences” on page 953
If you want to change the update interval for managed preferences, you can update the existing settings XML file.
“Discontinuing managed preferences” on page 954
To stop setting preferences through the Expeditor managed settings framework, remove the reference to the settings XML file and unlock any previously read-only settings.

Changing the URL for the settings XML file in the plugin_customization.ini file:

If you must change the URL for the managed settings file, do so by updating the plugin_customization.ini file.

About this task

Follow these steps to update the plugin_customization.ini file with the new file name or URL.

Procedure

1. Verify that the settings XML file is in the location where it will be called from the plugin_customization.ini file.
2. In the plugin_customization.ini file, change the key that defines the Expeditor Managed settings framework and the name and location of the settings XML file.com.ibm.rcp.managedsettings.provider.file/URL and the name and location of the settings XML file to be used. For example:
   or
   com.ibm.rcp.managedsettings.provider.file/URL=file://c:/data/newsettings.xml

Results

The next update runs with the old URL, but subsequent updates run with the new URL. If the new URL is not reachable at the time of the update, the setting will not be saved and the original URL will continue to be used. The URL will not be changed until it is updated at a time that the URL can be reached.

Configuring preferences for the Sametime embedded client for Lotus Notes

To configure preferences for clients running the Sametime embedded client for Lotus Notes, you may use the Domino desktop policy settings document.

About this task

The Domino desktop policy settings document Custom Settings tab contains a Managed Settings option, through which you can define preferences.
Related information

- Pushing Eclipse preference settings to Notes clients
- Creating a desktop policy settings document

**Sametime client preferences**

This section lists the preferences that can be managed for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

**Accessibility preferences:**

The following table lists the accessibility preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>useAcc</td>
<td>Boolean</td>
<td>Specifies whether or not to optimize chat transcript for screen readers (will replace the transcript with a different format).</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>optimizeAlerts</td>
<td>Boolean</td>
<td>Specifies whether or not to optimize notification settings for screen readers (will turn off bring to front, flash window, turn on sounds).</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>useLessVerbose</td>
<td>Boolean</td>
<td>Specifies whether or not to set less verbose messages for screen readers (less verbose will not read status change events and typing events in the chat window).</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>useArrowKeyForQuickFind</td>
<td>Boolean</td>
<td>Specifies whether to use the arrow key for quick find.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>useSystemColor</td>
<td>Boolean</td>
<td>Specifies whether to use the system color.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

**Auto-status change preferences:**

The following table lists the auto-status change preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>lockPCWithOSLock</td>
<td>Boolean</td>
<td>Available &quot;Locking computer with operating system lock&quot; feature.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>keyboardMouseInactivity</td>
<td>Boolean</td>
<td>Available &quot;Keyboard and mouse inactivity&quot; feature.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>whenIamInAOnlineMtg</td>
<td>Boolean</td>
<td>Available &quot;When I am in an online meeting&quot; feature.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>selectStatusOnlyScreenShare</td>
<td>Boolean</td>
<td>Determines whether to select the &quot;Change my status only when I'm sharing my screen&quot; check box.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>autoChangeMyStatusInMtg</td>
<td>Boolean</td>
<td>Determines whether to select the &quot;Automatically change my status&quot; radio button. Note that if this radio button is set as true, then the &quot;Prompt me before changing my status&quot; radio button will be unavailable. If this is set as &quot;false&quot;, the &quot;Prompt me before changing my status&quot; radio button will be available. After com.ibm.collaboration.realtime.imhub/selectStatusOnlyScreenShare is set as true, com.ibm.collaboration.realtime.imhub/autoChangeMyStatusInMtg works for screen share status.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>minutesForIdleKeyboardMouse</td>
<td>Integer</td>
<td>Sets the &quot;When I have not used my keyboard or mouse for the following number of minutes:&quot; text field.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>backWhenUnlocked</td>
<td>Boolean</td>
<td>Determines whether to select the &quot;Return to previous status when activity is resumed&quot; in &quot;Locking computer with operating system lock&quot; check box.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 92. Auto-status-Change Preferences - com.ibm.collaboration.realtime.imhub release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>backWhenKeyboardMouseActive</td>
<td>Boolean. Default is true.</td>
<td>Determine whether to select the &quot;Return to previous status when activity is resumed&quot; in &quot;Keyboard and mouse inactivity&quot; check box.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

Calendar preferences:

The following table lists the calendar preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 93. Calendar Preferences - com.ibm.collaboration.realtime.calendar release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>alertMeWhenMeetingStarts</td>
<td>Boolean</td>
<td>In Auto-Status Changes for Meetings scheduled in my calendar, specify whether to alert user when user has a meeting scheduled in the calendar.</td>
<td>8.5.1.1 and later</td>
</tr>
<tr>
<td>enabled</td>
<td>Boolean</td>
<td>Specify whether or not to enable auto status change for meetings scheduled in user's calendar.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>promptMe</td>
<td>Boolean</td>
<td>In Auto-Status Changes for meetings scheduled in my calendar, specify whether to prompt user before changing the status when user have a meeting scheduled in the calendar.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>statusMsg</td>
<td>String</td>
<td>In Auto-Status Changes for meetings scheduled in my calendar, specify the status message when user select &quot;Automatically change my status.&quot;</td>
<td>8.0 and later</td>
</tr>
</tbody>
</table>
### Table 93. Calendar Preferences - com.ibm.collaboration.realtime.calendar release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>setback</td>
<td>Boolean</td>
<td>In Auto-Status Changes for meetings scheduled in my calendar, specify whether to return to user's previous status when the meeting is over.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>outlook_enabled</td>
<td>Boolean</td>
<td>In Calendar Service page, specify whether to check Outlook calendar for meetings to allow auto status changes. It's valid only if the Outlook service is available.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>notes_enabled</td>
<td>Boolean</td>
<td>In Calendar Service page, specify whether to check Lotus Notes calendar for meetings to allow auto status changes. It's valid only if the Notes service is available.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>interval</td>
<td>Positive integer</td>
<td>value, unit is minutes. 10 minutes is the default.</td>
<td>In Calendar Service page, specify the interval that Sametime retrieves calendar information for an auto-status change. This value is not for the interval to update auto-status.</td>
</tr>
</tbody>
</table>

### Chat preferences:

The following tables list the chat preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.
### Table 94. Application Preferences - `com.ibm.collaboration.realtime.application` release 8.5.1.1 and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableNwayRichText</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether or not to enable the client to support rich text in a multi-user chat. Rich text is enabled in a multi-user chat session only if all clients participating in the chat session have this setting enabled.</td>
<td>8.5.1.1 and later</td>
</tr>
</tbody>
</table>

### Table 95. Chat History Preferences - `com.ibm.collaboration.realtime.chat.logging` release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>days.storage.max</td>
<td>A positive number.</td>
<td>Delete saved transcripts after this number of days. This setting will be overwritten by the value set on the server policy.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>delete.old</td>
<td>A positive number.</td>
<td>Delete saved transcript. This setting will be overwritten by the value set on the server policy.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logging.default</td>
<td>0 = Automatically save chats, 1 = Do not automatically save chats, 2 = Prompt me to save chats</td>
<td>Default chat logging action</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logging.enabled</td>
<td>Boolean. Default is false.</td>
<td>Specify whether or not to enable saving chat. If server policy is not configured to allow save chat, this setting will be ignored.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logging.service</td>
<td>service.notes = Lotus Notes logging, service.outlook = MS Outlook logging, service.file = File system logging</td>
<td>Type of chat logging service</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>display.context</td>
<td>True = Display, false = Do not display</td>
<td>Display the saved transcript between two users for the current day in the chat window.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 95. Chat History Preferences - `com.ibm.collaboration.realtime.chat.logging` release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>display.context.background</td>
<td>true = Display, false = Do not display</td>
<td>Display background highlighting when displaying saved transcripts in chats.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>root.location</td>
<td>A string of a valid path on the computer.</td>
<td>Location for automatically saved chats Directory path. Do not use ‘\’ as the file separator. Use ‘\’ or ‘/’ instead. Example using absolute path: <code>com.ibm.collaboration.realtime.chat.logging/ root.location= C:\\Documents\\user\\ SametimeTranscripts</code> Releases 8.0.2 and later support the use of a relative path. Example using a path relative to the user profile folder for Windows and Mac: <code>com.ibm.collaboration.realtime.chat.logging/ root.location= \SametimeTranscripts</code> For Linux, <code>com.ibm.collaboration.realtime.chat.logging/ root.location= SametimeTranscripts</code></td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 95. Chat History Preferences - com.ibm.collaboration.realtime.chat.logging  release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
</table>
| save.file.location     | A string of a valid path on the computer. | Default location for manually saved chats. Do not use '\\' as the file separator. Use '\\' or '/' instead. Example using absolute path: com.ibm.collaboration.realtime.chat.logging/ave.file.location=C:\Documents\user\SavedChats
Releases 8.0.2 and later support the use of a relative path. Example using a path relative to the user profile folder for Windows and Mac: com.ibm.collaboration.realtime.chat.logging/root.location=\SametimeTranscripts
For Linux, com.ibm.collaboration.realtime.chat.logging/root.location=SametimeTranscripts | 7.5.1 and later |
| prompt.save            | Boolean       | If using mail service for logging, specify whether to display a confirmation after manually saving chats to the mail file.                                                                                 | 7.5.1 and later |
| reset.user.resets.logging.prefs | Boolean. Default is false. | Specify whether to prompt user to reset logging preferences after resetting user.                                                                                                                         | 7.5.1 and later |
| firsthand.askprefs      | Boolean. Default is true. | Specify whether to prompt user to set logging preferences when Sametime launched for the first time. When the value is set to true, logging.enabled should also be set to define the default enablement state for saving chat transcripts. | 7.5.1 and later |

Table 96. Chat History UI Preferences - com.ibm.collaboration.realtime.chat.logging.ui release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowSaveOverride</td>
<td>Boolean</td>
<td>Specifies whether to show menu item &quot;Prevent Transcript save&quot; in chat window Tools menu</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 96. Chat History UI Preferences - com.ibm.collaboration.realtime.chat.logging.ui
release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>noPersonListLiveNames</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether to use Live Names in the chat history viewer person list.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

Table 97. Chat Window Preferences - com.ibm.collaboration.realtime.chatwindow release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>showuserinfo</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to display the business card in the chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showtimestamp</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to display timestamps in the chat transcript area.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showdatestamp</td>
<td>Boolean.</td>
<td>Specifies whether or not to display date stamps in the chat transcript area.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showemoticons</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to display emoticons in the chat transcript.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>usemyfont</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether or not to override chat partner’s font settings with my own.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>entersend</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not Enter is used to send a message or Shift+Enter. Enter sends, Shift+Enter newline</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showstatusupdates</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether or not to display status updates for my chat partner in the transcript.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>esccloses</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not ESC closes the chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showuserleft</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether or not to display a message when my chat partner closes their chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>warnWhenInMtg</td>
<td>Boolean</td>
<td>Specifies whether or not to pop a warning message when I try to open a chat window when a person is in a meeting.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>warnWhenAway</td>
<td>Boolean</td>
<td>Specifies whether or not to pop a warning message when I try to open a chat window when a person is away.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>dontPopWhenMin</td>
<td>Boolean</td>
<td>Specifies whether or not the chat window pops to the front when I manually minimize the window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showActionBar</td>
<td>Boolean</td>
<td>Specifies whether or not to show the top actions toolbar.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showStatusBar</td>
<td>Boolean</td>
<td>Specifies whether or not to show the status message bar at the bottom.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showToolsBar</td>
<td>Boolean</td>
<td>Specifies whether or not to show the message tools bar above the typing area.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showSendButton</td>
<td>Boolean</td>
<td>Specifies whether or not to show send button in the chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showQuickFind</td>
<td>Boolean</td>
<td>Specifies whether or not to show quick find in the tabbed chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>useTabs</td>
<td>Boolean</td>
<td>Specifies whether or not to use a single tabbed window for all chats.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>horizontalTabs</td>
<td>Boolean</td>
<td>Specifies whether to use horizontal or vertical tabs. Does not apply unless useTabs is true.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>warnNewMessageArrived</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to pop a message dialog when I try to close the window at the same time I am receiving a message.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>warnNewMessageArrivedThreshhold</td>
<td>Long. Default is 450.</td>
<td>It is used in conjunction with the warnNewMessageArrived preference. When warnNewMessageArrived is true, if set this to 10000 (10 seconds) and try to close chat window 5 seconds after the last message, the warning dialog will pop up. It is not recommended to change the default value.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>useDefaultGO</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to use the system's default orientation for typing or to manually set one.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>sendAreaGO</td>
<td>Integer.</td>
<td>Specifies which orientation to use in the typing area if useDefaultGO is false. Not set by default because useDefaultGO is true. Only accepts two values, 67108864 (SWT.RIGHT_TO_LEFT) or 33554432 (SWT.LEFT_TO_RIGHT)</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>timeformat</td>
<td>Integer. Default is 12.</td>
<td>Specifies the default time format to use (12 or 24 hour clock).</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>maxChatsShowWarn</td>
<td>Boolean</td>
<td>If using tabbed window, specifies whether or not to show a warning dialog when current chat count exceeds the predefined value.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>maxChats</td>
<td>Integer. Default is 50.</td>
<td>Specifies a predefined value for maxChatsShowWarn</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>saveChats</td>
<td>Boolean</td>
<td>Specifies whether or not to save opened chats across sessions.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>transcript.view.limit</td>
<td>Integer. Default is 0.</td>
<td>Specifies a limit to the number of text/graphics lines that are maintained in the chat window (upper window). Setting to 0 means no limit.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>ProvideTabbedBrowserCache</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether when using tabbed chats if the browser window can be cached to improve memory when the chat is not active.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>persistPosition</td>
<td>Boolean</td>
<td>Specify whether to remember the position of normal chat window (does not apply to tabbed or multiple parties chat). If it is set, the chat window position is remembered each time on window close action and used as the default location for next chat window open action.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>xpos</td>
<td>Integer</td>
<td>Specify the X value of chat window position.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>ypos</td>
<td>Integer</td>
<td>Specify the Y value of chat window position.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 97. Chat Window Preferences - com.ibm.collaboration.realtime.chatwindow release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>windowWidth</td>
<td>Integer</td>
<td>Specify the width of chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>windowHeight</td>
<td>Integer</td>
<td>Specify the height of chat window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>sendAreaHeight</td>
<td>Integer</td>
<td>Specify the height of the input box of chat window.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

Table 98. RTC Adapter Plugin Preferences - com.ibm.collaboration.realtime.rtcadapter release 8.5.2 and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>disableRichText</td>
<td>Boolean</td>
<td>Specifies whether or not to disable rich text for all chats.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>disableRichTextWithAnon</td>
<td>Boolean</td>
<td>Specifies whether or not to disable rich text for chats with anonymous users.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

Community preferences:

The following table lists the community preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 99. Community Preferences - com.ibm.collaboration.realtime.community release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>kioskMode</td>
<td>Boolean</td>
<td>Sets whether or not the client will function in kiosk mode.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logoutWhenIdle</td>
<td>Boolean</td>
<td>Sets the initial value of whether or not the client logs out when idle. This pref will only take effect for new Sametime users with no previous workspace. For any existing user, this pref will be overridden to &quot;false&quot; when the autostatus settings are retrieved from the server since the pref did not exist prior to release 8.0.1.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>logoutWhenIdleOverride</td>
<td>Boolean</td>
<td>Provides a mechanism for an admin to override the user's logoutWhenIdle setting. If set to true, then the client will always logout when idle, and the user will not be able to change the value in the UI.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logoutWhenLocked</td>
<td>Boolean</td>
<td>Sets the initial value of whether or not the client logs out when locked. This pref will take effect for new Sametime users with no previous workspace. For any existing user, this pref will be overridden to 'false' when the autostatus settings are retrieved from the server since the pref did not exist prior to release 8.0.1.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>logoutWhenLockedOverride</td>
<td>Boolean</td>
<td>Provides a mechanism for an admin to override the user's logoutWhenLocked setting. If set to true, then the client will always logout when locked, and the user will not be able to change the value in the UI.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>tokenLoginOnly</td>
<td>Boolean</td>
<td>Specifies the whether or not to force login by token for the default community. Part of login extensibility (see Sametime 801 SDK). Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Specifies the initial community host value. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>useAuthServer</td>
<td>Boolean</td>
<td>Specifies the initial useAuthServer value for the default community. Part of login extensibility (see Sametime 801 SDK). Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>authServerUrl</td>
<td>String</td>
<td>Specifies the initial authentication server URL value for the default community. Part of login extensibility (see Sametime 801 SDK). Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>defaultAuthType</td>
<td>String</td>
<td>Specifies the authentication type for the default community. Part of login extensibility (see Sametime 801 SDK). Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>keepAlive</td>
<td>Boolean. Default is true</td>
<td>Specifies the initial keep alive value. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>keepAliveInterval</td>
<td>Integer. Default is 60</td>
<td>Specifies the initial keep alive interval value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>loginByToken</td>
<td>Boolean</td>
<td>Specifies the initial loginByToken value for the default community. Part of login extensibility (see Sametime 801 SDK). Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Specifies the initial name for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>port</td>
<td>Integer. Default is 1533</td>
<td>Specifies the initial community port value. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
### Table 99. Community Preferences - com.ibm.collaboration.realtime.community release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>savePassword</td>
<td>Boolean</td>
<td>Specifies the initial savePassword value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>connectionType</td>
<td>String</td>
<td>Specifies the initial connectionType value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>proxyHost</td>
<td>String</td>
<td>Specifies the initial proxy host value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>proxyPort</td>
<td>Integer</td>
<td>Specifies the initial proxy port value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>proxyUserName</td>
<td>String</td>
<td>Specifies the initial proxy user name for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>proxyPassword</td>
<td>String</td>
<td>Specifies the initial proxy password for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>proxyResolvesLocally</td>
<td>Boolean</td>
<td>Specifies the initial proxyResolvesLocally value for the default community. Must be set prior to client launch.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>loginTokenRefreshInterval</td>
<td>Integer</td>
<td>Specifies the login token refresh interval in milliseconds. The default is 900000, or 15 minutes.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>

### Contact list preferences:

The following table lists the contact list preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>sortGroups</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to alphabetically sort groups in the contact list.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>sortContacts</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to alphabetically sort contacts in the contact list.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysEditStatusMsgActive</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to always edit the status message when changing status to available.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysEditStatusMsgAway</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to always edit the status message when changing status to away.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysEditStatusMsgInMtg</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to always edit the status message when changing status to in a meeting.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysEditStatusMsgDnd</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to always edit the status message when changing status to in a do not disturb.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showActionToolBar</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to show the action toolbar in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showStatusBar</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to show the status bar in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showQuickFind</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to show quick find in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>flashAddedContacts</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to flash newly added contacts.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showAddDialogSuccess</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to open a confirmation dialog after a contact has been added.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showAddGroupSuccess</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to open a confirmation dialog after a group has been added.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>showAddPartnerSuccess</td>
<td>Boolean</td>
<td>Specifies whether by default to open a confirmation dialog after a chat partner has been added (through add button in chat window).</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>autoSyncDefaultCommunityBuddyList</td>
<td>Boolean</td>
<td>Specifies whether by default to synchronize the 7.5 XML buddylist with the previous pre 7.5 contact list used by older clients. Windows only.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>launchAtStartup</td>
<td>Boolean</td>
<td>Specifies whether or not to launch Sametime at system startup. The preference is valid only for standalone and windows platform. If the preference is set it in plugin_customization.ini or managed preferences framework, it does not work for the first launch of the Sametime client.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>hideWhenMinimized</td>
<td>Boolean</td>
<td>Specifies whether by default to hide the contact list window when minimized. The preference is valid only for the Sametime Connect client for Microsoft Windows.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showCommunityIconBackground</td>
<td>Boolean</td>
<td>Specifies whether by default to show the community icon behind the contacts.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>statusImgBackgroundTransparency</td>
<td>Integer</td>
<td>Specifies the transparency of the community background image. 0 is very prominent, 100 is completely transparent.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showHoverBizCard</td>
<td>Boolean</td>
<td>Specifies whether or not to show the business card when hovering over contacts.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>hideContactsWhenOffline</td>
<td>Boolean</td>
<td>Specifies whether or not to hide the contact list tree when offline.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>showBuddyListConflictDialog</td>
<td>Boolean</td>
<td>Specifies whether or not to show the contact list conflict dialog when synchronizing the remote contact list.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>buddyListConflictPref</td>
<td>String</td>
<td>Specifies the default behavior to follow in case of a remote/local synchronization conflict. Options include &quot;merge&quot;, &quot;keepLocal&quot;, and &quot;replaceLocal&quot;.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>warnWhenWatchLimitExceeded</td>
<td>Boolean</td>
<td>When the watch limit is in effect, specifies whether or not to warn user when the number of contacts that can be monitored is exceeded</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>warnWhenContactLimitExceeded</td>
<td>Boolean</td>
<td>When &quot;LimitContactListSize&quot; policy is set, specifies whether or not to warn user when the contact list is approaching the maximum number allowed.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showShortNames</td>
<td>Boolean</td>
<td>Specifies whether or not to show short names for contact list.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysOnTop</td>
<td>Boolean</td>
<td>Specifies whether or not to make the contact list window always on top.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showOnlineOnly</td>
<td>Boolean</td>
<td>Specifies whether or not to show online contacts only in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showStatusToolBar</td>
<td>Boolean</td>
<td>Specifies whether or not to show My Status ToolBar in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showContactList</td>
<td>Boolean</td>
<td>Specifies whether or not to show the contact list in the contact list window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>confirmMultiPartyChatInvitationToMoreThanX</td>
<td>Boolean</td>
<td>Specifies whether or not to confirm when users start events with groups larger than a specified number of people. The number value is specified by confirmMultiPartyChatInvitationToMoreThanXNumber.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>confirmMultiPartyChatInvitationToMoreThanXNumber</td>
<td>Integer</td>
<td>Specifies a limit number. See confirmMultiPartyChatInvitationToMoreThanX.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>launchMinimized</td>
<td>Boolean</td>
<td>Specifies whether or not to minimize Sametime when launching. It's valid only for standalone and windows platform.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>limitPublicGroupSubscriptions</td>
<td>Boolean. Default is true.</td>
<td>Takes contact list size of public groups into account to calculate the contact list size limit. The default value is true, which means that users cannot add a public group to their contact lists if doing so exceeds the contact list size. If users already have public groups in their contact lists, this preference causes the client to subscribe to each group in the list, from smallest to largest, until the limit is reached. Any other groups left in the contact list are shown as unsubscribed groups. Disabling a group subscription causes the client to add as many groups from the unsubscribed list as it can until the contact list size is reached again. Setting the value to false does not include the contact list size of public groups to calculate the contact list size limit.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>


Table 100. Contact List Preferences - com.ibm.collaboration.realtime.imhub release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxPublicGroupSize</td>
<td>Integer</td>
<td>The maximum number of contacts a public group can have that allows users to subscribe to it. Groups that exceed this size cannot be added to the contact list. If the group already exists in the contact list, users cannot subscribe to the group. You can set this preference when the <code>limitPublicGroupSubscriptions</code> preference is enabled.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>excludedPublicGroups</td>
<td>String</td>
<td>A comma-delimited list of public group names that should not be subscribed to (for example, <code>employees_Active,employees_All</code>). Groups in this list cannot be added to the contact list. If the group already exists in the contact list, users cannot subscribe to the group. You can set this preference when the <code>limitPublicGroupSubscriptions</code> preference is enabled.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

External application preferences:

The following table lists the external application preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 101. External application Preferences - com.ibm.collaboration.realtime.ui release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>external.application.use.default.mail</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or to use default mail program for email.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>AllowEMailFunction</td>
<td>Boolean. Default is true.</td>
<td>Provides a mechanism for disable/enable the mail function entries. If set to true, user can use mail function in Sametime client; if set to false, the menu(toolbar about mail function will be disabled.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>external.application.use.custom.browser</td>
<td>Boolean</td>
<td>Specifies whether or not to use a custom browser on Linux.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
### External application Preferences

#### Table 101. External application Preferences - com.ibm.collaboration.realtime.ui release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>external.application.use.custom.mail</td>
<td>Boolean</td>
<td>Specifies whether or not to use a custom mail application on Linux.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>external.custom.browser</td>
<td>String</td>
<td>Specifies the custom browser on Linux.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>external.application.mail</td>
<td>String. &quot;System Default&quot;, &quot;Lotus Notes&quot;, &quot;Evolution&quot;, &quot;KMail&quot; and &quot;Thunderbird&quot; on Linux. &quot;Lotus Notes&quot;, &quot;Outlook Express&quot; and other available mail applications on Windows.</td>
<td>Specifies the default mail application.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>external.application.use.default.mail</td>
<td>Boolean</td>
<td>Specifies whether or not to use default mail application.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>external.custom.mail</td>
<td>String</td>
<td>Specifies the user mail application on Linux.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>disableHostnameWarning</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether or not to validate that the server name is a fully qualified domain name.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>

#### File transfer preferences:

The following table lists the file transfer preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

#### Table 102. File Transfer Preferences - com.ibm.collaboration.realtime.filetransfer release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowTransferToAnonymous</td>
<td>Boolean</td>
<td>Specifies whether or not to disable file transfers to anonymous users. Setting the value to true does not prevent incoming file transfers from anonymous users.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>
Table 102. File Transfer Preferences - com.ibm.collaboration.realtime.filetransfer release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>saveFileLocation</td>
<td>A text string of a valid full path to a folder on the user's computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the path on the user's computer where files from File Transfers will be saved. Do not use '' as the file separator. Use '' or '/' instead. Example using absolute path: com.ibm.collaboration.realtime.filetransfer/saveFileLocation=C:\Documents\user\SametimeFileTransfer</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Releases 8.0.2 and later support the use of a relative path. Example using a path relative to the user profile folder for Windows and Mac: com.ibm.collaboration.realtime.filetransfer/saveFileLocation=\SametimeFileTransfer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Linux, com.ibm.collaboration.realtime.filetransfer/saveFileLocation=SametimeFileTransfer</td>
<td></td>
</tr>
</tbody>
</table>

Live Text and Widgets preferences:

The following scenarios show the Live Text and Widgets preferences for the IBM Sametime Connect client. These scenarios apply to setting preferences for the stand-alone client.

For instructions about configuring Live Text and Widgets for the Sametime embedded client for Lotus Notes, see Controlling Widgets and Live Text access using Domino policy in the Lotus Notes information center.

Case 1 (default): Disable both Live Text and Widgets

This is the default scenario, set with the following preference in plugin_customization.ini:

com.ibm.rcp.toolbox.admin/toolboxvisibleMaster=false

Case 2: Enable both Live Text and Widgets

Enable both Live Text and Widgets by setting the following preference to true in plugin_customization.ini:

com.ibm.collaboration.realtime/enableSametimeLiveText=true

Note: This overrides the setting for toolboxvisibleMaster. You do not need to manually set toolboxvisibleMaster to true.

Case 3: Enable only Live Text, not Widgets
To enable only Live Text, managed preferences is required. Configure the following managed preferences:

```xml
<ManagedSettings>
  <settingGroup name="com.ibm.collaboration.realtime">
    <!-- Enable live text support in Sametime -->
    <setting name="enableSametimeLiveText" value="true" isLocked="false"/>
  </settingGroup>
  <settingGroup name="com.ibm.rcp.toolbox.admin">
    <!-- Disable widget support in Sametime -->
    <setting name="toolboxvisible" value="false" isLocked="true"/>
    <setting name="toolboxenableRecognizers" value="true" isLocked="true"/>
  </settingGroup>
</ManagedSettings>
```

Case 4: Enable only Widgets, not Live Text

To enable only Widgets but not Live Text, managed preferences are required. Configure the following managed preferences:

```xml
<ManagedSettings>
  <settingGroup name="com.ibm.collaboration.realtime">
    <!-- Disable live text support in Sametime -->
    <setting name="enableSametimeLiveText" value="false" isLocked="false"/>
  </settingGroup>
  <settingGroup name="com.ibm.rcp.toolbox.admin">
    <!-- Enable widget support in Sametime -->
    <setting name="toolboxvisible" value="true" isLocked="true"/>
    <setting name="toolboxenableRecognizers" value="false" isLocked="true"/>
  </settingGroup>
</ManagedSettings>
```

Location preferences:

The following table lists the location preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>manualModeSelected</td>
<td>Boolean</td>
<td>Specifies whether or not to detect location changes automatically.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>manualModeVisible</td>
<td>Boolean</td>
<td>Specifies whether the check box 'Do not automatically detect location changes' is visible.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>optIn</td>
<td>Boolean</td>
<td>Specifies whether or not to share user's location information with other users.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>advancedView</td>
<td>Boolean</td>
<td>Specifies whether or not to show the advanced view for Location.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
### Table 103. Location Preferences - com.ibm.collaboration.realtime.location release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>showProfWindow</td>
<td>Boolean</td>
<td>Toggle for do not show the alert for editing location settings at location change again.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

### Login preferences:

The following table lists the login preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

### Table 104. Login Preferences - com.ibm.collaboration.realtime.login release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableAutoReconnect</td>
<td>Boolean</td>
<td>Specifies whether or not to enable automatic re-connection to the Sametime server in case the client is inadvertently disconnected.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>autoReconnectAttemptInterval</td>
<td>long</td>
<td>Specifies the interval in milliseconds at which the client will attempt to reconnect.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>autoReconnectAttempts</td>
<td>long</td>
<td>Specifies the number of attempts to reconnect. The value -1 means to never stop trying.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>verifyConnectionPriorToLogin</td>
<td>Boolean</td>
<td>Specifies whether or not to verify that a network connection is available before logging in.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>notifyWhenNetConnLost</td>
<td>Boolean</td>
<td>Specifies whether or not to alert the user when the network connection is lost.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>alwaysLoggedIn</td>
<td>Boolean</td>
<td>Keeps &quot;Automatically log in&quot; and &quot;Remember password&quot; disabled and checked and disables all &quot;Log out&quot; menu items.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>disableExit</td>
<td>Boolean</td>
<td>Keeps the &quot;Exit&quot; menu items disabled.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>disableHostName</td>
<td>Boolean</td>
<td>Sets edit state of host name text field on login dialog.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>displayResetUserBtn</td>
<td>Boolean</td>
<td>Makes the reset button show or not on the login dialog. If the preference is set to true and com.ibm.collaboration.realtime.community/host is set to true, the reset button will automatically be disabled.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>allowSave</td>
<td>Boolean</td>
<td>Specifies whether or not to allow saving password.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>earlyStartupLogin</td>
<td>Boolean</td>
<td>Specifies whether or not to show login dialog when the client starts.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Table 104. Login Preferences - com.ibm.collaboration.realtime.login  release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>resetUser</td>
<td>Boolean.</td>
<td>Specifies whether or not to reset user information when the client starts.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>displayAuthServerSSO</td>
<td>Boolean.</td>
<td>Specifies whether or not to display Authentication server information in the community Log In tab.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

Lotus Notes preferences:

The following table lists the Lotus Notes preferences that can be managed for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 105. Lotus Notes Preferences - com.ibm.collaboration.realtime.calendar.notes.connector  release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>install_directory</td>
<td>String.</td>
<td>Specify the Lotus Notes installation directory. Do not use '' as the file separator. Use '' or '/' instead. For example, com.ibm.collaboration.realtime.calendar.notes.connector/install_directory=D:\Notes</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>notes_password</td>
<td>String</td>
<td>Specify the Notes password</td>
<td>8.0 and later</td>
</tr>
</tbody>
</table>

Sametime Advanced preferences:

The following table lists the preferences for the Sametime Advanced client, for sites that have installed Sametime Advanced. The Sametime Advanced client is a plugin added to the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 106. Global Preferences - com.ibm.collaboration.realtime

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableAdvanced</td>
<td>Boolean.</td>
<td>Applies to Sametime Advanced only. When the value is set to true, the Sametime Advanced plug-ins installed with the client become active.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>enableInstantShare</td>
<td>Boolean</td>
<td>Applies to Sametime Advanced only. If enableAdvanced is set to false, but the value of enableInstantShare is set to true, the instant share feature is available. Otherwise, the value of enableInstantShare is ignored.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>sametimeAdvancedServerName</td>
<td>String</td>
<td><strong>Required.</strong> Fully qualified WebSphere Application Server host name, for example: sales.</td>
<td></td>
</tr>
<tr>
<td>sametimeAdvancedServerPort</td>
<td>String</td>
<td><strong>Required.</strong> Sametime Advanced server port number.</td>
<td></td>
</tr>
<tr>
<td>sametimeCommunityServer</td>
<td>String</td>
<td><strong>Required.</strong> Default Sametime community host name. This is the server users log in to for awareness and chat.</td>
<td></td>
</tr>
<tr>
<td>broadcastToolsServerName</td>
<td>String</td>
<td><strong>Required.</strong> Fully qualified WebSphere Application Server host name.</td>
<td></td>
</tr>
<tr>
<td>broadcastToolsServerPort</td>
<td>String</td>
<td><strong>Required.</strong> WebSphere Application Server port number. The port number is normally 1883 for HTTP and 8883 for SSL, but can be any port specified by the administrator.</td>
<td></td>
</tr>
<tr>
<td>useHTTPS</td>
<td>Boolean</td>
<td>If you are using SSL while connecting to the server, set to true. If you are using HTTP set to false.</td>
<td></td>
</tr>
<tr>
<td>advancedServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Sametime Advanced server. Set to 0 for a direct connection to the server. Set to 1 to connect through a reverse proxy.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 106. Global Preferences - com.ibm.collaboration.realtime (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcastServerConnectionType</td>
<td>String</td>
<td>Connection type to connect to the Broadcast tools server. Set to 1 for a direct connection to the server. Set to 2 to connect using SSL.</td>
<td></td>
</tr>
<tr>
<td>useHttpProxy</td>
<td>Boolean</td>
<td>Set to true if you are using an HTTP forward proxy, otherwise set it to false.</td>
<td></td>
</tr>
<tr>
<td>proxyHost</td>
<td>String</td>
<td>Enter the proxy IP address or host name if you are using a HTTP proxy, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>proxyPort</td>
<td>String</td>
<td>Enter the HTTP proxy port to which you are connecting.</td>
<td></td>
</tr>
<tr>
<td>proxyUserName</td>
<td>String</td>
<td>Enter the user name if the HTTP proxy requires one for authentication, otherwise leave it blank.</td>
<td></td>
</tr>
<tr>
<td>reverseProxyBaseURL</td>
<td>String</td>
<td>Enter the reverse proxy base URL to use if connecting through a reverse proxy. For example: <a href="http://mycompany.com/mycontext">http://mycompany.com/mycontext</a>. Leave blank otherwise.</td>
<td></td>
</tr>
<tr>
<td>reverseProxyUserName</td>
<td>String</td>
<td>Enter the reverse proxy user name if the proxy is authenticating. Leave blank if you are not using reverse proxies.</td>
<td></td>
</tr>
<tr>
<td>jmsProtocol</td>
<td>String</td>
<td>Indicates whether the client connects with a secure connection using the Security Secure Sockets Layer (SSL) or not. The default is disthub (to connect without SSL). Enter disthubs to connect with SSL.</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>liveNameResolveTimeout String</td>
<td>string</td>
<td>Time allowed in milliseconds for awareness names to resolve. The default is 10000.</td>
<td></td>
</tr>
<tr>
<td>notifyNewOpenCommunities Boolean</td>
<td>boolean</td>
<td>Alert users when a new open community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewModeratedCommunities</td>
<td>boolean</td>
<td>Alert users when a new moderated community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>notifyNewPrivateCommunities</td>
<td>boolean</td>
<td>Alert users when a new private community is created. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnDoNotDisturb</td>
<td>boolean</td>
<td>Blocks broadcasts when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockBroadcastOnInMeeting</td>
<td>boolean</td>
<td>Blocks broadcast when user is in a meeting. The default is false. Set to true to block broadcasts when user is in a meeting.</td>
<td></td>
</tr>
<tr>
<td>notifyChatRoomAddMember Boolean</td>
<td>boolean</td>
<td>Alert users when a chat room has a new member. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnDoNotDisturb</td>
<td>boolean</td>
<td>Blocks chat room notifications when user has set client to &quot;Do not disturb&quot;. The default is true.</td>
<td></td>
</tr>
<tr>
<td>blockChatRoomNotifyOnMeeting</td>
<td>boolean</td>
<td>Blocks chat room notifications when user is in a meeting. The default is false. Set to true to block chat room notifications when user is in a meeting.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 106. Global Preferences - com.ibm.collaboration.realtime (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcastServerUserIdType</td>
<td>String</td>
<td>The default is &quot;email&quot; to use the Sametime ID's email directory field. You need to use the same property value to log in to both the Sametime client and Sametime Advanced.</td>
<td></td>
</tr>
<tr>
<td>useTokens</td>
<td>Boolean</td>
<td>Determines whether or not the client uses LTPA token at login. The default is true. Set this to false only if there is no way to set up Single Sign-on between the Sametime and Sametime Advanced servers.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 107. Community Preferences - com.ibm.collaboration.community

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginTokenRefreshInterval</td>
<td>Integer</td>
<td>LTPA token timeout in seconds. IBM recommends 86100000 (23 hours and 55 minutes).</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| appsharePreference      | String        | Set the `instantshare` plug-in to use the application sharing component of either the Sametime Meeting Server or the Sametime Classic meeting service:  
  • 1 - Try the Sametime Meeting Server application sharing component, and if it fails try the Sametime Classic meeting service application sharing component (default).  
  • 2 - Use only the Sametime Meeting Server application sharing component.  
  • 3 - Use only the Sametime Classic meeting service application sharing component. |         |
| useAlternateServer      | Boolean       | If the value is true, instant share uses the host name defined by alternateMeetingServer for instant share sessions. The default is false. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use. |         |
| alternateMeetingServer  | String        | If the value of useAlternateServer is true, enter a host name here. Instant share uses the host name defined by alternateMeetingServer for instant share sessions. These settings apply when appsharePreference is set to 1 or 3 and the Classic Meeting service is in use. |         |
Table 108. Instant Share Preferences - com.ibm.collaboration.realtime.instantshare (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>useTokens</td>
<td>Boolean</td>
<td>Set to &quot;true&quot; only if InstantShare is configured to use an alternate server and LTPA token is required at login.</td>
<td></td>
</tr>
</tbody>
</table>

Microsoft Outlook preferences:

The following tables list the preferences that you can configure for Sametime Connect clients and Sametime embedded clients who use Microsoft Outlook.

Table 1 lists the available preferences for instant messaging with Microsoft Outlook; Table 2 lists the available preferences for online meetings using Sametime Meeting Integrator for Microsoft Outlook.

Table 109. Sametime Microsoft Outlook Preferences - com.ibm.collaboration.realtime.exchange

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExchangeTranscriptFolder</td>
<td>A mail box folder name</td>
<td>The name of the Microsoft Exchange mail box folder used for storing chat history.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>ExchangeMessageStore</td>
<td>A message store such as 'Mailbox - John Doe'</td>
<td>The name of the message store used for storing chat history.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td>ExchangeStorageId</td>
<td>The ID of a storage method</td>
<td>The storage method used for storing chat history. For example, com.ibm.collaboration.realtime.exchange.storage.outlook.OutlookStorage.</td>
<td>8.0 and later</td>
</tr>
</tbody>
</table>

Table 110. Sametime Meeting Integrator for Microsoft Outlook Preferences - com.ibm.collaboration.realtime

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtg802SettingsEditable</td>
<td>True or false</td>
<td>Determines whether or not 8.0.2 meetings (&quot;Classic meetings&quot;) settings are editable by the user.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>MeetingServerUrl</td>
<td>A server URL</td>
<td>The URL of the Sametime Classic Meeting (8.0.x) server. For example, <a href="http://sametime.mycompany.com">http://sametime.mycompany.com</a></td>
<td>8.0 and later</td>
</tr>
</tbody>
</table>
Table 110. Sametime Meeting Integrator for Microsoft Outlook Preferences - com.ibm.collaboration.realtime (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>MeetingServerUsesSSO</td>
<td>True or false</td>
<td>Whether Single-Sign-On should be used to authenticate with the Sametime Classic Meeting (8.0.x) server.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>AlwaysCreateMeetings</td>
<td>True or false</td>
<td>Whether a meeting should always be created on a Sametime Classic Meeting (8.0.x) server when an appointment is scheduled in Outlook.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Mtg85SettingsEditable</td>
<td>True or false</td>
<td>Whether meetings settings are editable by the user</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Meeting85Server</td>
<td>A server host name</td>
<td>The host name of the Sametime Meeting server. For example, sametime.mycompany.com</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Meeting85ServerUsesSSO</td>
<td>True or false</td>
<td>Whether Single-Sign-On should be used to authenticate with the Sametime Meeting server.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>

Example entries in plugin_customization.ini:

```
com.ibm.collaboration.realtime.exchange/ExchangeTranscriptFolder=STTranscript
com.ibm.collaboration.realtime/MeetingServerUrl=http://sametime.mycompany.com
com.ibm.collaboration.realtime/MeetingServerUsesSSO=true
com.ibm.collaboration.realtime/AlwaysCreateMeetings=false
```

Meeting preferences:

The following tables list the meeting preferences that can be managed for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 111. Meeting Preferences - com.ibm.collaboration.realtime.meetings release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>hasMic</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether the user's computer has a microphone.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>hasSpeakers</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether the user's computer has speakers.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>hasCamera</td>
<td>Boolean. Default is false.</td>
<td>Specifies whether the user's computer has a camera.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>hideLegacyMeetingUI</td>
<td>Boolean. Default is false.</td>
<td>For hiding all legacy meeting UI.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>connectionType</td>
<td>Default is 0.</td>
<td>Controls how the meetings client connects to the server. The default is 0, which makes a direct connection from the client to the server. Change this to 1 if the client connects to the server through a reverse-proxy connection.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>serverName</td>
<td>String.</td>
<td>Name of the meeting server to connect to. For example, renovations.ibm.com</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>serverPort</td>
<td>String. Default is 80.</td>
<td>Specifies server port number.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>useCommunityCredentials</td>
<td>String. Default is true.</td>
<td>If the user can re-use their credentials from the community server they are logged into, set this to true. Otherwise, false. The community server and meeting servers must both be configured for single sign-on.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>useHTTP</td>
<td>String. Default is true.</td>
<td>Uses HTTP</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>useHTTPS</td>
<td>String. Default is false.</td>
<td>Uses HTTPS</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>useHTTPProxy</td>
<td>String. Default is false.</td>
<td>If clients should connect using a forward HTTP proxy, set this to true.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>proxyServerName</td>
<td>String.</td>
<td>Name of proxy server to use. For example, proxy.ibm.com</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>proxyServerPort</td>
<td>String</td>
<td>Port number of the proxy</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>reverseProxyUrl</td>
<td>String.</td>
<td>URL for the reverse proxy. If the client is using a reverse proxy to connect, set this to the right proxy URL.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>canRemoveServer</td>
<td>String. Default is true.</td>
<td>Set this to “false” if this server should not be removed by the end user.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>canAddOtherServers</td>
<td>String. Default is true.</td>
<td>Set this to “false” if users cannot add other servers.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>communityServerName</td>
<td>String.</td>
<td>Name of the community server. This must match the community server name that is configured in the client.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>hideUI</td>
<td>String. Default is false.</td>
<td>Hides the entire Sametime 8.5.x Meeting user interface.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>loginByToken</td>
<td>Boolean. Default is false.</td>
<td>If the community server and meeting server are configured in the same single sign-on domain, this key, when set to true, forces the meeting client to log in with the LTPA token from the community server. If the meeting server is configured to re-use the community server credentials, the client automatically attempts to log in with a user name and LTPA token before falling back to a user name and password. Note that clients running releases earlier than 8.5.2 can also use an LTPA token but do not attempt to do so automatically and have no fallback mechanism. This value cannot be applied to specific meeting servers. Because it is a global setting for all servers, do not use this value if you have these older clients and some community servers and meetings servers that are not configured for single sign-on.</td>
<td>8.5 through 8.5.1.1. Not used in 8.5.2.</td>
</tr>
<tr>
<td>meetings.launchURLRichClient</td>
<td>Boolean. Default is true.</td>
<td>Set the value to &quot;false&quot; to redirect from the browser to the Sametime Connect client when a user joins a meeting room anonymously.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>meetings.showMeetingAlert</td>
<td>Boolean. Default is true.</td>
<td>By default, displays the meeting alert for scheduled meetings. Set the value to &quot;false&quot; to skip meeting alerts.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>meetings.showMeetingAlertMins</td>
<td>A number from 0 - 99.</td>
<td>If the preference is set to display meeting alerts for scheduled meetings on the calendar, this preference is the number of minutes before that meeting to display the alert.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>meetings.recentRoomCount</td>
<td>String. A number from 0 - 99.</td>
<td>Indicates how many rooms should be displayed in the Recent Rooms view in the meeting shelf.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>
### Table 112. Meeting Preferences - com.ibm.rtc.meetings.shelf release 8.5.x and higher (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>instantMeetingShowDialog</td>
<td>Boolean</td>
<td>When set to &quot;true,&quot; this preference allows the user to specify which room</td>
<td>8.5.2 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to use when inviting another user to a room. Otherwise, the default</td>
<td>later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>room configured in preferences is used for invitations.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 113. Meeting Screen Sharing Preferences - com.ibm.rtc.meetings.appshare release 8.5 and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>lastServerConnectionSetting</td>
<td>Boolean</td>
<td>The default value of false disables peer-to-peer connections when screen</td>
<td>8.5.1 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sharing. Setting the value to &quot;true&quot; allows peer-to-peer connections.</td>
<td>later</td>
</tr>
<tr>
<td>lastScreenSharingSliderSetting</td>
<td>Integer</td>
<td>Sets the position of the sharing quality slider on the screen sharing host</td>
<td>8.5.1 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dialog:</td>
<td>later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 - Fastest speed, possibly reducing quality</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 - Middle, balance between speed and quality (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3 - Best quality, possibly reducing speed</td>
<td></td>
</tr>
<tr>
<td>maximumP2PConnections</td>
<td>Integer</td>
<td>The maximum number of peer-to-peer connections that can be accepted when</td>
<td>8.5 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hosting a screen sharing session.</td>
<td>later</td>
</tr>
</tbody>
</table>

### Table 114. Meeting User Interface Preferences - com.ibm.rtc.meetings.ui release 8.5.2 and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginEnforceEmailValidation</td>
<td>Boolean</td>
<td>Setting this value to false omits the e-mail address validation on the</td>
<td>8.5.2 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>meeting server configuration page and when the user logs in. Do not set</td>
<td>later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this value to &quot;false&quot; if clients connect to older Meeting Servers because</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>it can cause policy validation issues in the client.</td>
<td></td>
</tr>
</tbody>
</table>
Table 115. Meeting Participant Preferences- com.ibm.rtc.meetings.participants release 8.5.1.1 and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateCanonicalDisplayNames</td>
<td>Boolean. Default is true.</td>
<td>By default, if the user name in a meeting room is the full canonical name (&quot;cn=name/ou=org unit/o=org&quot;), the name is truncated. Set this flag to &quot;false&quot; to prevent the conversion from occurring.</td>
<td>8.5.1.1 and later.</td>
</tr>
</tbody>
</table>

Table 116. Meeting Polling Preferences- com.ibm.rtc.meetings.polling release 8.5.1.1 and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>pollingDisabled</td>
<td>Boolean. Default is false.</td>
<td>Set this parameter to &quot;true&quot; to disable the polling tool. This entry is superseded by a server policy introduced in release 8.5.2. For clients connecting to older servers, this preference can be used to disable the tool.</td>
<td>8.5.1.1.</td>
</tr>
</tbody>
</table>

Related tasks

"Preparing servers running on WebSphere Application Server for single sign-on" on page 855
Prepare for single sign-on (SSO) by exporting a LTPA key from the servers running on WebSphere Application Server. This step applies to the Sametime Media Manager SIP Proxy and Registrar server, the Sametime Meeting server, and Sametime Advanced. If you plan to enable the Click to Call feature, it also applies to the Sametime Unified Telephony Application Server. The Sametime Proxy Server does not need to be set up for single sign-on.

Notification preferences:

The following table lists the notification preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 117. Notification Preferences - com.ibm.collaboration.realtime.alertmanager release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>pref_alertbubble_window_corner</td>
<td>string. Default is &quot;SE&quot;. Four possible values, &quot;NE&quot;, &quot;NW&quot;, &quot;SE&quot;, &quot;SW&quot; (corresponding to northeast, northwest, southeast, southwest).</td>
<td>This stores one of four possible values of which corner of the user's screen the alert bubble will appear.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_window_width</td>
<td>positive integer value</td>
<td>Stores the width in pixels of the alert bubble.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_window_height</td>
<td>positive integer value</td>
<td>Stores the height in pixels of the alert bubble.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
### Attribute | Variable type | Description | Release
--- | --- | --- | ---
`pref_alertbubble_window_edge_padding` | Positive integer value | Stores the amount in pixels that the alert bubble's top and bottom edge will be from the edge of the desktop. | 7.5.1 and later
`pref_alertbubble_show` | String value, "standard" = show standard OS window, "less" or others = show alert bubble for an alert | Determines whether to show the alert bubble or a standard OS window for an alert. | 7.5.1 and later
`pref_alertbubble_close_alerts` | Boolean. TRUE = automatically close alert, FALSE = do not automatically close alert | Determines whether to automatically close an alert after it appears. | 7.5.1 and later
`pref_alertbubble_close_alerts_delay` | Positive integer value | If alerts are set to automatically close, this is the delay amount in seconds before the alert is closed. | 7.5.1 and later
`pref_alertbubble_animation` | String value, "none" = no window animation, "slide" = animate using slide effect, and "fade" = animate using fade effect. The default value is "slide" | Specify the Alert bubble animation type. | 7.5.1 and later
`pref_alertbubble_bring_window_to_front` | Boolean | The default value, whether to Bring the Popup window to front. | 7.5.1 and later
`pref_alertbubble_flash_taskbar` | Boolean | The default value, whether to Flash the taskbar to indicate new Popup window. | 7.5.1 and later
`pref_event_0_playsound` | Boolean | Determines whether one on one chat events play a sound. | 7.5.1 and later
`pref_event_1_playsound` | Boolean | Determines whether invitations to multi-party chat events play a sound. | 7.5.1 and later
`pref_event_2_playsound` | Boolean | Determines whether announcement events play a sound. | 7.5.1 and later
`pref_event_3_playsound` | Boolean | Determines whether Invitations to Sametime Classic online meeting play a sound. | 7.5.1 and later
Table 117. Notification Preferences - com.ibm.collaboration.realtime.alertmanager release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>pref_event_6_playsound</td>
<td>Boolean</td>
<td>Determines whether status alert events (Alert me When) play a sound.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_7_playsound</td>
<td>Boolean</td>
<td>Determines whether Location Awareness events play a sound.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_0_soundfile</td>
<td>Text string</td>
<td>The sound file that will play for one on one chat events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '\' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_0_soundfile=C:\Documents\sound.wav</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_1_soundfile</td>
<td>Text string</td>
<td>The sound file that will play for Invitations to multi-party chat events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '\' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_1_soundfile=C:\Documents\sound.wav</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_2_soundfile</td>
<td>Text string</td>
<td>The sound file that will play for announcement events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '\' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_2_soundfile=C:\Documents\sound.wav</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_3_soundfile</td>
<td>Text string</td>
<td>The sound file that will play for Invitations to Sametime Classic online meeting events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '\' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_3_soundfile=C:\Documents\sound.wav</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>pref_event_6_soundfile</td>
<td>Text string. Full path to a valid sound file of .WAV format.</td>
<td>The sound file that will play for status alert events (Alert me When) events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '&quot;' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_6_soundfile=C:\Documents\sound.wav.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_7_soundfile</td>
<td>Text string. Full path to a valid sound file of .WAV format.</td>
<td>The sound file that will play for Location Awareness events, if playing sounds is enabled for this event. Don't use '' as the file separator. Use '&quot;' or '/' instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_7_soundfile=\Documents\sound.wav.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_0_option_1</td>
<td>Boolean</td>
<td>For one on one chats, determines whether to bring chat window to front.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_0_option_2</td>
<td>Boolean</td>
<td>For one on one chats, determines whether to flash the taskbar to indicate new window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_0_option_3</td>
<td>Boolean</td>
<td>For one on one chats, determines, whether to show a system tray icon to indicate new message.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_1_option_1</td>
<td>Boolean</td>
<td>For invitations to multi-party chats, determines whether to bring invitation window to front.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_1_option_2</td>
<td>Boolean</td>
<td>For invitations to multi-party chats, determines whether to flash the taskbar to indicate new invitation.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_9_option_1</td>
<td>Boolean</td>
<td>For calls, determines whether to bring the invitation window to front.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>
Table 117. Notification Preferences - com.ibm.collaboration.realtime.alertmanager release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>pref_event_9_option_2</td>
<td>Boolean</td>
<td>For calls, determines whether to flash the taskbar to indicate new window.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>pref_event_9_timeout_seconds</td>
<td>Integer, unit is second</td>
<td>For calls, specify the seconds before incoming invitation time out.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>allow_response</td>
<td>Boolean</td>
<td>For Send Announcement dialog, determines whether to allow recipients to send responses.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_9_alert_incoming</td>
<td>Boolean</td>
<td>For calls, determines whether to display incoming invitation.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>pref_event_10_playsound</td>
<td>Boolean</td>
<td>Determines whether calendar events play a sound.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>pref_event_10_soundfile</td>
<td>Boolean</td>
<td>The sound file that will play for calendar events, if playing sounds is enabled for this event.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>

**People preferences:**

The following table lists the people preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 118. People Preferences - com.ibm.collaboration.realtime.people release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookupExpirationDays</td>
<td>Integer. Default is 7.</td>
<td>Specifies the number of days a user's directory info is considered up to date. A value of 0 means refresh a user’s directory info for each client session.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>wrapBusinessCard</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to wrap text in business card</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showNoPhotoPhoto</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether or not to show a placeholder image in business card when user doesn't have a photo.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>isCaseInsensitive</td>
<td>Boolean. Default is false.</td>
<td>Specifies if it is case insensitive when looking up people. The default of false means the search is case-sensitive. If you plan to set this to true, first turn off case sensitivity in the IBM Sametime Community server and restart the server.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>userInfoReplaces</td>
<td>Boolean</td>
<td>When set to true, contact names refresh automatically with the contact's business card name. When this preference is enabled, users can also update contact names manually. They can update one name by right-clicking a contact name and choosing Refresh Person Info. They can also update all names by selecting Tools &gt; Refresh Contact Nicknames. For the preference to work, the person attributes in the LDAP directory used with the Sametime Community Server must meet the following requirements. Verify or change these settings by using the Sametime System Console to administer the Sametime Community Server. • Community Services tab - The attribute used for the internal user ID must be different from the attribute used for the person's display name. • Business card tab - The attribute used for the business card name must be the same as the attribute used for the person's display name.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>DefaultDisplayName</td>
<td></td>
<td>Default is false.</td>
<td></td>
</tr>
</tbody>
</table>

Table 118. People Preferences - com.ibm.collaboration.realtime.people release 7.5.x and later (continued)
### Table 118. People Preferences - com.ibm.collaboration.realtime.people release 7.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>refreshNicknamesOnFirstStartup</td>
<td>Boolean</td>
<td>Determines whether clients automatically replace all existing display names and nicknames in the contact list with business card names after clients start up and log in. You can set this preference when the <code>userInfoReplacesDefaultDisplayName</code> preference is enabled. Tip: To prevent the task from running each time you install on a new machine or reset the workspace, use managed preferences to set this preference temporarily for all new and upgrading clients. Disable the preference after all clients have run once.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

### Related tasks

“Turning off case sensitivity on the Sametime Community Server” on page 345

You must turn off case sensitivity on the IBM Sametime Community Server to allow awareness in IBM Lotus iNotes and WebSphere applications.

### Rules manager preferences:

The following tables list the rules manager preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

#### Table 119. Sametime Rules Manager Preferences - com.ibm.collaboration.realtime.telephony.sti.rulesmgr release 8.5.1 and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>blockIncomingCalls</td>
<td>Boolean</td>
<td>Block all incoming calls.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>rulesForComputerOnlyUsers</td>
<td>Boolean</td>
<td>Causes default rules to only apply for computer only users.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>hideCallRoutingPrefs</td>
<td>Boolean</td>
<td>Hide the call routing preference pages.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>disableRulesEditing</td>
<td>Boolean</td>
<td>Disable the ability to edit call routing rules.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>disableOfflineCalling</td>
<td>Boolean</td>
<td>Disable ability for a computer only user to call an offline contact.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>
Table 119. Sametime Rules Manager Preferences - com.ibm.collaboration.realtime.telephony.sti.rulesmgr release 8.5.1 and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>disableExternalCalling</td>
<td>Boolean. Default is true.</td>
<td>Disable ability for a computer only user to call an external contact or phone number.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>disableNonComputerCalls</td>
<td>Boolean. Default is true.</td>
<td>Disable ability for a computer only user to call using anything other than their computer.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>hidePreferredDevices</td>
<td>Boolean. Default is false.</td>
<td>Hide the preferred device dropdown.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>disablePreferredDevices</td>
<td>Boolean. Default is true.</td>
<td>Disable the preferred devices dropdown.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>hideAllocatedDevices</td>
<td>Boolean. Default is true.</td>
<td>Hide allocated devices so they cannot be used to answer calls or as a transfer target.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>disablePreferredNumberChanges</td>
<td>Boolean. Default is true.</td>
<td>Disable the ability to add new preferred numbers.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>replaceConditions</td>
<td>Boolean. Default is true.</td>
<td>Replace the users conditions with the defaults.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>computerOnlyPrefix</td>
<td>String. Default is +999.</td>
<td>Unified number prefix which identifies a user as a computer only user.</td>
<td>8.5.1 and later</td>
</tr>
<tr>
<td>callRoutingConditions</td>
<td>String. Default is /config/callRoutingConditions.xml.</td>
<td>URL pointing to an XML file which defines the default call routing rules.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>

Spell checker preferences:

The following table lists the spell checker preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 120. Spell Checker Preferences - com.ibm.collaboration.realtime.spellchecker release 7.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkSpelling</td>
<td>Boolean. Default is true.</td>
<td>Specifies whether by default to check spelling as you type.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>dictionaryLanguage</td>
<td>String. Default is en-US.</td>
<td>Specifies the default language to use for spellchecking. Must have corresponding dictionary installed.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>
Telephony, Audio, and Video preferences:

The following table lists the telephony, audio, and video preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 121. Global Preferences - com.ibm.collaboration.realtime release 8.5.1 and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableSUT</td>
<td>Boolean. Default is false.</td>
<td>Applies to Sametime Unified Telephony subscribers only. When the value is set to true, the Sametime Unified Telephony plug-ins installed with the client become active. Subscribers see telephony status icons in the contact list and features such as call history and the phone book are enabled. Restart the client for the change to take effect.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>
Table 121. Global Preferences - com.ibm.collaboration.realtime release 8.5.1 and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableTelephonyStatus</td>
<td>Boolean</td>
<td>Set the value to true to enable the display of telephony presence status icons for live names on the contact list or elsewhere. This is used for telephony presence published using the Sametime Telephony Presence Adapter, which is used by both Sametime Unified Telephony and some third-party telephony presence solutions. If you set enableSUT to true, it is not necessary to also set enableTelephonyStatus to true. When Sametime Unified Telephony is enabled, telephony status shows regardless of this preference value. However, in environments with both Sametime Unified Telephony users and nonusers, you can set enableTelephonyStatus to true so nonusers can see telephony presence for Sametime Unified Telephony users.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>
Table 121. Global Preferences - com.ibm.collaboration.realtime release 8.5.1 and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableExtendedStatus</td>
<td>Boolean. Default is false.</td>
<td>Set the value to <code>true</code> to enable the use of extended status icons for live names on the contact list or elsewhere. Extended status icons are most often used for telephony presence status, however some third-party applications use extended status icons for other types of status. To display telephony status icons for applications that use the Sametime Telephony Presence Adapte, use enableTelephonyStatus rather than enableExtendedStatus. It is only necessary to set enableExtendedStatus when not using telephony presence from the Sametime Telephony Presence Adapter. As with enableTelephonyStatus, enableExtendedStatus is ignored when you set enableSUT to <code>true</code>, since Sametime Unified Telephony always shows telephony status icons.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>

Table 122. Telephony, Audio, and Video Preferences - com.ibm.collaboration.realtime.telephony.ui release 8.5 and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>deviceIn</td>
<td>A valid string value for the device. The default value is &quot;Default device&quot;.</td>
<td>For computer sound devices, specifies which device is selected for Microphone.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>deviceOut</td>
<td>A valid string value for the device. The default value is &quot;Default device&quot;.</td>
<td>For computer sound devices, specifies which device is selected for Speakers.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>deviceRing</td>
<td>A valid string value for the device. The default value is &quot;Default device&quot;.</td>
<td>For computer sound devices, specifies which device is selected for Ringing.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>mic_boost_disabled</td>
<td>Boolean</td>
<td>For computer sound devices, specifies whether or not to disable microphone boost.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>always_show_my_video</td>
<td>Boolean</td>
<td>Specifies whether or not to show my video automatically when I participate in a video-enabled session.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>closeWindow2</td>
<td>Boolean</td>
<td>Specifies whether or not to close the call window automatically when user disconnect.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>warnCallAway</td>
<td>Boolean</td>
<td>Specifies whether or not to warn me if user is Away before starting new calls.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>warnCallInTheMeeting</td>
<td>Boolean</td>
<td>Specifies whether or not to warn me if user is Away before starting new calls.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>warnCallDND</td>
<td>Boolean</td>
<td>Specifies whether or not to warn me if user is on Do Not Disturb before starting new calls.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>warnCallOnThePhone</td>
<td>Boolean</td>
<td>Specifies whether or not to warn me if user is On the Phone before starting new calls. For SUT only.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>participantView</td>
<td>Integer</td>
<td>Specifies the default participant view for 3-6 participants.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>callwindowAlwaysOnTop</td>
<td>Boolean</td>
<td>Specifies whether or not to keep call window always on top. For windows only.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>enableSoundAlerts</td>
<td>Boolean</td>
<td>Specifies whether or not to enable sound alerts.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>soundCalleeRing</td>
<td>A valid absolute sound file path.</td>
<td>The sound file that will play for incoming voice or video chats, if sound alerts is enabled.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>soundHangUp</td>
<td>A valid absolute sound file path.</td>
<td>The sound file that will play when connection ended, if sound alerts is enabled.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>soundPause</td>
<td>A valid absolute sound file path.</td>
<td>The sound file that will play when pause audio, if sound alerts is enabled.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>soundResume</td>
<td>A valid absolute sound file path.</td>
<td>The sound file that will play when resume audio, if sound alerts is enabled.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>soundAlert</td>
<td>A valid absolute sound file path.</td>
<td>The sound file that will play for incoming call alerts, if sound alerts is enabled.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>muteSoundEnabled</td>
<td>Boolean</td>
<td>Specifies whether or not to mute other Sametime alerts during calls.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>preferredConferencingSolution</td>
<td>&quot;ext_avc&quot; or &quot;st_avc&quot;. If set to &quot;st_avc&quot;, Sametime Audio/Video Conferencing will be used instead.</td>
<td>For Connection and Conference Settings, specifies whether or not to use the external service for user’s video calls.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>auto_vc_non_sut</td>
<td>Boolean</td>
<td>Specifies whether or not to always establish a computer-to-computer (Voice Chat) session when callee does not have Sametime Unified Telephony.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td>Release</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>hideTelephonyUI</td>
<td>Boolean</td>
<td>Specifies whether or not to hide all telephony and audio/video user interface elements, include menu items, toolbar actions, and preference pages. This can be used in environments that either do not use any telephony or audio/video features, or use third-party telephony or audio/video solutions that provide their own user interface.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>showCallComputer</td>
<td>Boolean</td>
<td>Set the value to true to enable the Call Computer command on the call menu and live name context menu. Call Computer starts a computer voice chat call using Sametime audio/video conferencing, regardless of the selected preferred device and service provider preference. This setting is primarily intended for Sametime Unified Telephony users, but can be enabled for any user.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td>callActionProviderId</td>
<td>String</td>
<td>For Multiple TCSP service providers, this value specifies the audio service provider ID selected by user to initiate calls.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>
Table 123. Update Preferences - com.ibm.collaboration.realtime.update release 8.5.x and later

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>firstTimeRestartDelayMinutes</td>
<td>Integer</td>
<td>Defines how long to delay for the first prompt after an automatic update is completed. Prompts immediately by default.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>
Table 123. Update Preferences - com.ibm.collaboration.realtime.update release 8.5.x and later (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>restartAction</td>
<td>restart.now - user is presented with a restart dialog with Restart Now button only.</td>
<td>Defines how restart should be initiated on the client after an update is completed. Note this preference is just valid for administrator-initiated updates, but be invalid for users' manual updates by Tools -&gt; Plug-ins menu.</td>
<td>8.5 and later</td>
</tr>
<tr>
<td></td>
<td>restart.now.or.later - user is presented with a restart dialog with Restart Now and Wait x minutes buttons.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>restart.on.next.login - user is presented with an info message that the plug-in updates will be effected on next restart.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>restart.now.no.prompt - the client is restarted automatically when update is completed without any user interaction.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default is restart.now.or.later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>restartRemindDelayMinutes</td>
<td>integer. Default is 5.</td>
<td>Defines how long to delay the restart of the client after an update is completed. This setting is ignored if restartAction is set to restart.now or restart.on.next.login.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>

Example entry in plugin_customization.ini:
com.ibm.collaboration.realtime.update/restartAction=restart.now.no.prompt
com.ibm.collaboration.realtime.update/restartRemindDelayMinutes=1

**Automatically updating communities with the managed-community-configs.xml file**

You can distribute updates to IBM Sametime client communities automatically using a managed-community-configs.xml file. The managed-community-configs.xml file is policy-based, so you can control communities for different user groups.
About this task

You can also use the managed-community-configs.xml file to manage secondary communities, while preventing users from adding or deleting communities. Set the Allow Multiple Communities policy to false and use the managed-community-configs.xml to define the desired secondary communities. The client allows the user to log into secondary communities defined in the .xml file, but the user cannot delete secondary communities defined in the file.

At login time, the client receives policies and checks for the existence of a managed-community-configs.xml file according to the Sametime update site URL policy. For example, if the administration update site URL is http://example.com/updates, the client looks for the file in http://example.com/updates/managed-community-configs.xml.

Follow these steps to create and post a managed-community-configs.xml file.

Procedure

1. Create a settings XML file and save it as managed-community-configs.xml.
2. Add settings for communities and actions in the file.
3. Post the file to the policy-configured administration update site URL.

What to do next

One additional step is required if you change the settings file to update the host name of a community to a new server that is part of the same community, meaning that users' contact lists are still valid with the new host. You must set the ST_COMMUNITY_ID in the sametime.ini file of both servers to the same value and ensure that all the communities in your cluster are using the same community ID. This will prevent duplicate communities from being created on the client when logging into the new host for the first time.

Managed community settings


The managed-community-configs.xml file uses these element types:

- Action elements specify what action to take: Add, Update, Delete, or Reset. They are set as <managed-community-action> elements.
- Community elements specify the community attributes to which the actions apply. They are set as <managed-community> elements.

Only define attributes that are mandatory. For example, do not include the "loginAtStartup" attribute unless you want to prevent your users from changing that setting. If the user's configuration differs from any defined attribute, the user's configuration is updated. Although you cannot lock the user interface, any settings that a user changes during a session revert back at the next login.

The following tables describe the attributes for each element. The required attributes must be present in the file.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>The unique ID of the managed community. This setting should be the same value as the &quot;host&quot; attribute.</td>
</tr>
<tr>
<td>host</td>
<td>Yes</td>
<td>The host to manage. The client only updates communities whose host matches the host of the managed community.</td>
</tr>
<tr>
<td>newHost</td>
<td>No</td>
<td>Attribute used to update the host of a community that matches the &quot;host&quot; attribute. This is the new host to connect to. The attribute only applies to &quot;update&quot; type managed community actions. The user’s contact list is assumed to be valid for the new community. If the contact list is not valid, use the &quot;reset&quot; managed community action instead.</td>
</tr>
<tr>
<td>name</td>
<td>No</td>
<td>The name of the community. Not recommended. To set the community ID, use ST_COMMUNITY_ID in the server’s sametime.ini to set the community name for all clients.</td>
</tr>
<tr>
<td>savePassword</td>
<td>No</td>
<td>Whether or not to save the password. Set the value to &quot;true&quot; to save the password.</td>
</tr>
<tr>
<td>loginAtStartup</td>
<td>No</td>
<td>Whether or not to automatically log in. Set the value to &quot;true&quot; to log in automatically.</td>
</tr>
<tr>
<td>useGlobalConnContext</td>
<td>No</td>
<td>Whether or not to use the global connection context. You must set this to &quot;true&quot; if you are updating connectionType to a value other than &quot;direct&quot;.</td>
</tr>
<tr>
<td>connectionType</td>
<td>No</td>
<td>The connection type corresponds to the options in the Connection settings page. Valid values include useBrowserSettings, direct, tls-direct, http-direct, socks4-proxy, socks5-proxy, http-proxy, and reverse-proxy.</td>
</tr>
<tr>
<td>authServerUrl</td>
<td>No</td>
<td>The server URL for SSO authentication.</td>
</tr>
</tbody>
</table>
Table 124. `<managed-community>` attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authType</td>
<td>No</td>
<td>The authentication type for SSO. Value can either be TAM-SPNEGO or ST-DOMINO-SSO.</td>
</tr>
<tr>
<td>port</td>
<td>No</td>
<td>The port to use if it is not the default 1533.</td>
</tr>
<tr>
<td>proxyHost</td>
<td>No</td>
<td>The hostname of the proxy.</td>
</tr>
<tr>
<td>proxyPort</td>
<td>No</td>
<td>The port of the proxy.</td>
</tr>
<tr>
<td>loginByToken</td>
<td>No</td>
<td>Whether or not to log in by token. Set the value to &quot;true&quot; to log in by token. Note that if the token login fails and the password is available, the password-based authentication will proceed.</td>
</tr>
<tr>
<td>sendKeepAlive</td>
<td>No</td>
<td>Whether or not to send the keep alive signal. Set the value to &quot;true&quot; to send the keep alive signal.</td>
</tr>
<tr>
<td>keepAliveInterval</td>
<td>No</td>
<td>The interval at which to send the keep alive signal.</td>
</tr>
</tbody>
</table>

Table 125. `<managed-community-action>` attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>managed-community-id</td>
<td>Yes</td>
<td>The unique ID of the managed-community. Use the same value as the &quot;host&quot; attribute of the managed community</td>
</tr>
<tr>
<td>Attribute</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| type                        | Yes       | The type of action. Values can be "update", "add", "delete" or "reset".  
  • Add actions result in the addition of secondary communities.  
  • Delete actions result in the deletion of secondary communities. The default community cannot be deleted.  
  • Update actions result in an update to communities whose host value match the host value of the managed community. If no attributes are different, the update action does not result in any change.  
  • Reset actions are used to reset the client configuration to a new default community. If a reset action is found, it is applied before any other action type and no other actions are processed. The user is prompted to restart, but may opt not to. The managed community referenced by the reset action represents the new default community that is to be used when the user next restarts. |
| restart                     | No        | By default, update actions only result in a restart if the host name is changed. Add this optional attribute and set the value to "true" to restart the client after other update events. To prevent the default restart after the host name is changed, add this attribute, but set it to "false." |
| applyDefaultCommunityUsername | No        | Attribute that can be used with an "add" type managed community action to indicate whether or not the default community user name should be applied to the new community when it is added. Set the value to "true" apply the default community user name. |
Table 125. `<managed-community-action>` attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>createNewConfig</code></td>
<td>No</td>
<td>Optional attribute for use with the reset action type. When you set this to &quot;true,&quot; the previous default community is completely replaced by the new community. The user name and password are empty, requiring the user to repopulate these values. Without this attribute, or with the attribute set to false, the new default community configuration enabled with a reset action retains the user name, password, and connection options of the former default community.</td>
</tr>
</tbody>
</table>

Sample managed-community-configs-xml file

The sample file below adds a new community and updates two others. The connection type is reverse-proxy.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<managed-communities>
  <managed-community id="sales.usma.example.com" host="sales.usma.example.com" loginByToken="true" authServerUrl="http://sales.usma.example.com" auth
  <connection connectionType="reverse-proxy" proxyHost="http://usma.example.com:81/sales"/>
  </managed-community>
  <managed-community id="sametime.example.com" host="sametime.example.com" newHost="sametimenew.example.com"/>
  <managed-community id="sametimenew.example.com" host="sametimenew.example.com"/>
  <managed-community-action type="update" managed-community-id="sales.usma.example.com"/>
  <managed-community-action type="update" managed-community-id="sametime.example.com"/>
  <managed-community-action type="add" managed-community-id="sametimenew.example.com"/>
</managed-communities>
```

Action examples

Adding a new community

The example below adds a new secondary community using the global connection defaults. Administrator-defined secondary communities are not impacted by the **Allow user to add multiple server communities** policy. Even if the policy is set to Not selected, the client recognizes they are defined by the administrator and allows the user to log into them. Administrator-defined communities cannot be deleted.

```xml
<managed-communities>
  <managed-community id="acct.sales.usma.example.com" host="acct.sales.usma.example.com"/>
  <managed-community-action type="add" managed-community-id="acct.sales.usma.example.com"/>
</managed-communities>
```

Updating the default community host

This example updates the default community host from "sales.usma.example.com" to "sales2.usma.example.com."
Updating the default community host again

This example updates the default community host from "sales.usma.example.com" or "sales2.usma.example.com" to "sales3.usma.example.com."

```xml
<managed-communities>
  <managed-community id="sales.usma.example.com" host="sales.usma.example.com" newHost="sales3.usma.example.com"/>
  <managed-community-action type="update" managed-community-id="sales.usma.example.com"/>
</managed-communities>
```

Updating the secondary community host

This example updates "acct" to "acct2" and ensures acct2 is added as a secondary community for all new users.

```xml
<managed-communities>
  <managed-community id="acct2.sales.usma.example.com" host="acct2.sales.usma.example.com"/>
  <managed-community id="acct.sales.usma.example.com" host="acct.sales.usma.example.com" newHost="acct2.sales.usma.example.com"/>
  <managed-community-action type="add" managed-community-id="acct2.sales.usma.example.com"/>
  <managed-community-action type="update" managed-community-id="acct.sales.usma.example.com"/>
</managed-communities>
```

Updating the secondary community host again

This example updates "acct2" to "acct3", and also ensures acct3 is added as a secondary community for all new users.

```xml
<managed-communities>
  <managed-community id="acct3.sales.usma.example.com" host="acct3.sales.usma.example.com"/>
  <managed-community id="acct2.sales.usma.example.com" host="acct2.sales.usma.example.com" newHost="acct3.sales.usma.example.com"/>
  <managed-community-action type="add" managed-community-id="acct3.sales.usma.example.com"/>
  <managed-community-action type="update" managed-community-id="acct2.sales.usma.example.com"/>
</managed-communities>
```

Switching users to a new default community with a different user directory

If the new community is a different community with a different user backend, use the reset managed-community-action type to reset the user to the new community. Assuming the user credentials are valid in the new community, after restarting, the user logs into the new community. To include additional secondary communities as part of this new configuration, define them on the new server's managed-community-configs.xml file, using add actions for the desired secondary communities. When the reset action is found, if the current default community does not match the community defined by the administrator, or if createNewConfig is set to true, the client saves the new configuration locally. When the client next restarts, the default community defined by the administrator replaces the previously defined default community.
**Configuring Sametime for mobile users**

Configure IBM Sametime with Sametime Mobile to provide connectivity for users with support mobile devices.

**About this task**

Configuring Sametime for mobile users involves the following tasks:

**Configuring the Lotus Domino server for Sametime Mobile support**

To enable support for IBM Sametime Mobile on the IBM Lotus Domino server, you need to create a Web Site Rule document in the Domino Directory and establish a URL redirection.

**About this task**

Complete the following steps to enable support for Sametime Mobile on the Lotus Domino server.

**Procedure**

   a. In the Domino Directory, open the Server document for the Lotus Domino server that hosts the Sametime Community server.
   b. Click the Create Web - URL Mapping/Redirection button.
   c. In the Basics tab, select URL > Redirection URL.
   d. Click the Mapping tab and enter the following information:
      - In the Incoming URL path field, enter /mobile/*.
      - In the Redirection URL string field, enter stcenter.nsf/WebMobileDownloads?OpenView.
   e. Click Save & Close.
2. Configure MIME type support on the Lotus Domino server.
   a. With a text editor, open the file httpd.cnf, located in the Domino data directory.
   b. Add the following lines to the file at the end of the section "other application formats" but before the section "Fallback MIME types":

```plaintext
AddType .jad text/vnd.sun.j2me.app-descriptor
AddType .jar application/java-archive
AddType .alx application/octet-stream
```

---

Related reference

"Sametime Instant Messaging user policy settings" on page 1052

You can grant or limit access to features in IBM Sametime Instant Messaging by enabling or disabling various policies for users. Instant Messaging policy changes take effect in 60 minutes by default.
c. Save and close the modified file.

3. Restart the HTTP task on the server.

What to do next

After these steps are completed, the Sametime Community server can be used with the Sametime Mobile client; however, before allowing users to download Sametime Mobile, you should provision the client with appropriate server details. This simplifies the user experience and prevents the user from entering incorrect connectivity details.

Configuring Sametime on the iPhone device

Provide your users with the following steps to run IBM Sametime on the iPhone device.

Before you begin

The Sametime iPhone client runs within a client's browser session, and is hosted on a Sametime Proxy server. For more information on installing the Sametime Proxy Server, see Installing a Sametime Proxy Server.

Users in your deployment must have JavaScript enabled on the iPhone to use the Sametime iPhone client. From the iPhone home screen, go to **Settings -> Safari**, and toggle the JavaScript preference to **ON** under the Security section.

Procedure

1. Start the Safari browser.
2. Go to the Sametime login page by entering the following URL, replacing `serverhostname.domain:port` with the fully qualified domain name and port of the Sametime Proxy Server.

   ```
   http://serverhostname.domain:port/stwebclient/iphone_index.jsp
   ```

   The default value for `port` is **9080** or **9043** if SSL has been deployed.

   Loading Sametime the first time takes a little longer than usual, depending on your connection speed. Subsequent loads of Sametime will be faster, since much of the Sametime application is stored locally on the device after that first load.

3. Now add a Sametime icon to your desktop, which allows you to start Sametime from the home screen. From the Sametime login page, select **Add to Home Screen** on the Safari menu, then click **Add** in the upper right of the screen.

What to do next

Point your users to the following video to get them started with the Sametime iPhone client: Video: Using Sametime on iPhone (8.5).

Configuring Sametime Mobile for client downloads

Configure IBM Sametime Mobile support on an IBM Sametime Community server.
Before you begin

These instructions assume that you do not use the IBM Sametime Enterprise Meeting Server in your Sametime deployment. If you use the Enterprise Meeting Server, proceed to the topic, Configuring Sametime Mobile for client downloads in the Sametime Enterprise Server Meeting help, instead.

Note: Sametime Mobile does not support meeting features.

About this task

Sametime provides three options for connecting mobile devices to the Sametime Community server:

• Connect with a Virtual Private Network (VPN) such as IBM Lotus Mobile Connect or RIM BlackBerry Enterprise Server Mobile Data Services (MDS).
  This connection model provides end-to-end connectivity from the device into the corporate intranet, allowing for applications to access intranet resources securely. Sametime Mobile would access the server, and intranet, in the same manner as any other application installed on the device. This is typically the most flexible approach as it allows the client to utilize a variety of application that may be hosted on the corporate intranet.

• Connect with an authenticating HTTP Proxy, such as IBM HTTP Server or Apache HTTP Server.
  The Sametime Mobile client supports connecting through a standard web proxy that issues HTTP 401 or 407 challenge requests with HTML Form Basic Authentication (Digest is not supported at this time). The reverse proxy server must use cookies for authentication. This setup typically places the HTTP proxy in the demilitarized zone (DMZ) of the network, with port 80 opened to the Internet and another port opened from the proxy to the back end application.
  For more information on configuring IBM HTTP Server as an authenticating proxy, see the IBM WebSphere information center at http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp.
  It is recommended that the server be configured with a valid SSL certificate obtained from a trusted and well-known supplier; mobile devices support a variety of root certificates, and most reputable certificate providers function with these devices (self-signed SSL certificates are typically not usable with mobile devices). In addition, most mobile devices must have their time and date set properly to work with SSL-secured servers.

• Connect with a direct connection from the client to the server.
  By default, Sametime Mobile clients communicate with the Sametime Community server over port 8082, using the Sametime Links protocol and 128-bit encryption. Sametime Links is also accessible over the standard Sametime client port of 1533, and optionally port 80 if HTTP Tunneling is enabled.
  Appropriate firewall rules should be enabled to allow traffic to pass through on the selected port.

Follow the instructions below to configure Sametime Mobile for client downloads.

Procedure

1. Start the Sametime Community server and log in.
2. Fill in configuration information for the mobile devices supported in your environment by completing the following steps:
   a. Click Administer the server.
b. Expand Configuration and under it, click Sametime Mobile. The Configuration - Sametime Mobile page displays a link for each supported mobile device.

c. Click the link that represents a device you want to configure.

d. Enter the appropriate configuration information for your device.

The devices supported with the current release of Sametime Mobile are listed below this topic; refer to the appropriate device for additional configuration details.

e. Click Update to save your changes.

What to do next

The following mobile devices are supported with this release of Sametime Mobile:

**Microsoft Windows Mobile 5 and 6**
Configure IBM Sametime Mobile support for Microsoft Windows Mobile 5 and Microsoft Windows Mobile 6 devices.

These configuration steps provision information for users of the following mobile devices. These steps are optional but highly recommended. These settings affect both the Windows Mobile MIDP client as well as the new Unified Communications and Collaboration (UCC) Windows Mobile client.

- Microsoft Windows Mobile 6 Standard
- Microsoft Windows Mobile 6 Professional
- Microsoft Windows Mobile 5 Pocket PC
- Microsoft Windows Mobile 5 Smartphone

**Hint for user's first time login**

Enter a user name suffix, for example an email suffix such as @example.com. During login, the User name field displays this suffix as a default value, so that users need only add their names before the suffix.

**Sametime server name**

Enter the fully qualified host name of the Sametime Community Server that mobile devices will connect to by default; for example, sametime.example.com.

**Port**

Enter the default port used to connect to the specified Sametime Community Server.

**Proxy connection**

Select this setting if mobile users will connect to the Sametime Community Server through a proxy server. If you enable a proxy connection, you must enter a valid proxy URL in the field that follows.

**Proxy URL**

Enter the URL for the proxy server that will connect Sametime Mobile users to the Sametime Community server.

**Use Sametime Connect user ID and password**

Select this option if you want Sametime Mobile users to connect to the proxy server with their IBM Sametime Connect user name and password instead of using the device's proxy user name and password.

**Nokia Eseries**

Configure IBM Sametime Mobile support for Nokia Eseries devices.
The following configuration steps provision information for users of Nokia Eseries mobile devices. These steps are optional but highly recommended.

**Hint for user’s first time login**

Enter a user name suffix, for example an email suffix such as@example.com. During login, the **User name** field displays this suffix as a default value, so that users need only add their names before the suffix.

**Sametime server name**

Enter the fully qualified host name of the Sametime Community server that mobile devices will connect to by default; for example, sametime.example.com.

**Port**

Enter the default port used to connect to the specified Sametime Community Server.

**Proxy connection**

Select this setting if mobile users will connect to the Sametime Community Server through a proxy server. If you enable a proxy connection, you must enter a valid proxy URL in the field that follows.

**Proxy URL**

Enter the URL for the proxy server that will connect Sametime Mobile users to the Sametime Community Server.

**Use Sametime Connect user ID and password**

Select this option if you want Sametime Mobile users to connect to the proxy server with their IBM Sametime Connect user name and password instead of using the device’s proxy user name and password.

**RIM BlackBerry 9000 and 9530 Series**

Configure IBM Sametime Mobile support for RIM Blackberry 9000, and 9530 Series devices.

The following configuration steps provision information for users of RIM Blackberry 9000, and 9530 Series mobile devices. A BES server is currently required to provision these settings through the BES IT Policy. These steps are optional but highly recommended.

**Hint for user’s first time login**

Enter a user name suffix, for example an email suffix such as@example.com. During login, the **User name** field displays this suffix as a default value, so that users need only add their names before the suffix.

**Sametime server name**

Enter the fully qualified host name of the Sametime Community server that mobile devices will connect to by default; for example, sametime.example.com.

**Specify the connection**

Select one of the following connection types:

- **BES MDS Connection Service**: Select this setting to establish a connection using the Blackberry Enterprise Server. If you use a BES connection, you must set up automatic provisioning using the **Automate provisioning of devices with BES** setting described below.
- **Direct connection**: Select this setting to establish a direct connection using the HTTP port.
• **Proxy connection**: Select this setting if mobile users will connect to the Sametime Community Server through a proxy server. If you enable a proxy connection, you must enter a valid proxy URL in the field that follows:
  
  - **Proxy URL**: Enter the URL for the proxy server that will connect Sametime Mobile users to the Sametime Community server.
  
  - **Use Sametime Connect user ID and password**: Select this option if you want Sametime Mobile users to connect to the proxy server with their IBM Sametime Connect user name and password instead of using the device's proxy user name and password.

**Automate provisioning of devices with BES**
A Blackberry Enterprise Server (BES) is required to provision the Sametime Mobile client with this information. Follow the on-screen instructions to generate an IT Policy string and copy it to the BES server. The BES documentation provides further information on generating a custom "IT Policy Rule" named "SametimeMobile" with a "Multiline String" value copied from this text field. If a BES server is not being used, the BlackBerry client is still fully functional, but each user will need to configure the appropriate information for server name, proxy, ports, and so on.

**Sony Ericsson M600/P900/P1i Series**
Configure IBM Sametime Mobile support for Sony Ericsson M600, P900, and P1i devices.

The following configuration steps provision information for users of Sony Ericsson M600, P900, and P1i mobile devices. These steps are optional but highly recommended.

**Hint for user’s first time login**
Enter a user name suffix, for example an email suffix such as @example.com. During login, the **User name** field displays this suffix as a default value, so that users need only add their names before the suffix.

**Sametime server name**
Enter the fully qualified host name of the Sametime Community server that mobile devices will connect to by default; for example, sametime.example.com.

**Port**
Enter the default port used to connect to the specified Sametime Community Server.

**Proxy connection**
Select this setting if mobile users will connect to the Sametime Community Server through a proxy server. If you enable a proxy connection, you must enter a valid proxy URL in the field that follows.

**Proxy URL**
Enter the URL for the proxy server that will connect Sametime Mobile users to the Sametime Community Server.

**Use Sametime Connect user ID and password**
Select this option if you want Sametime Mobile users to connect to the proxy server with their IBM Sametime Connect user name and password instead of using the device's proxy user name and password.
Configuring a Sametime Proxy Server

Configure connection settings to enable the IBM Sametime Proxy Server to communicate with other servers in the deployment.

Related tasks
“Working with Sametime servers that are enabled for SSL” on page 787
Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

“Setting up single sign-on (SSO) for Sametime clients” on page 855
Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Configuring connectivity
Configure connectivity from the IBM Sametime Proxy Server to the Sametime Community Server and Sametime Meeting Server. Connect to a business card server, set up click-to-call, a FIPS server, and clustering.

Configuring connectivity to a Sametime Community Server
By default, the IBM Sametime Proxy server works with an entire Sametime community, but you can optionally configure it to work with one or more clusters of IBM Sametime Community Servers instead.

Before you begin
Before completing this task, ensure that Sametime Community server is configured correctly.

About this task
Complete the following steps to connect the Sametime Proxy Server to the Sametime Community server.

For information on connecting the Sametime Proxy Server to an 8.0.2 Sametime Community Server, see Configuring Sametime 8.5.1 Media and Proxy Servers with an 8.0.2 Community Server using Sametime System Console in the Sametime wiki.

Procedure
1. Login to the Sametime System Console with administrator privileges.
   Example: https://yourserver.com:8701/ibm/console
2. Expand the Sametime System Console twistie.
3. Select Sametime Proxy Servers
4. Select the Deployment Name for the Sametime Proxy Server deployment you wish to configure.
5. Enter the name of the Sametime Community cluster. Separate each cluster name by comma.
   For example: CN=abc/O=ABC,CN=efg/O=EFG
This field designates which Sametime Community Server or cluster will be connected to the current Sametime Proxy Server in a distributed environment. You can choose to leave this field empty in the following situations:

- You want to connect to all Sametime Community Servers simultaneously
- You only have one Sametime Community Server deployed
- You only have one Sametime Community Server cluster deployed

6. Click **Apply**.

7. Click the **Save** link in the "Messages" box at the top of the page.

8. Restart the server or cluster:

   - For a stand-alone server, restart it now as follows:
     a. On the server's Configuration page, click the **Status** tab.
     b. On the Status page, click the **Start/Restart** button at the top of the table.
     c. Click the **Refresh** button and verify that all components are active.
   - For a clustered server, synchronize nodes and restart the cluster as follows:
     a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
     b. Select all nodes in the cluster
     c. Click **Full Resynchronize**.
     d. Back in the navigator, click **System Administration > Node agents**.
     e. Click a node agent, and then click **Restart**; repeat for each node agent.

---

**Configuring connectivity to a Sametime Meeting Server**

Connecting the Sametime Proxy server to a Sametime Meeting server allows browser clients to log in to a Community Server and authenticate automatically with Meeting servers.

**Before you begin**

Configure Single Sign-On (SSO) between the meeting server and the Community Server (either Sametime Community Server or Sametime Standard) that this Sametime Proxy Server will connect to.

**About this task**

Complete the following steps to connect the Sametime Proxy server to a meeting server.

**Procedure**

1. Log in to the Sametime System Console with administrator privileges.
   Example: https://yourserver.com:8701/ibm/console
2. Click **Sametime System Console > Sametime Proxy Servers**.
3. Select the **Deployment Name** for the Sametime Proxy Server deployment you are configuring.
4. Select the type of meeting server to which the Sametime Proxy server will connect.
   The Sametime Proxy server can connect to any of the following meeting servers:
   - Sametime Classic Server (for releases of Sametime 8.5 and higher that are using classic-style meetings hosted on an older Sametime server)
   - Sametime Standard server (used in releases prior to Sametime 8.5)
- Sametime Enterprise Meeting Server (used for clustering meeting servers in releases prior to Sametime 8.5)
- Sametime Meeting Server (for releases of Sametime 8.5 and higher)

5. (Optional) Enable SSL.

6. Enter the fully qualified host name of the meeting server that you selected above.
   For example: sametime_meeting.example.com

7. Enter the port number for that meeting server.
   If you choose Sametime Classic Meeting server, the host name and port fields will be grayed out since the same fully qualified host name and port is used for the Sametime Community server.

8. Click Apply.

Related concepts

“Authentication by token using the Domino Single Sign-On (SSO) feature” on page 860
The Domino Single Sign-On (SSO) feature must be enabled on the Sametime server. This feature creates Lightweight Third Party Authentication (LTPA) tokens that enable web browser users to log in a single time to access multiple Sametime, Domino, or IBM WebSphere servers that are in the same DNS domain. This capability is called "single sign-on."

Configuring Connections as the business card server

By default, the IBM Sametime Proxy Server retrieves business card information from the Sametime Community Server. You can configure the connection to use a Connections server instead by completing the tasks below.

About this task

This feature requires the use of Connections 2.5.0.1 or later. The binding between Sametime users and Connections users is based on email address, so email addresses need to be enabled on the Connections server.

Setting up business cards on the Sametime Community Server

Enable the business cards feature on the IBM Sametime Community Server.

Procedure

2. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.
3. Click the Business Card tab.
4. Add "Email address" to the business card:
   a. Locate Email address in the "Select" list under the "User information" section.
   b. Click Email address, and then click Add->> to add it to the "Selected" list.
   c. Move down to the attributes table.
   d. Locate "Email address" in the "Attribute Name" column.
   e. In the corresponding "Attribute value" column, enter the name of the email field in LDAP directory that is registered with the Sametime System Console.
For example, if the "email" field in the LDAP uses "InternetAddress" then that is the value you enter here.

f. Click the Update button.

5. Click OK.

**Selecting Connections as the business card server**

Configure the IBM Sametime Proxy Server to use a Connections server as the business card provider.

**Procedure**

1. Log in to the Sametime System Console with administrator privileges.
   
   Example: https://yourserver.com:8701/ibm/console

2. Click **Sametime System Console > Sametime Proxy Servers**.

3. Click the Sametime Proxy Server's link to open its Configuration page.

4. Under "General Properties" navigate to the "Business card server" section.

5. Click **Connections Server** and enter the server's address.
   
   The address for a Connections Profile server typically looks like this:
   
   http://connections_server.example.com/profiles

6. Click OK, and then click **Apply**.

**Setting up click-to-call**

Click-to-call enables users of the IBM Sametime Web Client and Meeting Room clients to make calls if the administrator has configured a telephony conferencing server.

**Before you begin**

Before completing this task, ensure that your telephony conferencing server is configured correctly. If you will use Sametime Unified Telephony, make sure the following tasks have been competed before attempting to create the connection as described in this topic:

1. Install the Sametime Unified Telephony API on the Telephony Application Server (for information, see the Sametime Unified Telephony API Guide).

2. Configure LDAP access for the API on the Sametime Unified Telephony server (for information, see the Sametime Unified Telephony API Guide).

3. Set up single-sign on to support the Click to Call feature.

4. Import the SSL certificate from the Sametime Unified Telephony server into the Sametime Proxy Server's Cell truststore.

**About this task**

Complete the following steps to connect the IBM Sametime Proxy server to the telephony conferencing server.

**Procedure**

1. Login to the Sametime System Console with administrator privileges.
   
   Example: https://yourserver.com:8701/ibm/console

2. Expand the **Sametime System Console** twistie.

3. Select **Sametime Proxy Servers**

4. Select the **Deployment Name** for the Sametime Proxy Server deployment you wish to configure.
5. Select a telephony service:
   - **No telephony** (default)
   - **Enable TCSPSI (Telephony Control Service Provider Interface)**
   - **Enable Sametime Unified Telephony**
     - If using Sametime Unified Telephony, enter the **Host name** and **Port** (9080 is the default) of the Telephony Application Server.

6. Enable Secure Sockets Layer (SSL) encryption by clicking **Enable SSL**.
   - **Note**: This step is required when you use Sametime Unified Telephony.

7. Click **OK**, and then click **Apply**.

8. Restart the server if you are using Sametime Unified Telephony.

---

**Configuring a Sametime Media Manager**

This section describes how to configure the components of the Sametime Media Manager.

**Related tasks**

- “Working with Sametime servers that are enabled for SSL” on page 787
- Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

- “Setting up single sign-on (SSO) for Sametime clients” on page 855
- Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

**Configuring anonymous authentication in the SIP Proxy and Registrar**

Enable anonymous authentication on the SIP Proxy and Registrar if your site supports anonymous access from Sametime browser clients using audio-visual features.

**Mapping an anonymous user ID to the anonymous security role**

Map the anonymous user ID to the anonymous security role AnonymousUsers to allow the SIP Proxy and Registrar to distinguish between authenticated users and anonymous users. All anonymous registrations map to the same anonymous user ID.

**Before you begin**

The anonymous user ID must exist in the WebSphere Application Server file-based repository or LDAP repository. Choose a user ID that is not used for Sametime client authentication.

If you do not already have a WebSphere Application Server anonymous user, follow these steps to create one in the WebSphere Application Server file-based repository:
1. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
2. Click Users and Groups > Manage Users.
3. Click Create.
4. Provide values for all required fields.
5. Click Create.
6. When the user has been created, click Close.

Procedure
1. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
2. Click Applications > WebSphere enterprise applications.
3. Click IBM Lotus SIP Registrar.
4. Under Detail Properties, click Security role to user/group mapping.
5. Select the AnonymousUsers security role and click Map Users.
6. In the Search string field, type the same anonymous user ID that you identified in the "Before you begin" section (for example, anonymous@example.com). Then click Search.
7. Select the user from the list and click "->" to move the user to the Selected list.
8. Click Apply and then Save.
9. Restart the SIP Proxy and Registrar server for the change to take effect.

Enabling anonymous authentication through the Trust Association Interceptor
WebSphere Application Server requires the anonymous Trust Association Interceptor (TAI) to be enabled to allow access to anonymous Sametime browser clients using audio-visual features.

Procedure
1. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
2. Click Security > Global security.
3. Click Web and SIP security > Trust association.
5. Click com.ibm.sip.auth.AnonymousAuthTAI.
6. Find the custom property anonymous.user.id. Add the property if it does not exist.
   For its value, use the same anonymous user ID that you mapped to the anonymous security role for the SIP and Proxy Registrar (for example, anonymous@example.com).
7. Find the custom property enable.anonymous.auth.tai. Set the value to true to enable anonymous authentication.
8. Click Apply and then Save.
9. Restart all WebSphere Application Server processes.

Changing the maximum number of anonymous audio-visual users
By default, the SIP Proxy and Registrar allows 5,000 anonymous audio-visual users to connect simultaneously. To raise or lower that limit, change the setting on the Registrar Administration page.

Procedure
1. Log in to the Integrated Solutions Console for the SIP Proxy and Registrar.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registrar Administration.
5. Change the value of the Maximum Anonymous users field.
6. Click OK.

**Configuring dual external TCSPPI adapters**

IBM Sametime supports the use of up to two external TCSPPI adapters; for example, one to support audio, and another for video.

**How do external TCSPPI adapters work?**

IBM Sametime supports the use of up to two external TCSPPI adapters.

The Sametime Media Manager supports a single internal TCSPPI adapter called “Sametime Audio\Video Conferencing”. In addition, you can deploy up to two external TCSPPI adapters; for example, one to support audio, and another for video.

Telephony Conferencing Service Provider Interface (TCSPPI) is a protocol used to establish audio and video calls. The TCSPPI service provider in Sametime Media Manager provides telephony and audio/video services, which are implemented by the TCSPPI adapters hosted on the server’s Conference Manager component. All new TCSPPI external adapters must be deployed on the computer hosting the Conference Manager (if the component is clustered, the external provider can use its own SIP-based MCU to switch RTP data between Sametime Connect clients and different SIP endpoints). A sample “MyAV” TCSPPI adapter is included in the Sametime Software Developer Kit (SDK). The following diagram, an excerpt from the SDK, shows this sample MyAV adapter integrated with Sametime:

![Diagram of Sametime Media Manager with MyAV adapter](image)

**Limitations on using external adapters**

Limitations on deploying external adapters:
- You can deploy one external TCSPPI adapter for audio/telephony within a given community.
- You can deploy one external TCSPPI adapter for video within a given community – the adapter will implicitly support audio as well.
- You can deploy a maximum of two external TCSPPI adapters, irrespective of the number of communities.
• Sametime provides only one policy to control access to the available TCSPI adapters, so a user will get access to all of them, or none. The name of the policy is "Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings."

• If both Sametime Unified Telephony and an external TCSPI telephony adapter are deployed, users will only have access to a single telephony service, even if multiple communities are deployed.

In addition, users with access to Sametime Unified Telephony will see that as their only option for a telephony provider in the client Preferences settings (the user cannot change the setting).

• Deploying multiple instances of the same external TCSPI adapter is not supported. Each adapter must have a unique service provider ID.

Limitations on clients using the external adapters:
• In the client, the Preference settings will allow the user to select one adapter for audio/telephony and one adapter (but not necessarily the same one) for video.
• Users with access to Sametime Unified Telephony will see that as their only option for a telephony provider in the client Preferences settings (the user cannot change the setting).
• For calls made with Sametime Unified Telephony, only callees who also use Sametime Unified Telephony see the "Incoming Call" window.
• For calls made with a TCSPI telephony adapter, the following callees see the "Incoming Call" window:
  – Callees using the same service
  – Callees in the same community
  – Callees using Sametime Unified Telephony (the call is directed to the callee's unified number and the Sametime Unified Telephony UI is used)

Client-Server compatibility when external adapters are deployed

Access to external TCSPI adapters is controlled through a Media Manager policy. When deploying more than one external TCSPI adapter, either upgrade all clients to Sametime 8.5.2 (even users who will not access both external adapters) to ensure clients are enabled to use the adapters, or use the policy to limit access to 8.5.2 clients only.

The following table details support for external TCSPI adapters in deployments that include Sametime servers and clients from multiple releases.

<table>
<thead>
<tr>
<th>Server release</th>
<th>Number of adapters</th>
<th>Client releases</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5.1</td>
<td>1</td>
<td>Mix of 8.5.2 and earlier</td>
<td>The external TCSPI adapter is available to all users for whom the &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; policy is enabled, regardless of client version.</td>
</tr>
<tr>
<td>8.5.2</td>
<td>1</td>
<td>Mix of 8.5.2 and earlier</td>
<td>The external TCSPI adapter is available to all users for whom the &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; policy is enabled, regardless of client version.</td>
</tr>
</tbody>
</table>

Table 126. Client-Server compatibility with external TCSPI adapters
Table 126. Client-Server compatibility with external TCSPi adapters (continued)

<table>
<thead>
<tr>
<th>Server release</th>
<th>Number of adapters</th>
<th>Client releases</th>
<th>Behavior</th>
</tr>
</thead>
</table>
| 8.5.2          | 2                  | Mix of 8.5.2 and earlier | • Only 8.5.2 clients can be enabled to use the external TCSPi adapters.  
• Older clients will have access to one external TCSPi adapters. If you install multiple adapters, you can designate one as the "default" adapter by setting this parameter in the default adapter's ConferenceManager.properties file:  
DefaultService=true  
Older clients see the default adapter and other adapters are ignored.  
Use the "Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings" policy to limit access to 8.5.2 clients. |

Deploying dual external TCSPi adapters

Configure the IBM Sametime Media Manager to use dual external TCSPi adapters.

About this task

The "MyAV" adapter is a reference implementation of an external adapter intended for use as a learning aid. Starting with release 8.5.2 Sametime supports up to two external adapters; for example, you can deploy one adapter to support audio, and another for video.

Procedure

To deploy an external adapter, complete these steps:
1. Define one adapter as the default:  
The default adapter is used for calls in which no service provider ID is specified, as happens with clients from releases before Sametime 8.5.  
   a. Open the adapter's ConferenceManager.properties file for editing.  
   b. Locate the DefaultService parameter and set it to true.  
      DefaultService=true  
   c. Save and close the file.
2. Locate the sametime_tcspi folder on the Conference Manager.  
The sametime_tcspi folder is typically stored in the following location:  
• Stand-alone Media Manager (with Conference Manager included) or dedicated Conference Manager server  
  Linux  
  /opt/IBM/WebSphere/AppServer/profiles/STMSAppProfile  
  Microsoft Windows  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSAppProfile  
• Conference Manager primary node (clustered)  
  Linux  
  /opt/IBM/WebSphere/AppServer/profiles/STMSAppProfile  
  Windows
3. Decide whether to store every adapter in a subfolder, or to leave the files comprising one adapter (any one of the adapters) at the root of the `sametime_tcspi` folder.

4. Copy the adapter's files and folders to the Conference Manager's `sametime_tcspi` folder.

An external adapter comprises the following files:

- JAR file(s) containing the executable code
- `ConferenceManager.properties` file containing the adapter properties
- `properties` subdirectory containing translated string files
- Other configuration files needed by the particular adapter

Be sure to copy all of the adapter files and folders to the Conference Manager.

5. If the Conference Manager is deployed in a cluster, repeat this procedure for every cluster member.

6. Restart the Conference Manager server (or cluster):

- Stand-alone server:
  a. Click the **Status** tab.
  b. On the Status page, click the **Start/Restart** button at the top of the table.
  c. After a few seconds, click the **Refresh** button and verify that the Conference Manager is now active.

- Cluster:
  a. Stop the deployment manager:
     1) Click **System Administration > Deployment manager**.
     2) Click the **Configuration** tab.
     3) On the Configuration tab of the deployment manager settings, click **Stop**.

  b. Start the deployment manager:
     1) Open a command window and navigate to the `app_server_root/profiles/DM_profile_name/bin`.
     2) Run the `startManager` command.

    **Linux**
    ```
    cd /opt/IBM/WebSphere/AppServer/profiles/DM_profile_name/bin
    startManager.sh
    ```

    **Microsoft Windows**
    ```
    cd C:\Program Files\WebSphere\AppServer\profiles\DM_profile_name\bin
    startManager.bat
    ```

7. Do one of the following:

- Upgrade all Sametime clients to release 8.5.2 to ensure access to the external adapters.
- Set the policy to limit access to 8.5.2 clients only (older clients will have no access to any external adapters in this case).
**Configuring a Sametime Meeting Server**

This section describes how to configure a Sametime Meeting Server.

**Related tasks**

“Working with Sametime servers that are enabled for SSL” on page 787

Communications between Sametime servers are encrypted when they are set up to run with the Secure Sockets Layer (SSL). The IBM Sametime servers that run on IBM WebSphere Application Server install with SSL enabled, but you can change the SSL certificates they use.

“Setting up single sign-on (SSO) for Sametime clients” on page 855

Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

**Configuring the Sametime Meeting Server for document conversion**

IBM Sametime Meeting Server lets you take files of various formats (slides, images, and documents) and converts them so they can be shared in a meeting room as slides.

**About this task**

This section shows you how to configure the Sametime Meeting Server for document conversion technology.

**Note:** There are no special configuration steps for using document conversion technology on Windows servers.

Some documents are converted locally using the installed client, which results in higher quality presentation images. Whether or not local conversion is possible depends on the file type, the operating system the client is running on, and which native applications are installed locally. For more information, see the technote called “What document types are locally/client converted when adding them to a meeting room?” at the following Web address:


**Configuring the Sametime Meeting Server for document conversion on AIX**

Follow these steps to configure document conversion technology on an AIX server. A separate remote IBM Meeting server can be deployed specifically for document conversion and can run on Windows or any other supported operating system.

**Procedure**

1. Set the following environment variables. The WebSphere path might be different in your deployment.
2. Install the X Virtual Frame Buffer (Xvfb) and configure it so it runs whenever you start Websphere
   a. Install the XVFB packages from your operating system CDs:
      • OpenGL.OpenGL_X.dev.vfb.05.01.0000.0000 or the equivalent
      • X11.vfb.05.01.0000.0000 or the equivalent
   b. Log in from a terminal shell as the root user and run the following command:
      /usr/bin/X11/X -vfb -x GLX -x abx -x dbe -force :1 &
   c. Verify that the VFB is running properly by entering the following command:
      /usr/lpp/X11/Xamples/bin/xprop -display server_name:1 -root | grep VFB
      Where server_name is the name of your AIX server and 1 is the display number you have associated with this instance of the XVFB. It can be any number except 0. The following message appears:
      XVFB_SCREEN(STRING) = "TRUE"
3. Set the DISPLAY variable to the display number you defined in the previous step:
   DISPLAY=server_name:1
   export DISPLAY

Configuring the Sametime Meeting Server for document conversion on Linux

Follow these steps to configure document conversion technology on a Linux server. A separate remote IBM Meeting server can be deployed specifically for document conversion and can run on Windows or any other supported operating system.

Procedure

1. If you have legally licensed true-type fonts available, copy them to /opt/IBM/WebSphere/STMeetingsServer/stellent/fonts. Make sure that the extensions for the fonts are lowercase (*.ttf) and each font has the correct permission level (755).
2. Set the following environment variables. The WebSphere path might be different in your deployment.
   PATH=$PATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export PATH
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export LD_LIBRARY_PATH
   GDFONTPATH=/opt/IBM/WebSphere/STMeetingsServer/stellent/fonts
   export GDFONTPATH

Note: The LD_LIBRARY_PATH variable can be overwritten other scripts. If you are able to convert image files and not other documents (.txt, .doc, .ppt, etc.), then this might be the cause. Type 'set' in a terminal to see if this variable is still set and has the correct value.

Note: The GDFONTPATH variable must not contain a ':' in the beginning. The only value that should be set here is the path to the fonts. Do not append anything before or after.
**Configuring the Sametime Meeting Server for document conversion on Solaris**

Follow these steps to configure document conversion technology on a Solaris server. A separate remote IBM Meeting server can be deployed specifically for document conversion and can run on Windows or any other supported operating system.

**Procedure**

1. If you have legally licensed true-type fonts available, copy them to `/opt/IBM/WebSphere/STMeetingsServer/stellent/fonts`. Make sure that the extensions for the fonts are lowercase (*.ttf) and each font has the correct permission level (755).

2. Set the following environment variables. The WebSphere path might be different in your deployment.

   ```
   PATH=$PATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export PATH
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export LD_LIBRARY_PATH
   GDFONTPATH=/opt/IBM/WebSphere/STMeetingsServer/stellent/fonts
   export GDFONTPATH
   ```

   **Note:** The GDFONTPATH variable must not contain a ':' in the beginning. The only value that should be set here is the path to the fonts. Do not append anything before or after.

3. If you cannot obtain suitable fonts for the GDFONTPATH option, you may set up an X Virtual Frame Buffer for conversion. Xvfb is already installed on Solaris 9 in `/usr/openwin/bin`. Solaris 8 users must obtain a separate implementation of Xvfb.

   a. Log in from a terminal shell as the root user and run the following command:

   ```
   /usr/openwin/bin/Xvfb :1 -screen 0 1280x1024x8 &
   ```

   You can assign any number except 0 in place of the number 1 in the above example. This is the display number you wish to have associated with this instance of the XVFB. You might get a "No such file or directory" message. This is normal.

   b. Verify that the VFB is running properly by entering the following command:

   ```
   ps -ef | grep vfb
   ```

   You should see the Xvfb process running.

4. Set the `DISPLAY` variable to the display number you defined in the previous step:

   ```
   DISPLAY=server_name:1
   export DISPLAY
   ```

---

**Configuring the Sametime Meeting Server for document conversion on IBM i**

Follow these steps to configure document conversion technology on an IBM i server. A separate remote IBM Meeting server can be deployed specifically for document conversion and can run on Windows or any other supported operating system.
Before you begin

The following products must be installed in order to run conversion services on IBM i:

- Portable Application Solutions Environment (PASE), 5722SS1, 5761SS1, or 5770SS1, option 33
- OS/400® - Additional Fonts, 5722SS1, 5761SS1, or 5770SS1, option 43

Procedure

1. The number set in the DISPLAY environment variable must match the number used in the command to start the XVFB server in the next step.

```
ADDENVVAR ENVVAR(DISPLAY) VALUE('localhost:10') LEVEL(*SYS) REPLACE(*YES)
ADDENVVAR ENVVAR(LIBPATH) VALUE('/qibm/proddata/websphere/appserver/v7/STMeetingsServer/stellent') LEVEL(*SYS) REPLACE(*YES)
ADDENVVAR ENVVAR(PATH) VALUE('/usr/bin:.:/QOpenSys/usr/bin:/qibm/proddata/websphere/appserver/v7/STMeetingsServer/stellent') LEVEL(*SYS) REPLACE(*YES)
```

2. The X Virtual Frame Buffer is used in the file conversion process. It must be running for file conversions to take place. From an IBM i command line, run the following command. This example was formatted for readability; you must enter the command as a single line.

```
QSYS/SBMJOB CMD(QSYS/CALL PGM(QSYS/QP2SHELL) PARM('/usr/bin/X11/X' '-vfb' ':10' '-d' '24'))
USER(QEJBSVR) JOB(QSTXVFB1) JOBQ(QSYSNOMAX)
```

This command starts the XVFB on DISPLAY :10

Note: To check whether the XVFB server is running, use this command:

```
WRKACTJOB JOB(QSTXVFB*).
```

The environment variables must be set when the Sametime Meeting Server starts. The XVFB server must be running for file conversions to occur. If the Sametime Meeting Server was already running during this setup, then the Sametime Meeting Server must be restarted before files will be converted.

Deploying a remote Meeting Server for higher-quality document conversion

If the primary IBM Meeting Server runs on an operating system where conversion quality is lower than on a Microsoft Windows server, you can use a remote Meeting Server to convert documents and presentations for the meeting room.

About this task

In the primary Meeting Server’s configuration page, use the `docshare.remote.url` configuration key to point to the secondary server being used for remote document conversion.

Procedure

1. Install a secondary Sametime Meeting Server. If the server is running on Windows, there are no special configuration steps for using document conversion technology on Windows servers. Otherwise, configure the server for document conversion.


3. Open the configuration page for the primary Meeting Server and click Edit.
4. Provide a URL for the `docshare.remote.url` configuration key in the following format:
   

   where `www.secondary-meeting-server.com` is the fully qualified host name of the secondary Meeting Server.

5. Click **Apply** and **OK**.

### Assigning administrators to the Meeting Room Center

The administrator role must be assigned to a subset of users that are allowed to see meeting statistics for all meeting rooms.

#### About this task

The default IBM Sametime Meeting Server installation maps all users to the administrator role, which allows all users to see meeting statistics. Meeting statistics will show all meeting rooms, including those that are hidden. Map the administrator role to a subset of users that are allowed to see meeting statistics for all rooms.

#### Procedure

1. Log in the Integrated Solutions Console.
2. Click **Applications** > **Application Types** > **WebSphere enterprise applications**.
3. Click the Sametime Meeting Server.
4. Under Detailed Properties, click **Security role to user/group mapping**.
5. To map the administrator role to a select set of users or groups, follow these steps:
   a. Select the role **Admin**, and click **Map Users...** or **Map Groups...**.
   b. Select the name of the user or group and click the right arrow.
   c. Click **OK**.
6. To remove all authenticated users from the administrators role, follow these steps:
   a. Select the role **Admin**.
   b. Click **Map Special Subjects**.
   c. Select none.
   d. Click **OK**.
Chapter 14. Administering

IBM Sametime administrators set up and maintain users and their ability to use Sametime features. They also maintain and monitor the servers.

This section contains information about user registration and policies and the tools that you can use to administer the server.

Related tasks
“Installing WebSphere Application Server updates” on page 476
If you must install additional WebSphere Application Server software updates, perform this step on each of the servers in your deployment running on WebSphere Application Server.

Starting and stopping servers

You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Sequence for starting and stopping servers

Follow the sequence below when starting or stopping servers associated with a Sametime server.

Start server sequence
1. Start the Deployment Manager.
   If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.
2. Start the node agent.
3. Start the Sametime server.

Stop server sequence
1. Stop the Sametime server.
2. Stop the node agent.
3. Stop the Deployment Manager.
   If you installed a server in a cell profile, the Deployment Manager is on the same machine as the Sametime server. If you installed a server in a cluster, the Deployment Manager is probably not on the same machine unless you are running on IBM i.

Note: Before uninstalling WebSphere Application Server, you must stop the application server. If the server belongs to a cluster, you will also need to stop all node agents in the cluster, and then stop the Deployment Manager. Finally, close all browsers and command windows that may have been accessing the WebSphere Application Server.
Server command directories

Run the commands from a command window on the machine where the server is installed and navigate to the appropriate bin directory shown in the following table.

Table 127. Server command directories

<table>
<thead>
<tr>
<th>Type</th>
<th>Profile /bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stSSC_profile_root/bin</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stM_profile_root/bin</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stP_profile_root/bin</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stMS_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stgw_profile_root/bin</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stAdv_profile_root/bin</td>
</tr>
</tbody>
</table>

AIX, Linux, or Solaris

**Note:** The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

Table 128. Start server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Linux only:</td>
</tr>
<tr>
<td></td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STMediaServer</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>./startNode.sh</td>
</tr>
<tr>
<td></td>
<td>./startServer.sh STAdvancedServer</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.
### Table 129. Stop server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td><code>.stopServer.sh STConsoleServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Meeting Server</td>
<td><code>.stopServer.sh STMeetingServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopServer.sh STMeetingHttpProxy</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Proxy Server</td>
<td><code>.stopServer.sh STProxyServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Media Manager</td>
<td><code>.stopServer.sh STMediaServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td><code>.stopServer.sh RTCGWServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td><code>.stopServer.sh STAdvancedServer</code> -username username -password password</td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username -password password</code></td>
</tr>
</tbody>
</table>

### Windows

The Start Programs menu is also a convenient way to start and stop Sametime servers running on WebSphere Application Server.

**Note:** The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

### Table 130. Start server commands for Windows

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMeetingServer</td>
</tr>
</tbody>
</table>
Table 130. Start server commands for Windows (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STMediaServer</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>startNode.bat</td>
</tr>
<tr>
<td></td>
<td>startServer.bat STAdvancedServer</td>
</tr>
</tbody>
</table>

**Note:** Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

Table 131. Stop server commands for Windows

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer.bat STConsoleServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stopServer.bat STMeetingServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopServer.bat STMeetingHttpProxy -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer.bat STProxyServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>stopServer.bat STMediaServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stopserver.bat RTCGWServer</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>stopServer.bat STAdvancedServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>stopNode.bat -username username -password password</td>
</tr>
</tbody>
</table>
**IBM i**

*Note:* The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

**Table 132. Start server commands for IBM i**

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>startNode startServer STConsoleServer</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>startNode startServer STMeetingHttpProxy startServer STMeetingServer</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>startNode startServer STProxyServer</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>startNode startServer RTCGWServer</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>Not supported on IBM i</td>
</tr>
</tbody>
</table>

*Note:* Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

**Table 133. Stop server commands for IBM i**

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>stopServer STConsoleServer -username username -password password stopNode -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>stopServer STMeetingServer -username username-password password stopServer STMeetingHttpProxy -username username-password password stopNode -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>stopServer STProxyServer -username username-password password stopNode -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>Not supported on IBM i</td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td>stopServer RTCGWServer -username username-password password stopNode -username username -password password</td>
</tr>
</tbody>
</table>
Related concepts
“How installing cell profiles affects starting and stopping servers” on page 481
If you chose the configuration type “Cell Profile” when you installed a Sametime Proxy Server, Sametime Media Manager components, or a Sametime Meeting Server, you installed a self-contained set of WebSphere Application Server components for each server. You have this configuration type if you installed different Sametime servers on the same machine or on multiple machines that are not clustered.

Related tasks
“Starting and stopping the Deployment Manager” on page 481
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.
“Starting and stopping WebSphere Application Servers on Windows” on page 486
Use the Start Programs menu in Microsoft Windows to start or stop any Sametime servers running on WebSphere Application Server.

Sametime component URLs
This section lists the URLs for IBM Sametime servers and components.

The following table lists the URLs for logging in to Sametime:

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single Integrated Solutions Console URL is only applicable if you deploy a cluster and choose to use the Sametime System Console as the Deployment Manager for all Sametime products.</td>
<td>The default port is 8700 for all platforms except IBM i. For IBM i, the port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime System Console Deployment Manager Profile and use the setting specified for the &quot;Administrative console port.&quot; For the default profile name (STSCDmgrProfile), the file is located here: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDmgrProfile/logs/AboutThisProfile.txt</td>
<td></td>
</tr>
<tr>
<td>Sametime component</td>
<td>URL</td>
<td>Logging in</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----</td>
<td>------------</td>
</tr>
</tbody>
</table>

The default port is 9060 for all platforms except IBM i.

For IBM i, the port number may not be 9060. To check the port, open the logs/AboutThisProfile.txt file for the Websphere Application Server profile that is running the ISC for your Gateway server and use the setting specified for the "Administrative console port."

If you have installed a single Sametime Gateway server, this will be the one Sametime Gateway profile you have. If you have a cluster setup, this profile will be the Deployment Manager profile that your Sametime Gateway server has been clustered with.
Table 134. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime web client</td>
<td><a href="http://proxyserverhostname.domain:port/stwebclient/index.jsp">http://proxyserverhostname.domain:port/stwebclient/index.jsp</a></td>
<td>Log in with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>To verify the port number being used by the Lotus Sametime Proxy Server, log in the Lotus Sametime System Console. In the WebSphere Application Server administrative console, click Servers - WebSphere application servers - STProxyServer - ports -WC_defaulthost to find the port number. For IBM i, to verify the HTTP port number being used by the Lotus Sametime Proxy Server, open the AboutThisProfile.txt file for the Sametime Proxy Application Server Profile and use the setting specified for the HTTP transport port. The default profile name is STPAppProfile. On IBM i, look for the AboutThisProfile.txt file in the following location:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs/AboutThisProfile</td>
<td></td>
</tr>
</tbody>
</table>
### Table 134. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meeting Room Center</strong></td>
<td><a href="http://meetingserver">http://meetingserver</a> hostname.domain:port/stmeetings</td>
<td>Log in with your user name and password.</td>
</tr>
<tr>
<td><strong>Sametime Community Server Administrator Tool</strong></td>
<td><a href="http://communityserver">http://communityserver</a> hostname.domain:port/stcenter.nsf</td>
<td>Log in with your Domino administrator's name and password. Under Administrator Tools, click Administer the server.</td>
</tr>
</tbody>
</table>

#### Adding administrators

Add yourself or others as administrators for the WebSphere Application Server-based IBM Sametime components.

#### About this task

You must give yourself and users that you designate as administrators the same roles as the wasadmin in order to manage Sametime using the Sametime System Console. The wasadmin ID is the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.

#### Procedure

1. From a browser, enter the URL for the Sametime System Console.
2. Enter the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.
   The default name is wasadmin.
3. Click **Applications > Application types > WebSphere enterprise applications**.
4. Click Sametime System Console (deployment.ear).
5. Under Detail Properties, click **Security role to user/group mapping**.
6. Note the roles for wasadmin. For information on the access level of the roles see "Administrative roles" in the WebSphere Application Server information center.
Click Cancel to return to the Integrated Solutions Console.

7. Click Users and Groups.

8. Select either Administrative user or Administrative group to assign yourself and other designated administrators to the Administrator and Admin Security Manager roles, and other roles assigned to wasadmin.

   Note: An administrator cannot map users and groups to the administrator roles without having the Admin Security Manager role.

9. Save your changes.

Changing the administrator password

The following topics explain how to change your administrator passwords.

Updating your DB2 administrator password

If you change your administrator password in IBM DB2, you must update your password in the Sametime System Console, as well as the Meeting Server and, if applicable, Sametime Advanced. If you do not update your password, IBM Sametime stops working.

Procedure

1. Log in to the Integrated Solutions Console for the Sametime System Console.
2. Click Resources > JDBC > Data sources.
3. Click the data source in the table.
4. Under Related Items, click JAAS - J2C authentication data.
5. Click your DB2 administrator alias.
6. Under General Properties, type your new password.
7. Click Apply and then click OK.
8. Repeat this procedure for the Sametime Meeting Server and, if applicable, the Sametime Advanced server.
9. Restart the Sametime System Console and Meeting Server or Advanced Server.

   The changed password only takes effect after you restart the server, so be sure to restart the server.

Updating your LDAP Bind password

You can change the LDAP Bind password that you defined when you first connected the LDAP server.

About this task

Change your LDAP Bind password by running the Connect to LDAP Servers prerequisite in the Sametime System Console. Changing the password updates the Sametime Community Server database, stconfig.nsf and the WebSphere Application Server. Then send the update to any other Deployment Managers in the environment and to the Directory Assistance database on the Sametime Community Server.
Procedure

1. From the Sametime System Console, run the Connect to LDAP Servers prerequisite. Update the LDAP Bind password when you are prompted to do so and save the changes.
   The change updates the LDAP repository configured for WebSphere Application Server.

2. Wait for the next scheduled update task to run, which updates the LDAP Server document in the Sametime Community Server configuration database (stconfig.nsf) with the password change.

3. If the Sametime System Console is the Deployment Manager for all Sametime servers, proceed to the next step.
   If there are other Deployment Managers in the Sametime environment, update the Bind password on each Deployment Manager. Make the change by editing the LDAP repository as described in the WebSphere Application Server information center topic Lightweight Directory Access Protocol repository configuration settings.

   a. From the Notes client, open the Directory Assistance database (usually named da.nsf) on the Community Server.
   b. Open the Directory Assistance document for the LDAP server.
   c. On the LDAP tab, under Connectivity Settings, update the Administrator password.
   d. Save and close the document.

5. Restart the Community Servers, Deployment Managers, and Application Servers that share the LDAP repository.

Related tasks

“Connecting to an LDAP server” on page 265
Use the IBM Sametime system console to connect IBM Sametime servers to an LDAP server that has already been installed and configured. An LDAP server is required for these server offerings: community server, meeting server, media manager, and gateway.

“Creating a Directory Assistance document” on page 710
The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the LDAP server.

Updating your WebSphere Application Server administrator password

You can change your WebSphere Application Server administrator password.

About this task

You can change your WebSphere Application Server administrator (wasadmin) password on the following WebSphere-based Sametime servers. If you change the wasadmin password on any of these servers, then you must also update the wasadmin password for that server that is stored in the Sametime System Console.

- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Gateway Server
The complete Sametime Media Manager installations are listed under both the Media Manager and the SIP Proxy and Registrar administration listings. There is only one entity and changing the connection properties in one place is reflected in the other.

A FIPS Proxy Server uses the same credentials as the Sametime Proxy Server on which it was installed. Changing the credentials in either location affects both administrative connections. The FIPS Proxy Server list depends on a valid server connection, so if the connection information is not correct, the FIPS Proxy server is not be listed. You can correct this by editing the connection properties in the Sametime Proxy Server listing.

**Procedure**

1. Change the wasadmin password of the WebSphere-based Sametime application server.
   a. Log in to the Integrated Solutions Console on the WebSphere-based Sametime application server.
   b. Click Users and Groups > Manage Users.
   c. Under Search for Users, select User ID in the Search by field, and then enter wasadmin in the Search for field. Click Search.
   d. Click wasadmin in the results dialog.
   e. Enter a new password in the Password and Confirm Password fields.
   f. Click Apply and then click OK.
2. Update the wasadmin password that you changed in the previous step on the Sametime System Console.
   a. Log in to the Integrated Solutions Console for the Sametime System Console.
   b. Click Sametime System Console > Sametime Servers.
   c. Click the Sametime application server that has the wasadmin password that you changed in step 1.
   d. Locate the deployment name and click Edit under Connection Properties.
   e. Enter a new password.
   f. Click Save and then click Done.

**Managing users with policies**

All IBM Sametime users are automatically assigned to default policies. Sametime Instant Messaging, Meetings, and Media Services each has a default policy to be applied to users. You can create additional user policies, and assign users and groups to these policies.

**Before you begin**

If you upgraded from an earlier release, complete the steps for migrating policy assignments before setting any new ones.
About this task

When a user authenticates, Sametime applies a default policy if no other policy can be found for that user. You can create new policies that grant or limit access to features, and assign users to these policies. Users can be assigned to more than one policy. If a user belongs to more than one policy, then Sametime uses the policy weight to determine policy precedence. Custom policies can be designed for specific groups in the company, and the default policy can be inherited or assigned. Meetings policy changes take effect immediately, while Instant Messaging and Media Services policy changes take effect within an hour.

There is also an anonymous policy that is assigned by default to users who have not authenticated, and unauthenticated users always receive this policy.

Note: If your deployment includes the Sametime System Console, you must manage policies there because all settings made in the legacy Sametime Administration Tool (STCenter.nsf) are ignored. This includes the override all feature, as well. Moreover, there is no automatic migration of policies from the Sametime Administration Tool to the Sametime System Console. You must do this manually because Sametime Administration Tool policies do not map one-to-one to policies in the Sametime System Console.

Do not use the ampersand character (&) in the policy's name or in any one of the values of policy attributes.

Related concepts
“Migrating policy settings from releases earlier than 8.5” on page 767
You must manually migrate your pre-8.5 IBM Sametime policy settings from the Administration Tool to new policy settings in the Sametime System Console. Review the settings used in the Administration Tool on the community server and write them down; recreate them on the new system console.

Related tasks
“Upgrading policies from Release 8.5 or 8.5.1” on page 694
Changes in the way policies are defined on the backend require you to take steps after upgrading the servers to ensure that your IBM Sametime Release 8.5 or 8.5.1 policies work with the new design.

Finding policies associated with a user

You can find all the policies associated with a user for all the IBM Sametime products to which the user has access.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click any user Sametime component. It does not matter which component that you select, because your search results display all the policies for all the Sametime components to which the user has access.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Click Find Active Policies.
6. Select the criterion for the user for which you want to find the associated policies in the **Search by** field.
   - User ID
   - Name
   - E-mail address
7. Enter the entire or partial user ID, email address, or name of the user or group in the **Search for** field. If you enter partial information, use an asterisk as a wild card character for missing or incomplete information. For example, type `sm*` for all names starting with `sm`.
8. Select the number of listings in the search results in the **Maximum results** field.
9. Click **Search**. The results display the users that match your search criteria.
10. Select a name in the results table, and then click **Find Active Policies** to show the policies for that user.
11. Click **Done**.

**Creating new user policies**

You can create user policies, and assign users and groups to these policies.

**About this task**

You can set policy for users to have access to specific IBM Sametime features, depending upon their level of need. For example, the maximum size for a file being transferred is set by default at 1 megabyte to help manage traffic over the server(s); however, if you have a group that routinely transfers large files for business reasons, you can create a new policy specifically for those users and set the maximum size of files that they can send to a much higher number.

**Note:** When you create a new policy, it uses the default policy settings as the base settings in the new policy. You can update these settings.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. Click the Sametime product for which you want to create a policy.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Click **New**.
6. Enter a name to use to identify the policy in the **Policy Name** field.

   **Note:** Do not use the following special characters in the policy’s name or in any one of the values of policy attributes:
   - Ampersand (&)
   - Apostrophe (’)
   - Quotation mark ("")
   - Greater than character (>)
   - Less than character (<)
7. Specify the features that you want to enable or disable for the users or groups that you will assign to this policy. Some instant messaging features are flagged with IC characters after the field label. This flag indicates that a feature is only available for installed clients. The feature is not available to browser clients.

8. Click OK.

Results

Tip: You can follow these same basic steps to delete or edit a policy. Delete a policy by selecting the policy and then click the Delete button. Edit a policy by clicking the policy name. You cannot delete the anonymous or default policies, but you can edit them. If you edit a policy, you cannot change the policy ID. To do this, you must make a copy of the policy by selecting it and clicking Duplicate, then you can enter a new ID in the copy. Before you delete the original, be sure to reassign the users and groups to the copy and give it the proper policy weight.

What to do next

You can now assign users and groups to this policy.

Assign users and groups to policies

You can assign users and groups to specific user polices to grant or limit access to features in IBM Sametime.

About this task

You cannot assign users to the default or anonymous policies. Authenticated users are automatically assigned to the default policies. Unauthenticated users are assigned to anonymous policies.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime component with the policy to which you want to assign a user or a group.
   • Instant Messaging
   • Meetings
   • Media Manager
5. Select a policy name from the list, and click Assign.
6. Click Add Users or Add Groups.
   At this point you could remove a user from a policy, by selecting the user in the list and then clicking Remove.
7. Select the criterion for searching for the user or group that you want to add to the policy in the Search by field.
   • User ID
   • Name
   • E-mail address
8. Enter user ID, email address, or name or partial name with wildcard characters (asterisks) of the user or group in the Search for field
9. Select the number of listings on each search results page in the **Maximum results** field.

10. Click **Search**. The results display the DN, display name, and email address of the users that matched your search.

11. Select a user and click **Assign**.

12. Click **Done**.

**Sametime Instant Messaging user policy settings**

You can grant or limit access to features in IBM Sametime Instant Messaging by enabling or disabling various policies for users. Instant Messaging policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take effect by editing the `REFRESH_RULES_INTERVAL` setting in the `sametime.ini` file.

All unauthenticated users have the anonymous policy, Sametime Instant Messaging Anonymous Policy, applied to them. For authenticated users, the Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match, then the default policy, Sametime Instant Messaging Default Policy, is applied.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

*Table 135. Chat*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must set this community as the default server community</td>
<td>Determines if this community can be connected to as a secondary community or if must it be the default community for the Sametime Connect client. When this policy is selected, users must log in to this community before they can log in to other communities. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 135. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to add multiple server communities</td>
<td>If this is checked, community preferences and menus are available to users. When the <strong>Allow user to add multiple server communities</strong> policy is set to <strong>Not selected</strong>, users cannot add their own secondary communities. When the policy becomes enabled, clients cannot log in to any secondary communities that were not set by the administrator. Administrator-defined secondary communities are not impacted by the policy. The client recognizes they are defined by the administrator and allows the user to log into them. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Allow user to add external users using</td>
<td>Allowing users to connect to external communities such as AIM, OCS, and Google Talk. If this policy is not allowed, the check box and text for adding external users by email address is not available in clients.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Sametime Gateway communities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow user to save chat transcripts</td>
<td>If this is enabled, users see the File-Save option in the chat window. Chat history capabilities are available. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically save chat transcripts</td>
<td>This is not valid unless <strong>Allow user to save chat transcripts</strong> is selected. If this is not selected, then users do not see preferences for chat history or the chat history viewer in their clients. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1054  Sametime Advanced: Installation and Administration Guide
<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum days to save automatically saved chat transcripts</td>
<td>If <strong>Allow to automatically save chat transcripts</strong> is selected, then a value must be entered in this field. Users cannot set a larger value in their clients than the one specified here. This setting does not apply to browser users.</td>
<td>365</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>Limit contact list size</td>
<td>This limits the number of contacts that users can enter in their contact lists.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Contacts</td>
<td>If <strong>Limit contact list size</strong> is selected, then a value must be entered in this field. Specify the number of contacts that users can enter in their contact lists.</td>
<td>500</td>
<td>500</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow all Sametime Connect features to be used with integrated clients</td>
<td>If this is not selected, some Sametime Connect features do not display when Sametime is integrated with other products. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow mobile client</td>
<td>This feature lets users deploy Sametime awareness and chat features mobile device.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Table 135. Chat (continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime update site URL</td>
<td>Provides a URL where users can retrieve updates to features for the Sametime Connect client. This setting does not apply to browser users.</td>
<td>updates.sametime.ibm.com</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table 136. Image Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow custom emoticons</td>
<td>Allows all actions on the preferences palette: new, import, export, add picture, add palettes. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow screen capture and images</td>
<td>Allows pasting and right-click copying of image and screen captures. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Set maximum image size for custom emoticons, screen captures, and inline images</td>
<td>This setting includes images pasted inline through the palette emoticons, cut and paste, screen captures, and print screen. It does not include images sent through file transfer. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 136. Image Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB</td>
<td>If set maximum image size for custom emoticons, screen captures, and inline images is selected, then a value must be entered in this field. Users see a message if they attempt to send a file that is larger than the specified size. This setting does not apply to browser users.</td>
<td>500</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

### Table 137. File Transfer

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to transfer files</td>
<td>Allows user to transfer files to other users. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Maximum file transfer in Kilobytes</td>
<td>Limits the size of the file that can be transferred by the specified value. In kilobytes. This setting does not apply to browser users.</td>
<td>1000</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Allow client-to-client file transfer</td>
<td>Allows users to transfer files without passing the files through the Sametime server. These files are not logged. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 137. File Transfer (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use exclude file types transfer list</td>
<td>Limits the types of files that users can transfer. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>

| Types to exclude from transfer. Type the three-letter extension of each file type, separated by a comma or semicolon | If Use exclude file types transfer list is selected, then a value must be entered in this field. Type the three-letter extension of each file type, separated by a comma or semicolon. Accepts bmp, gif, txt, pdf, sxi, sxc, sxw file extensions. Comma separated, values, and spaces are acceptable. This setting does not apply to browser users. | exe, com, bat | Blank | No |

Table 138. Plugin Management

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to install plug-in</td>
<td>Allows users to install plugins and updates from the Sametime Connect Tools &gt; Plug-ins menu. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Meetings user policy settings

You can grant or limit access to features in meetings by enabling or disabling various policies for users. Policy changes take effect immediately.

All unauthenticated IBM Sametime users have the anonymous policy, Sametime Meetings Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match the default policy, Sametime Meetings Default Policy is applied.

Sametime does not allow anonymous users to create meeting rooms. Therefore, any policy that is related to authenticated users or the ability to create meeting rooms, does not apply to anonymous users.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

Note: Although Sametime Classic meetings are still managed on the server itself, you can set user policy for Sametime Classic meetings on the Meetings policy tab in the Sametime Classic Meetings section.

Table 138. Plugin Management (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime optional plug-in site URLs. Type the URLs separated by a comma or semicolon</td>
<td>If no value is specified, then the Check for Optional Features item on the Tools &gt; Plug-ins menu not valid. This setting does not apply to browser users.</td>
<td>Blank. Type the URLs separated by a comma or semicolon</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 139. General Meeting Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum persistent meeting rooms this user can own</td>
<td>Users are limited to creating this number of meeting rooms per user. When this limit is reached or set to zero, users cannot create more meeting rooms.</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Allow user to create instant (nonpersistent) meeting rooms</td>
<td>If not selected, user does not see the capabilities for creating instant meetings. User can, still see the capabilities for using an existing room.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Automatically connect to meeting server when logging into Sametime Connect</td>
<td>If not selected the user must manually connect to each meeting room server to view the meetings there. This setting is stored with the client, so that changes in the policy do not take effect until after the next time the user logs in to the server. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching of meeting rooms</td>
<td>If not selected, users can attend meeting rooms only with a direct URL. The meeting room manager interface never shows. Only affects browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching of hidden meeting rooms</td>
<td>If selected, the interface allows the user to explicitly search for hidden meeting rooms by exact name. If not selected, the interface for searching for hidden meeting rooms does not appear, and hidden meeting rooms are never returned in search results.</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Show &quot;Scheduled Meetings&quot; view</td>
<td>Determines whether to show the &quot;Scheduled Meetings&quot; view in the shelf. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Allow meetings to be recorded</td>
<td>Allows users to record meetings for rooms they have created. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow meeting content to be downloaded</td>
<td>Allow users to download content from the meeting library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Meeting room group chats</td>
<td><strong>Hidden</strong> - Users cannot see or create group chats. <strong>Read-only</strong> - Users can only read what others have typed into the group chat. <strong>Interactive</strong> - Users can type and read group chats.</td>
<td>Interactive</td>
<td>Interactive</td>
</tr>
<tr>
<td>Allow meeting room polls</td>
<td>Determines whether a presenter can send a poll to meeting participants.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Allow annotations of uploaded content</td>
<td>Determines whether a presenter can use meeting room annotation tools when sharing documents from the meeting room library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 139. General Meeting Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum file upload size, in Megabytes</td>
<td>Maximum file upload size for an individual user in megabytes. Users cannot upload a larger file into the library.</td>
<td>50</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 140. Meeting Room Library
Table 140. Meeting Room Library (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum total size of library in Megabytes</td>
<td>Maximum total size in megabytes of files that a meeting room library can hold. When the library contains the maximum size or if the size is set to zero, users cannot upload files to the library. In addition, when the library's maximum storage capacity has been reached, users may be unable to upload all their files even though their individual file upload size.</td>
<td>200</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 141. Screen Sharing

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen sharing</td>
<td><strong>Disabled</strong> - Users cannot share screens or applications.</td>
<td>Entire screen, frame, and applications</td>
<td>Entire screen, frame, and applications</td>
</tr>
<tr>
<td></td>
<td><strong>Share an application</strong> - Users can share a specific application. No other applications or their desktops are shared.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Entire screen, frame, and applications</strong> - Users share their whole screen including any applications that they open on their screens.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow user to control another user's shared screen</td>
<td>Allow others to control a user's shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow peer-to-peer application sharing</td>
<td>Whenever this user hosts screen sharing, peer-to-peer can be used by any viewers that support it.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
</tbody>
</table>
Table 141. Screen Sharing (continued)

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce bandwidth limitations.</td>
<td>Any time the user hosts sharing, the experience is limited by the value specified in the Maximum bandwidth size.</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Maximum bandwidth size, in Kilobytes per second:</td>
<td>This is not used unless &quot;Enforce bandwidth limitations&quot; is selected.</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

Table 142. Sametime Classic Meetings.

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to create instant meetings and breakout sessions.</td>
<td>Lets users start a meeting from the contact list, from an existing chat, and from within a meeting (breakout session).</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow Sametime IP audio and video in instant meetings and breakout sessions.</td>
<td>No Does not allow use of Sametime Internet Protocol audio and video in instant meetings and breakout sessions.</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IP audio only</td>
<td>Allow use of Sametime Internet Protocol audio but not video in instant meetings and breakout sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP video only</td>
<td>Allows use of Sametime Internet Protocol video but not audio in instant meetings and breakout sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 142. Sametime Classic Meetings (continued).

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow participation in meeting room chats.</td>
<td>Allows participants in the meeting to use the chat window to communicate with any other participant in the meeting.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow screen sharing</td>
<td><strong>No</strong> - Users cannot share screens or applications.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Application only</strong> - Users can share a specific application. No other applications or their desktops are shared.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Entire screen, frame, and applications</strong> - Users share their whole screen including any applications that they open on their screens.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow user to control another user's shared screen</td>
<td>Allow others to control a user's shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>

**Media Manager user policy settings**

You can grant or limit access to media features in by enabling or disabling various policies for users. Media Manager policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take affect by editing the `REFRESH_RULES_INTERVAL` setting in the `sametime.ini` file.
All unauthenticated users will have the anonymous policy, Media Manager Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match for the default policy, Media Manager Default Policy is applied.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

*Table 143. Telephony, Audio, and Video*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings</td>
<td>Allows outside vendors to provide audio and video for instant messages and instant meetings. This setting does not apply to browser meetings.</td>
<td>Not selected</td>
<td>Not selected</td>
<td></td>
</tr>
<tr>
<td>Allow changes to preferred numbers</td>
<td>If not selected, user cannot add telephony devices. This gives the administrator control over the devices that can make or receive calls in the system. &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; must be selected to specify this setting.</td>
<td>Selected</td>
<td>Selected</td>
<td></td>
</tr>
</tbody>
</table>
Table 143. Telephony, Audio, and Video (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
</table>
| Voice and video capabilities available through the Sametime Media Server: | Allows users to use computer audio and video in instant messages and instant meetings. Choices are:  
• None  
• Audio only  
• Audio and video | Audio and video | Audio and video |  |
| | This setting does not apply to browser users. | | |  |

Table 144. Sametime Unified Telephony

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
</table>
| Allow changes to the permanent call routing rule | If this setting is not selected a lock appears next to this rule in the user’s preferences.  
“Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings” must be selected to specify this setting.  
This setting does not apply to browser users. | Selected | Selected |  |
Table 144. Sametime Unified Telephony (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of &quot;Offline&quot; status in call routing rules.</td>
<td>Allows users to add their own devices to make and receive calls. &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; must be selected to specify this setting. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td></td>
</tr>
</tbody>
</table>

Changing a user policy's weight

IBM Sametime products implement user policies that have higher weights over policies with lower weights. You can change the weight of policies.

About this task

User policies in Sametime have weights. A policy’s weight determines whether or not its attributes take precedence over the attributes of other policies. For a given user or group assigned two or more policies, Sametime implements the policy with the highest weight. Anonymous policies always have the lowest weight; default policies have the next lowest weight. For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match. If no group matches are found, the default policy applied. You can change the weight of policies by moving them up and down the policy list of a Sametime product.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime component with the policy with the weight that you want to change.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Select a Policy ID from the list, and click Move Up or Move Down. Moving the policy up increases its weight; moving the policy down decreases its weight. You cannot change the weight of a default or anonymous policy.
Using nested groups in policy assignments

You can configure whether or not Sametime considers nested groups when it applies policies and how many levels deep that Sametime searches for the highest weighted group.

About this task

For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match to which the user belongs. By default, Sametime searches through four levels of nested groups when determining the highest weighted policy.

For example, a fourth level assigned group would mean that the group is four levels above the user. In the following example the EMEAGroup is four levels above the user: EMEAGroup (level 4) contains UKGroup (level 3), which contains LondonGroup (level 2), which contains MarketingGroup (level 1), which contains the user.

Follow these steps to change the number of levels of nested groups that Sametime searches for the highest weighted policy. If a policy is assigned to a group higher than the nesting depth, that the default policy is assigned. Entering a large number as the maximum nested group depth can have an impact on performance.

Note: To change the maximum nested group depth for the Sametime Instant Messaging user policy, edit DIR_SEARCH_LEVEL_LIMIT parameter of the Sametime Community Server sametime.ini file.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click Preferences.
5. Enter a numerical value of -1 or greater in the Maximum Nested Group Depth field.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Sametime searches an infinite number of levels of nested groups.</td>
</tr>
<tr>
<td>0</td>
<td>Sametime searches for the user ID directly, and does not look in groups, nested or otherwise.</td>
</tr>
<tr>
<td>1</td>
<td>Sametime searches within groups, but not nested groups (groups within groups).</td>
</tr>
<tr>
<td>2 or greater.</td>
<td>Sametime searches nested groups up to and including the level specified.</td>
</tr>
</tbody>
</table>

6. Enter a number in minutes in the Policy Cache Timeout field. The default value is 30 minutes. The Policy cache stores policy assignments. This cache reduces the number of database operations required to provide policy information. For example, if Sametime calculates that user1 gets policy1, that is
stored in the cache. The next time that something requests user1’s policy it does not have to calculate it. The timeout is how long the information stays in the cache.

7. Enter a number in minutes in the Group Membership Cache Timeout field. The default value is 30 minutes. The Group Membership cache stores the group membership information. This cache alleviates potential LDAP load issues due to group membership look-ups. You might want to update this timeout to reflect your site’s LDAP administration operating procedures.

8. Click Apply.
9. Restart the servers.

Example

In following examples, use the this group structure:
1. Group1 contains user1
2. Group2 contains user2 and group1
3. Group3 contains user3 and group2
4. Group4 contains user4 and group3
5. Group5 contains user5 and group4
6. Group6 contains user6 and group5

Example 1: Nested group matches
Policy1 has a weight of 2 and is assigned Group6. Nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.

User1 and User2 get the default policy because they are not within the group search depth limit.

Example 2: Nesting has priority over policy weight
Policy1 has a weight of 2 and is assigned Group5. Policy2 has a weight of 3 and is assigned Group6. The nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets policy1 because it is in the 4th group nesting level from Group5.
3. User3 gets policy1 because it is in the 3rd group nesting level from Group5.
4. User4 gets policy1 because it is in the 2nd group nesting level from Group5.
5. User5 gets policy1 because it is in the 1st group nesting level from Group5.
6. User6 gets policy1 because it is in the 4th group nesting level from Group5.

Even though policy2 has a higher weight, it is not assigned to User2, User3, User4, and User5 because they have a lower level policy match.

Example 3: Policy weight breaks ties

Chapter 14. Administering
Policy1 has a weight of 3 and is assigned to Group6. Policy2 has a weight of 2 and is assigned to Group6. The nesting level is the default of 4.

1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.

Since both Policy1 and Policy2 were at the same level, Policy1 won the tie breaker because it has a higher weight.

---

**Administering a Sametime System Console**

This section describes how to manage the IBM Sametime System Console.

**Backing up the console database**

The IBM Sametime System Console database stores information about all the Sametime servers that are connected to it.

**About this task**

Back up the database regularly to protect the server data and to minimize downtime if you need to restore lost or corrupted data. Follow the instructions in the DB2 information center:

http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp

**Starting the Sametime System Console so you can administer servers**

When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

**Before you begin**

Verify that the Deployment Manager is running for the cell.

**Procedure**

1. Open a command window (on IBM i, run QSH command).
2. Navigate to the local app_server_root/profiles/STSCAppProfile profile directory and change to the bin directory.
3. Run the following command. Note that the name of the server is case sensitive:

   **AIX, Linux, or Solaris**
   
   ./startNode.sh
   
   ./startServer.sh STConsoleServer

   **Windows**
   
   startNode.bat
   startServer.bat STConsoleServer

   **IBM i**
   
   startNode
   startServer STConsoleServer
Related tasks

“Logging in to the console” on page 483
Use the Sametime System Console and its underlying WebSphere Application Server Integrated Solutions Console to prepare for server installations and configure and administer servers running on WebSphere Application Server after installation.

“Starting and stopping the Deployment Manager” on page 481
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

Related reference

“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Administering a Sametime Community Server

This section describes how to manage an IBM Sametime Community Server

About this task

Use the instructions in this section to manage connectivity, community services, anonymous access, and business cards on the Sametime Community Server.

Managing administrator access and roles

Manage administrator access and roles using the Sametime Administration Tool.

Starting the Sametime Administration Tool

You administer Sametime through a web browser application. You must enable Java applets and JavaScript or ActiveX Controls in your browser to use the Sametime Administration Tool.

About this task

To start the Sametime Administration Tool:

Procedure

1. Enter the URL for the Sametime server:
   http://hostname/stcenter.nsf
   where hostname is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime server you want to administer.

   Note: For versions of Sametime that do not support web conferencing, enter the following URL in your browser: http://hostname.

   Note: For Sametime Entry and other Sametime offerings that do not include web conferencing, access the server page by typing http://hostname/ into a browser URL field where hostname is the fully qualified name of your Sametime server.

2. From the Sametime server home page (Sametime Welcome page), click Administer the Server.
3. Enter the administrator name and password specified during the Sametime server installation. The Sametime Administration Tool opens in its own web browser window.

Related concepts
User requirements for basic password authentication
When accessing the Sametime server with a Web browser, a user must enter a user name and Internet password to access any protected database on the Sametime server.

Adding a new Sametime administrator
Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

Adding a Sametime administrator in Domino LDAP
Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

A Sametime administrator name and password is specified during the Sametime installation and setup process. The administrator specified during the Sametime server installation and setup can access all features of the Sametime Administration Tool and can provide other administrators with access to the Sametime Administration Tool.

This is the procedure for adding an administrator in Domino. If your Sametime server is configured for LDAP, then you must create the new administrator using your LDAP Directory tools.

Creating a Person document for the administrator:
Administrators must have a Person document in the Domino Directory.

About this task
Follow these steps to create a Person document using the Sametime Administration Tool. If the administrator whom you are adding already has a Person document that contains a last name, user name, and Internet password, skip this procedure.

Procedure
1. From the Sametime server home page, click **Administer the Server**.
2. From the Sametime Administration Tool, click LDAP Directory:
3. Choose **Add Person**.
4. In the Person document, select the Basics tab.
5. Enter the user's first, middle, and last name in the appropriate fields. Only the last name is required.
6. Enter a name for the user in the User Name field. An entry in this field is required for the user to authenticate with the Sametime server.
   You can use any of the following characters in a user name: A - Z, 0 - 9, dash (-), period (.), underscore (_), and space. Using other characters can cause unexpected results.
7. Enter an Internet password for the person in the "Internet password" field. An entry in this field is required for the user to authenticate when accessing the Sametime Administration Tool. There are no restrictions on the number of characters used in the Internet password.

Password character restrictions
In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
 : \ } ' " &

8. Click **Save & Close**. The Person document is added to the Directory.

**Creating an Administrators Group document:**

Create a group document to hold the names of Sametime administrators.

**About this task**

Use the Sametime Administration Tool to create an Administrators Group document.

**Procedure**

1. From the Sametime server home page, click **Administer the Server**.
2. From the Sametime Administration Tool:
   - If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino.
   - If you are using an LDAP directory with the Sametime server, select LDAP Directory.
3. Choose "Add Sametime Administrators - Create a group for the administrators."
4. Click **Add Group**.
5. Enter a name for the group in the "Group name" field (for example, "Administrators" or "Sametime Administrators").
6. For group type, select Multipurpose.
7. Optional: Enter a description of the group in the Description field.
8. In the Members field, list the names of users you want to access the Sametime Administration Tool.

   Make sure to enter the name exactly as it is entered in the topmost entry of the "User name" field of a user's Person document.
10. Enter the names of the group owners in the Owners field. Generally, the group owner is the administrator creating the group. Only the administrator listed in the Owners field can modify this Group document. If the Owners field is blank, any administrator can modify this Group document.
11. Click **Save & Close**.

**Adding the Administrators Group document to Sametime database ACLs:**

Add the Administrators Group document to Sametime database Access Control Lists (ACLs) and provide the Manager access level to the group.

**About this task**

In addition to ACL access levels, you must also specify the ACL privileges and roles that the Administrators Group (or an individual user) has in each database. Generally, for an Administrators Group, select all ACL privileges and roles.
Note: If you are adding individual user names to Sametime database ACLs instead of a group name, database roles can be used to prevent or allow access to specific features of the Sametime Administration Tool.

Add the Administrators Group to the ACLs of the following Sametime databases.

- **Sametime Configuration (stconfig.nsf)** - Stores the configuration parameters that are set from the Sametime Administration Tool.
- **Domino Directory or Address Book (names.nsf)** - Stores Person and Group documents, ACL settings, and other configuration information for the Domino/Web Application Services.
- **Sametime Log (stlog.nsf)** - Stores logging information.
- **Domino Web Administration (webadmin.nsf)** - Contains the Domino Web Administration client, which includes monitoring features for the HTTP Services and free disk space. This is the full Domino Web Administration client that is included with Domino servers.

**Procedure**

1. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose "Add Sametime Administrators - Give the administrator group Manager access for all appropriate databases, such as stconf.nsf and stcenter.nsf." The Access Control options appear.
3. From the Databases list, select Sametime Configuration (stconfig.nsf).

   **Note:** The database filename appears below the Databases list.
4. Click Access.
5. Click Add. Enter the Administrators Group document name in the dialog box (for example, "Administrators" or "Sametime Administrators").
   If you are adding individual user names, enter the person's user name in the dialog box. Enter the name as it is entered in the top entry of the "User name" field on the user's Person document.
6. Click OK.
7. Select the Administrators Group name (or individual person's name) from the list in the Database Security window.
8. In the User Type drop-down list, select Group (or Person if you are adding an individual user's name).
9. In the Access drop-down list, select Manager.
10. Make sure that all ACL privileges, such as "Create documents" and "Delete documents," are selected.
11. Click Roles.
12. If you want the Administrators Group to have access to the full range of administrative functions, select all roles. Click OK.
   The roles determine which administration tasks the members of the group can perform. If you are adding individual user names to the ACLs, you can use the roles to control the administrative features that are available to individual administrators. For more information, see Roles in Sametime databases ACLs.
13. Click Submit.
14. After adding the Administrators Group to the ACL of the Sametime Configuration database (stconfig.nsf), repeat steps 4 through 14 to add the Administrators Group to the ACL of each of the Sametime databases listed below:
   - Domino Address Book or Domino Directory (names.nsf)
   - Sametime Online Meeting Center (stconf.nsf)
   - Sametime Log (stlog.nsf)
   - Sametime Self Registration (streg.nsf)
   - Domino Web Administration (webadmin.nsf)

Modifying the Server document of the Sametime server:

Add the Administrators Group document (or the name of an individual user) to two fields on the Server document.

Procedure
1. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose "Add Sametime Administrators - Edit the Server document."
3. Click Security.
4. In the "Administrators" field of the Administrators section, type the name of the Administrators Group (or enter the name of an individual user).
   
   Note: Type a group name exactly as it appears in the Group document. If you are entering an individual user name in this field, type the user name exactly as it is entered in the topmost entry of the "User name" field on the Person document. Separate multiple entries in the "Administer the server from a browser" field with commas.
5. In the "Run unrestricted methods and operations" field of the Programmability Restrictions section, type the Administrators Group name (or an individual user's name). Separate multiple entries in this field with commas.
6. Click Save & Close.

Adding and removing names from an Administrators Group document:

Control access to the Sametime Administration Tool by editing the Group document.

About this task

Adding a user's name to the Administrators Group document provides the user with access to the Sametime Administration Tool. Removing a user's name from the Group document revokes the user's access to the Sametime Administration Tool.

Procedure
1. From the Sametime server home page, click Administer the Server.
2. From the Sametime Administration Tool:
If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.

If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.

3. Choose “Add Sametime Administrators - Create a group for the administrators.”

4. Double-click a group name.

5. Select **Edit Group**.

6. In the Members field, add or remove a user’s name from the Group document. If you add a user’s name, the user must have a Person document in the Domino Directory that contains a last name, user name, and Internet password. Make sure to enter the name exactly as it is entered in the top entry of the “User name” field of a user’s Person document.

   The user must enter a last name or user name and the Internet password from the Person document to access the Sametime Administration Tool.

7. Click **Save & Close**.

---

Sametime database default ACL settings

See the following tables to determine the default ACL settings for Sametime databases.

**Table 145. stconfig.nsf database default ACL settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents<strong>Y</strong></td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**Table 146. stconf.nsf database default ACL settings**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents<strong>Y</strong></td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>
Table 147. names.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td></td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 148. stpolicy.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 149. stlog.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Reader</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 150. stnamechange.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Manager</td>
</tr>
</tbody>
</table>

Chapter 14. Administering  1077
Table 150. stnamechange.nsf database default ACL settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**Roles in Sametime database ACLs**

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

For example, the Sametime Configuration database (stconfig.nsf) ACL contains three roles: ServerMonitor, ServerAdmin, or DatabaseAdmin. If you assign only the ServerMonitor role to an administrator, the administrator can monitor server memory, disk space, and other server statistics but cannot perform any other administrative functions. Assign all roles to an administrator if you want the administrator to have full access to all administrative functions.

Access Control List (ACL) roles are defined in the following Sametime databases:

**Roles in the Sametime Configuration database (stconfig.nsf):**

The Sametime Configuration database (stconfig.nsf) stores the values for parameters that are available from the Sametime Administration Tool. The roles in this database affect the administrative tasks that an administrator can perform from the Sametime Administration Tool.

The following table lists the commands and features available with the Sametime Administration Tool and the roles that an administrator must be assigned in the stconfig.nsf database to use the Sametime Administration Tool commands and features. If an administrator does not have the appropriate roles, the Sametime Administration Tool does not display the command.

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Command or feature</th>
<th>Role required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message From Administrator</td>
<td>Sends message to all users logged into Community Services</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Monitoring</td>
<td>All monitoring features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Logging</td>
<td>All logging features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
</tbody>
</table>
### Roles in the Domino Directory (names.nsf):

The Domino Directory (or Address Book) contains the Person and Group documents that you create and edit when you use the Sametime Administration Tool. The roles in the Domino Directory determine who can create or edit a particular type of document in the Directory.

The Domino Directory also contains the Server document that you access to provide another user with administrative privileges to the Sametime Administration Tool.

**Note:** If you use Sametime in a Domino environment, the Domino Directory roles function the same as they do on Domino servers.

The Domino Directory contains eight roles. The privileges for each role are listed in this table:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserCreator</td>
<td>Allows an administrator to create Person documents in the Domino Directory</td>
</tr>
<tr>
<td>UserModifier</td>
<td>Allows an administrator to edit all Person documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupCreator</td>
<td>Allows an administrator to create Group documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupModifier</td>
<td>Allows an administrator to edit all Group documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerCreator</td>
<td>Allows an administrator to create Server documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerModifier</td>
<td>Allows an administrator to edit all Server documents in the Domino Directory</td>
</tr>
</tbody>
</table>

**Note:** The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.
### Related reference

#### Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

#### Roles in the Sametime Meeting Center (stconf.nsf):

The Sametime Meeting Center database contains only the Sametime Admin role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime Admin</td>
<td>Allows an administrator to see hidden meetings displayed in the All Meetings view of the Meeting Center. Allows an administrator to see the Hidden Meetings view in the Meeting Center. This view displays only hidden meetings. Allows the administrator to alter the meeting details of any meeting. For example, the administrator can delete or change the end time of a meeting that the administrator did not create. Allows an administrator to see and use the &quot;Delete the Recording,&quot; &quot;Export the Recording,&quot; &quot;Replace the Recording,&quot; and Import Recording options in the Meeting Center forms. These features enable the administrator to manage the recorded meeting files if the administrator makes the Record and Playback feature available on the Sametime server.</td>
</tr>
</tbody>
</table>

**Note:** The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.

#### Related reference

Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

#### Roles in the Domino Web Administration database (webadmin.nsf):

The Domino Web Administration database is available on the Sametime server to enable administrators to monitor the HTTP server and access logging information about the Domino Application Services.
The following table defines the roles in the Domino Web Administration database:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerAdmin</td>
<td>A Sametime administrator requires this role to access the Server document when providing other users with access to the Sametime Administration Tool.</td>
</tr>
<tr>
<td>ServerMonitor</td>
<td>A Sametime administrator requires this role to access the Monitoring - Miscellaneous functions of the Sametime Administration Tool. These monitoring functions enable the administrator to monitor HTTP commands and requests, server memory usage, and free disk space. The Sametime administrator also requires this role to access the Logging - Domino Log functions of the Sametime Administration Tool, which report information about the Domino Application Services.</td>
</tr>
<tr>
<td>DatabaseAdmin</td>
<td>A Sametime administrator requires this role to change database ACLs from the Sametime Administration Tool.</td>
</tr>
<tr>
<td>FileRead</td>
<td>This feature provides access to the Configuration - System Files (read-only) command of the Domino Web Administration Tool. This feature is usually not used with Sametime.</td>
</tr>
<tr>
<td>FileModify</td>
<td>This feature provides access to the Configuration - System Files (read/write) command. This feature is usually not used with Sametime.</td>
</tr>
</tbody>
</table>

**Related reference**

Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

Domino log

To access the Domino log, choose Logging - Domino Log in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

**Managing trusted IP addresses**

Whenever you install a server that communicates with a community server, you must add the new server's IP address to the community server's settings.

**About this task**

The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server's IP address to the community server.
If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to complete include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).

You do not need to add the system console's IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the **Connectivity** tab.
5. Under **Trusted Servers**, enter the IP address of the server that must connect to the Sametime Community Server in the **New IP Address** field, and click **Add**.

   **Note:**
   - If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.
   - For the media manager, enter the Conference Manager server IP address.

   To delete an IP address from the list, select it and click **Delete Selected**.
6. Click **OK**.
7. Restart the community server for the change to take effect.

**Managing community services**
Community services settings support all online presence (or awareness), instant messaging, and chat features at a server-wide level. These settings supersede any feature settings that you set at the policy level for users or groups. Community services settings carry a greater weight.

**Managing general community services**
The general community services settings control the interaction of the IBM Sametime Community Server with an LDAP directory and the maximum number of users allowed on the server.

**About this task**
These settings must be addressed for each server within a Sametime Community Server cluster.

**Procedure**
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.

4. Click the **Community Services** tab.

5. Use the following table to set general server-wide settings for users of the Sametime Community Server.

*Table 151. Server-wide settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of entries on each page in dialog boxes that show names in the directory</td>
<td>Controls the number of user and group names that display when a user browses the directory. When an user browses the names and groups in the directory, the directory entries (names and groups) are listed on “pages” in a dialog box. The default is 100 entries per page. It is best to use a setting between 100 and 200 entries. Higher settings cause more data to be transmitted on the network when a user browses the directory.</td>
</tr>
<tr>
<td>How often to poll for new names added to the Sametime community directory (minutes)</td>
<td>Controls how frequently the cache of user names is updated with new information from the directory. The Sametime Community Server maintains a cache that contains information about the users and groups in the community. This cache must be or refreshed periodically to ensure that users who have recently been added to a directory can be displayed in the presence lists of all Sametime clients. The update occurs only if changes are made to the directory during the update interval. The default setting is 60 minutes.</td>
</tr>
<tr>
<td>How often to poll for new servers added to the Sametime community (minutes)</td>
<td>Controls the time interval in which the Sametime Community Server receives an updated list of all Sametime servers. If you have deployed more than one Sametime Community Server, the community services on each server must maintain a list of all other Sametime Community Servers in the Sametime community. Community services uses this list to ensure that users who have different home servers or different home clusters can see each other in presence lists and communicate through instant messaging and chat. The default setting is 60 minutes.</td>
</tr>
<tr>
<td>Maximum user and server connections to the community server</td>
<td>Controls the maximum number of connections allowed to Sametime Community Server. The connections include both client connections and server-to-server connections. A client connection occurs when a user starts the Sametime client. Server-to-server connections occur when you have deployed multiple Sametime Community Servers and different home servers are specified for users. The limit is 20,000 connections.</td>
</tr>
</tbody>
</table>
Table 151. Server-wide settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select the authentication type that users can use while logging into the Community server:</td>
</tr>
<tr>
<td></td>
<td>• LTPA or Sametime token</td>
</tr>
<tr>
<td></td>
<td>• LTPA only</td>
</tr>
<tr>
<td></td>
<td>Controls the authentication type. When LTPA or Sametime Tokens option is selected, the Sametime Community Server accepts authentication tokens generated by both Single-Sign On (SSO) and the Secrets and Tokens databases on the Sametime Community Server. This option is selected by default. When LTPA only is selected, the Sametime Community Server accepts authentication tokens generated only by SSO (LTPA tokens).</td>
</tr>
</tbody>
</table>

6. Click OK.
7. Restart the Sametime Community Server for settings to take effect.

Saving transcripts of chats and meetings
You can enable the Sametime Community Server to save transcripts from two-way and multiple-user chats and from chats in meetings. Two-way chats are managed with the server’s native Chat Logging application. Multiple-user chats and meeting chats are managed with the Places server application.

Enabling local chat logging:

Each text chat has a transcript, the record of the text messages exchanged between chat partners during a chat session. You can configure the IBM Sametime Community Server to automatically log all chats and announcements, making these transcripts available to users for viewing in their chat history.

Procedure
1. In a text editor, open the sametime.ini file, which is located in the Sametime Community Server installation directory (for example: C:\Program Files\lotus\domino).
2. In the [Config] section, set the value for ST_LOG_ALL_CHATS.
   • ST_LOG_ALL_CHATS=0 is the default behavior, which logs only part of the two-user chats.
   • ST_LOG_ALL_CHATS=1 logs all two-user chats.
3. In the [Config] section, set the value for CHAT_LOGGING_MANDATORY.
   • CHAT_LOGGING_MANDATORY=0 is the default behavior, which makes chat logging optional. If this line is missing, Sametime also uses the default behavior to make chat logging optional.
   • CHAT_LOGGING_MANDATORY=1 enforces chat logging.
4. In the [Config] section, set the value for REMOTE_CHAT_LOGGING to 1.
   • REMOTE_CHAT_LOGGING=0, the default, does not enable remote chat logging.
   • REMOTE_CHAT_LOGGING=1 ensures that a given server can enable remote chat logging for multiple-user chats and chats in meetings.
5. In the [Config] section, set the value for CL_USE_USER_DN. If this setting is not found, the server defaults to using the Sametime user ID as the user’s identifier for a chat log.
   • CL_USE_USER_DN=0 uses the Sametime user ID as the user’s identifier for a chat log.
• CL_USE_USER_DN=1 uses the user DN and if the DN is not found, uses the Sametime user ID as the user’s identifier for a chat log. The DN may be either the Sametime user ID or another attribute.

Announcement originators and recipients can only be identified by their Sametime user IDs. Banning and logging must be done with Sametime user IDs rather than DNs. Do not set the value to 1 if that behavior does not work for your environment.

6. In the [ST_BB_NAMES] section, set the value for ST_CHAT_LOG. The StChatLogFile library (or libstchatlogfile.so on AIX, Linux, and Solaris platforms) is a sample of how to implement a chat logging black box using the Sametime SDK.
   • ST_CHAT_LOG=N/A
     The default of N/A means that Sametime does not attempt to load any chat logging black box. If you do not want StChatLog.dll to be used by Sametime, leave the default of N/A; do not remove the line.
   • ST_CHAT_LOG=File
     The value File describes the suffix to an StChatLog base name of the chat logging black box library. For example, to load your StChatLogMyCustom.dll file, set the value to ST_CHAT_LOG=MyCustom.

Note: The StChatLogFile sample is not supported, and is not recommended for use in deployment environments.

7. Close and save the file.
8. Log in to the Integrated Solutions Console.
9. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
10. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
11. Click the Community Services tab.
12. In the Server Features section, under Enable chat logging, select one of the following choices:
   • Always
     With mandatory logging, the sametime.ini file must have this value to classify the server as a mandatory chat logging server:
     CHAT_LOGGING_MANDATORY=1
   • When available
     When logging is enabled when it is available, the sametime.ini file must have these values to allow remote chat logging:
     – REMOTE_CHATLOGGING=1
     – CHAT_LOGGING_MANDATORY=0 (or is not provided)
   • Never
     With logging set to Never, the sametime.ini file must have these values to allow remote chat logging for other servers:
     – REMOTE_CHATLOGGING=1
     – CHAT_LOGGING_MANDATORY=0 (or is not provided)
13. Click OK.
14. Restart the Sametime Community Server for settings to take effect.
What to do next

To find out more IBM Sametime chat logging and how to extend its features, see this article in the Sametime wiki: New features of IBM Sametime 8.x chat logging and how to extend its SDK.

Enabling remote chat logging for places:

Mandatory chat logging server settings on a user’s home server determine if chat logging is mandatory for this server’s users. If a user has access to multiple-user chats or chats in meetings on servers that do not require mandatory logging, set up the server that manages a given n-way chat as a remote chat logging server to fulfill the mandatory chat logging requirement. Remote logging handles chat logs for multiple-user chats and chats in meetings if a local Chat Logging service is disabled (either Never chat logging mode is defined or a local Chat Logging service is down). The two-way chats are logged on the home server of the chat participants. If two-way chat participants have different home servers, the chat is logged on both servers. Mandatory chat logging configuration requires all servers in the distributed environment to be running Sametime 8.5.2.

About this task

A home server with mandatory chat logging must have the following settings to be recognized by remote logging servers:

- The server logging mode is set to Always in the Community Services tab in the Sametime System Console (or STRICT if set in stconfig.nsf).
- CHAT_LOGGING_MANDATORY=1 flag is set in the [Config] section of the sametime.ini file.

All servers involved in remote logging must be configured like this:

- The server logging mode is set to When available or Never in the Community services tab in the Sametime System Console (or OFF or RELAX if set in stconfig.nsf).
- REMOTE_CHATLOGGING=1 flag is set in the [Config] section of the sametime.ini file.

In most cases, the n-way chat logging is logged on users’ home servers. The one exception is if a user whose home server is set to mandatory chat logging joins a chat that is already being logged on a remote chat logging server. In that case, the n-way chat continues to be logged only on that server in Always logging mode. N-way chats are not logged on multiple servers.

Other chat logging settings are determined by the server’s chat logging black box. If chat logging fails, for example, if there is a database error, the chat log for a mandatory chat user is destroyed.

Allowing users to transfer files to each other

Community Services allow users to transfer files to each other over the network while using Sametime Connect.

About this task

When you enable this feature, you should also set a file size limit and virus scanning preference.
Computer viruses can be spread through transferred files. To protect against this possibility, users should have current third-party anti-virus software installed. The Virus scan files setting should be enabled and set to scan all files.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. In the Server Features section, click Allow users to transfer files to each other.
6. To increase or decrease the size of files that users can transfer, enter a value in the Maximum file transfer size, in Kilobytes field.
7. Under Virus scan files, select one of the following choices:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>If scanning cannot be done, the file is not transferred</td>
</tr>
<tr>
<td>When available</td>
<td>The file is sent with a message that the file was not scanned, allowing the user to decide how to handle the file, or it is not sent if scanning reveals a virus</td>
</tr>
<tr>
<td>Never</td>
<td>Files are not scanned</td>
</tr>
</tbody>
</table>

8. Click OK.
9. Restart the Sametime Community Server for settings to take effect.

**Allowing users to send announcements**

Community Services allows users to send unencrypted announcements to others who are online in the Sametime Community.

**About this task**

When you enable this feature users can:

- Send unencrypted announcements to anyone who is online in Sametime Connect or in an online meeting. To receive an announcement, a user must be online, and in either active or away status. Users who are offline or have a status of "do not disturb" do not receive announcements.
- Allow the recipients of the announcement to respond to the announcement, or prevent them from responding.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. In the Server Features section, click Allow users to send announcements (unencrypted one-way messages).
Managing anonymous access to virtual places

The Sametime Software Development Kit provides developers with the capability to build applications that create virtual places. Anonymous users can enter a virtual place and have awareness of other users in the same virtual place.

About this task

This capability to have awareness of other users in the same virtual place is sometimes called place-based awareness. Place-based awareness differs from community-wide awareness. With community-wide awareness, users can have awareness of any user in the community who is online. IBM Sametime Connect provides users with community-wide awareness functionality. Anonymous users are not allowed to have community-wide awareness in any Sametime clients.

The Anonymous users can enter virtual places field controls the ability of anonymous users to enter virtual places created by custom-built applications created with the Sametime Software Development Kit. For more information on virtual places, see the IMWC Directory and Database Access Toolkit documentation available from IBM developerWorks at http://www.ibm.com/developerworks/lotus/downloads/toolkits.html.

Enter information for anonymous access to a virtual place. Each attendee who accepts the default name has a number added to the end (For example, User1, User2).

This task must be completed separately for each server within a Sametime Community Server cluster.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Anonymous tab.
5. Click the Anonymous users can enter virtual places

Note: The following fields do not take effect unless the Anonymous users can enter virtual places field is selected.

6. If you want to let an anonymous user have a unique display name when accessing a Sametime application that includes awareness, click Users of Sametime applications (databases such as stconf.nsf or websites) can specify a display name so that they do not appear online as "anonymous." A display name entry dialog box appears when a user accesses the Sametime application. This display name allows the anonymous user to be individually identified in any presence lists in the Sametime application.

Note: The ACL settings of the application must allow anonymous access, too.
7. If you want to have a domain name automatically appended to the display name entered by the user at the name entry dialog box, click **Default domain for anonymous users**.

8. If you want a name to appear by default in the name entry dialog box, click **Default name**. For instance, if the **Default name** field contains the entry User the first person entering a meeting sees User displayed by default in the name field of the name entry dialog box. If the person accepts the default and enters the application, the person is identified as **User1** in any presence list in the application.

9. Specify the level of access that an anonymous user of an application enabled with Sametime technology has to the directory. You can limit an anonymous user's ability to view names in the directory. For example, you might prevent anonymous users from browsing all names in a directory or searching for names in the directory.

   - **Users cannot browse or search the Directory**
     Anonymous users cannot search or browse the directory.
   - **Users can type names to add them to an awareness list**
     Anonymous users can type text in an user search interface to search for person or group entries in the directory. However, users cannot view or browse a list containing all entries in the directory. Users might perform such searches to add users to a presence list.
   - **Users can browse the directory (see a list of names) or type names (resolve users and groups)**
     Anonymous users can type text in an user search interface and search for group or person entries in the directory. Anonymous users can also browse lists that contain all entries in the directory. When this option is selected, anonymous users can see all group and name entries in the directory, but cannot see the content of a group entry (the list of names within a group entry). Users cannot browse the LDAP directory on the LDAP server.
   - **Users can browse the directory to see group content and names, or type names**
     Anonymous users have all searching and browsing privileges described for the **Users can browse the directory (see a list of names) or type names (resolve users and groups)** setting above. In addition, users can search and browse within group entries in the directory and access the user and group names that are specified within group entries in the directory.

10. Click **OK**

11. Restart the Sametime Community Server for settings to take effect.

**Sending a message to all users**

Use the Sametime Administration Tool to simultaneously send a single message to all users currently logged in to Community Services from any Sametime client.

**About this task**

Follow these steps to send a message to all users currently logged in to Community Services.

**Procedure**

1. Open a browser and navigate to the Sametime Community Server.
   
   Type the following address:

   ```
   http://host_name/servlet/auth/admin
   ```
where host_name is the fully qualified host name of the server; for example:
http://commsvr1.example.com/servlet/auth/admin

2. From the Sametime home page, click Administer the Server.
3. Log in as the Sametime administrator.
4. Select Message From Administrator.
5. Enter the message in the text box provided.
6. Click Send. You receive a confirmation that your message was sent.

Managing business cards

You can configure the IBM Sametime Community Server so that business card information about an individual displays when a user hovers over a name in a chat window or a contact list.

About this task

Business card can access user information from any of three types of storage repositories: the native Domino directory, the LDAP directory (including Domino LDAP), or a custom Notes application. Each repository stores user information differently, so to facilitate user searches, Sametime provides a search engine, called a black box, for each storage type.

Since there are three different storage types, Sametime provides three different black boxes to search for user information (one per storage type). These are:
- LDAP – used to search a LDAP directory
- Notes – used to search a native Domino directory
- Notes_custom_db – used to search a customized Notes application

Using information in the LDAP server or the native Domino directory, you can choose the fields that represent the information that you want to display in the business card. The available fields are:
- Photo
- Name
- Company
- E-mail address
- Telephone
- Address or location
- Title

You can set up or change the details you want to retrieve by changing the values for these fields on the main Business Card page.

Configuring business cards using an LDAP directory

Follow these steps to configure the business card using an LDAP directory. Domino LDAP is considered an LDAP directory.

Before you begin

Before you start setting up your business cards, be sure the following conditions are true for your site.
- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account and password
- The Sametime Community Server is running
- **For Domino LDAP only:** To allow anonymous users to access required user details, you can edit the All Servers document in names.nsf. Under the LDAP tab, all LDAP attributes that you want to be retrieved by anonymous users should be added to the list of Anonymous Users Can Query.

**About this task**

This task must be completed separately for each server within a Sametime Community Server cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.
4. Click the Business Card tab.
5. In the Business Card Contents section, select the attribute you want displayed in users' business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.
6. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

Domino LDAP does not contain the **postalAddress** field. The value retrieved for this LDAP attribute is the concatenation of **City**, **State/Province**, and **Country**. Also, Domino LDAP contains a hidden field for the **ou** attribute. This field cannot be set through the Domino LDAP, and a third-party LDAP management tool can be used to add a value to it.

7. If you select User Defined for an Attribute Value, then enter an attribute to map to the Attribute Name.
8. Click OK.
9. Restart the Sametime Community Server.

What to do next

Special considerations

In a configuration where:
- Sametime is configured with LDAP
- UserInfo is configured to ignore configuration updates
- The Sametime ID is configured to an attribute different then a DN

You must add additional parameters to the UserInfoConfig.xml file to correctly support this type of Sametime ID.

1. Open the UserInfoConfig.xml file.
2. Locate the StorageDetail tag of the relevant LDAP and add the following flags:
   - UserIdAttribute= <the chosen attribute for userid such as cn>
   - PersonObjectClass= <the required object class such as OrganizationalPerson>
3. Save and close the file.
4. Restart the server.

Configuring business card photos for Domino LDAP:

To store photos in Domino LDAP and enable UserInfo to retrieve them, please follow the steps below. A third-party LDAP management tool is required for adding a JPEG Photo field to Domino LDAP. Most LDAP V3-compliant tools will work.

Before you begin

Configuring Business Card with an authenticated LDAP bind account is highly recommended. Allowing Anonymous LDAP Schema write access is a security risk and additional security changes to Domino Directory Access Control List may be required to allow anonymous write access to Domino LDAP.

Procedure

1. Use Domino Administrator to enable Domino LDAP write access. Within default Configuration Setting Document LDAP, click Yes next to Allow LDAP users write access.
2. Using the third party LDAP tool, connect to the Domino LDAP server and bind as a Domino Administrator. Once a successful connection is made, select a user and add an Attribute. The Attribute name for Domino LDAP should be specified as: jpegphoto;binary and the type should be selected as binary. Note the name being used for the attribute. If you use just jpegPhoto or Photo as the name, depending on the LDAP tool, you might not be able to store images in the field. The -;binary is required for Domino LDAP to understand the binary data.
3. Use the third party LDAP tool to import the JPEG or GIF photo into the new field.

   Note: The size of the image should be smaller then 64kb.
4. Use ldapsearch or the LDAP tool to check that the photo has uploaded successfully.
5. Log in to the Integrated Solutions Console.
   a. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
   b. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the **Business Card** tab.
   d. In the Business Card Contents section, select the **Photo** attribute, and then click **Add** to include it in the business card.
   e. Under **Attribute Definition**, choose **User Defined** as the attribute value for **Photo**.
   f. In the User Defined column next to **Photo**, type `jpegphoto;binary`.
   g. Click **OK**.

   a. Expand the **Configurations > Servers**, and select the **Configurations** view. Open this document in **Edit** mode and click the Basic tab. Enable the **Use these settings as the default settings for all servers** option. The LDAP tab appears.
   b. Click the LDAP tab. Click **Choose Fields that Anonymous Users Can Query via LDAP**.
   c. Click **New** in the window that displays.
   d. Type `jpegphoto` in the field and click **OK** to save the value. Click **OK** again to close the window.
   e. Save and close the document.

7. Restart the LDAP server. From the server console, type `tell ldap quit` and then `load ldap`.


9. Browse to **UserInfoConfig.xml** file within the Domino Install folder. Under Details section, check to make sure **Photo** field is set to `jpegPhoto;binary`.

   ```xml
   <Detail Id="Photo" FieldName="jpegPhoto;binary" Type="image/jpeg"/>
   ```

10. Restart the Sametime Community Server.

### Configuring business card photos for the Sametime browser client:

Follow these steps to configure the business card photo that displays for users that chat using the IBM Sametime browser client.

#### Before you begin

Enable the **PhotoURL** attribute in your LDAP directory. Refer to the documentation for your LDAP directory.

#### Procedure

1. In the Sametime Community Server, find the **UserInfoConfig.xml** file.
2. Open the file with a text editor, and add the following tag to the Details section:

   ```xml
   <Detail Id="PhotoURL" FieldName="PhotoURL" Type="text/plain"/>
   ```
3. Restart the Sametime Community Server.
4. Upload user photos into a web server repository, so that users can access the photos using a URL. For example: http://iddirectory.mycompany.com/userphoto/mybuscardpic.jpg

Verifying business card configuration:

After you have configured your business card feature, you can verify the configuration.

About this task

To display user information, the business card uses an IBM Sametime Community Server application named UserInfo. UserInfo retrieves and delivers user information for each client request to view a user’s business card. Follow these instructions to verify your business card configuration.

Procedure

1. Open \lotus\domino\UserInfoConfig.xml in a text editor. When you use an LDAP directory to store user information, the UserInfoConfig.xml should look like this:

   ```xml
   <UserInformation>
   <Resources>
   <Storage type="LDAP">
   <CommonField CommonFieldName="MailAddress"/>
   <StorageDetails HostName="ldap.mycompany.com" Port="389" UserName="username"
   Password="password" SslEnabled="false" SslPort="636" BaseDN="/o=ibm" Scope="2"
   SearchFilter="(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)
   (mail=%s)))"/>
   <!-- Add another StorageDetails tag to support another ldap server. The listing order
   implies the searching order -->
   <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
   <SslProperties KeyStorePath="" KeyStorePassword=""/>
   <Details>
   <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
   <Detail Id="Name" FieldName="cn" Type="text/plain"/>
   <Detail Id="Title" FieldName="title" Type="text/plain"/>
   <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
   <Detail Id="Company" FieldName="ou" Type="text/plain"/>
   <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
   </Details>
   </Storage>
   </Resources>
   <ParamsSets>
   <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
   <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
   </ParamsSets>
   <BlackBoxConfiguration>
   <BlackBox type="LDAP" name="com.ibm.sametime.userinfo.userinfobb.UserInfoLdapBB"
   MaxInstances="5"/>
   </BlackBoxConfiguration>
   </UserInformation>

2. Verify that stconfig.nsf has valid data for the LDAP document and the UserInfo document.

3. Verify that the HTTP server has been restarted after any changes have been made to the xml file.

Configuring business cards using a Domino directory

This task demonstrates how to configure the business card using the Domino directory.

Before you begin

Prerequisites:
IBM Lotus Domino and IBM Sametime Community Server have been installed
and configured
Sametime authentication is configured to use an Domino directory
The Sametime Community Server is running

About this task
Note: IBM recommends that you use a third party LDAP directory, and not
Domino, because Domino does not have a standard field for photos (a jpegPhoto
field). Using a third party LDAP directory avoids unnecessary replacement of the
default jpegPhoto field.

Follow these steps to configure the Business Card to display data that is stored in a
single data repository—a Domino directory.

Procedure
1. Open an Internet browser and enter this URL into the URL-locator field:
   http://example.com/stcenter.nsf, substituting the host name example.com with
   your server’s actual host name.
2. Click Administer the server, and then log in as Administrator.
3. Click the plus sign next to Configuration to expand the contents, and then click
   Business Card Setup.
4. In the User Information section, select the entry you want displayed in users’
business cards, and then click Add to move the entry to the right-side list box.
   To remove preselected entries, click the entry and click Remove. In most cases,
   the Attribute name and Attribute value section of the business card interface
   requires no modification; however, if the information you want displayed in the
   users’ business cards is not mapped to the default fields provided by the users’
   person documents, then you might need to update the Attribute name and
   Attribute value section. The following table lists the default attribute value that
   is mapped to each attribute name.

   Table 153. Attribute names and values

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

5. Click Update to save the changes.
   To display user information, the business card feature uses a server application
called UserInfo which is designed to retrieve and deliver user information for
each incoming request from a client to view a specific user’s business card. To
ensure this application is configured properly to search the proper data storage,
confirm the settings as defined in UserInfo.xml.
6. Open the UserInfoConfig.xml file in a text editor. The file is located in the
   Domino program directory (\lotus\domino\UserInfoConfig.xml). Here is a
   section of the UserInfoConfig file edited for XYZ’s scenario:
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
  <BlackBoxConfiguration>
    <BlackBox type="NOTES" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesBB">
      MaxInstances="4"/>
  </BlackBoxConfiguration>
</UserInformation>

**What to do next**

There might be specific configurations where the names in the Domino directory include commas (,). By default, these special characters are treated as LDAP separators. In order to treat them as regular characters, add the following flag to UserInfoConfig.xml:

```xml
<UserInfoConfig>
  <UseUnformattedNotesNames />
</UserInfoConfig>
```

This setting take affect after the server is restarted.

**Photos in the Domino directory:**

The Domino directory does not have a standard field for photo, but photos can be retrieved from the Domino Name and Address Book (NAB) as follows:

1. Add a rich text field or rich-text lite field to the Person form of the Name and Address Book in Domino.
   a. Open names.nsf in Domino Designer.
   b. Open the Person form.
   c. Click the section where you want to add the field. A sub-form will open.
   d. In the sub-form, click where you want to add the field.
   e. Select Create > field from the menu, and edit the field’s properties.
   f. Add the name to the field and select Rich Text as the type.
   g. Save the form.

2. To store photo information in the newly-added rich-text field, choose either:
   - Import--click on the rich text field and choose Create > Picture. This adds the file contents to the field.
   - Attach--save the image file in the rich text field as an attachment.
3. Using the Sametime Administration tool, go to the Business Card Attribute page.

4. In the text box for the Photo attribute, type the name of the rich text field that you added to the Name and Address Book, above, matching the case, then click Update.

5. Restart the Sametime server.

Photo types used by Domino are .jpeg and .gif.

**Configuring business cards to use two repositories**

For retrieving business card information, you can set up a dual repository:

When you set up dual repositories, you set up a primary repository and a secondary repository:

**Primary repository** – The first storage repository search by the UserInfo application to retrieve user information; must always be the Sametime directory.

**Secondary repository** – The second storage repository searched by the UserInfo application to retrieve user information.

**Note:** The primary storage can never be of the same type as the second repository; for example, the primary and secondary storage cannot both be a Domino directory.

There are a variety of ways you can use dual repositories:

- The dual repository with Domino/LDAP directories
- The dual repository with LDAP/Domino directories
- The dual repository with Domino/Custom Notes databases
- The dual repository with LDAP/Custom Notes databases

**Configuring a dual repository with LDAP and a native Domino Directory:**

For retrieving business card information, you can set up a dual repository of an LDAP directory and a native Domino Directory.

**Before you begin**

This section describes how to configure the business card using two storage repositories: LDAP directory as the primary storage, a native (non-LDAP) Domino Directory as the secondary storage.

**About this task**

These directions assume the following:

- Lotus Domino & IBM Sametime Community Server have already been installed & configured to run properly
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- All LDAP attributes needed by business card accessible for query via anonymous connection or using a specific bind account/password
- The Sametime Community server is running
- Business card information can be retrieved from your Sametime directory
A Notes database based off of the Domino directory template (pubnames.ntf) has been created and contains person documents for each corresponding user account defined in the Sametime directory. (In our example, this database is named bcardstorage.nsf; and the user accounts correspond to the accounts in the Sametime directory by users’ email address.

Procedure
1. Using Lotus Notes, open your Directory Assistance database (typically da.nsf). If such a database does not exist, you must create one based upon the Directory Assistance template.
2. Click Add Directory Assistance to add an additional directory assistance document, and then specify the secondary storage. See the sample Directory Assistance document for the bcardstorage.nsf below:

**DIRECTORY ASSISTANCE**

<table>
<thead>
<tr>
<th>Basics</th>
<th>Naming Contexts (Rules)</th>
<th>Replicas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain type: Notes</td>
<td>Domain name: BCard</td>
<td>Company name: BCard</td>
</tr>
<tr>
<td>Search order: 2</td>
<td>Make this domain available to: Notes Clients &amp; Internet Authentication/Authorization</td>
<td>LDAP Clients</td>
</tr>
<tr>
<td>Group Authorization: No</td>
<td>Enabled: Yes</td>
<td></td>
</tr>
</tbody>
</table>

Naming contexts (Rules) tab

**Note:** For Business Card purposes, the secondary storage does NOT have to be trusted for credentials.
Replicas tab

3. Once you have completed the changes, save and close the document. The resultant Directory Assistance database may show the following:

Note: The directory assistance database must be listed on the Basics tab of the Sametime server document in the Directory assistance database name field. If it is not listed, fill in the field, and restart the Sametime server to effect that change.

4. Log in to the Integrated Solutions Console.

5. Click Sametime System Console > Sametime Servers > Sametime Community Servers.

6. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.

7. Click the Business Card tab.

8. In the Business Card Contents section, select the attribute you want displayed in users’ business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.

9. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

10. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.

11. In the **Attribute Definition** table, change the **Attribute Value** for the attributes that will be retrieved from the secondary storage to **User Defined** and leave the **User Defined** field blank. For example, if you are retrieving users' Telephone and Title information from the Domino Directory; therefore, change the values for the Telephone & Title attributes to **User Defined**, and leave the **User Defined** field blank, and then click **OK** to save the changes.

**Note:** These values are blank to ensure they are retrieved from the secondary repository (the Domino Directory) and not from the primary repository, which is the LDAP directory.

12. Modify the **UserInfoConfig.xml** file located in the Domino program directory (`\lotus\domino\UserInfoConfig.xml`) using a text editor. The **UserInfo** application fetches and delivers user information for each incoming client request (an user's request to view a particular user's business card). When you are using an LDAP directory as primary storage and a Domino Notes directory as secondary storage, make the following modifications. Add an additional Storage tag of Notes type within the Resources tag:

```xml
<Storage type="NOTES">
  <CommonField CommonFieldName="MailAddress"/>
  <Details>
    <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
    <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
  </Details>
</Storage>
</Resources>
</Storage>
```

**Note:** The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are retrieving Title and Telephone information from Domino.

13. To ensure Telephone and Title fields come from Domino, remove the following from the Details tag of the LDAP storage type:

```xml
   <Detail Id="Title" FieldName="title" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
```

14. Add the following to the `<BlackBoxConfiguration>` section. Make sure it is listed after the LDAP blackbox as the order defines the search order:
Note: Since Sametime is the storage to be searched first by the UserInfo application, and the LDAP directory is the Sametime directory, the NOTES black box must be listed after the LDAP black box.

15. Once these changes are made, the UserInfoConfig.xml looks like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="LDAP">
      <StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2" SearchFilter="(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s))") />
    </Storage>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
</UserInformation>
```

16. UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user—from multiple sources. By default, the user's email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

17. Restart your Sametime Community and Domino servers to effect the changes.

Results

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and the Domino Directory.

Configuring a dual repository with LDAP and a custom application:
For retrieving business card information, you can set up a dual repository of an LDAP directory and a custom IBM Lotus Notes application.

Before you begin

This section describes how to configure the business card using two storage repositories: LDAP with a custom Lotus Notes application repository. Here, we describe how you can set up LDAP as the primary storage, and a custom Lotus Notes application as the second storage.

These directions assume the following:
• Lotus Domino & IBM Sametime Community Server have already been installed & configured to run properly
• Sametime authentication is configured to use an LDAP directory
• The LDAP server is running and accessible by the Sametime Community Server
• Business card information can be retrieved from your Sametime directory
• A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf).
• To use a custom Lotus Notes application as a secondary repository, each user record in the custom application must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).

About this task

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.
4. Click the Business Card tab.
5. In the Business Card Contents section, select the attribute you want displayed in users’ business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.
6. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.

Table 154. Attribute names and values

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
</tbody>
</table>
### Table 154. Attribute names and values (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

7. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.

8. In the **Attribute Definition** table, change the **Attribute Value** for the attributes that will be retrieved from the secondary storage to **User Defined** and leave the **User Defined** field blank. For example, if you are retrieving users' Telephone and Title information from the custom Lotus Notes application; therefore, change the values for the Telephone & Title attributes to **User Defined**, and leave the **User Defined** field blank, and then click **Reset** to save the changes.

**Note:** These values are blank to ensure they are retrieved from the secondary repository (the Lotus Notes application) and not from the primary repository, which is the LDAP directory.

9. Modify the UserInfoConfig.xml file located in the Domino program directory (`\lotus\domino\UserInfoConfig.xml`) using a text editor. The UserInfo application fetches and delivers user information for each incoming client request (an user's request to view a particular user's business card). When you are using an LDAP directory as primary storage and a custom Notes application as secondary storage, make these modifications:

a. Add the following **NOTES_CUSTOM_DB Storage** tag inside the Resources tag:

   ```xml
   <Storage type="NOTES_CUSTOM_DB">
   <StorageDetails DbName="bcardstorage.nsf " View="$BCardView"/>
   <Details>
   <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
   </Details>
   </Storage>
   
   **Note:** In the `<StorageDetails>` tag, the following settings are specified:
   - DbName = database_path Filename of the custom Notes application (relative path to the domino data directory)
   - View = view_name The name of the Notes view that displays the documents containing the user records.
   - The `<Details>` section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Notes application database.

b. The attributes Title and Telephone must come from the custom Notes application rather than from LDAP, so remove the following information from the `<details>` tag of the LDAP storage: `<Detail Id="Title" FieldName="title" Type="text/plain"/>` `<Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>

   Add the following information to the `<BlackBoxConfiguration>` section.
   Make sure it is listed after the LDAP blackbox as the list order defines the
d. The UserInfoConfig.xml now looks like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="LDAP">
      <CommonField CommonFieldName="MailAddress"/>
      <StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2" SearchFilter="(&(objectclass=organizationalPerson)((cn=%s))(givenname=%s)(sn=%s)(mail=%s))"/>
      <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
      <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE -->
      <SslProperties KeyStorePath="" KeyStorePassword=""/>
      <Details>
        <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
        <Detail Id="Name" FieldName="cn" Type="text/plain"/>
        <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="ou" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="NOTES_CUSTOM_DB">
      <StorageDetails DbName="bcardstorage.nsf" View="$BCardView"/>
      <Details>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
</UserInformation>
```

e. UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user from multiple sources. By default, the user's email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:<br>

```xml
<CommonField CommonFieldName="MailAddress"/>
```

10. Restart the Sametime Community Server and the Lotus Domino server to effect the changes.

What to do next

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and a custom Notes application.

Configuring a dual repository with Domino Directory and LDAP:
You can configure Business Card with the use of two (dual) repositories—Domino and LDAP. The primary storage repository is the native (non-LDAP) Domino Directory, and the auxiliary storage is the LDAP directory.

**Before you begin**

These directions assume the following:
- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Sametime authentication is configured to use an Domino directory
- The Sametime Community Server is running
- The LDAP server is running and is accessible by the Sametime Community Server
- All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account/password
- Business card information can be retrieved from your Sametime directory

**About this task**

Enter this URL in the address window of a browser: http://hostname/stcenter.nsf, using your server’s actual host name.

**Procedure**

1. Click **Administer the server**, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click **Business Card Setup**.
3. In the User Information section, select the entry you want displayed in users’ business cards, and then click **Add** to move the entry to the right-side list box.
   To remove preselected entries, click the entry and click **Remove**. The following table lists the default attribute value that is mapped to each attribute name in the **Attribute Names and Attribute Values** section.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the **Attribute Names and Attribute Values** section, remove the attribute values for the attributes that will be retrieved from the auxiliary storage. In the following example, the Telephone information is retrieved from the LDAP directory, so delete the value for the Telephone attribute. Removing attributes insures they are pulled from auxiliary storage, and not primary storage.
5. Click **Update** to save the changes.

To display user information, the business card feature uses a server application called **UserInfo** which is designed to retrieve and deliver user information for each incoming request from a client to view a specific user's business card. To ensure this application is configured properly to search the proper data storage, confirm the settings as defined in **UserInfo.xml**.

6. When Domino Directory is primary storage and LDAP is auxiliary storage, make the following modifications:

   a. Add the following LDAP `<storage>` tag within the `<Resources>` tag:

   ```xml
   <Storage type="LDAP">
     <SimpleLogin>HostName=ldap.austin.ibm.com Port=389</SimpleLogin>
     <Authentication UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2">
       <SearchFilter>(&(objectclass=organizationalPerson) (|(cn=%s)(givenname=%s)(sn=%s)(mail=%s)))" />
     </Authentication>
     <Details>
       <Detail Id="Telephone" FieldName="telephonenumber" Type="text/plain"/>
     </Details>
   </Storage>
   ```

   Update the `SimpleLogin` tag with the appropriate settings for your LDAP directory. The Details section defines the attributes that Sametime will retrieve from the corresponding storage repository. In this example, we are pulling the **telephonenumber** attribute from the LDAP directory.

   b. To ensure the telephone number is retrieved from LDAP, and not from Domino, remove the following from the `<details>` tag of the DominoNotes storage type:

   ```xml
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
   ```

   After you have made these changes, the **UserInfoConfig.xml** file should look like the below:

   ```xml
   <UserInformation>
     <Resources>
       <Storage type="NOTES">
         <CommonField CommonFieldName="MailAddress"/>
       </Storage>
       <Details>
         <Detail Id="Location" FieldName="Location" Type="text/plain"/>
         <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
         <Detail Id="EmailAddress" FieldName="InternetAddress" Type="text/plain"/>
         <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
         <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
       </Details>
     </Resources>
   </UserInformation>
   ```

---

**Table 156. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>
Since the UserInfo application can retrieve data for a user from multiple data sources, a common field must be shared among the storage repositories. This field must be unique for its corresponding directory. By default, users' email address are used as the common attribute. Consequently, users must be uniquely identified by their email addresses. If another attribute is preferred, the following line must be updated to reflect the field for that attribute:

```
<CommonField CommonFieldName="MailAddress"/>
```

7. Restart your Sametime server and the Domino server to effect all the changes.

**Configuring a dual repository with Domino Directory and custom:**

For retrieving Business Card information, you can set up a dual repository of a Domino Directory and a custom Lotus Notes application.

**Before you begin**

This section describes how to configure the Business Card using two storage repositories: Domino Directory with a custom Lotus Notes repository. Here, we describe how you can set up Domino Directory as the primary storage, and a custom Lotus Notes application as the secondary storage.

These directions assume the following:

- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Business card information can be retrieved from your Sametime directory
- A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf)
• To use a custom Lotus Notes application as an auxiliary repository, each user record in the custom database must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).

Procedure
1. Click Administer the server, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click Business Card Setup.
3. In the User Information section, select the entry you want displayed in users' business cards, and then click Add to move the entry to the right-side list box.
   To remove preselected entries, click the entry and click Remove. The following table lists the default attribute value that is mapped to each attribute name in the Attribute Names and Attribute Values section.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the Attribute Names and Attribute Values section, if the information you want displayed in users' business cards is not mapped to the appropriate attributes used in your company, then you may need to update it.
5. To prepare attributes for use by the auxiliary storage, in the attribute name/attribute value section, remove the values for the attributes that are to be retrieved from the auxiliary storage. In this example, we are retrieving the Telephone information from the custom Notes application; therefore, you should delete the value for the Telephone attribute, and then click Update to save the changes. These values are removed to ensure the appropriate values are retrieved from the auxiliary data repository, and not the first.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

6. Modify the UserInfoConfig.xml file located in the Domino program directory (\lotus\domino\UserInfoConfig.xml) using a text editor. The UserInfo application fetches and delivers user information for each user’s request to view a particular user’s business card.
a. Add the following NOTES_Custom_DB Storage tag inside the Resources tag:

```
<Storage type="NOTES_CUSTOM_DB">
  <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
  <Details>
    <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
  </Details>
</Storage>
```

**Note:** In the StorageDetails tag, the following settings are specified:

- **DbName =** database_path Filename of the custom Lotus Notes application (relative path to the domino data directory)
- **View =** view_name The name of the Notes view that displays the documents containing the user records
- The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Lotus Notes application.

b. Since the Telephone number must come from the custom Notes application, ensure the information is not retrieved from the Domino directory by removing the following information from the Details tag of the Notes storage:

```
<Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
```

c. Add the following information to the BlackBox Configuration section. The Notes black box must come first since the listed order defines the search order:

```
<BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametimeuserinfo.userinfobb.UserInfoNotesCustomBB" MaxInstances="4"/>
```

**Note:** The Sametime directory must be configured as the primary storage so it can be searched first by the UserInfo application. In this example, the Domino directory is the Sametime directory; therefore, the NOTES_CUSTOM_DB black box is listed **AFTER** the Notes black box.

Now the UserInfoConfig.xml should look like this:

```
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="EmailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="NOTES_CUSTOM_DB">
      <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
      <Details>
        <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
</UserInformation>
```
7. So the *UserInfo* application can retrieve data for a single user from multiple sources, a common field must be shared among the storage repositories. By default (though any unique value may be used), the user’s email address is the common attribute, so in both storage repositories, users must be uniquely identified by their email addresses. If you want to use a different attribute, you must update this line to show which attribute you plan to use:

```
<CommonField CommonFieldName="MailAddress"/>
```

8. Restart the Sametime server and the Domino server to effect all the changes.

**What to do next**

You have successfully configured the business card to display information for a single user from dual storage repositories: the Domino directory and a custom Notes application.

**Additional configurations for black boxes**

Though Sametime ships with two black boxes or special implementations already present for configuring with LDAP or Domino, additional black boxes can be configured to retrieve data from more than one resource. A special configuration can be used to designate NOTES as its first box, if Sametime is configured with Domino, and with LDAP as its second black box.

For a Sametime installation that is configured to work with Domino but that can also retrieve data from Domino LDAP, Notes would be listed as the first black box, and LDAP as the second. Each of these special configurations requires manual settings in the *UserInfoConfig.xml* file.

This version of Sametime includes an additional black box that enables data retrieval from a separate Notes database (other than the Domino directory). This black box should be applied as a part of a special configuration designated to retrieve data from the Sametime directory and from an additional Notes database that contains users’ business card details.

See the topic “Retrieving data from a customized database” on page 1111 for more information on how to configure data retrieval from the additional Notes database.

A newly-written black box or special implementation can be used to retrieve data from any selected data resource. The black box should be implemented and configured according to the Application Programming Interface (API) and to the instructions published with the Sametime Software Development Kit (SDK).

**For 8.5 and 8.5.1 only**

To use the customized black box, an additional configuration setting is required. In the `sametime.ini` file, under the *Config* section, add the following flag:

```
USERINFO_LOAD_SVC_IN_SERVLET=1
```

For additional help with these special configurations, please contact Support.
Retrieving data from a customized database:

For the user data included in the Business Card, Administrators can retrieve details about the user from separate Notes databases that are dedicated to storing user details and that function independently of the Domino directory that is used for Sametime.

About this task

Retrieving user data from customized Notes databases allows you to:

- Retrieve some details from the Sametime Domino directory and the rest from a customized Notes database (Domino)
- Retrieve some details from the LDAP directory Sametime is configured to work with and the rest of the details from an additional Notes database.

An additional black box, which functions as a customized special implementation, is provided to enable data retrieval from the customized Notes database. This 'customized' black box should always be preceded by a call to the black box that handles the Sametime directory. A CommonField tag is used for synchronization between the black boxes. If the common field is defined as MailAddress, then the value retrieved for MailAddress from the first storage (LDAP or Domino) is used as the ID to query for in the customized database. The application first queries the database using the userID received as a parameter; if no record is found, it queries the database again, using the value retrieved for the CommonFieldName as userID. To use the customized database feature:

- Perform the following manual steps:

Procedure

1. Open UserInfoConfig.xml and update the CommonField tag in the first 'storage' section to hold the ID property of a Detail tag that represents the same detail in the different storage types. This detail tag is assigned a different field name in each storage section, but the value in each of these fields should be identical for the specific user. The default value for the Common field tag is "MailAddress." The attributes holding the email address for a user should have the same value in both storages.

2. Using the Administrator's Tool, update the Business Card attribute page with the values to be retrieved from the Sametime directory, leaving blank the field name for items required from the customized database.

3. Remove the Detail tags of the fields you left blank in the set-up page from the first 'storage' section in the UserInfoConfig.xml file.

4. Add an additional 'storage' section to the UserInfoConfig.xml as the second storage. This storage section is a new section added specifically for this feature; it differs from the standard Notes storage section through the additional parameters specified below:

```xml
<Storage type="NOTES_CUSTOM_DB">
    <StorageDetails DbName="" View="$users" />
    <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain" />
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain" />
        <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain" />
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain" />
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain" />
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain" />
    </Details>
</Storage>
```

Chapter 14. Administering
5. In the newly-added "storage" section, delete the Detail tags of the items that you do not want to retrieve from this database, and update:
   a. The DbName property, including the full path
   b. The view name (if needed)
   c. The mapping of the "Detail" tag so each item is mapped to the correct field name of the new database

6. Add a BlackBox tag to the BlackBoxConfiguration section in UserInfoConfig.xml as a second record:
   ```xml
   <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userinfo.userinfoxbb.
   UserInfoNotesCustomBB" MaxInstances="4" />
   ```

7. Restart StConfiguration and the HTTP task.

What to do next

Note: For complete information on how to use these "black boxes" and on how to use all the storage repositories for LDAP, Sametime, and Domino, see the section in Business Card entitled "Using repositories." This section provides detailed information on how to store and retrieve user data contained in both single and dual repositories.

Mapping a detail to multiple attributes

An optional setting in UserInfoConfig.xml file lets you map a detail to more than one attribute. As a result, the returned value for a detail is composed of a list of attributes retrieved from the storage.

About this task

You can do this by mapping an item to a comma-separated list of attributes.

```xml
<Detail Id="Telephone" FieldName="telephoneNumber,mobile" Type="text/plain" />
```

The response can contain a list of values separated by any character chosen by the administrator. To apply the new separator, edit the UserInfoConfig.xml file.

Procedure

1. Open UserInfoConfig.xml in an editor.
2. Choose the Detail tag that you want to use to retrieve a list of attributes.
3. Complete the FieldName property with the list of attributes to retrieve, separated by commas.
4. Add an additional property: DisplaySeparator. Set its value to the required character that should appear in the response xml between any 2 retrieved attributes values. For example,
   ```xml
   <Detail Id="Telephone" FieldName="telephoneNumber,mobile" Type="text/plain" DisplaySeparator="/" />
   ```
5. Log in to the Integrated Solutions Console.
   a. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
   b. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the Business Card tab
   d. Verify that the mapping of this detail (the Telephone detail in the example) is empty.
   e. Click OK.
6. Restart the server.

**UserInfoConfig Debug tracing**

If additional information is need to trace a problem, tracing information can be collected. To enable trace collection, set the `USERINFO_DEBUG_LEVEL` flag of the `sametime.ini` file.

1. Stop the IBM Sametime Community Server.
2. Set or add this flag in the debug section of `sametime.ini` file:

```
USERINFO_DEBUG_LEVEL=5
```

   The trace file will have a name and format like `UserInfo_091021_1818.txt` for the UserInfo Server Application and `UserInfoHTTP_091231_2240.txt` for the UserInfo servlet. You can find the file in the Trace folder.

   **Linux and IBM i only:** If you are running Sametime Community Server 8.5.1 on Lotus Domino 8.5.2, then edit the `domino_directory/servlets.properties` file by removing `UserInfoServlet` from the `servlets.startup` line.

3. Restart the Sametime Community Server.
4. When the server is fully started, send an http request using a web browser to activate the servlet.

**Resolving problems with business cards**

If Business Cards are not displaying user information as expected, check the server configuration, then the client, and finally, the business cards themselves.

**Checking the server configuration**

Check and validate the configuration on the storage repository you use with the Sametime Community Server. A configuration problem is the most likely cause of problems with Business Cards. For more information, see the appropriate section in Managing business cards.

**Checking the UserInfo servlet on the client**

The UserInfo servlet on the client receives and responds to client requests. The servlet must be working correctly to provide the requested details for Business Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.

1. Determine the distinguished name (DN) of the user whose Business Card you want to view. Here are sample DNs of the various directory types:
   - Domino directory: `cn=sametime User/O=IBM`
   - Active directory: `cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com`
   - TDS directory: `uid=Sametime user,ou=Austin,o=IBM`

2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:
   - `[protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1&UserId=[User DN]`
   - `[protocol] = {http, https}`
   - `[hostname] = {Fully qualified hostname of the Sametime server}`
   - `[User DN ] = {The full distinguished name of the user for whose information you are seeking}"

   **Examples:**
   - Domino Directory:
http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/o=IBM

- Active Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User.cn=users,dc=austin,dc=ibm,dc=com

- TDS Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime user,ou=Austin,o=IBM

**Note:**
- Do not use spaces in the URL for the UserInfo servlet operation.
  A space is translated into `%20` in the URL, and the servlet will not produce a result; for example:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/o=IBM

  is translated to:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime%20User/o=IBM

  The characters "%20" are inserted before the word "User" to represent the space.
- The name "UserInfoServlet" is case sensitive.
- Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you've composed into a web browser's address field, and view the result.

You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.

An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:
- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

**Checking the client**

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.

**Checking that Business Cards meet requirements**

Finally, verify that the business cards follow these requirements.
- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

**Note:** Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.
- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage
Changing user names

After users have been registered in IBM Sametime, you can change their names if their user IDs must change due to a name or location change.

About this task

The name conversion tool or use the AdminP feature should be used for changing user names as needed. To eliminate the need to run name changes in the future, you can migrate older user IDs to a unique directory attribute, which requires you to run the name conversion tool only once. This can be done only for an LDAP directory and only when the names in the directory are already synchronized with Sametime.

Related tasks

“Migrating older user IDs to a unique directory attribute” on page 777

If you are using an older release, you can migrate user IDs to a unique ID, so you do not need to run the name change utility when a person’s name changes in the directory. Having a constant user ID attribute eliminates the need to change a user ID when a name changes.

Changing names as needed

When you change user or group names in the directory, the change is not reflected in IBM Sametime Community Server databases. In order to synchronize the directory names with the names in the Sametime Community Server databases, you must run the name conversion utility.

About this task

Running the name conversion utility updates Sametime Community Server user or group names with the latest directory changes. The name conversion utility uses a comma-separated value list that you compile to change names, delete names, or convert all names from Domino to Domino LDAP formatted names.

Users create a contact list, a privacy list, and an alert-me-when list in the IBM Sametime Connect client by selecting user names or group names from the Domino or Domino LDAP directory that is used with the IBM Sametime Community server. These contact, privacy, alert-me-when lists are stored in the user information database (vpuserinfo.nsf) on Sametime Community servers. When a user starts the Sametime Connect client, the lists are downloaded from the database to update the lists stored on the client’s local computer.

You do not need to run the name conversion utility when you add new users or groups to the Domino or LDAP directory.

Run the name conversion utility manually on a stand-alone Sametime Community server, or on a server in a cluster which will replicate the change throughout the cluster.

Note: Be sure to stop the Domino server before you run the name conversion utility.

Preparing for changing names:
Before you can run the name conversion utility, you need to perform the following tasks:

About this task

You do not need to use the name conversion utility if you add new users or groups to directory. Use the name conversion utility only if you change user names or group names that exist in the directory.

Creating a comma separated value file:

A comma-separated value (CSV) file created in a text editor provides the name conversion utility with the information it needs to make a name change to user contact, privacy, and alert-me-when lists. The CSV file includes the type of change and typically provides details such as the old name and the new name, and optionally, the display name.

Procedure

1. Use a text editor that supports UTF-8 saving format to create a comma-separated file.
2. Create a CSV for only one type of change; you cannot mix name change types in the same CSV.
   - ID
   - ORGANIZATION
   - DELETE
   - LDAP
   - REPORT
3. Name and save the file with an extension of .csv in a directory accessible by the Sametime server. The text file should be saved in UTF-8 format.

Syntax for comma-separated value file used in name change utility:

A CSV file created in a text editor provides the server with the information it needs to make a name change to user contact lists or privacy lists. The CSV file includes the type of change (or descriptor) and typically provides details such as the old name and the new name, and optionally, the display name.

You can create the CSV text file using any text editor. Some spreadsheet programs also allow you to export spreadsheet values to a CSV file. The CSV file should include only the list of comma-separated old name, new name pairs that reflect the changes you have made to the directory. Do not include any header information in your CSV file. Name the file at your discretion. After you create the CSV file, store it in a network location that is accessible from the Sametime server. You must browse to this file to import it when you create the Name Change Task from the Administrator's tool in Sametime.

When you create a CSV file, you must format it correctly following the syntax rules below. CSV files are case-sensitive and sensitive to spaces. You can create multiple CSV files. The CSV file can include only one descriptor:

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Change specified first names, last names, display names, or group names.</td>
</tr>
<tr>
<td>Descriptor</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ORGANIZATION</td>
<td>Change the organization name for all users.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Changes all contact list information from Domino directory format to LDAP format. For example, a user listed as CN=Maria Smith/OU=Sales/O=IBM changes to CN=Maria Smith,OU=Sales,O=IBM.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Remove specified individual contact names from contact lists and privacy lists.</td>
</tr>
<tr>
<td>REPORT</td>
<td>This feature can be used to confirm a name change in the vpuserinfo.nsf database by taking snapshots before and after the change and comparing them. To use this descriptor, create two CSV files in the trace folder that capture the vpuserinfo.nsf tables for user's contact list, alert me list, and privacy list. The CSV file names will be similar to: ConvertStorage_110308_0548.csv ConvertPrivacy_110308_0548.csv The first file contains the contact list and alert me list. The second file contains the privacy list. This feature is also available for releases prior to release 8.5.2 as a hotfix. See Technote #1469735 for more information.</td>
</tr>
</tbody>
</table>

The second part of the CSV file includes one line for each change that includes the old name, the new name, and, optionally, the new display name.

Changing the user and group IDs.
### CSV File Syntax

<table>
<thead>
<tr>
<th>ID</th>
<th>&quot;old ID&quot;, &quot;new ID&quot;[,&quot;new display name&quot;]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>

where the [ ] indicate that the new display name is optional but if you use it, you must precede it with a comma as in the first example (where 'Maria Brown' is the new display name), and the new display name must immediately follow the comma (if you leave a blank space between the comma and the new display name, the conversion will not work).

### Example

Sample CSV showing changes from a Domino directory:

**Note:** These examples have been formatted for spacing issues; make sure your syntax adheres to any restrictions noted in the text.

<table>
<thead>
<tr>
<th>ID</th>
<th>&quot;CN=Maria Smith/OU=Sales/O=IBM&quot;,</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;CN=Maria Brown/OU=Sales/O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Maria Brown&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=John/OU=New York/O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=John/OU=Texas/O=IBM&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;52e811 85256500/Old Group&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;52e811 85256500/New Group Name&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;New Group Name&quot;</td>
</tr>
</tbody>
</table>

Note that "52e811 85256500" in the example above is replica ID of Domino Directory. Be sure to change the colon in the replica ID to a space. For example: "52e811:85256500" should be "52e811 85256500".

Sample CSV showing changes from an LDAP directory:

<table>
<thead>
<tr>
<th>ID</th>
<th>&quot;CN=Maria Smith,OU=Sales,O=IBM&quot;,</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;CN=Maria Brown,OU=Sales,O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Maria Brown&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=John,OU=New York,O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=John,OU=Texas,O=IBM&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=Old Group,OU=groups,O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;CN=New Group Name,OU=groups,O=IBM&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;New Group Name&quot;</td>
</tr>
</tbody>
</table>

Changing the organization name.

<table>
<thead>
<tr>
<th>CSV File Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORGANIZATION</td>
<td>Sample CSV showing changes from a Domino or LDAP directory:</td>
</tr>
<tr>
<td>&quot;oldOrg&quot;,&quot;newOrg&quot;</td>
<td>ORGANIZATION</td>
</tr>
<tr>
<td></td>
<td>&quot;lotus&quot;, &quot;ibm&quot;</td>
</tr>
</tbody>
</table>

Changes all contact list information from Domino directory format to LDAP format (converts forward slashes in the hierarchical name to commas).

<table>
<thead>
<tr>
<th>CSV File Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Sample CSV:</td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
</tr>
</tbody>
</table>

You cannot change the format from LDAP to Domino.

Delete specified users and groups.
CSV File Syntax | Example
--- | ---
DELETE uid | Sample CSV:
  
  *uid=John Deere,ou=sametime,dc=ibm,dc=com
  *uid=Marta Smith,ou=sametime,dc=ibm,dc=com
  *cn=portaladminid,o=example.com

Verify a name change.

CSV File Syntax | Example
--- | ---
[REPORT] | Sample CSV:
  
  *[REPORT]

Creating a Name Change task:

Create a name change task on the IBM Sametime Community server.

Before you begin

Before you create a name change task, create a comma-separated value (CSV) file of the name changes in the Sametime Community Server directory.

About this task

A name change task is not actually a scheduled program; its timestamp merely indicates when the task was created and not when it will be run. The list of tasks is ignored until you run the `stnamechange.cmd` program, which then operates on all of the tasks in the list, using the `.CSV` files specified in the Name Change page.

Follow the steps below to create a name change task.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server where you want to add a name change task. If you want to create a task to run on multiple servers, then click the deployment name of any of the servers on which you want to run the task.
4. Click the Name Change tab.
5. Click New.
   
   **Note:** If you only want to edit a task, you can click the name of the scheduled task to edit it.
6. Enter a name in the Name of Task field. The name is at your discretion. By default, the name is the date the task is created.
7. Optional: Enter a description for the task.
8. Browse for the CSV file you want to use, and then click OK.
9. The name change task appears in the list of scheduled tasks.
   All tasks listed here run when the stnamechange.cmd is run.

Results

After you have completed these steps on one Sametime Community server, it is necessary to repeat this process on other servers in distributed environment.

When you are finished configuring the task, name changes are saved to the stnamechange.nsf file. For a clustered environment, create this task on one server per cluster. All other servers receive the changes through the cluster replication process.

Lotus Domino picks up all valid name change tasks in the stnamechange.nsf file. You choose the servers or cluster on which the name change task runs on a regular basis using general scheduling tools. The application does not run by default; you must run the task manually.

To Delete a name change task, on the Name Change page, select the task, and then click **Delete**. If any name changes are entered incorrectly, you can import a new CSV file.

Running the name conversion utility:

To run a name change task, start the name conversion utility. The name conversion utility uses the CSV file to update user contact and privacy lists with the latest directory changes.

Before you begin

Before you begin, create a comma-separated value file with name changes, and then create a name change task. IBM recommends running the name conversion utility at off-peak hours, and stopping the Domino server before you begin.

About this task

Starting the name conversion utility starts the name change task. You can create many tasks, but name change conversion utility executes only one task at a time. You can have only one name change task scheduled or in progress. If a name change task is scheduled or in progress, you cannot create another name change task until the existing name change task completes.

It is not necessary to run the name change conversion utility on every IBM Sametime Community Server in a cluster. For clusters, the task should run once on one server and then replicated to other servers in the cluster. Note that the **All servers** option on the Name Change page in the Sametime System Console does not work because of the procedure for replicating across all servers. If you create a Name Change task and select **All servers**, only the server you are logged on to contains the task--other servers do not. This is viewable in stnamechange.nsf through the Notes client. The correct procedure is to create the name change task on all the servers in the community.

Running the name conversion utility on Windows:

Follow these steps to run the name conversion utility on Microsoft Windows.
Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Type the following command:
   stnamechange.cmd
3. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server.
   Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on UNIX:
Follow these instructions to run the name conversion utility on a UNIX operating system.

Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Open a new shell and change to the domino data directory.
   cd /domino/notesdata
3. Type the following command:
   ./stnamechange.sh domino_bin_directory domino_data_directory
   For example:
   ./stnamechange.sh /domino/opt/lotus/notes/80020/linux /domino/notesdata
4. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server.
   Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on IBM i:
Follow these instructions to run the name conversion utility on an IBM i operating system.

Procedure
1. Stop the IBM Sametime Community Server.
2. From an IBM i command line, run the "QSH" command. This command starts the QShell interpreter, where the Name Change task is run.
3. Type the following commands:
cd server data directory
stnamechange server data directory domino_bin_directory

where domino_bin_directory is an optional parameter. The default directory is /qibm/proddata/lotus/notes, which causes the command to use the latest version of Lotus Domino installed on the system.

If the Sametime Community server is using an earlier release of Domino, specify the appropriate Domino bin directory.

<table>
<thead>
<tr>
<th>Lotus Domino version used by Sametime Community server</th>
<th>Associated domino bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino 8.5.2</td>
<td>/qibm/proddata/lotus/domino852</td>
</tr>
<tr>
<td>Domino 8.5.1</td>
<td>/qibm/proddata/lotus/domino851</td>
</tr>
<tr>
<td>Domino 8.5.0</td>
<td>/qibm/proddata/lotus/domino850</td>
</tr>
<tr>
<td>Domino 8.0.2</td>
<td>/qibm/proddata/lotus/domino802</td>
</tr>
<tr>
<td>Domino 8.0.1</td>
<td>/qibm/proddata/lotus/domino801</td>
</tr>
<tr>
<td>Domino 8.0.0</td>
<td>/qibm/proddata/lotus/domino800</td>
</tr>
</tbody>
</table>

4. When the command completes, press F3 to exit QSH.

To verify whether all of the names were changed successfully, view the following files in the /trace subdirectory of the server data directory:

namechange_YYMMDD_XXXX.txt
name_change_summary_report_YYMMDD_XXXX.log

If you encounter problems, add VP_NCSA_TRACE=1 to the Debug section of the sametime.ini file to collect additional debug information when you run the name change utility.

5. Restart the Sametime Community Server.

Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Name Change task replication:

When you create a name change task, the task is saved in a file called stnamechange.nsf, and this file is replicated to all home IBM Sametime Community Servers so that updates can be made to each server's vpuserinfo.nsf database. The file vpuserinfo.nsf is the Sametime user information database that contains contact lists and privacy lists.

Set up a Domino replication task to replicate stnamechange.nsf among all servers. By default, stnamechange.nsf is replicated to all servers in a cluster, but not between clusters. This step makes it unnecessary to add future tasks to each stnamechange.nsf database in the environment. When a new task is added, all servers get the new information as a result of the replication procedure.

Note that the All servers option on the name change page in the Sametime System Console does not work because of the procedure for replicating across all servers. If you create a name change task and select All servers, only the server you are logged on to contains the task--other servers do not. This is viewable in stnamechange.nsf through the Notes client. The correct procedure is to create the name change task on all the servers in the community.
If several Sametime Community Servers operate as a cluster, create a name change task on only one server in the cluster. The vpuserinfo.nsf database replicates in real time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster. Declaring the task in one cluster can populate all the clusters because you set replica information for the stnamechange.nsf between all the clusters.

Sample deployments

The examples below illustrate how you might run name change tasks in different Sametime Community Server deployments.

Example Deployment 1

In this example, the Sametime community has the following characteristics:

Three Sametime Community Servers are deployed.

None of the servers are clustered.

With this deployment, you must create and run the name change task three times—one on each server. Though you create the task only once, you run it three times, and the run can be scheduled automatically.

Example Deployment 2

In this example, the Sametime community has the following characteristics:

Eight Sametime Community Servers are deployed.

Three Sametime Community Servers operate as Community Services cluster 1.

Three Sametime Community Servers operate as Community Services cluster 2.

Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster.

With this deployment, you must run the name change task four times. You can schedule the tasks to run automatically on one Sametime Community Server in Community Services cluster 1, on one Sametime Community Server on Community Services cluster 2, and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster.

Example Deployment 3

In this example, the Sametime community has the following characteristics:

• Six Sametime Community Servers are deployed
• Three Sametime Community Servers operate as a Community Services cluster
• Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster
• One Sametime server is not used as a home Sametime server and is not part of a Community Services cluster
With this deployment, you must create the name change task three times. Create the name change task on one of the Sametime Community Servers in the Community Services cluster and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster. You do not need to create the name change task on the Sametime Community Server that is not part of a cluster.

Name Change task status:

This topic describes the status of the name change tasks, how to view tasks in progress, and how to delete a name change task.

After you create a name change task, the task defaults to the Scheduled status. A scheduled task begins executing on the IBM Sametime Community Server at the time specified in the server setting on the Name Change page of the Sametime System Console (Sametime System Console > Sametime Servers > Sametime Community Servers > server_name > Name Change). You cannot edit a name change task that has the Scheduled status. The only way to change a scheduled task is to delete the task and then create a new task in its place.

Once a task begins executing, its status changes from Scheduled to In Progress if any of the servers have the name change task with the status that is in progress or scheduled. You cannot delete a task that is in progress. If all the servers have tasks that are marked Check error log or Disabled, the name change task can be marked Finished.

Finished means the task has completed the name change successfully. At this status level, you can add or delete any task.

Check error log means there were errors incurred while the task was running. At this stage, you can add or delete a task.

Note: The status column provides only the status of the task running on the server being used; it does not provide a summary of the task across servers and clusters of servers.

You can have only one name change task scheduled or in progress on a IBM Sametime Community Server. If a name change task is scheduled or in progress, you cannot create another name change task on the Sametime Community Server until the existing name change task completes.

You cannot delete a task that is marked In Progress. You can delete a task that is marked Scheduled, Finished or Check log status. There is a log file on the server that collects failures in Name Conversion.

- A user name that is changed in the directory but is not yet changed in the vpuserinfo.nsf database will appear as offline in the contact list and privacy list of another user until the name change task executes on the other user's home Sametime Community Server.
- All members of a changed group appear as offline in the contact list and privacy list of a user until the name change task executes on the user's home Sametime Community Server.

You can view the status of the names being changed. The vpuserinfo.nsf database includes a view for name change tasks. The task you are running is not marked complete. If several Sametime Community Servers operate as a Community Services cluster, you view the status of a name change task on only one Sametime
Community Server in the cluster. The database replicates in real-time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster.

Below is an example of viewable statuses. In the example, Servers X, Y, and Z are not clustered, and servers A, B, and C are clustered.

<table>
<thead>
<tr>
<th>Servers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server X</td>
<td>task is created on Server X</td>
</tr>
<tr>
<td>Server Y</td>
<td>task does NOT appear in Name Change page</td>
</tr>
<tr>
<td>Server Z</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server A</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server B</td>
<td>task does NOT appear in the Name Change page, and it does NOT appear in the log file</td>
</tr>
<tr>
<td>Server C</td>
<td>task does NOT appear in the Name Change Status page, and it does NOT appear in the log file</td>
</tr>
</tbody>
</table>

**Note:** Turn on the `sametime.ini` flag if you are working locally:

```
NC_LOCAL_CONVERSION = 1
```

### Changing names with AdminP

This feature allows IBM Sametime to synchronize name change updates made to the IBM Lotus Domino directory via the Domino Administration Process (AdminP) with updates to Sametime User Information database (vpuserinfo.nsf).

Prior to Sametime 8.0.1, when a Lotus Domino Administrator executed name changes through the Lotus Domino Administrator client and the AdminP process, the users' names were changed automatically in the Lotus Domino Directory but were not changed in the corresponding Sametime records. The administrator had to manually generate a CSV text file that contained the renaming information, and run the Sametime name change utility on one or more servers, depending on the configuration.

In Sametime 8.0.1, this process is enhanced, allowing Sametime to update VPUserlnfo.nsf and add a new CSV text file to stnamechange.nsf whenever a change is made in the Domino Directory.

**Note:** It is still necessary to manually run the name conversion utility even when AdminP integration code is working. The Name Change Integration with AdminP feature creates a new Name Change task and only partially updates vpuserinfo.nsf. For example, it does not update the contact lists that include the old name. For a full update, the Name conversion utility must be executed.
In addition, the AdminP functionality is only available for Sametime servers that use Lotus Domino authentication running on Lotus Domino 8.0.2 or later. If the Sametime server is using LDAP authentication, or if you are using a version of Lotus Domino earlier than 8.0.2, you cannot use the AdminP feature to change names.

**AdminP integration components**

The following components contain the code for the Name change integration with AdminP feature. These components are located under the Domino program directory (by default \Lotus\Domino in Windows):

- StUpdateAdminP.dll -- the code loaded by the AdminP process. This DLL file receives notifications from Domino regarding renaming operations. We will refer to it as the AdminP add-in.
- AdminpUpdate.jar -- the java code executed by the StUpdateAdminP.dll
- NameChangeUtils.jar -- a library that provides services of updating the different Sametime databases. called by AdminUpdate.jar to perform the actual change in vpuserinfo.nsf and stnamechange.nsf

**Known issues with AdminP integration**

Please note the following issues concerning AdminP integration with Sametime:

- This feature is supported starting in Domino 6.0, but is currently not available with Domino 8.0.1.
- In Sametime, this feature is supported starting with release 8.0.1.
- Only name updates are handled; deletions and additions are not supported by AdminP.
- To complete the name change process, you must still execute the name change application (AdminP integration simplifies the process but does not replace it)
- When Sametime databases are being updated as a result of the AdminP operation, warning messages are seen on the Domino console. These messages are not an indication of any issue with the process and should be ignored.

**Enabling AdminP integration:**

The name change AdminP integration will run on one Sametime server in each cluster, is part of a Sametime server installation, and is disabled by default.

**Before you begin**

The name change AdminP integration functionality is only available for Sametime 8.0.1 servers hosted on Microsoft Windows and configured to use IBM Domino Directory for authentication. If your deployment uses an LDAP directory, you must use the Name Conversion utility as in previous releases. For information on the Name Conversion utility, see the topic, "About the Name Conversion utility" in this Sametime information center.

**About this task**

Enable the AdminP integration for your Sametime environment by completing the following steps:
Procedure

1. Remove the comment marker from the following statement in the notes.ini file:
   
   EXTMGR_ADDINS=StUpdateAdminP.dll

   If there are multiple servers in one community, only perform this step on one server.

2. Using a text editor, open sametime.ini and confirm that the following flags are set as follows:
   
   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\java;C:\Lotus\Domino\StConfig.jar;
   C:\Lotus\Domino\StConfigXml.jar;C:\Lotus\Domino\AdminUpdate.jar
   ST_JAVA_JVM_PATH=C:\Lotus\Domino\ibm-jre\jre\bin\classic\jvm.dll
   ST_JAVA_LIB_PATH=C:\Lotus\Domino

   The paths may be different based on your deployment.

   Note: Ensure ST_JAVA_CLASS_PATH contains the full path of the AdminpUpdate.jar file (the default path is \Lotus\Domino\AdminpUpdate.jar).

3. If the Sametime community consists of more than one Sametime server, ensure that the following databases are replicated among all of the servers in the community: names.nsf, admin4.nsf.

   A Domino administrator can configure Connection documents to ensure these databases are replicated on a defined schedule. For more information on how to create Connection documents, see the "Scheduling server-to-server replication" topic in the Domino Administrator Help information center.

   Now the environment is setup properly for Sametime to capture name changes carried out by the AdminP.

4. Run the stnamechange.cmd as described in the topic, "Running Name Change Tasks on Sametime servers in a community" in this Sametime information center.

Specifying an administration server for databases:

AdminP uses administration servers to manage administrative changes that apply to IBM Domino databases. Either the administrator or the database manager can specify the administration server for a database. Perform this procedure on an as-needed basis.

Before you begin

To change the administration server for a Domino database, you must have Manager access to the database or be designated as a Full access administrator on the Security tab of the Server document.

About this task

Procedure

1. From the IBM Lotus Domino Administrator, open the domain containing the server with the database for which you are setting an administration server.

2. From the Servers pane, select the server containing the database you are setting as an administration server.

3. Click the Files tab and then select the database to which you are assigning an administration server.

4. From the “Tools” pane, click Tools > Database > Manage ACL.

5. Click Advanced.
6. Complete these fields and then click **OK**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server</td>
<td>Choose one of these: &lt;br&gt; • None -- If you do not want an administration server assigned for the database. &lt;br&gt; • Server -- Select a server from the list.</td>
</tr>
<tr>
<td></td>
<td>Choose one of these according to whether you want modifications to the indicated fields to occur during a rename group, rename user, or rename server action; or during a delete server, delete group, or delete user action: &lt;br&gt; • Do not modify Names fields -- Names fields are not updated during any of the above rename and delete actions. &lt;br&gt; • Modify all Readers and Authors fields -- Reader and Author fields are updated during the rename and delete actions listed above. &lt;br&gt; • Modify all Names fields -- All names fields are updated during any of the rename or delete actions listed above.</td>
</tr>
</tbody>
</table>

7. If you will be processing administration requests across domains, complete the procedure in the topic "Creating a Cross-domain Configuration document" in the Domino Administration information center.

*Sample configurations:*

AdminP operates with various configurations of the IBM Sametime server and IBM Domino.

**Sametime and the Domino Directory are hosted on the same machine**

The Sametime and Domino directory are on the same server. When a rename is made the AdminP add-in is notified and the callback updates the relevant databases. After the Name Change Utility is run all users can see each other's updated names.
Two or more Domino servers, each hosting Sametime and a Domino Directory

The Domino directories are replicated between all servers. Names.nsf and admin4.nsf are replicated on all servers. A name change executed on either one of these servers will trigger the AdminP process on both servers. Each AdminP process updates only the database that their administration server matches. This setting avoids replication conflicts.

Domino Directory hosted remotely from Sametime but within the same Domino domain

One or more Sametime servers and Domino directory are in the same domain. Each Sametime server accesses the Domino Directory through the directory assistance feature. Since all are in the same domain and the remote directory is accessed through da.nsf, updates are done on the remote directory and are received on the Sametime server. The Sametime server triggers the update of the databases that set their administration server to be the local server and activate the callback in the AddIns.
Domino Directory hosted remotely from Sametime, in a different Domino domain

This time, the Sametime servers and the Domino directory are in different domains. For rename updates to go from the Domino directory on Domain A to the Sametime servers on Domain B, a cross domain configuration should be applied on these domains. When a name is updated on the directory in domain B, a mail message is sent to domain A (assuming cross domain configuration is applied). This mail message is treated as a request for the AdminP and is added to the admin4.nsf which logs the request for the AdminP process.

Refer to the Domino Administration guide for additional information on cross-domain configuration.

Domino Directory hosted remotely from Sametime, in a different Domino domain, and not serving as primary directory

The Sametime servers and Domino directory are in different domains, and the Domino directory is not the primary directory for the deployment.
As in the previous configuration, the Cross Domain Configuration should be applied and the da.nsf on the Sametime servers should point to the required NAB in the remote Domino server (instead of names.nsf).

Two or more Domino Directories on remote servers, replicated with one or more Sametime servers

The Sametime servers and the Domino directories are in different domains. A Cross Domain Configuration should be applied and the da.nsf on each Sametime server should point to the required NAB in the remote Domino cluster. One server in the Domino environment (domain B) should be defined as the Administration server of the Primary address book for the Domino Domain. The da.nsf of each Sametime server should point to the NAB on this server.

Changing a person’s name with AdminP:

You can use the AdminP feature to change a user’s name in IBM Sametime.
About this task

To change a name in an environment with the AdminP add-in enabled:

Procedure
1. From the IBM Lotus Domino Administrator, click the People & Groups tab.
2. In the left-hand column, choose People under the selected directory.
3. Select the name that you want to change; for example, "Sara Lester".
4. On the right-hand side, select the People tab and choose Rename.
5. In the "Rename selected HTTP, POP3, and IMAP people" dialog box, specify the time frame allowed for a user to login with both the old and the new names and click Next.
6. Now select a user name, fill in information in the appropriate fields to change the name, and click Next.

For example, to change Sara's last name from "Lester" to "Webster," type Webster in the Last Name field. Domino processes these name changes periodically (every 60 minutes by default). When the process is complete, the changes are reflected in vpuserinfo.nsf and stnamechange.nsf as follows:
- In vpuserinfo.nsf, the storageUserId of the renamed user is changed to the new name. For example, "Sara" storageUserId is changed from "CN=Sara Lester" to "CN=Sara Webster".
- In stnamechange.nsf, a new name change task is created, containing a CSV file that describes the name change.

An adminp.csv file containing your changes is then attached to the newly created task. For example, the adminp.csv file for changing Sara's last name looks like this:

<table>
<thead>
<tr>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;CN=Sara Lester/O=ExampleCorp&quot;, &quot;CN=Sara Webster/O=ExampleCorp&quot;, &quot;Sara Webster/ExampleCorp&quot;</td>
</tr>
</tbody>
</table>

7. Run the stnamechange.cmd to complete the name change process.

For more information, refer to the topic "Running Name Change Tasks on Sametime servers in a community" in this Sametime Information Center. Additional information is available in the Tech Note "NameChange administration tasks in Sametime 8" at the following web address:

http://www.ibm.com/support/docview.wss?&uid=swg21290627

Troubleshooting AdminP integration:

If your AdminP integration does not work properly, use the information below to help resolve issues.

The AdminP feature is not working

1. Ensure the AdminP name change add-in is enabled by the following line in the notes.ini:

   EXTMR_ADDINS=StUpdateAdminP.dll

2. Turn on the trace files flags, rename in the directory, and analyze the trace files.

The trace files indicate that the JNI does not find the java class

1. Ensure the following files are located in the program directory:
   - nadminp.exe
   - StUpdateAdminP.dll
   - AdminpUpdate.jar
2. Ensure the following directory flags in sametime.ini have the correct values:
   - ST_JAVA_CLASS_PATH
   - ST_JAVA_JVM_PATH
   - ST_JAVA_LIB_PATH

Working with trace files:

Trace files are located in the trace directory.

The Trace flags are located in the [Debug] section of sametime.ini:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>StUpdateAdminP_080608_1046_2508_000.txt</td>
<td>C trace files</td>
</tr>
<tr>
<td>stupdateJava_080608_1122.txt.0</td>
<td>Java code trace files for the AdminP name change addin and Name Change API together</td>
</tr>
</tbody>
</table>

Validation

Do the following to validate that a name change worked:
1. Rename a user in the Domino directory.
2. On the Domino console, type: `tell adminp process all` (this will process all the AdminP requests immediately).
3. Verify that a new task with the correct name change was added to stnamechange.nsf.
4. Verify that the user's "StorageUserId" value was renamed.

Updated trace information

Verify that the StUpdateAdminP_080624_1451_3192_000.txt trace file contains a line similar to the following:

080624_145626,INF,DEBUG , JNI call completed for name = CN=Sara Lester/O=ExampleCorp

Verify that the stupdateJava_080624_1456.txt.0 trace file contains lines similar to the following:

Jun 24, 2008 2:56:23 PM
com.ibm.sametime.stupdate.StUpdateDBs updateDb
FINE: from java method old name is CN=Sara Lester/O=ExampleCorp newName = CN=Sara Webster/O=ExampleCorp

Jun 24, 2008 2:56:23 AM
com.ibm.sametime.namechangeutils.NameChangeUtils updateInfoUserID
INFO: completed.
Changing the IP address of an IBM i Sametime Community Server

Your IBM i Sametime Community Server should be set up so that it uses host names and does not refer directly to IP addresses. This allows you to change the IP address for your Sametime Community server by simply updating the host table and DNS.

About this task

To change the IP address for your Sametime Community server, follow these steps:

Procedure

1. Update your host table so that the new IP address is associated with the appropriate host name. Make sure that the fully qualified host name is listed first among the entries for your IBM i Sametime Community Server, before any short names. For more information, see "Updating the host table on IBM i."

2. Likewise, update your DNS entries so that the new IP address is associated with the appropriate host name. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see "Updating the Domain Name Server for IBM i."

3. Stop and restart the Sametime Community Server for the changes to take effect.

Changing the host name of an IBM i Sametime Community Server

The command CHGLSTDOM simplifies the process for changing the host name setting of an IBM i Sametime Community Server.

About this task

The procedure described in this section can also be used to correct problems with the configuration of your Sametime server. For example, if your TCP/IP host table did not correctly list the fully qualified host name first at the time that you setup your Sametime Community Server, many elements of your server configuration may be incorrect. You can correct this problem by following this procedure to change the host name of your Sametime Community Server.

To change the host name, follow these steps:

Procedure

1. Update your host table so that the new host name is associated with the appropriate IP address. Make sure that the fully qualified host name is listed first among the entries for your Sametime server, before any short names. For more information, see "Updating the host table on IBM i."
2. Likewise, update your DNS entries so that the new host name is associated with the appropriate IP address. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see "Updating the Domain Name Server for IBM i."

3. End the IBM i Sametime Community Server.

4. Update the host name for the Domino server using the CHGDOMSVR command. For detailed information on changing the configuration of a Domino server, refer to "Updating the configuration of existing IBM i Domino servers."

5. On any IBM i command line, type the following and press F4:
   CHGLSTDOM

6. On the Change Sametime on Domino display, specify the following and then press Enter:
   - The name of the IBM i Sametime Community Server where you want to make this change (for example, stdom1).
   - The new fully qualified host name for the IBM i Sametime Community Server (for example, stdom1.acme.com).
     - Updates the Ports - Notes Network Ports - Net Address field in the Server document.
     - Adds the host name to the Internet Protocols - HTTP - Host name field in the Server document.
     - Updates Sametime files that reference the host name.

   **Note:** If your server is enabled for both IPv4 and IPv6 addressing, you must manually update the sametime.ini file so that "VPS HOST=" is set to an explicit IP address, rather than the host name, after running the CHGLSTDOM command. See Configuring the Community Services for IPv6 for detailed instructions.

7. Start the IBM i Sametime Community Server.

8. Open the Domino directory (names.nsf) on your IBM i Sametime Community Server and edit the Server document. Look at the Internet Protocols - HTTP tab in the Server document and locate the Basics - Host name(s) field.

9. The Basics - Host name(s) field may contain more than one name. If any of the names are incorrect or not needed, delete them. Make sure that the correct fully qualified host name is listed first in the field.

   **Note:** If your server is configured for both IPv4 and IPv6 addressing, there are additional considerations when updating the Host name field. See Configuring Lotus Domino for IPv6 on IBM i for detailed instructions.

10. Save and close the Server document.

11. If you are using HTTP Tunneling with multiple IP addresses, then additional configuration updates are required. See "Updating the host names when using HTTP Tunneling with multiple IP addresses" later in this section.

12. Stop and restart the IBM i Sametime Community Server for the changes to take effect.

What to do next

Updating the IBM i host names when using HTTP Tunneling with multiple IP addresses
If you are using HTTP Tunneling with multiple IP addresses, then you must update your configuration manually after using the CHGLSTDOM command to change the IBM i server host name. If you are not using HTTP Tunneling with multiple IP addresses then this step is not applicable.

The CHGLSTDOM command placed the new host name in the tunneling host name fields, but did not preserve the required prefixes, such as community-, meeting- and broadcast-, in the Sametime configuration. Use the Sametime Administration tool to update the host names in the following fields in the "Connectivity" section:

- Community Services Network settings -> Address for client connections-Host name should have prefix of community-
- Community Services Network settings -> Address for HTTP tunneled client connections-Host name should have prefix of community-

**Monitoring the Sametime Community Server**

The IBM Sametime monitoring charts allow you to monitor Sametime Community server statistics by providing up-to-the-second information about Community Services, web statistics, and free disk space on the server.

**About this task**

All monitoring charts are available from the Monitoring menu in the Sametime Administration Tool. The charts that are available from the Miscellaneous link in the Monitoring menu are part of the Domino web Administration Tool. These charts provide information on web statistics, server memory, and disk space. To view the status of the Sametime Community services since the last server restart, click the Overview link in the Sametime Administration Tool. Also note that the time of day that is listed in the monitoring charts is calculated according to the browser's time zone, not the server's time zone.

**Procedure**

1. Enter the URL for the Sametime Community server:
   
   http://hostname/servlet/auth/admin

   Where hostname is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime Community server you want to administer.

2. Enter the administrator name and password specified during the Sametime Community server installation.

3. Select Monitoring.

   **Note:** To view the status of the Sametime services since the last server restart, click Overview.

4. Select the appropriate chart for monitoring.

**Monitoring general Sametime Community Server status**

General Server Status monitoring chart allows you to see the status of the IBM Sametime Community Server at a glance.

**Total Community Logins**

The Total Community Logins chart displays current information about:

- **Total Community Logins** - The total number of logins to Community Services on the Sametime Community Server that you are monitoring. The Total
Community Logins chart includes multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

- **Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, the Total Unique Logins chart records only one login for that user. A user logged in from multiple clients is considered a single unique login. Use this chart to determine the current number of Community Services users.

- **Total 2-way Chats** - The total number of 2-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with another user, that chat will be counted in the Total 2-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total n-way Chats** - The total number of multi-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with two other users, that chat will be counted in the Total n-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total Number of Active Places** - The Total Number of Active Places chart lists the combined number of n-way Chats and active meetings. Both n-way Chats and online meetings are counted as Active Places; 2-way Chats are not counted in this chart.

**Monitoring Sametime Community Services logins**
A user can be logged in to the IBM Sametime Community Services from more than one client.

To access the Logins chart, open the Sametime Administration Tool and select Monitoring > Logins. The Logins chart displays:

- **Community Server Total Logins** - The total number of logins to Community Services, including multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

  Internal components of the Community Services also log in to the Community Services. These are intra-server connections between Community Services components that occur as part of the normal operations of the Community Services. These logins are also counted in the total logins chart.

- **Community Server Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, this chart records only one login for that user. A user logged in from multiple clients is considered a single "unique" login. Use this chart to determine the current number of Community Services users.

The Logins chart updates at the time interval specified in the Polling Interval (seconds). Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click Refresh.
**Monitoring miscellaneous Domino web Administration statistics**

The Miscellaneous charts are part of the IBM Lotus Domino Web Administration pages. The IBM Sametime Community Server uses features in the Lotus Domino server and its associated web administration pages.

You can monitor various statistics and events from the Lotus Domino Web Administration pages, including:

- Memory
- Statistics
- Disk Space

To access the Domino Web Administration pages, choose **Monitoring > Miscellaneous** in the Sametime Administration Tool, and then click the link that appears at the bottom: **You can view the Lotus Domino web Administration pages in a new browser window.**

**Monitoring the Domino log**

To access the Domino log, choose **Logging - Domino Log** in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

The Domino log is only available from the Sametime Administration Tool. If you record Sametime log information in a text file, the text file does not include information about the Domino log.

A administrator can view additional information about the Sametime server in the Domino log database (log.nsf). The Domino log database records server activity information related to the Domino server and Domino databases, including databases used by the Sametime server (such as the Sametime Meeting Center). During setup, the Domino log database is automatically created and the server is assigned Manager access in the database's Access Control List (ACL). The default access for all other users is Reader.

The Domino log database records information about all server activities, such as database size and usage, server events, calls made to and from the server, and billing for server services. Check the Domino log to monitor:

- Available server disk space
- Available server memory
- Server load
- Server performance
- Databases that need maintenance

**Content of the Domino log**

The administrator cannot use the Sametime log settings or the Sametime Administration Tool options to determine what appears in the Domino log. The Domino log records information about the activities of the Domino server on which Sametime is installed. Generally, the default settings should provide an adequate record of server activity. However, you can record additional information in this log file by altering settings in the notes.ini file. Recording this additional information might be necessary to troubleshoot a specific system problem.

For more information, see the Maintenance section of the Domino R5 Administration documentation.
Views in the Domino log

The Domino log includes many views that do not apply to Sametime. Use the table below to determine which views are relevant for Sametime.

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database-Sizes</td>
<td>Lists the size of the database, the percentage of the database's disk space in use, and the weekly usage for all databases on the server. Use this view to check unused views, database size, and unused space in a database.</td>
</tr>
<tr>
<td>Note:</td>
<td>The stconf.nsf database grows in size depending on the number of meetings that have been created. You can archive this database frequently to prevent it from growing too large.</td>
</tr>
<tr>
<td>Database-Usage</td>
<td>Lists the date and time the database was accessed, the type of access, and the name of the user accessing the database for all databases on the server. Use this view to check unused views and unused space in a database.</td>
</tr>
<tr>
<td>Mail Routing Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>Shows Sametime events and error messages not contained in other views. Messages are sorted in order of occurrence. Use this view to check for Sametime error messages, server crashes, and corrupted databases.</td>
</tr>
<tr>
<td>NNTP Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Object Store Usage</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Passthru Connections</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By Date</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By User</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Replication Events</td>
<td>Not used by the Sametime server.</td>
</tr>
</tbody>
</table>
Sample Billing Shows the same information provided in the Usage views, but the information is not categorized. The information in this view can be easily exported to a spreadsheet.

Use this view for billing purposes, such as Meeting Center usage, network usage, and database usage.

Usage-By Date Shows Sametime user transactions sorted by date. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating documents. Each record lists the date and time of the transaction, the user name, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check database use on a specific date and users' transactions with the server.

Usage-By User Shows Sametime user transactions by user name. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating a document. Each record lists the user name, the date and time of the transaction, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check a particular user's transactions on a database.

**General log settings**

The General log settings allow you to specify the format for the Sametime log and to control the information that the log records.

The four types of General log settings are: (Note that meeting server events do not apply to Sametime Limited Use.)

- **Database or text file settings** - Allow you to specify the format for the log and to automatically remove information from the log.

- **Sametime statistics settings** - Allow you to control whether to log statistics related to chats, meetings, and users.

- **Server community events to log settings** - Allow you to control which Community Services events are recorded in the Sametime log.

- **Meeting server events to log settings** - Allow you to control which Meeting Services events are recorded in the Sametime log.

**Log output location:**
To access the "Database or text file" settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The "database or text file" settings allow you to specify the format for the log and to automatically remove old information from the log.

**Enable logging to a Domino database (STLog.nsf)**

Select this setting to record Sametime Meeting Services and Community Services data in the Sametime log database (stlog.nsf). During setup of the Sametime server, the Sametime Log database is automatically created, and the administrator specified during setup is assigned Manager access in the database Access Control List (ACL). The server is also assigned Manager access to the database so that it can write information to the log. The default access for all other users is Reader.

When this option is selected, a Sametime administrator can view all of the information in the Sametime log by opening the Sametime Administration Tool and selecting Logging. The links available from the Logging menu display different views of the Sametime log database.

When this option is selected, you can use the "Remove history after (days)" setting to prevent the Sametime log from growing too large.

If the "Enable logging to a Domino database" option is not selected, Sametime activity is not recorded in the Sametime database, and the links beneath the logging option in the Sametime Administration Tool do not appear.

If you select this option, you cannot select the "Enable logging to a text file" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Remove history after (days)**

Select this setting to automatically remove old information from the Sametime log database (stlog.nsf). In the field provided, specify the age (in days) of information that is automatically removed from the database. The default setting is 60 days.

This setting only applies to the Sametime log database; it does not remove Sametime log information stored in text files. You must manually delete old text files.

After selecting this option, click Update and restart the server for the setting to take effect.

**Logger output location**

Select this setting to record Sametime log information in a text file. When this option is selected, a new Samtime log text file is created every day. By default, the name of each text file contains the date on which the file was created (for example, log_23_Mar_2009.txt). After you select this option, specify a path and file name for the log file in the "Path to log text file" field; for example, in Microsoft Windows: d:\notesdata\chatlogs\txtfiles\log.txt
To view the file, open it in your preferred text editor. You cannot view the text file log from the Sametime Administration Tool.

If you log Sametime activity to a text file:
• Sametime activity is not recorded in the Sametime log database, and the links beneath the logging option in the Sametime Administration Tool do not appear. You cannot access the Domino log when you log to a text file.
• You must manually delete the text files from the server hard drive periodically to conserve hard disk space.

If you select this option, you cannot simultaneously select the "Enable logging to a Domino database" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Sametime Community Server log size and content settings**

To access the log settings, choose Logging - Settings in the Sametime Administration Tool.

The IBM Sametime Community Server uses these log settings:
• General settings - Allow you to specify the format and content of the Sametime Community Server log.
• Capacity Warnings - Allow you to set server usage parameters. When these parameters are exceeded, warning messages are written to the Sametime log. These messages help you monitor server usage and determine the cause of slow server performance.

**Sametime Community Server events log settings:**

To access the IBM Sametime Community Server events log settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The Community Server events log settings allow you to control which Community Services events are recorded in the Sametime Community Server log. After selecting any of these options, click Update for the settings to take effect.

**Note:** The settings take effect within a reasonable time period. The longest time period you will wait for these settings to take effect is the time interval specified for the "How often to poll for new servers added to the Sametime community" setting in the Configuration - Community Services settings of the Sametime Administration Tool. The default time interval for that setting is 60 minutes.

**Successful logins**

Select this setting to record information about successful Community Services logins and logouts in the Community Logins/Logouts section of the Sametime log. This option is selected by default.

**Failed logins**

Select this setting to record information about failed logins to Community Services in the Place Login Failures, Meeting Login Failures, and Community Logins/Logouts sections of the Sametime log.
Community server events and activities

Select this setting to record information about Community Services events in the Community Events section of the Sametime log. For example, you can view the name and status of each service.

Administering a Sametime Proxy Server

This section describes how to manage a IBM Sametime Proxy Server.

Updating Sametime Proxy Server connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Proxy Server.

Before you begin

If you are configuring the Sametime Proxy Server to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Proxy Server. These settings are only used by the Sametime System Console to connect to the Sametime Proxy Server.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Proxy Server.
3. In the Sametime Proxy Servers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's User name and Password for connecting to the Sametime Proxy Server.
5. By default, the Sametime Proxy Server trusts other Sametime components. If you want to change this, then select Do not auto-accept SSL certificate.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.
Related tasks

“Adding a Sametime server SSL certificate to the Sametime System Console” on page 830

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

Administering a Sametime Media Manager

The audio/video services are enabled by default following an IBM Sametime Media Manager installation. You can enable and disable the audio/video services from the Sametime System Console. This section describes how to manage the Sametime Media Manager.

About this task

The Sametime Media Manager manages Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between those participants. The Sametime Media Manager supports interactive IP audio and video capabilities and enables clients with the appropriate hardware (sound card, microphone, speakers, and camera) to transmit and receive real-time audio and video in a Sametime meeting room.

Updating Sametime Media Manager connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Media Manager.

Before you begin

If you are configuring the Sametime Media Manager to use SSL (Secure Socket Layer), make sure the server’s certificate has been added to the Sametime System Console’s trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Media Manager. These settings are only used by the Sametime System Console to connect to the Sametime Media Manager.

Follow these steps to update connection setting information.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator’s User name and Password for connecting to the Sametime Media Manager.
5. By default, the Sametime Media Manager trusts other Sametime components. If you want to change this setting, then select Do not auto-accept SSL certificate.
6. Click **Save**.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

**Related tasks**
- “Adding a Sametime server SSL certificate to the Sametime System Console” on page 830
- If you need to enable SSL (SecureSocketLayer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

### Managing UDP ports for voice chat and video calls

Change the default UDP ports for computer-to-computer voice chats and video calls in an IBM Sametime deployment.

**Before you begin**

When the NAT traversal feature is enabled, the Connect client no longer uses the traditional ports (20830+2); instead it uses random ports for ICE negotiation. You should still leave the original ports open so they can be used by older clients that are not supported by the NAT traversal feature.

**About this task**

IBM Sametime comes with voice chat. With voice chat, users can place and receive audio calls using their computer’s and their chat partners’ computer audio capabilities. Once a user has a computer-to-computer voice chat started, the user can convert it to a video call so that the user can both see and hear call participants.

Voice chat works with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to speak to other users orally over the computer. The client machines use a single port (UDP port 20830 is the default) for all audio chats, so this port must be opened for both incoming and outgoing UDP traffic.

Video calls also work with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to see video of users with whom they are chatting over the computer. The client machines use a single port (UDP port 20832 is the default) for all video calls, so this port must be opened for both incoming and outgoing UDP traffic.

**Note:** The client might require ports for the audio and video channels to send RTP and RTCP packets over UDP.

Follow these steps to change the UDP ports:

**Procedure**

1. Log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. The Sametime Media Manager listens for inbound audio streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for audio calls** field.

6. The Sametime Media Manager listens for inbound video streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for video calls** field.

7. Click **OK**.

8. Restart the Sametime Media Manager.

---

**Managing multiple audio and video streams**

The IBM Sametime Media Manager manages multiple audio and video streams in a meeting.

**About this task**

The Sametime Media Manager scans the meeting participants and locates the person currently speaking (transmitting audio packets). The Sametime Media Manager performs switching operations as different people speak during a meeting. When a meeting participant speaks, the Sametime Media Manager locks onto that client's audio stream and distributes that stream to all other clients in the meeting. When a participant stops speaking, the Sametime Media Manager waits for a brief period of time, and then begins scanning for the other active audio clients.

The video follows the audio. When the Sametime Media Manager switches to a new audio source (speaking person), the Sametime Media Manager through its connections to the clients, ensures that the icon indicating the current speaker is properly updated for all clients. After this update, the Sametime Media Manager sets the video source to the person currently speaking. It is important to ensure that the video does not switch too quickly. Rapid video switching reduces usability. You can control the time interval that must pass before the video switches to the new speaking person.

**Note:** If the current speaker does not have video capabilities or has the video window paused, the Sametime Media Manager sends the next loudest speaker's video as the active speaker to all participants.

By default, the Sametime Media Manager can lock onto and broadcast a maximum of five audio streams at the same time. In a meeting, if five people speak at the same time, it is possible for all meeting participants to simultaneously hear five people speaking. The Sametime Media Manager designates the audio stream that has been transmitting the longest (generally, the person who started speaking first) as the primary audio stream. The source of the primary audio stream is also the source of the video stream. Audio and video services provided by the Sametime Media Manager have been tested and optimized for sessions with 20 participants. The actual number of participants will vary based on network and environmental conditions. The higher the number of switched audio streams, then the more bandwidth that is required.

In meetings, especially in large meetings, IBM recommends that participants, who are not talking, mute their speakers to reduce noise.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. Under Presence, type a number between 2 and 16 in the **Number of switched audio streams** field to change the number of simultaneous audio streams.

   **Note:** The more switched audio streams, the more people are heard simultaneously in a meeting. Meetings could become quite noisy, so use caution when you increase this number.
6. Under **Set the time in milliseconds before switching to the next active speaker**, select a number in **Video switching wait time** to control the time interval that must pass before the video switches to the new speaking person.
7. Click **OK**.
8. Restart the Sametime Media Manager.

### Changing the SIP transport protocol in the Sametime Media Manager

You can change the transport protocol that IBM Media Manager uses for the SIP Proxy and Registrar.

#### About this task

SIP makes use of elements called proxy servers to help route requests to the user’s current location, authenticate and authorize users for media services, and provide Sametime Media features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

The transport protocol determines the network transport mechanism to use for sending SIP messages. The SIP proxy application examines all requests sent by the Sametime Media Manager to determine whether a given request is sent by an appropriate proxy application. All requests are routed according to the transport protocol defined here.

In a multiple machine deployment where Sametime Media Manager components are installed on different machines, you must update the SIP transport protocol on all components: Conference Manager, Packet Switcher, and SIP Proxy and Registrar. Moreover, if you change the SIP transport protocol from TLS to TCP, then the port changes are automatically reflected in the stavconfig.xml file on the Conference Manager. You must manually change the ports in the stavconfig.xml files of the Packet Switcher component.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. Under **Server Integration**, select a **Transport protocol** of TLS or TCP. UDP is not supported.
6. Set how frequently in seconds you want SIP to check if a client is still connected. Enter a number between 30 and 300 in the **Session expiration** field.

7. Click **OK**.

8. Update SIP Registrar security role settings by following these steps.
   a. Log in to the SIP Proxy and Registrar.
   b. Click **Applications > Enterprise Applications**.
   c. Click **IBM SIP Registrar setting**.
   d. Under Detail Properties, click **Security role to user/group mapping**.
   e. Change security role settings from **All Authenticated in Application's Realm** to **Everyone** if the protocol is updated to TCP. Do this by selecting the checkbox for the **AllAuthenticatedUsers** role, then select **Map Special Subjects** and select **Everyone**. Leave **All Authenticated in Application's Realm** if the protocol is selected as TLS.

9. Restart the Sametime Media Manager.

**What to do next**

If you have deployed the Conference Manager, Packet Switcher, and SIP Proxy and Registrar on separate application servers, and you have changed the SIP transport protocol from TLS to TCP, the Conference Manager **stavconfig.xml** file automatically reflects this change. You must edit the **stavconfig.xml** files on the Packet Switcher to reflect this update by changing the secure ports to nonsecure ports. Follow the steps in “Configuring ports for Transport Layer encryption on an upgraded Sametime Media Manager” on page 819.

**Managing media encryption and codecs**

You can manage the type of media encryption and codecs used in meetings on the IBM Sametime Media Manager.

**About this task**

A codec compresses streaming data, such as audio or video, on the transmitting side and decompresses it for playback on the receiving side. Codecs reduce the amount of bandwidth required to send streaming data. Generally, higher compression conserves more bandwidth. Higher compression also results in poorer audio or video quality and requires more resources to compress and decompress the data streams.

You can change the type audio and video codecs.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. Follow the procedure appropriate for your deployment:
   - **Single box deployment with all components on one machine**: Under Audio Video Media, keep the default encryption option as **Disable** or click **Enable**. Calls made between the Sametime Connect client and any other endpoint supporting SRTP including another Sametime Connect client or a partner
conference bridge are encrypted. Audio/video conferences with three or more participants using the Media Manager Packet Switcher or the Sametime Unified Telephony Media Server are not encrypted.

- **Non-clustered distributed and clustered deployments:**
  a. Under Audio Video Media change the encryption option to **Enable** or **Disable**. This action only automatically updates the `stavconfig.xml` file of the Conference Manager component.
  b. A manual update is required on Packet Switcher deployments. Update the `stavconfig.xml` encryption field values to **NoEncryption** if you have selected **Disable**, or to **SRTP** if **Enable** is selected, into the Deployment Manager server’s scope `stavconfig.xml` files, and run Full-resynchronize on nodes, then restart the Packet Switcher servers.

  **Note:**

  **NoEncryption** and **SRTP** are the only string literals to update `stavconfig.xml` with.

  The Sametime Community server default refresh interval is one hour. The Sametime Connect client gets the updated server policy attribute after one hour.

6. Prioritize the audio codecs by using the **Up** and **Down** buttons to move the audio codecs in the list.

   Sametime Media Manager supports the following audio codecs:
   - **ISAC** - Internet Speech Audio Codec (iSAC) is a wideband and adaptive bit rate codec. The bit rate ranges from 10 to 32 kbps (Kilobit per second) depending on the available network bandwidth. This is the default codec.
   - **iLBC** - Internet Low Bit-rate Codec (iLBC) is a narrowband low bit rate speech codec. It requires 15.2 kpbs bandwidth.
   - **G.722.1** - Popular wideband audio codec that operates at one of three selectable bit rates: 32000, 24000, 16000. G7221 is a licensed royalty-free standard audio codec providing high quality, moderate bit rate audio coding.
   - **G.711** - Old and widely supported narrowband codec. It requires 64 kbps bandwidth but consumes less CPU to process.

7. Prioritize the video codecs by using the **Up** and **Down** buttons to move the video codecs in the list.

   Sametime Media Manager supports two video codecs:
   - **H264** - Also known as AVC and MPEG-4 part 10. It provides high quality, block-oriented, motion-compensation-based video codec for video conferencing. It supports the Baseline Profile without Flexible Macroblock Ordering (FMO).
   - **H263** - A legacy codec and lower quality than H264.

8. Click **OK**.

9. Restart the Sametime Media Manager.

**Managing video bit-rate**

You can change the video bit-rate that you use in meetings using the IBM Sametime Media Manager.

**About this task**

One of the key factors effecting video quality is the available network bandwidth. The higher the video resolution, the more bandwidth is required and the better
quality. The Sametime video codec can automatically adapt to the available bandwidth and reduces the bit-rate to a certain threshold for each chosen video resolution. However, the quality will suffer when the available bandwidth becomes too low, especially during peak utilization when the contention in the network routers causes packet loss. Use the following information as the guideline to set the desired codec resolution.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. Under Video Bit Rate, select a **Video Resolution**.
   - HD-720p 1280x720@60fps 4096kbps
   - HD 960x720@60fps 4096kbps
   - XGA 1024x768@35fps 6144kbps
   - WIDE FULL HD 1920x1080@30fps 10240kbps
   - FULL HD 1440x1080@30fps 8192kbps
   - HD-720p 1280x720@30fps 2048kbps
   - HD-720p 1280x720@30fps 1472kbps
   - HD-720p 1280x720@30fps 1024kbps
   - HD-720p 1280x720@30fps 768kbps
   - HD 960x720@30fps 2048kbps
   - 432P 720x432@30fps 1024kbps
   - 432P 720x432@30fps 768kbps
   - 432P 720x432@30fps 512kbps
   - VGA 640x480@30fps 1024kbps
   - VGA 640x480@15fps 896kbps
   - VGA 640x480@30fps 512kbps
   - VGA 640x480@30fps 384kbps
   - W288P 512x288@30fps 384kbps
   - CIF 352x288@30fps 768kbps
   - CIF 352x288@30fps 512kbps
   - QCIF 176x144@30fps 384kbps
   - QCIF 176x144@30fps 192kbps
   - SQCIF 128x96@30fps 128kbps
   - SQCIF 128x96@30fps 64kbps
   - 4CIF 704x576@25fps 1536kbps
   - 4CIF 704x576@25fps 512kbps
   - QVGA 320x240@20fps 384kbps
   - VGA 640x480@15fps 896kbps
   - CIF 352x288@15fps 384kbps
   - QCIF 176x144@15fps 128kbps
   - QCIF 176x144@15fps 64kbps
   - 4CIF 704x576@12fps 1024kbps
The video resolution is composed of the following elements:

- **Resolution name** - The video resolution name, for example Common Intermediate Format (CIF).
- **WidthxHeight** - The dimensions of the video in pixels.
- **Framerate** - Frames per second.
- **Bit-rate** - Maximum kilobits per second

6. Click **OK**.
7. Restart both the Sametime Media Manager and the Sametime Community Server.

### Changing the default number of maximum users

As demands on video conferencing change, you can update the maximum number of participants to ensure that your network can support this feature.

#### About this task

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

**Note:** The maximum number of users can set independently internally (on the Sametime Packet Switcher) and externally (on the MCU that bridges video-conferencing connections).

#### Procedure

1. On the server hosting IBM Sametime Media Manager, open the `ConferenceManager.properties` file. In a multiple-machine deployment where Sametime Media Manager components are installed on different machines, go to the server hosting the Conference Manager. You can adjust the maximum participants setting for each Service Provider Implementation (each adapter); each adapter has its own `ConferenceManager.properties` file.

   ```
   websphere_install_path/AppServer/profiles/profile_name/installedApps/cell_name/ConferenceFocus.ear/ConferenceFocus.war/ConferenceManager.properties
   ```

2. Edit the values in the following settings:

   - `MaximumAudioConferenceUsers=20`
   - `MaximumVideoConferenceUsers=20`

   For example, the Radvision TCSPi Adapter `ConferenceManager.properties` file contains this setting by default:

   ```
   # PerConferenceMaximum is the maximum number of users the service provider supports for each conference call.
   # MaximumConferenceUsers=200
   so you will probably want to lower value that to provide better performance within your network.
   ```

3. Restart the Sametime Media Manager.

### Administering a SIP Proxy and Registrar

This section describes how to manage the properties of a SIP proxy and registrar.
About this task

Session Initiation Protocol (SIP) is a protocol that manages communication in IBM Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between meeting participants. SIP makes use of elements called proxy servers to help route information to the user’s current location, authenticate and authorize users for meetings, and provide features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

Adding a Sametime Media Manager’s SSL certificate to the Sametime System Console

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

About this task

To enable SSL, you must extract the certificate from the Sametime product server and add it to the trust store of the Sametime System Console. The Sametime product servers include:

- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Gateway Server
- SIP Proxy and Registrar

Follow these instructions. See the WebSphere Application Server information center for more information on extracting and adding certificates.

Procedure

1. Log in to the Integrated Solutions Console for the Sametime product server.
2. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
3. Select the alias named root, and click Extract.
4. Enter the name of the .cer file, and select Base64 as the type for storing the process server signer certificate.
5. Log in to the Integrated Solutions Console for the Sametime System Console.
6. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
7. Click Add.
8. Enter an alias.
9. Enter the file name where you stored the extracted process server signer certificate from the product server.
10. Click Apply.
11. Restart the Sametime System Console deployment manager.
Updating SIP Proxy and Registrar connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the SIP Proxy and Registrar.

Before you begin

If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the SIP Proxy and Registrar. These settings are only used by the Sametime System Console to connect to the SIP Proxy and Registrar.

If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store using the Integrated Solutions Console (Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates). See the WebSphere Application Server information center for more information on adding certificates.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. In the SIP Proxy and Registrar list, click the Edit next to the deployment name of the SIP Proxy and Registrar with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's User name and Password for connecting to the SIP Proxy and Registrar.
5. By default, the SIP Proxy and Registrar trusts other Lotus Sametime components. If you want to change this, then select Do not auto-accept SSL certificate.
6. Click Save.
7. Click Done to return the SIP Proxy and Registrar list.
8. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Managing SIP proxy properties

You can set properties for the SIP proxy server.

About this task

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users to access media services, and provide Sametime media features to users.
Procedure
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.
3. Click the Deployment Name of the SIP Proxy server.
4. In **SIP Proxy and Registrar**, click **Proxy Administration**.
5. Use the following table to set basic SIP proxy properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Record route mode</strong></td>
<td>When record route mode is enabled, the optional Record-Route header is inserted by the SIP proxy server that wants to remain in the signalling path for the duration of the session. The Record-Route header is used to establish a route for transactions belonging to a session. When record route mode is disabled, SIP messages flow directly through the SIP gateways once a call has been established.</td>
</tr>
<tr>
<td><strong>Parallel search mode</strong></td>
<td>When parallel search mode is enabled, a SIP proxy server sends many requests to possible user locations when it receives an incoming request. Instead of sending one request and then waiting for the final response before sending another request, a parallel search sends requests without waiting for the result of previous requests.</td>
</tr>
<tr>
<td><strong>Add public IP to outgoing request</strong></td>
<td>When this option is enabled, the SIP proxy server adds an IBM-Destination-Public-IP header field to outgoing initial requests. This header contains the public IP of the endpoint.</td>
</tr>
</tbody>
</table>

6. Specify Handled Domains. These are domains that are managed by the SIP Proxy and Registrar.
7. Routing rules define how SIP messages are routed through the Sametime SIP proxy server. The table shows any existing rules, with the highest priority granted to the first rule in the table.
   - Click a rule to open it for editing or click **New** to create a new routing rule.
8. Click **OK**.
9. Restart the SIP Proxy and Registrar.

Creating and editing routing rules for SIP-based messaging
Add or edit routing rules that define how the SIP Proxy server routes SIP-based messages.

About this task
Routing rules tell Sametime where to direct SIP-based messages under certain conditions. The rule consists of one or more conditions, and a destination (SIP endpoint) where call requests that meet the conditions will be routed.

A routing rule uses the same transport protocol as the Sametime Media Manager components. For example, if the Media Manager is configured to use TLS for the SIP signalling, you must use TLS for all routing rules. The supported transport
protocols are TCP and TLS over TCP. UDP is not supported.

Procedure

Use the routing rules table in the Proxy Administration page to view, create, or edit rules.

1. On the Sametime System Console, log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. In the navigation tree, click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.
3. On the SIP page, look in the proxies table and click the **Deployment Identifier** of the SIP Proxy and Registrar.
4. On the SIP Proxy and Registrar page, click **Proxy Administration**.
5. In the routing rules table, do one of the following:
   - Click the name of a rule to edit it.
   - Click **New** to create a new rule.
6. Add or modify settings for the routing rule as follows:
   a. Type a name and description of the route in the **Name** and **Description** fields.
      
      It is helpful to indicate the route's direction and endpoint in the name so you can easily distinguish among routes in the routing rules table later.
   b. Use the "Conditions" section to configure the routing rule by defining at least one condition:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
<td>A predefined value indicating the type of request: INVITE, INFO, MESSAGE, or ANY. Select the appropriate value from the field's list; if you do not select a method, then all methods are accepted by this condition.</td>
</tr>
<tr>
<td><strong>Source Address</strong></td>
<td>The originating caller's IP address, which must match the pattern specified in the regular expression that you provide. You could specify a single IP address: 9,3,186,215 or use an expression to specify a range of IP addresses: 9,3,186,215</td>
</tr>
<tr>
<td><strong>Request URI</strong></td>
<td>The resource, usually the origin server, on which to apply the request. The URI must match the pattern specified in the regular expression that you provide. For example: .,.<em>,example,.,com,.,</em> matches both of these incoming initial requests: sip:,example,.,com:5060;transport=tcp SIP/2.0 and sips:,subdomain,example,com:5061 SIP/2.0</td>
</tr>
</tbody>
</table>
Table 159. Conditions fields and descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Header</td>
<td>The SIP URI of the originating caller. The URI must match the pattern specified in the regular expression that you provide. For example, .<em>20100@192.192.0.2\ .12:506&lt;01&gt;.</em> matches incoming initial requests with either of these contact header values: <a href="">sip:20110@192.0.2.12:5060;transport=tcp</a> or <a href="">sips:user9920100@192.0.2.12:5061;transport=tcp</a></td>
</tr>
</tbody>
</table>

c. In the "Destination" section, select the method to use for storing the address of the destination SIP endpoint:

Table 160. Destination addressing methods and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push a Route header field</td>
<td>Insert the destination address into a Route header field of the outgoing SIP request.</td>
</tr>
<tr>
<td>Replace a Request-URI</td>
<td>Replace the original Request-URI with the destination address when creating the outgoing request.</td>
</tr>
</tbody>
</table>

d. Construct the destination address using the method you selected in substep c.

Push a Route header field

Supply a value in one or more of the fields described in the table.

Table 161. SIP URI addressing fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>The scheme can be either SIP or SIPS (the secure version of SIP); the default is SIP. This field is required.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or fully qualified host name of the destination server (the SIP endpoint). For incoming calls, use the fully qualified domain name of the Sametime Media Manager’s Conference Manager component. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the destination server (the SIP endpoint) is listening on for SIP-based communications. This field is optional; if you do not provide a value, the server uses the correct port. Note: Make sure you specify the correct port for the transport protocol. For unsecured TCP communications, the Conference Manager typically uses port 5063; for encrypted TLS communications, the Conference Manager typically uses port 5062.</td>
</tr>
</tbody>
</table>
Table 161. SIP URI addressing fields and descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>The network transport protocol to use for sending SIP messages: <strong>TCP</strong> or <strong>TLS over TCP</strong> (UDP is not supported). Use the same transport protocol throughout the entire route (from the Sametime client to the SIP Proxy/Registrar to the third-party SIP endpoint). For example, if the Media Manager is configured to use TLS for SIP communications, you must use TLS for all routes. This field is optional; if you do not provide a value, the server supplies a transport protocol.</td>
</tr>
</tbody>
</table>

**Replace a Request-URI**

Construct regular expressions to define the original **Request-URI pattern** and its replacement **Output pattern**, which are explained in the table.

Table 162. URI pattern fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request-URI pattern</td>
<td>A regular expression defining the pattern of the original Request URI. Use this field to extract fields or parameters from a Request-URI of a SIP request. A variable stores the part of the Request-URI matched by the part of the regular expression inside the parentheses, indicated by a number. The variables are recalled with the dollar-sign, for example, $1, $2, and so on. These fields or parameters can be used to build the Output pattern. This field is optional.</td>
</tr>
<tr>
<td>Output pattern</td>
<td>A regular expression defining the pattern of the destination’s URI (address). This field can contain either a SIP URI or a replacement expression with variables for example, $1, $2, and so on. Variables store the portion of a parenthesized pattern captured from the Request-URI pattern field. After processing any captured variables, the resulting field value must be a valid SIP or SIPS URI. <strong>Note:</strong> If you do not provide a value in the Request-URI pattern field, this field must contain a valid SIP or SIPS URI.</td>
</tr>
</tbody>
</table>

**Remember:** Regular expressions must follow a strict notation, different from other notation forms you may use. For example, the operating system shell notation for a wildcard (series of 0 or more characters) is the asterisk character: *, The regular expression equivalent for a wildcard is different: it is a combination of a dot followed by an asterisk, as follows: .* Before adding the regular expression to the routing rule, you should test the expressions using any of the testing engines available online. To learn more about creating regular expressions, see the Java Regular Expressions class on the Oracle web site.

e. Click **OK** to save the rule.
f. Repeat from step 5 until all your routing rules have been defined.
You must create at least one inbound route and one outbound route between
Sametime and each third-party SIP endpoint. You can create different
versions of a route using different sets of conditions (all of a route’s
conditions must be satisfied for that route to be selected), and you can
prioritize routing rules as explained in the next step.

7. Prioritize the routing rules by arranging them in the sequence in which you
want them processed:
It is acceptable to have inbound routes mixed with outbound routes in the
sequence because if a message does not satisfy all of the routing conditions, the
route will be ignored.
a. In the routing rules table, select the a route and click the Move Down
   button or the Move Down button until the route is positioned in the correct
   sequence.
b. Repeat as needed until the rules appear in priority sequence.

8. Save the set of routing rules and priorities by clicking Save link in the
   "Messages" box at the top of the page.

9. Restart the SIP Proxy and Registrar’s server or cluster:
   • For a stand-alone Media Manager or SIP Proxy and Registrar, restart it now
     as follows:
     a. In the server’s Integrated Solutions Console, click Servers > Server Types
        > server_type.
     b. In the list of servers, select your server and click the Restart button at the
        top of the table.
     c. Click the Refresh button and verify that all components are active.
   • For a cluster of SIP Proxy/Registrars, synchronize the nodes before restarting
     them:
     a. In the Deployment Manager’s Integrated Solutions Console, click System
        Administration > Nodes.
     b. Select all nodes in the cluster, and then click the Full Resynchronize
        button at the top of the table.
     c. Back in the navigation tree, click System Administration > Node agents.
     d. Select all nodes in the cluster, and then click the Restart button at the top
        of the table.

**Example**

The following examples show different combinations of values for Request-URI
pattern and Output pattern that produce specific destination addresses.
   • Route all incoming SIP requests to this destination:
     sip:example.com;transport=tcp
     Request-URI pattern: empty
     Output pattern: sip:example.com;transport=tcp
     Because the Request-URI pattern field is empty, the destination is modified on
     all incoming requests.
   • Route incoming SIP requests to a new host, keeping the original user name
     Request-URI pattern: sip:(.*)0.*
     Output pattern: sip:$1@example.com
     The expression in parentheses for Request-URI pattern captures the user name in
     a variable and the output pattern refers to the variable as $1.
For example, assume an incoming initial SIP request with a Request-URI of sip:12345@company.com. The Request-URI pattern runs, resulting in the variable \$1=12345. The SIP URI for the destination address maintains the same user name, but adds a new host name: sip:12345@example.com.

- Route incoming SIP requests to "host," keeping the original user name if the user-name prefix in the Request-URI is "45"
  
  Request-URI pattern: sip:(45.+)@.*
  
  Output pattern: sip:$1@host

- Route incoming SIP requests to "host," omitting the prefix if the user-name prefix in the Request-URI is "45"
  
  Request-URI pattern: sip:45(.+)@.*
  
  Output pattern: sip:$1@host

Managing SIP registrar properties

You can set registration expiration properties for the SIP registrar.

About this task

SIP provides a registrar that allows users to send their current locations for use by proxy servers. The SIP registrar accepts user requests and places the information it receives from those requests into the registration table. Registration is how media services learn the current location of a Sametime user. Upon login, and at periodic intervals, the user sends registration messages to the SIP registrar application. These messages associate the user's SIP URI with the machine into which he is currently logged in. The registrar records this association, also called registration instance or a binding, to the registration table, where it can be used by the SIP proxy.

Follow these steps to set expiration properties for the SIP registrar.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registrar Administration.
5. In the Default Registration Expiration field, type a value in seconds to use as the registration expiration when there is no such parameter set in the user request.
6. In the Minimum Registration Expiration field, type a value in seconds for the minimum expiration interval the SIP Registrar is willing to honor. A request with an expiration interval lower than the minimum expiration will be rejected.
7. In the Maximum contacts for user field, type a value for the maximum number of contacts a user can register, for the same address-of-record.
8. In the Maximum Anonymous users field, type a value for the maximum number of anonymous users that can be registered with the IBM Lotus SIP Registrar.
9. Click OK.
10. Restart the SIP Proxy and Registrar.
Managing SIP registered bindings
Use the SIP Proxy Registration page to monitor SIP registrations.

About this task
The registration of the user occurs during client login and is extended by the client automatically if the client remains logged in. The registration table is a location service used by a SIP to obtain information about a user's possible location. The registration table specifies the SIP addresses associated with device addresses, as well as the expiration times for currently registered users.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registered Bindings. Use this page to find, view, or delete bindings.
5. Use the following table to view binding properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP URI</td>
<td>Identifies a user in IBM Sametime. A SIP URI contains the information to initiate and maintain a communication session with another user. It can have the following formats: sip:user_identifier@host or sips:user_identifier@host.</td>
</tr>
<tr>
<td>Device Address</td>
<td>The location of the machine into which the user is currently logged. The format is sip:host:port;transport=&lt;transport-type&gt;.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>The time when the registration expires, unless it is automatically extended by the Sametime client.</td>
</tr>
</tbody>
</table>

Managing the SIP Proxy and Registrar domains
Use the Handled Domains page to set the domains for which the SIP Proxy and Registrar are responsible.

About this task
If you do not add any domains to the Handled Domains page, then all domains will be managed by the SIP Proxy and Registrar.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Handled Domains.
5. To add a domain which will be handled by the SIP Proxy and Registrar, enter a domain in the Domain field and click Add.
6. Click OK.

**Administering a Sametime Meeting Server**

This section describes how to manage an IBM Sametime Meeting Server.

**About this task**

The Sametime Meeting Server supports real-time collaboration through screen sharing and a shared whiteboard. The Sametime Meeting Server also provides a variety of other types of support for the meeting activity occurring in Sametime.

**Updating Sametime Meeting Server connection properties on the console**

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Meeting Server.

**Before you begin**

If you are configuring the Sametime Meeting Server to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

**About this task**

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Meeting Server. These settings are only used by the Sametime System Console to connect to the Sametime Meeting Server.

Follow these steps to update connection setting information.

**Procedure**

1. Log in the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Server**.
3. In the Sametime Meeting Servers list, click the **Edit** next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's **User name** and **Password** for connecting to the Sametime Meeting Server.
5. By default, the Sametime Meeting Server trusts other Sametime components. If you want to change this setting, then select **Do not auto-accept SSL certificate**.
6. Click **Save**.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.
Related tasks

“Adding a Sametime server SSL certificate to the Sametime System Console” on page 830

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.

Managing file sharing

You can limit the types of files that can be shared in meeting rooms as well as edit file conversion settings for your IBM Sametime Meeting Server configuration.

About this task

You can edit but not delete any of the file conversion settings that come installed with IBM Sametime. You can delete any new settings that you have added.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Click the Server Configuration tab.
5. Click Edit.
6. Edit the appropriate configuration value. You can only edit the value; you cannot edit a configuration key name.

Table 163. Configuration key values

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.include</td>
<td>pdf, sam, bmp, gif, cgm, htm, html, jpg, jpeg, jpe, 123, wk3, wk4, 123, pre, prz, pic, lwp, xls, xlsx, ppt, pptx, doc, docx, sdd, sxi, sxo, sdc, sxc, pcx, pct, png, rft, rtf, ods, odp, odt, tiff, tif, eps, txt, bat, ini, vsd, wmf, wpd, wpg, wpg2, xml</td>
<td>List of file type extensions that can be converted by the Sametime Meeting Server for document sharing. Separate extensions by a comma.</td>
</tr>
<tr>
<td>docshare.fileio.codebase</td>
<td>c:\temp\docshare</td>
<td>Location of the temporary directory for document sharing used by the Sametime Meeting Server.</td>
</tr>
</tbody>
</table>

Examples:
- c:\temp\docshare
- /opt/temp
Table 163. Configuration key values (continued)

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.native.codebase</td>
<td><code>c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe</code></td>
<td>Location of the executable file for the Sametime Meeting Server document conversion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Examples: <code>c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe</code> or <code>/opt/IBM/WebSphere/STMeetingServer/stellent/exporter</code></td>
</tr>
<tr>
<td>docshare.remote.url</td>
<td>Blank.</td>
<td>URL to a remote Sametime Meeting Server for document conversion. Leave blank for local conversion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>http://hostname.domain.com/DocumentShare/docshare</code></td>
</tr>
</tbody>
</table>

7. Click OK.

Results
Configuration changes immediately take effect.

Requiring meeting passwords
You can require that all meeting rooms in IBM Sametime have passwords.

About this task
Meeting rooms are not required to have passwords by default. You can change this configuration setting so that meeting rooms are required to have passwords.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Click the Server Configuration tab.
5. Click Edit.
6. Scroll down to the meetingroomcenter.passwords configuration key. You can only edit the value; you cannot edit a configuration key name.
7. Change the Configuration Value to one of the following values:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No password required. This is the default value.</td>
</tr>
<tr>
<td>1</td>
<td>Password required. The password must contain at least five characters.</td>
</tr>
<tr>
<td>2</td>
<td>Strong password required. A strong password must contain eight or more characters, mixed upper and lower case letters, at least one number, and at least one special character (for example: comma, exclamation point, or asterisk).</td>
</tr>
</tbody>
</table>

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

- \  
- %  
- &  
- <  

8. Click OK.

**Results**

This configuration change immediately takes effect.

**Limiting guest access to the Meeting Room Center**

You can prevent unauthenticated users (guests) from accessing the Meeting Room Center.

**About this task**

Unauthenticated users have limited access to the Meeting Room Center. They can view information in the Meeting Room Center, but they can never create meeting rooms or edit meeting room information. You can change this default value to completely deny them access to the Meeting Room Center. This change does not prevent guest access to an actual meeting; it only prevents access to the Meeting Room Center.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Scroll down to the **meetingroomcenter.allowGuestAccess** configuration key. You can only edit the value; you cannot edit a configuration key name.
7. In the **Configuration Value** field, type 0 to deny unauthenticated user access to the Meeting Room Center.

   **Note:** If you change your mind, or if you ever want to grant unauthenticated user access, type 1.

8. Click OK.
Results

This configuration change immediately takes effect.

Defining a Sametime Proxy server for awareness in meeting rooms

You must define the IBM Sametime Proxy server that is used for awareness so that Sametime users can be detected when they are in Sametime meeting rooms.

Before you begin

You must have a Sametime Proxy server installed and configured. You must set up SSO between the Sametime Meeting Server and the Sametime Community Server.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Click the Server Configuration tab.
5. Click Edit.
6. Scroll down to the meetingroomcenter.stProxyAddress configuration key. You can only edit the value; you cannot edit a configuration key name.
7. Enter the URL for the Sametime Proxy server used for awareness in the Configuration Value field. For example: http://myhostname.mydomain.com:9080
8. Click OK.
9. Restart the Sametime Meeting Server.

Related tasks

Setting up SSO between the Sametime Meeting Server and the Sametime Community Server

Configure servers for single sign-on (SSO) as a convenience to users running the Sametime browser client. With SSO configured, users who log in once to any server in the DNS domain do not have to log in again when they access any other server running on Domino or WebSphere Application Server. Enabling SSO between the servers also helps the Connect Client as well. If the community server is in the single sign-on domain, the component services can re-use the token from the Connect client to login to other services.

Customizing the Sametime Meeting Server configuration

You can customize your IBM Sametime Meeting Server by changing configuration keys. You can also add your own configuration keys.

About this task

The custom configuration keys that you create yourself display after the configuration keys that come pre-configured with the Sametime Meeting Server. Custom configuration keys that you create yourself can be edited and these are the only configuration keys that can be deleted. Do not delete any of the pre-configured custom configuration keys unless directed to do so by IBM.
Table 164. Pre-configured custom configuration keys

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.timeout.minutes</td>
<td>5</td>
<td>Upload duration (in minutes). Upload a file to the meeting room. If the file cannot be converted in X minutes, then the file cannot be converted any more.</td>
</tr>
<tr>
<td>docshare.jpeg.quality</td>
<td>90</td>
<td>Quality of shared document. The lower the value, the lower the quality.</td>
</tr>
<tr>
<td>meetingroomcenter.maxRoomsPerPage</td>
<td>100</td>
<td>Number of rooms listed on a page in the Meeting Room Center. The configuration key is ignored if the value is less than 100.</td>
</tr>
<tr>
<td>meetingroomcenter.openRoomInNewWindow</td>
<td></td>
<td>Determines if meetings opened from the web browser room manager open in a new window or in the current window.</td>
</tr>
<tr>
<td>meetingroomcenter.stProxySSLAddress</td>
<td></td>
<td>Detects which protocol (SSL or non-SSL) was used to access the meeting server and picks the correct Sametime proxy address to use.</td>
</tr>
<tr>
<td>rtc4web.ejectionTimeout</td>
<td>300</td>
<td>Length of time in seconds that users are locked out of a room when they have been ejected.</td>
</tr>
<tr>
<td>meeting.managedAccess.override</td>
<td>do not enforce</td>
<td>Determines whether rooms on the Sametime Meeting Server use managed access, or whether it is optional.</td>
</tr>
<tr>
<td>meetingroom.allowGuestAccess</td>
<td>(allow guest access)</td>
<td>Determines whether guests can access meeting rooms.</td>
</tr>
</tbody>
</table>

**Procedure**
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Click the Server Configuration tab.
5. Click Edit.
6. Enter the name of your Configuration Key.
7. Enter the Configuration Value.
8. Click OK.
Turning on full-text indexing in the Meeting Room Center

By default, the Meeting Room Center searches the Meeting Room Center database for rooms without using an index. If the database becomes too big, your deployment might experience performance degradation during searches. You can enable full-text indexing on the room name and owner name fields for enhanced performance on large datasets.

About this task

Full-text indexing takes advantage of the IBM DB2 Text Search service to build, maintain, and search by an enhanced set of indexes on the meeting room name and owner name. This augments search performance.

Full-text indexing is only used when you explicitly search for listed meeting rooms from the meeting room search box. It is not used when you search for hidden rooms, access My Meeting Rooms or access a Selected Contact's Meeting Rooms. Full-text indexes are created for both the room name and owner name.

Full-text indexes are updated every 12 hours. Rooms created in the past 24 hours cannot be found by their full-text index, but can be found by a limited table scan. This action avoids missing a room because the index has not been created, yet. Once a room has been live for more than 24 hours, full-text indexing is available.

Follow these steps to enable full-text indexing:

Procedure

1. Copy enableFullTextIndexing.bat (Windows) or enableFullTextIndexing.sh (Linux, Unix) from the root directory of the Sametime Meeting Server install image to the DB2 bin directory.
   If you have an extremely large database, this script can be edited to customize the location of the index files.

2. Run the command to start the DB2 Text Search service, which sets up the full-text indexes and enables the database for full-text searches.
   - Windows
     enableFullTextIndexing.bat STMS dbadmin password
   - AIX, Linux, or Solaris
     enableFullTextIndexing.sh STMS dbadmin password
   Replace STMS with the name of the Meeting Server database if you chose a different database name when you created it.
   Replace dbadmin and password with the DB2 Application user ID and password you created when you installed DB2.

3. Follow these instructions to turn on full-text indexing for the Meeting Room Center in the Sametime System Console.
   a. Log in to the Integrated Solutions Console.
   b. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
   c. In the Meeting Servers list, click a server with the configuration that you want to change.
   d. Select Server Configuration.
   e. Click Edit.
f. Change the value of meetingroomcenter.useFullTextIndexing to true. This setting is a custom key. If a search has been previously performed on the server, then the key and the value display in the interface.
g. Click OK. The changes take effect within one minute.

What to do next

If you restart the server, the service does not restart automatically.

On Windows, you can go into Services and change the DB2TS service to start automatically. From the Start menu, click Run, and type services.msc, and change the DB2TS services to start automatically.

On Linux, you can edit one of the startup scripts to start db2ts when you restart. The command to start db2ts is db2ts start for text.

For more information on DB2 maintenance, see Best Practices for DB2 maintenance in Sametime.

Turning off full-text indexing in the Meeting Room Center

Follow these steps to disable full-text indexing in the Meeting Room Center.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Select Server Configuration.
5. Click Edit.
6. Change the value of meetingroomcenter.useFullTextIndexing to false.
7. Click OK. The changes take effect within one minute.

What to do next

These steps are sufficient to turn off full-text indexing; however, the full-text indexes still exist and take up disk space. If you want to permanently delete the full-text indexes, copy dropFullTextIndexing.bat/sh to the DB2 bin directory and run dropFullTextIndex.bat/sh database_name. For example, dropFullTextIndexing.bat STMS. If you remove the database, the dropFullTextIndexing script should be run first to properly clean up the indexes.

Configuring remotely connected Sametime Meeting Servers

You can configure two different IBM Sametime Meetings deployments to be aware of each other.

Before you begin

Determine the routing prefix. The routing prefix is the alias which will be used to route requests to the remote server. This value can be any string value and should make logical sense to the user since it will appear in the meeting URL. For example, if you are setting up routing between the US and Europe, you may want to choose /eu for the routing prefix for Europe and /us for the United states. This
value will be entered into a URI Group and will be used as the key to routing http requests to the remote server.

**About this task**

Configuring remotely connected Sametime Meeting Servers uses routing features built into the WebSphere proxy server to route http requests to other http servers. Connecting remote servers requires setting up generic server clusters and the appropriate URI Groups and routes which define the remote server.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Servers > Generic Server Clusters**, and then click **New**.
3. Enter a logical name for the Server cluster, for example Europe.
4. Select **http** or **https** as the protocol.
5. Click **Save**.
6. Open the Generic Cluster entry you just saved and click **Ports**.
7. Add the hostname and port number for the remote server.
8. Create a URI Group for your routing Prefix.
   a. In the navigator on the left side of the Integrated Solutions Console, click **Environment > URI Groups**, and then click **New**.
   b. Enter a logical name for the URI group, for example European route.
   c. Click **Save**.
9. Add the generic server cluster and URI group to the proxy server.
   a. In the navigator on the left side of the Integrated Solutions Console, click **Server > Proxy servers**
   b. Click the proxy server process you would like to add remote routing for.
   c. Click **Http Proxy Server Settings**.
   d. Click **Routing Rules**.
   e. Click **New** and enter a name, for example, Europe.
   f. Select **proxy_host** as **Name of the Virtual Host**.
   g. Select the **URI Group** to specify the URI to route /eu/*.
   h. Select the **Generic Server Cluster** to send the messages to, for example, eu.company.com.
   i. Click **Save**.
10. Add a special custom property that identifies this as a remote Sametime server connection
    a. Open the Saved Routing Rule.
    b. Click **Custom Properties** and click **New**.
    c. In the name field add SametimeRemoteCluster, and specify **true** in the Value column.
    d. Click **Save**, and then click **Save** again.
11. Save the master configuration.
12. Restart the proxy server process to begin routing to the remote cluster.

**Monitoring meeting room statistics**

You can view usage statistics for IBM Sametime meeting rooms in the Meeting Room Center.
About this task

Only administrators can view statistics for meeting rooms. Other Sametime users cannot view meeting room statistics. Deleted meeting rooms are not included in these statistics.

Procedure

1. Log in to the Sametime Meeting Room Center.  
   http://hostname/stmeetings/
2. Click Meeting Room Statistics.
3. Click one of the following views:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the total number of rooms and active participants, and the total size of all libraries. An active participant is a participant that is currently in a room.</td>
</tr>
<tr>
<td>Active rooms</td>
<td>Lists all the rooms by meeting room name that currently have participants.</td>
</tr>
<tr>
<td>Usage by room</td>
<td>Lists all active and inactive rooms by meeting room name.</td>
</tr>
<tr>
<td>Usage by owner</td>
<td>Lists all room owners by Sametime ID. Rooms can be active or inactive.</td>
</tr>
</tbody>
</table>

You can click on a column heading in any view to sort the information.

In the Active room or Usage by room views, you can click an owner or room name to get detailed usage statistics on that particular owner or room. In the Usage by owner view, you can click an owner name to get detailed usage statistics.

Backing up user data for Sametime meeting rooms

All IBM Sametime meeting room user data is stored in an IBM DB2 database, and can be backed up using the DB2 backup commands.

About this task

The default Sametime configuration requires that DB2 be shut down for backup. This is because by default, DB2 is configured to reuse the recovery logs. If you want online backup, the database can be configured to archive the recovery logs. In that case, the database is backed up, and all archived recovery logs are backed up. The recovery logs that have been backed up must also be periodically removed. If the database runs out of space to archive the recovery logs, the database will stop accepting changes until space is available.

Database backup and recovery is fully outlined in the DB2 information center. See "Backup overview."

Example for online backup

db2 update database configuration for STMS using logretain on
db2stop
db2start

Perform an offline backup to be kept:
db2 backup database STMS
Afterwards, you can perform online backups:

db2 backup database STMS online include logs

## Backing up WebSphere Application Server configurations

As part of a routine maintenance schedule or before upgrading Sametime servers that run on WebSphere Application Server, back up the WebSphere Application Server configurations.

### About this task

Run the backupConfig command for each of the configurations that are relevant to Sametime. Note the exact name and location of the backed-up configurations so that you can find them if you need to roll back to an earlier configuration.

1. Back up the Deployment Manager configuration.
2. Back up the application server configuration.
3. Back up the federated node configurations.

For more information, see backupConfig command in the WebSphere Application Server information center.
Chapter 15. Tuning

IBM Sametime administrators can make adjustments to the servers they maintain to provide optimal performance for users as they use instant messaging and web conferencing.

This section contains information about tools provided by WebSphere Application Server and Sametime that help you fine-tune server response time.

Increasing the number of open files on a Sametime server running on Linux

If your IBM Sametime server is hosted on Linux, increase the number of concurrent open files on the server to prevent performance problems.

About this task

Java opens many files and Sametime uses a lot of file descriptors. When a high number of concurrent users (for example, 1,000 or more) connect to the Sametime Community Server, the server may run out of file descriptors.

Prevent this situation by increasing the upper limit on the number of file descriptors in the Linux configuration file.

Procedure

1. Use a text editor and open /etc/security/limits.conf.
2. Add the following lines to the file:
   
   * soft nofile 65535
   * hard nofile 65535

3. Save the file.
4. Restart the Linux server for the operating system change to take effect for all processes.

Tuning a Sametime Community Server

Complete the following tuning procedures to enhance performance.

About this task

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

In addition to the topics in this section, see Optimizing Sametime's Name Lookup solution on the Sametime wiki.

Tuning Sametime LDAP settings

Complete the following procedures to enhance performance
Managing Sametime LDAP internal queues

You can manage advanced configuration settings for the maximum and minimum (MAX/LOW) number of LDAP requests that are pending per connection in the pending queue.

The following settings can be specified in the [Directory] section of the sametime.ini file.

- **ST_DB_LDAP_PENDING_MAX**
  Defines the maximum number of LDAP requests that can be pending per connection in the pending queue. Each connection is for a different type of request; whether search or bind. A Pending Resolve Request is a request that has been sent to the LDAP Server. The request is considered pending until the IBM Sametime Community Server receives a response from the LDAP server for that request. The Sametime Community Server sends, at most, MAX PENDING Requests to the LDAP server. After MAX Pending Requests are sent to the LDAP server on a particular connection, the Sametime Community Server does not send any additional LDAP requests on this connection until the Pending Queue Size drops to the ST_DB_LDAP_PENDING_LOW Pending Request queue size.

  For versions prior to Sametime 8.5, the value is set to 10 by default. In Sametime 8.5 and higher, the value is set to 60 by default. Any Sametime service that connects to the LDAP server utilizes the LOW and MAX PENDING queue.

- **ST_DB_LDAP_PENDING_LOW**
  Strongly linked to the ST_DB_LDAP_PENDING_MAX setting and to the request queueing feature of Sametime. Once ST_DB_LDAP_PENDING_MAX is reached for a certain connection, new LDAP requests are not sent on this connection until the number of pending operations drops to the value set by the ST_DB_LDAP_PENDING_LOW setting.

  For versions prior to Sametime 8.5, the value is set to 5 by default. In Sametime 8.5 and higher, the value is set to 30 by default.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sametime 8.5</th>
<th>Sametime pre-8.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST_DB_LDAP_PENDING_MAX</td>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>ST_DB_LDAP_PENDING_LOW</td>
<td>30</td>
<td>5</td>
</tr>
</tbody>
</table>

Special considerations for the PENDING MAX/LOW settings

As the PENDING MAX/LOW settings (ST_DB_LDAP_PENDING_MAX and ST_DB_LDAP_PENDING_LOW) relate to each LDAP connection, Sametime Community Server might be configured to work with multiple connections per Sametime module, and one connection may stop handling requests while other connections are working well.

The MAX and LOW pending queue sizes are highly dependent upon many factors, such as the resources available to the Sametime Community Server process on the host machine, the resources available to the LDAP process on the LDAP server, the network latency between the Sametime Community Server and LDAP servers, the types of generated searches, and so on. As a result, there is no golden number to guarantee the greatest efficiency for all configurations. By default, MAX and LOW are set to 10 and 5, respectively. However, advanced guidelines for optimizing LDAP configurations generally recommend 60 and 30. IBM typically recommends a size of 120 and 100 for larger corporations with high-powered LDAP servers.
Example of a Pending Low/Max Queue in Sametime.ini:

ST_DB_LDAP_PENDING_LOW = 5
ST_DB_LDAP_PENDING_MAX = 10

As the Sametime Community Server receives LDAP queries (for example, Sametime Resolve or Authentication requests requiring LDAP look ups), Sametime tries to fulfill those queries by sending corresponding LDAP queries to the LDAP Server. These LDAP queries remain in the “Pending” queue until they are resolved or responded back from the LDAP Server or timed out.

If the PENDING MAX value is 10, the Sametime Community Server does not send more than ten requests to the LDAP Server initially until at least 5 requests are resolved by the LDAP Server so that the low end threshold value specified by PENDING_LOW is reached. Once the number of requests waiting for responses reaches the PENDING_LOW value, the Sametime Community Server once again starts sending more requests to the LDAP Server but repeats the cycle and limits the number of requests in flight to the LDAP Server.

Note: If the MAX and LOW sizes for the Pending Queue are not set appropriately, it is possible to overwhelm the LDAP server or artificially reduce the potential high throughput of LDAP requests sent by the Sametime Community Server to the LDAP server.

**Tuning the Sametime LDAP bind operation**

There are different types of bind operations supported by the LDAP protocol. The most common are anonymous and simple bind, also known as authenticated bind.

**About this task**

An anonymous bind is the easiest way to establish a connection with the LDAP server. However, the anonymous client will have limited access to the directory when compared to authenticated clients. Using a simple bind, a client can be authenticated on the LDAP server by providing its DN and password in plain text. The server verifies that such a person exists in the directory and that the supplied password is correct.

The LDAP protocol is asynchronous, so a client can send multiple requests to the LDAP server on the same connection, and does not need to wait for the response of one request before sending the next one. Each request is identified by a request ID, and every response is associated with the original request ID. However, some LDAP servers limit the maximum number of requests that can be pending per single connection.

The following settings are under the [Directory] section of the sametime.ini file:

- ST_DB_LDAP_PENDING_BIND_MAX=X
- ST_DB_LDAP_PENDING_BIND_LOW=Y

These settings only affect the bind requests allowing other requests (mainly search requests) to be sent to LDAP in different rates.

To force the IBM Sametime Server to send BIND requests synchronously use the following settings:

- ST_DB_LDAP_PENDING_BIND_MAX=1
- ST_DB_LDAP_PENDING_BIND_LOW=0
This settings make sure that no other requests will be sent to LDAP on the same connection before getting the response to the bind request. For more information see the TechNote Adding the ability to send bind requests to LDAP synchronously.

**Tuning multiple connections in Sametime LDAP**

You can edit advanced configuration settings to increase the number of connections per Sametime module.

**About this task**

The **ST_DB_LDAP_CONNECTIONS_NUMBER** setting increases the number of concurrent connections from the IBM Sametime Community Server to the LDAP server(s) specified in the StConfig.nsf per Sametime module. The default setting is set to one connection per module except for StAuthentication.dll, which has two connections.

Before increasing the value to greater than one consider the following points:

- Assume that **ST_DB_LDAP_CONNECTIONS_NUMBER=3**. Note that a value of 3 means that the Sametime Community Server creates $3^N$ connections to the LDAP server, where $N$ stands for the number of Sametime components that have an open connection to LDAP. In addition, meeting and Domino components are connected to LDAP so the overall number of connections is greater than $3^N$.
- This setting should only be modified if requests are taking an exceptionally long time to process due to long processing queues and there are plenty of resources available on the Sametime Community Server and the LDAP server. Increasing the value of this setting increases the number of LDAP threads available to service the request and multiplies the resource requirements for each one of the Sametime LDAP modules.

**Tuning the Sametime LDAP Keep Alive Interval setting**

You can manage advanced configuration settings to make sure that there is consistent traffic over the LDAP connection.

Specify the **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting in the **[Directory]** section of the sametime.ini file.

The **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting defines the duration (in minutes) to wait while keeping alive messages that are sent by the IBM Sametime Community Server on idle LDAP connections. Its default value is set to 1 minute. **ST_DB_LDAP_KEEPALIVE_INTERVAL** is an LDAP-based dummy search message whose purpose is to avoid the LDAP server or any network device along the way between the Sametime Community Server and the LDAP server from closing idle connections. This setting is needed in certain LDAP environments where the LDAP server abruptly closes or resets the LDAP connection between Sametime Community Server and LDAP due to no traffic activities on this connection per interval of time set by the LDAP server. To avoid this situation, make sure that there is consistent traffic over the connection by turning on the **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting.

**Tuning the Sametime LDAP Respray Interval setting**

You can manage advanced configuration settings to set how often the connection to the LDAP server should be dropped and re-established.

The **ST_DB_LDAP_RESPRAY_INTERVAL** setting in the **[Directory]** section of the sametime.ini file defines the frequency, in minutes, that the connection to the LDAP server should be dropped and then re-established. In pre-8.5 versions of
Sametime 8.5, the RESPRAY interval must be higher than the KEEPALIVE interval. By default, the ST_DB_LDAP_RESPRAY_INTERVAL setting is disabled.

Note: In pre-8.5 versions of Sametime, the RESPRAY interval must be higher than the KEEPALIVE interval. Bear in mind that the RESPRAY operation is an expensive resource task, and might impact performance in an environment where the RESPRAY intervals are set to low values.

**Tuning the Sametime LDAP Maximum Number of Results per Search Query setting**
You can manage advanced configuration settings to define the LDAP maximum number of results per search query.

Specify the ST_DB_LDAP_MAX_RESULTS setting in the [Directory] section of the sametime.ini file to define the maximum number of entries that can be returned in a single search when searching for people or groups. The default value is 1000.

**Tuning the Sametime LDAP Minimum Number of Characters to Match setting**
You can manage advanced configuration settings to define the minimum number of characters in the search string required to perform a search.

The ST_DB_LDAP_MIN_WILDCARD setting in the [Directory] section of the sametime.ini file defines the minimum number of characters to match when searching the LDAP user using wild card characters. When trying to resolve a user or group with a name that is too short than that defined by the ST_DB_LDAP_MIN_WILDCARD setting, the IBM Sametime Community Server does not search the LDAP server.

For more information on sametime.ini file settings related to the LDAP directory and other techniques for tweaking the Sametime server behavior, refer to these two articles on the IBM Sametime wiki:
- Optimizing Sametime's Name Lookup solution
- Best Practices for using LDAP with Sametime

These articles provide information about fine-tuning a directory to achieve optimal performance and streamlined connections for Sametime.

**Advanced settings to control contact list size**
You can manage advanced configuration settings for controlling contact list size.

The MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT setting in the [Config] section of the sametime.ini file limits the number of users that the client can subscribe to, or see awareness on. A public group is counted as one subscription. This limit is published as a server attribute, and the client is responsible for enforcing it. In order to enforce this limit on the server, set the IGNORE_SUBSCRIBES_ABOVE_MAX value in the [Config] section of the sametime.ini file.

The ST_GROUPS_MAX_MEMBERS setting in the [Directory] section of the sametime.ini file limits the maximum number of users that the IBM Sametime Community Server will allow in a public group. A public group that is too big will appear empty. Once a group is marked too big, it will remain this way until the server is restarted, even if its contents have changed in the directory to less than
the maximum. Set the value to be a number from 1 - 1000. 1,000 members is the maximum recommended group size. You should not set a value of 0 (zero), which indicates the feature is off.

Policies and MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT

The Limit contact list size and Contacts policy settings control the size of the contact list and do not restrain subscriptions. For example, you can set this to 5 and open chat history which has 200 contacts, and the client subscribes to 205 users. If you set this to 5 and the user has 100 contacts on the list already, it does not remove anyone, but it prompts the user to do so. The MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT limits the client so it does not subscribe to users beyond this limit.

Sametime.ini file

```
[Config]
MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT=750
IGNORE_SUBSCRIBES_ABOVE_MAX=751

[Directory]
ST_GROUPS_MAX_MEMBERS=900
```

Sametime Unified Telephony considerations

For Sametime Unified Telephony environments the following settings must be applied:

<table>
<thead>
<tr>
<th>Sametime server version</th>
<th>IGNORE_SUBSCRIBES_ABOVE_MAX default Value</th>
<th>IGNORE_SUBSCRIBES_ABOVE_MAX required settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.x</td>
<td>-1 (disabled)</td>
<td>Must be -1. The setting can be omitted from sametime.ini, or explicitly set to -1.</td>
</tr>
<tr>
<td>8.5.x</td>
<td>-1 (disabled)</td>
<td>Must be -1. The setting can be omitted from sametime.ini, or explicitly set to -1.</td>
</tr>
</tbody>
</table>

Setting a Sametime Polling "Keep Alive" interval for client requests

You can have the Sametime Polling service keep a client request alive for a certain number of second in cases where a temporary connection loss prevents an immediate response. The setting applies to clients who connect through HTTP and use the Sametime Polling service.

About this task

The VP_MAX_PENDING_TIME setting in the [Polling] of the sametime.ini file defines the interval (in seconds) to keep messages pending that are sent by the client. Its default value is set to 0 seconds, which keeps a request pending indefinitely. When the VP_MAX_PENDING_TIME is set to a value larger than 0, the Sametime Polling service sends a response to the client after the specified number of seconds.
Tuning Sametime Media Manager

Complete the following tuning procedures to enhance performance.

Before you begin

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

Limiting participants in a video conference

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

About this task

Network factors affecting audio and video services include bandwidth and latency. The more bandwidth available to the server and the shorter latency will allow more participants per call. The bandwidth to the server is recommended at least 1Gbps (Gigabit per second), and latency from client to server should be less than 150ms.

Environmental conditions affecting audio and video services include server capacity, total number of simultaneous users, selected audio codec and video resolution, expected number of interactive participants, expected number of video participants, and expected number of simultaneous calls. These conditions will effect the limit of the number of participants per call.

Edit the ConferenceManager.properties for every Conference Manager and change the MaximumVideoConferenceUsers value to a number participants appropriate for your network and the environmental conditions at your site.

Procedure

1. On the server hosting the Sametime Media Manager Conference Manager component, navigate to the following directory:

   \WAS_INSTALL_ROOT\profiles\STMSAppProfile\installedApps\cell_name\ConfereceFocus.ear\ConferenceFocus.war

2. Open the ConferenceManager.properties file for editing.

3. Locate the section shown here:

   #
   # MaximumAudioConferenceUsers is the maximum number of users the service provider supports for each audio conference call.
   #
   # MaximumAudioConferenceUsers=20

   #
   # MaximumVideoConferenceUsers is the maximum number of users the service provider supports for each video conference call.
   #
   # MaximumVideoConferenceUsers=20

5. Save and close the file.
6. Restart the server so the change can take effect.
7. Repeat this process on every Conference Manager component. if you have a clustered deployment, apply to every cluster member.

Modifying the dynamic port range to improve Packet Switcher performance

Make sure that the port range is available for the IBM Sametime Media Manager Packet Switcher

About this task

The default range of audio and video ports on the Packet Switcher might fall in the range of dynamic port for the system. If the port is already allocated by a system process when the Packet Switcher tries to allocate it for a conference, the packet switcher marks this as a bad port and will not use this port again, until after restart. If too many ports in the range get marked as bad ports, this could lead to performance degradation. You can change the default port range by using the Sametime System Console (Sametime System Console > Sametime Servers > Sametime Media Manager > deployment_name) or in the stavconfig.xml.

Procedure

To determine UDP dynamic port range, type the following command from the command line:
Windows 2008:
neth int ipv4 show dynamicport udp

For Windows 2003, use 1025 as your start port and use 3975 as your end port for both TCP and UDP.
Linux:
cat /proc/sys/net/ipv4/ip_local_port_range

Setting log files size and rotation for the Sametime Media Manager

You can specify the maximum size and number of log files to be stored on the IBM Sametime Media Manager.

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the Sametime Media Manager retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Media Manager where the logs will be stored. If you installed Sametime Media Manager components on separate machines or as separate cell profiles, you must adjust the log file information on all Conference Manager and Packet Switcher servers.
**Procedure**

1. In the Integrated Solutions Console for the Sametime Media Manager component, click **Servers > Server Types > WebSphere application servers > STMediaServer**.
3. Under "Additional Properties," click **Logging and Tracing > JVM Logs**.
4. Under "General Properties," update the following fields both for **System.out** and **System.err** sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
6. Return to Additional Properties.
7. Under "Additional Properties," click **Logging and Tracing > Diagnostic Trace**.
8. Click **File** and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click **OK**.
10. Click **Save** to save these changes to the master configuration.
11. If the Sametime Media Manager is clustered, repeat these steps for each node within the cluster.

### Setting log files size and rotation for the SIP Proxy and Registrar

You can specify the maximum size and number of log files to be stored on the server.

**Before you begin**

Before performing this procedure, make sure you have the required disk space. IBM recommends that the SIP Proxy and Registrar retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20MB.

**About this task**

Complete these steps using the Integrated Solutions Console on the SIP Proxy and Registrar where the logs will be stored.
Procedure

1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere application servers > STMediaServer.**
2. Under "Server Infrastructure," click **Java and Process management > Process Definition.**
3. Under "Additional Properties," click **Logging and Tracing > JVM Logs.**
4. Under "General Properties," update the following fields both for **System.out** and **System.err** sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click **OK.**
6. Return to Additional Properties.
7. Under "Additional Properties," click **Logging and Tracing > Diagnostic Trace.**
8. Click **File** and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click **OK.**
10. Click **Save** to save these changes to the master configuration.

Tuning a WebSphere proxy server

This section contains procedures for tuning a WebSphere proxy server that is used by a cluster of IBM Sametime servers running on WebSphere Application Server.

About this task

Note that this section is not referring to the SIP Proxy, but rather to a WebSphere proxy server.

Disabling the proxy read-ahead mechanism on the WebSphere proxy server

You can disable the read-ahead mechanism on the IBM WebSphere proxy server to resolves a HIGH CPU issue that occurs when terminating connections with read-ahead enabled.

Procedure

1. Log in to the Integrated Services Console.
2. Click **Servers > Server Types > WebSphere proxy servers.**
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.

4. Under **Proxy Settings**, expand **HTTP Proxy Server Settings**.

5. Click **Proxy settings**.

6. Under **Additional Properties**, click **Custom properties**.

7. Click **New** to create a custom property.

8. Specify the **Name** of the new property as `http.connectionPoolReadAheadEnabled`.

9. Set the **Value** of the new property to `false`.

10. Click **New** to create another custom property.

11. Specify the **Name** of the new property as `dynacache.extension.lookup_timeout_property`.

12. Set the **Value** of the new property to `20000`.

13. Click **Apply**, and then click **Save**.

### Adjusting the WebSphere proxy server thread pool settings

Increase the WebContainer thread pool settings of the IBM WebSphere proxy server to match the same settings as the IBM Sametime Meeting Server.

**About this task**

A thread pool lets servers reuse threads instead of creating new threads at run time.

**Procedure**

1. Log in to the Integrated Services Console.

2. Click **Servers > Server Types > WebSphere proxy servers**.

3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.

4. Under **Additional Properties**, click **Thread pools**.

5. Click **Proxy**.

6. Under **General Properties**, make sure the **Minimum Size** and **Maximum Size** are both set to 50 threads.

7. Click **Apply**, and then click **Save**.

### Setting JVM verbose garbage collection and heap sizes on the Websphere proxy server

In order to monitor IBM WebSphere Application Server JVM heap for specific applications, enable the JVM verbose garbage collection logging for the WebSphere Application Servers.

**Procedure**

1. Log in to the Integrated Solutions Console.

2. Click **Servers > Server Types > WebSphere proxy servers**.

3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.


5. Click **Process definition**.

6. Under **Additional properties**, click **Java Virtual Machine**.
7. Under General Properties, make sure the Verbose garbage collection check box is cleared.
8. Under General Properties, make sure the Initial heap size is set to 512MB.
9. Under General Properties, make sure the Maximum heap size is set to 1024MB.
10. Click Apply, and then click Save.

Extending the HTTP persistent timeout on the WebSphere proxy server
You can extend the HTTP persistent timeout on the IBM WebSphere proxy server to stay connected longer.

Before you begin

About this task
The default rtc4web timeout value is 30 seconds. This is the default timeout for the WebSphere proxy server persistent timeout setting, too. This can causes a rare condition to occur where both sides of the connection can let go at the same time. In order to minimize this conflict, extend the WebSphere proxy server HTTP Persistent timeout to stay connected longer.

Procedure
1. Log into Integrated Solutions Console on the server where the WebSphere proxy server is configured.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
4. Under Proxy Settings, expand the HTTP Proxy Server Settings tree.
5. Click Proxy server transports.
6. Click HTTP_PROXY_CHAIN. It should be associated with port 80.
7. Click HTTP inbound channel (HTTP 3).
8. Under General Properties, set the Persistent timeout to 60 seconds.
9. Click Apply, and then click Save.
10. Click Servers > Server Types > WebSphere proxy servers.
11. Click the name of the proxy server.
12. Under Proxy Settings, expand the HTTP Proxy Server Settings tree.
13. Click Proxy server transports.
14. Click HTTPS_PROXY_CHAIN. It should be associated with port 443.
15. Click HTTP inbound channel (HTTP 4).
16. Under General Properties, set the Persistent timeout to 60 seconds.
17. Click Apply, and then click Save.
18. Repeat for every WebSphere proxy server that you configured for the cluster.
Chapter 16. Troubleshooting

When users or servers are having problems with IBM Sametime, administrators take steps to find and solve problems as quickly as possible.

This section contains information about troubleshooting and logging tools that can help you debug and fix problems affecting servers or users.

Other sources of information

Use the following links to find other hints and tips when troubleshooting Sametime servers:

- Sametime wiki:
  www.lotus.com/ldd/stwiki.nsf/
- Support Portal for Sametime:
  http://www.ibm.com/software/lotus/support/sametime/support.html
- Tech Notes for Sametime Gateway:
  www.ibm.com/support/search.wss?q=Sametime%20Gateway&rs=477&tc=SSKTXQ&dc=DB520&dtm

Troubleshooting Sametime clients

Use the following information to troubleshoot problems with IBM Sametime Connect and browser-based clients.

Logging and tracing on Sametime Connect

IBM Sametime Connect users can enable tracing on their clients.

1. On the machine where you use the Sametime Connect client, open the .config/rcpinstall.properties file in a text editor.
   To locate your Sametime workspace, see the topic Locating the Sametime Connect workspace.
2. Add the following lines to the end of the file, depending on what kind of issue you’re diagnosing.
   General client issues:
   com.ibm.collaboration.realtime.level=FINE
   Telephony and audio/video issues, including Sametime Unified Telephony and Meetings:
   General issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.tcspi.level=FINEST
   com.ibm.collaboration.realtime.multimedia.level=FINE
   Audio/video quality issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.softphone.level=FINER
   com.ibm.collaboration.realtime.multimedia.level=FINER

Note: In Sametime 8.5.1, the last line above will generate a substantial number of large audio/video trace files in your Sametime logs directory. During audio/video or Sametime Unified Telephony softphone calls, you might get 10
MB of tracing or more for each minute of the call. Do not use that level unless you have been instructed to do so and have ample free space on your hard drive.

**Instant messaging issues:**
- `com.lotus.sametime.community.kernel.level=FINER`
- `com.lotus.sametime.im.level=FINEST`
- `com.lotus.sametime.places.level=FINEST`
- `com.ibm.collaboration.realtime.rtcadapter.level=FINEST`
- `com.ibm.collaboration.realtime.people.internal.level=FINE`
- `com.ibm.collaboration.realtime.internal.sametime.level=FINER`
- `com.ibm.collaboration.realtime.login.level=FINEST`
- `com.ibm.collaboration.realtime.community.internal.level=FINEST`

**Login issues:**
- **General login failures:**
  - `com.ibm.collaboration.realtime.community.internal.level=FINEST`
  - `com.ibm.collaboration.realtime.im.community.level=FINEST`
  - `org.apache.commons.httpclient.level=FINE`
  - `com.ibm.rcp.internal.security.auth.module.level=FINEST`
  - `com.ibm.collaboration.realtime.login.level=FINEST`
  - `com.ibm.collaboration.realtime.community.internal.level=FINEST`
- **SSO failures:**
  - `com.ibm.collaboration.realtime.community.internal.level=FINEST`
  - `com.ibm.collaboration.realtime.im.community.level=FINEST`
  - `org.apache.commons.httpclient.level=FINE`
  - `com.ibm.rcp.internal.security.auth.module.level=FINEST`
  - `com.ibm.collaboration.realtime.login.level=FINEST`
  - `com.ibm.collaboration.realtime.calendar.level=FINEST`
  - `com.ibm.rcp.security.level=FINEST`

**Managed settings:**
- `com.ibm.collaboration.realtime.policy.sametime.managedsettings.level=FINEST`

**Meetings:**
- **General issues:**
  - `com.ibm.rtc.meetings.level=FINEER`
  - `com.ibm.rtc.spaces.level=FINEER`
  - `com.ibm.collaboration.realtime.appshare.level=FINEER`
  - `com.ibm.rtc.core.level=FINEER`
  - `com.ibm.sharedmaps.level=FINEER`
- **Calendar integration issues:**
  - `com.ibm.rtc.meetings.servers.level=FINEST`
  - `com.ibm.rtc.meetings.shelf.level=FINEST`
  - `com.ibm.rtc.meetings.shelf.ui.level=FINEST`
  - `com.ibm.rtc.meetings.util.level=FINEST`
  - `com.ibm.collaboration.realtime.calendar.level=FINEER`
  - `com.ibm.collaboration.realtime.calendar.notes.level=FINEST`
- **Connectivity issues:**
  - `com.ibm.rtc.core.level=FINEST`
  - `com.ibm.rtc.spaces.level=FINEER`
- **Screen sharing issues:**
  - `com.ibm.rtc.meetings.appshare.level=FINEER`
  - `com.ibm.collaboration.realtime.appshare.level=FINEER`
- **Document sharing/conversion issues:**
  - `com.ibm.rtc.meetings.documents.level=FINEER`
  - `com.ibm.rtc.meetings.appkit.image.level=FINEER`
  - `com.ibm.workplace.converter.level=FINEER`

3. Save and close the file.
4. Restart your Sametime Connect client.
5. View the error log and trace files in Sametime Connect, by clicking Help > Support > View Log and View Trace.
   In most cases, View Trace provides the most useful information.

6. (Optional) If you need to provide logs to someone else for diagnostics, you can use IBM Support Assistant to collect logs and other data.
   For the Sametime 8.5.2 Connect standalone client and Lotus Notes 8.5.2:
   a. Click Help > Support > Collect Support Data.
      After a few moments, the Collect Support Data dialog opens.
   b. Click Next to start the collection. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   c. Send the zip file to the person diagnosing the problem.
   For Lotus Notes 8.5.x:
   a. Click Help > Support > IBM Support Assistant.
   b. Select the Collect Data tab.
   c. Under Lotus Notes 8.5.x, select Notes General Problem Data Collection and click Add.
   d. Click Collect All to start the collection.
   e. When you are prompted for a reason, enter a descriptive response, and click OK.
   f. When you are prompted about collecting the .metadata directory, click OK.
   g. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   h. Send the zip file to the person diagnosing the problem.

Alternate logging and tracing (standalone client only)

If you are using the standalone IBM Sametime Connect client for Release 8.5.1 or later, you can use IBM Support Assistant to enable or disable logging for certain client components. You can also do this with the Sametime Connect 8.5 Connect client, but the procedure is different. This procedure gives you the opportunity to reproduce the issue during the collection process, optionally restarting the client if that's required to reproduce the problem. Although this procedure method doesn't provide as much control over logging as the procedure above, it does not require restarting your client in order to enable/disable logging. The Lotus Notes embedded client does not provide the ability to enable or disable logging for individual Sametime components.

1. Click Help > Support > Collect Support Data. After a few moments, the Collect Support Data dialog opens.
2. Click the Customize link. The Collect Data - Sametime dialog displays.
3. Expand the Sametime Connect node in Collector Selection and select Sametime Connect Custom Tracing, then click Add to add custom tracing to the Collector Queue.
4. Click Collect All. After a few moments, the User Input dialog opens.
5. Select up to three components to collect tracing data.
6. Click OK and follow the instructions on the screen to complete the data collection.
7. When the collection completes, a link to the collection zip file appears on the dialog. You might have to scroll down in the dialog to see the link.
Locating the Sametime Connect workspace

Both IBM Sametime Connect and IBM Lotus Notes store user-specific data, including configuration data, preferences, and trace logs, in a workspace folder on your local hard drive or a network drive. In order to diagnose Sametime Connect issues, you might be asked to update or collect files in your workspace.

About this task

The workspace location varies depending on whether you are using the standalone Sametime Connect client or Lotus Notes, the operating system, and the product release. This topic helps you locate your workspace.

Sametime Connect standalone client

This release of Sametime Connect uses the following default workspace locations:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 and Vista</td>
<td>C:\Users\user_name\AppData\Roaming\Lotus\Sametime</td>
</tr>
<tr>
<td>Microsoft Windows XP</td>
<td>C:\Documents and Settings\user_name\Application Data\Lotus\Sametime</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/Sametime</td>
</tr>
<tr>
<td>Linux (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Sametime Data</td>
</tr>
<tr>
<td>Mac OS (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
</tbody>
</table>

Note: If you upgrade an older Sametime Connect 8.x client to this release, the existing workspace location is used, rather than the default workspace location.

Lotus Notes

Lotus Notes stores the workspace in the Notes data directory. For Notes 8.5.1 and later releases, the default workspace locations are:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows (single-user client)</td>
<td>C:\Program Files\IBM\Lotus\Notes\Data\workspace</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/notes/data/workspace</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Notes Data/Expeditor/Applications</td>
</tr>
</tbody>
</table>

For Microsoft Windows, the location of the Notes data directory varies depending on whether the client is single user or multi user, whether you’re upgrading an existing client or installing a new one, and which version of Windows you’re using. For more information, see Notes installation directories for Windows in the Lotus Notes information center.
Troubleshooting audio and video in the Sametime Connect client

Enable diagnostics for audio and video in the IBM Sametime Connect client to assist with troubleshooting issues.

About this task

The following properties can be appended to the rcpinstall.properties file to enable audio and video diagnostic information. Find the file in the following location:

Microsoft Windows

In Microsoft Windows, this file is stored in the following directory: C:\Documents and Settings\user\Application Data\Lotus\Sametime\config\rcpinstall.properties.

Linux

home_dir/Lotus/Sametime/.config/rcpinstall.properties

Mac OS X

$HOME/Library/Application Support/Lotus Sametime Data/.config/rcpinstall.properties

The properties are listed by priority; they should not all be enabled at the same time.

# use for basic audio/video session troubleshooting
com.ibm.collaboration.realtime.multimedia.phonegrid.internal.client.level=FINE
# only use for ICE troubleshooting
com.ibm.ice.level=FINE
# only use for SIP troubleshooting
com.ibm.collaboration.realtime.telephony.softphone.level=FINE

The following notes about audio and video in the IBM Sametime Connect client can help you with issues raised by users.

Audio video call incompatibility

Sametime 8.5 and later releases require the Sametime Media Manager for computer audio and video calls. In order to participate in audio or video calls, all parties must be using Sametime 8.5 or later clients, and must be logged in to a Sametime 8.5 or later server configured with the Sametime Media Manager.

Troubleshooting the Sametime web audio-visual plugin

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

Enabling diagnostics for audio and video in the Sametime web audio-visual plugin

Enable diagnostics for audio and video for the IBM Sametime web audio-visual plugin to assist with troubleshooting.
About this task

The following logs help you and IBM Support troubleshoot and debug issues with the Sametime Web audio-visual plugin:

- UI traces
- Client logs
- Server logs

UI traces

To enable the UI traces for JavaScript processing, append the following parameters to the meeting or meeting room URL in the browser’s address bar:

?stmeetingsDebugLevel=debug&stmeetingsDebugScope=all

Client logs

Logs for the Sametime web audio-visual plugin are stored in the following locations:

- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\n- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

The logging level is set with the LogFileLevel parameter in the WebPlayer.ini file. Logging level options are:

- 0 (default - no log information)
- 2 (errors only)
- 8 (errors and traces)
- 16 (maximum level of errors, traces, and notifications)

Find the WebPlayer.ini file in the following location:

- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\n- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

ICE diagnostics

Enable diagnostics on the use of ICE with the log_level setting in the ice.properties file. The trace level fine is sufficient. Trace options are:

- fine
- finer
- finest

Find the ice.properties file in the following location:

- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\n- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/
GIPS Debug Trace

Set the GIPSDebugTraceEnable variable to true in the preferences.ini file.

Find the preferences.ini file in the following location:
- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Plugins/stwebsoftphone

Additional troubleshooting tools

Macintosh client running Firefox

Install XCode on the client machine, then install gdb, the GNU Project Debugger.
1. In a command window, type gdb and press Enter.
2. Type attach Firefox and press Enter.
3. Type c to continue.
4. When the browser crashes, type bt or backtrace and press Enter.
5. Copy all the traces into a file and include it in a Support request.
6. Type detach and q to exit.

Windows client

For Windows clients, running Internet Explorer 6 or 7, first try installing and using WinDBG, the Windows debugging tool available from Microsoft.
1. Start Internet Explorer.
2. Start WinDBG and use the File - Attach to a Process menu command to attach to the Internet Explorer process.
3. When a crash occurs, use View - Stack Trace to see the stack trace. Save the file as a .dmp file and include it in a Support request.

If WinDBG is changing the timing and not reproducing the crash, install and run the usercoredump.exe instead. Instructions are in this Microsoft Support article: How to use the Userdump.exe tool to create a dump file.

Install the program as described here: http://www.microsoft.com/downloads/details.aspx?familyID=E089CA41-6A87-40C8-BF69-28AC08570B7E&displaylang=en

Unless you have a specific need, disable the "dump on process termination" feature when you run the Setup.exe program.

Capture debugging information with one of these two methods:
- Set up user dump rules in advance.
  1. Go to the Control Panel and double-click Process Dump.
  2. Click New.
  3. Add Firefox.exe.
  4. Select Firefox and click Rules.
  5. Add a custom rule with the following selections:
Select c:\crashdump as the Dump file folder. Leave the default Exception Codes and select **Ignore exceptions that occur inside Kernel32.dll**. Set the MinDump Type as **Complete** and Save Mode as **Overwrite**. Do not select anything else.

6. Repeat the previous steps to add a custom rule for Iexplorer.exe.

- Capture process information after a crash.
- When the program stops responding, move to the version of Userdump.exe for your processor at the command prompt, and then type the following command:
  
  ```
  userdump PID
  ```

  where **PID** is the process ID (PID) of the program that has stopped responding. To obtain the PID of the program, open Task Manager, and then click the **Process** tab.

The user dump file is generated in the c:\crashdump folder and can be included in a Support request.

**Related concepts**

“Log file locations” on page 1235
Use this reference to locate log files for IBM Sametime components.

**Related tasks**

“Enabling logging and tracing for a Sametime Proxy Server” on page 1210
The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.

“Setting a diagnostic trace on a Sametime Media Manager server” on page 1211
You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Troubleshooting issues with the Sametime web audio-visual plugin**

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

**Installing the plugin**

- The plugin works only with Internet browser (32-bit) on supported 32-bit or 64-bit operating systems (32-bit certifications only).
- The plugin can be installed on the client by any user. If the plugin is installed under the Administrator account, verify that the plugin installed into %WINDIR%\Downloaded Program Files folder, then uninstall the plugin and install the plugin again without using the administrator account.
- If a new profile is created for Firefox on a Mac client at a non-default location, the plugin installation will not succeed. Modify the path to an absolute path for newly created profiles in the Firefox profiles.ini file.

**Issues with using the plugin**

The meeting moderator sees the “Waiting for moderator” message in the Conferencing Panel upon entering his or her own meeting room.

  Clear the browser’s cache, restart the browser, and then join the meeting again.
The message “Video Starting” appears, but the call does not start.
Take the following steps to ensure the connection can be completed:

1. Make sure that only one browser instance (tab or window) is opened for the Sametime Meeting Room client (a Sametime client cannot attend multiple meetings at the same time).

2. Exit the client.

3. On the client workstation, check the sip.log file to determine whether the client was able to register with the SIP Proxy and Registrar.

   Find the log in the Logs directory:
   Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Logs
   Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Logs
   Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Logs

   a. Look for a “200 OK” message from the SIP Proxy and Registrar.
   b. Search for “Message In -> SIP/2.0 200 OK” and “CSeq: 1 REGISTER”:

      If the “200 OK” message was received from the SIP Proxy and Registrar, then check the Sametime Proxy Server log for an indication of why the client registration failed.

      If there was no “200 OK” message received from the SIP Proxy and Registrar, then verify that the client can telnet to the server as described in the next step.

4. Test the telnet connection to the SIP Proxy and Registrar server by opening a command prompt on the client workstation and running the following command:

   telnet SIP_hostname_or_IPaddress port

   for example:
   telnet 10.10.10.10 5080

   If the client can telnet to the server, check whether the SIP Proxy server received the REGISTER request (using a network sniffer or WebSphere traces).

   If the client cannot telnet to the server, check your network connections.

The user's status disappears in the meeting room.
Refresh the page or exit and then re-enter the meeting.

If remote video is not rendering and a user pauses the video, “Hide My Video” does not hide the local video.
Refresh the page or exit and then re-enter the meeting.

The audio-video plugin may experience problems if Gmail, Skype, or NetMeeting applications are running.
For best results, exit those applications before entering the Sametime meeting room.

IE6 and IE7 performance deteriorates if a user leaves and rejoins an audio-visual call multiple times in multiple-window mode.
Run the meeting room client in single-window mode.

If a user attempts to join the same meeting from two types of clients, the attempt from the second client will be unsuccessful.
Leave the Meeting room from one client before joining the other.
Audio and video are not working as expected.
   Make sure that the appropriate latest sound and video device drivers are
   installed on the client machine.

The user sees a Conferencing Panel disabled in an A/V-enabled Meeting room
or does not see live names.
   Refresh the browser page. If that does not correct the problem, contact the
   administrator to make sure all Sametime servers are running and
   configured properly.

Troubleshooting meeting invitations
If users at your site are having difficulty inviting other users to meetings, verify
the host name for the meeting room in their client preferences.

About this task
If a user enters a value for a server preference that is not a fully qualified host
name, then the users that he or she invites into meetings might not be able to
attend.

Procedure
1. In the IBM Lotus Sametime Connect client, click File > Preferences...
2. In Preferences, click Server Communities.
3. Click the host name for the server community that hosts the meeting room.
4. Click the Server tab.
5. Verify that the host name is fully qualified.
   For example, it should be messaging.yourcompanya.com and not messaging.
6. If it is not a fully qualified host name, click Server Communities and remove
   the server community and re-add with the correct host name.
7. Click OK.

Resolving problems with business cards
If Business Cards are not displaying user information as expected, check the server
configuration, then the client, and finally, the business cards themselves.

Checking the server configuration
Check and validate the configuration on the storage repository you use with the
Sametime Community Server. A configuration problem is the most likely cause of
problems with Business Cards. For more information, see the appropriate section
in Managing business cards.

Checking the UserInfo servlet on the client
The UserInfo servlet on the client receives and responds to client requests. The
servlet must be working correctly to provide the requested details for Business
Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.
1. Determine the distinguished name (DN) of the user whose Business Card you
   want to view. Here are sample DNs of the various directory types:
   • Domino directory: cn=sametime User/O=IBM
   • Active directory: cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com
   • TDS directory: uid=Sametime user,ou=Austin,o=IBM
2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:

- [protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1
  &UserId=[User DN]
- [protocol] = {http, https}
- [hostname] = {Fully qualified hostname of the Sametime server}
- [User DN ] = {The full distinguished name of the user for whose information you are seeking}

**Examples:**

- Domino Directory:
  
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User/O=IBM

- Active Directory:
  
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User, cn=users, dc=austin, dc=ibm, dc=com

- TDS Directory:
  
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime
  user, ou=Austin, o=IBM

**Note:**

- Do not use spaces in the URL for theUserInfo servlet operation.
  A space is translated into %20 in the URL, and the servlet will not produce a result; for example:
  
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User/O=IBM
  
  is translated to:
  
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User/O=IBM
  
  The characters "%20" are inserted before the word "User" to represent the space.

- The name "UserInfoServlet" is case sensitive.
- Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you've composed into a web browser's address field, and view the result.

You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.

An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:

- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

**Checking the client**

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.
Checking that Business Cards meet requirements

Finally, verify that the business cards follow these requirements.

- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

*Note: Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.*

- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage (the directory used by Sametime for authentication). For example, if Sametime is configured to use the Domino directory, then the secondary storage cannot also be a Domino directory.

Troubleshooting a Sametime System Console

Use the following topics to troubleshoot problems in an IBM Sametime System Console.

Sametime System Console log locations

The following table shows you where to find IBM Sametime System Console logs.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Solutions Console administration logs</td>
<td>was_install_root\profiles\STSCDMgrProfile\logs</td>
</tr>
<tr>
<td>Find WebSphere Application Server-specific logs. The majority of messages that administrators are interested in are here.</td>
<td></td>
</tr>
<tr>
<td>Sametime System Console server logs</td>
<td>was_install_root\profiles\STSCAppProfile\logs</td>
</tr>
<tr>
<td>Find logs for the application server of the cell profile of the console.</td>
<td></td>
</tr>
<tr>
<td>Sametime System Console client registration utility</td>
<td>system_console_install_location\console\logs</td>
</tr>
<tr>
<td>Find logs for the product server registration into the console. This post-registration utility refers to product servers as being clients of the console. For example: c:\WebSphere\STServerCell\Console\logs</td>
<td></td>
</tr>
<tr>
<td>Product installation log for installer</td>
<td>temp\SSClogs</td>
</tr>
</tbody>
</table>

Determining Sametime server status using the Integrated Solutions Console

You can use the Integrated Solutions Console to determine if an IBM Sametime Meeting Server, Proxy Server, or Media Manager is running.

About this task

You should verify the node agent, the server, and installed applications are running.
Procedure
1. Log in to the Integrated Solutions Console.
2. Click System Administration > Node agents.
3. Locate the node for your server and verify that the Started indicator is displaying in the Status column.
4. Click Servers > Server Types > WebSphere application servers.
5. Locate your server and verify that the Started indicator is displaying in the Status column.
6. Click Applications > Application Types > WebSphere enterprise applications.
7. Locate your resource and verify that the Started indicator is displaying in the Application Status column.

What to do next
To start a server or node, see Starting and stopping servers from the Sametime System Console.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

The console.properties file
The console.properties file contains settings used to register an IBM Sametime server with the Sametime System Console. This file is used with both IBM WebSphere-based servers and IBM Lotus Domino-based servers.

Sample settings for registering a Sametime server with the Sametime System Console:
#Specify the fully qualified host name for Sametime System Console
SSCHostName=ssc.in.ibm.com

#SSC WAS credentials
SSCUserName=wsadmin
SSCPassword=password

#Specify true if you want to connect to Sametime System Console server using Secure Connection, else false.
SSCSSLEnabled=true

#Specify the HTTP port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.SSCHTTPPort=9080

#Specify the Secure Https port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.
SSCHTTPSPort=9446

#The log level for the Sametime System Console Client logs
# INFO - Information logs
# FINE - Information logs as well as severe messages
# FINEST - ALL logs (recommended)
LogLevel=FINEST
The productConfig.properties file for WebSphere-based servers

The productConfig.properties file contains settings used to register an IBM Sametime server running on IBM WebSphere with the Sametime System Console.

Sample settings for registering a WebSphere-based Sametime server with the Sametime System Console; settings will vary depending on the server and your own environment.

```
#ProductType - It specifies the type of product Installed
#Community Server - com.ibm.lotus.sametime.communityserver
#Proxy Server - com.ibm.lotus.sametime.proxyserver
#Media Server - com.ibm.lotus.sametime.mediaserver
#Gateway Server - com.ibm.lotus.sametime.gatewayserver
#Meeting Server - com.ibm.lotus.sametime.meetingserver
ProductType=com.ibm.lotus.sametime.meetingserver

# OfferingVersion = Version of the Installed Server
OfferingVersion=8.5.0.0

#InstallType=Installation Type -PN,SN,DM or Cell (WAS based Product) .For Domino Based STNODE.
InstallType=Cell

#DepName = Specify a unique Deployment Name with which you want to register the server.
DepName=Meeting Server 85

#MeetingInstallLocation - The location where the Product Specific files are copied.
#ProxyInstallLocation=C:\Program Files\IBM\Websphere\STPServerCell
#MediaInstallLocation=C:\Program Files\IBM\Websphere\MediaServerCell
#SSCInstallLocation=C:\Program Files\IBM\Websphere\STSCServerCell
#GatewayInstallLocation=C:\Program Files\IBM\Websphere\STGWServerCell
MeetingInstallLocation=C:\Program Files\IBM\Websphere\STMServerCell

#NodeIP- The IP of the machine on which the product server is installed
NodeIP=9.126.186.45

#NodeHostName- The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com

#WAS##
# Was Credentials - User Name and Password of Product Was server
WASUser=wsadmin
WASPadmin=wsadmin

#WASInstall - The root location where WAS is installed.
WASInstall=C:\ibm\WebSphere\AppServer

#WASSoapPort - The Soap Connector address for product WAS
WASSoapPort=8503

#WASHost - The hostname of the machine on which WAS is installed.
WASHost=myserver.abc.com

#WasCell - The Cell name of the Was Default profile
WasCell=myServerCell
```
#WASDMNode - The Node name of the Deployment Manager profile
WASDMNode=myServerDMNode

#WASNode - The Node name of the Secondary Node profile
WASNode=myServerNode

#WASAppProfile - The Appserver Profile name (Primary Node/Secondary profile)
WASAppProfile=STMAppProfile

#WASAppServerName - The servername for the AppServer profile.
WASAppServerName=STMeetingServer

#WASDMProfile - The Dmgr Profile name (DM profile)
WASDMProfile=STMDMgrProfile

#WASDMServerName - The servername for the DM profile
WASDMServerName=dmgr

#WASSNProfile - The SN profile name
WASSNProfile=STMSNProfile

#WASDMSoapPort - The Soap Connector address for DM Profile
WASDMSoapPort=8503

#WASDMHost - The Deployment Manager host name
WASDMHost=hare.abc.com

#PreRequisite Database Details

#DBHost - The hostname of the DB used by product.
DBHost=9.122.64.26

#DBPort - The port on which the database server listens
DBPort=50000

#DBAppID - The application username for Database server
DBAppID=db2inst1

#DBAppPassword - The application password for Database server
DBAppPassword=passw0rd

#DBName - The database Name used by the product
DBName=testDB

#PreRequisite Ldap Details

#LDAPHost - The hostname of ldap registered with the product.
LDAPHost=bluepages.ibm.com

#LDAPPort - The port of ldap registered with the product.
LDAPPort=389

#LDAPBindAnonymous - Is anonymous access allowed for ldap registered with the product.
LDAPBindAnonymous=true

#LDAPBindDN - The Bind Distinguished name for ldap registered with the product.
LDAPBindDN=cn=root

#LDAPBindPwd - The Bind password for ldap registered with the product.
LDAPBindPwd=password

#LDAPType - The Type of ldap registered with the product.
LDAPType=IDS6
#LDAPLoginField - The LoginField of ldap registered with the product.
LDAPLoginField=mail;cn;uid

#LDAPBaseDN - The search base of ldap registered with the product.
LDAPBaseDN=o=abc.com

#LDAPDisplayName - The display name of ldap registered with the product.
LDAPDisplayName=cn

#LDAPPersonObjectClass - The object class of ldap registered with the product.
LDAPPersonObjectClass=Person

#LDAPSSLEnabled - Specifies if configured LDAP is SSL enabled.
LDAPSSLEnabled=false

#PreRequisite Community Server Details
#STCommunityServerHost - The hostname of the community server registered with the product.
STCommunityServerHost=xyz.abc.com

#STCommunityServerPort - The Community server port which registered with the product.
STCommunityServerPort=1516

#ConferenceFocusHost - The Confernce Focus server hostname used by media server
ConferenceFocusHost=stdev3.abc.com

#ConferenceFocusPort - The WAS SIP port for Conference Focus
ConferenceFocusPort=5063

#AVPacketSwitcherHost - The Packet Switcher server hostname used by media server
AVPacketSwitcherHost=stdev3.abc.com

#AVPacketSwitcherPort - The port for Packet Switcher.
AVPacketSwitcherPort=5063

#ProxyRegistrarHost - The Proxy Registrar server hostname used by media server
ProxyRegistrarHost=stdev3.abc.com

#ProxyRegistrarPort - The port for Proxy Registrar
ProxyRegistrarPort=5080

#ComponentName - The component installed on the Media Server
ComponentName=Complete

#AVPacketSwitcherServerName - The WAS server name for media server.
AVPacketSwitcherServerName=STMediaServer

#AVPacketSwitcherSwitchId - It's a combination of "AVPacketSwitch" + NodeName.
AVPacketSwitcherSwitchId=PacketSwitchamalvadkMediaNode

#STReflectorHost - The Sametime reflector host
STReflectorHost=

#STReflectorPort - The Sametime reflector port
STReflectorPort=

#STMeetingServerHost - The Meeting server host name
STMeetingServerHost=

1200  Sametime Advanced: Installation and Administration Guide
The productConfig file for the Sametime Community server

The productConfig.properties file contains settings used to register an IBM Sametime Community Server with the Sametime System Console. This file is used only with the Sametime Community Server; a different copy of the file is used for IBM WebSphere-based servers.

Purpose

Example settings for registering a Sametime Community server with the Sametime System Console:

#ProductType - It specifies the type of product Installed
#Community Server - com.ibm.lotus.sametime.communityserver
#Proxy Server - com.ibm.lotus.sametime.proxyserver
#Media Server - com.ibm.lotus.sametime.mediaserver
#Gateway Server - com.ibm.lotus.sametime.gatewayserver
#Meeting Server - com.ibm.lotus.sametime.meetingserver
ProductType=com.ibm.lotus.sametime.communityserver

# OfferingVersion = Version of the Installed Server
OfferingVersion=8.5.0.0

#InstallType-Installation Type -PN,SN,DM or Cell (WAS based Product) .For Domino Based STNODE.
InstallType=STNODE

#DepName = Specify a unique Deployment Name with which you want to register the server.
DepName=Comm Server

#NodeHostName- The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com

Troubleshooting clustering

This section describes how to troubleshoot problems with clustering servers in IBM Sametime.

Each of the WebSphere-based Sametime products is installed with an SSCConnector servlet, which starts an mbean that allows the Sametime System Console to initiate a limited number of remote configuration commands before the Sametime product
is federated into the WebSphere cell of the Sametime System Console. During the clustering process, this mbean is contacted, and the application initiates the `addNode` command, which starts the federation process. During this process, the Primary Node's server where the mbean is running stops. This is required in order to federate properly. As a result, the Sametime System Console actually has no communication with the Primary Node during the federation process.

The Sametime System Console tests as many factors as possible to ensure that the federation succeeds prior to actually running the `addNode` command, and gives the user a warning if one of these conditions is found. Once the `addNode` command is initiated, the Sametime System Console begins polling the Deployment Manager configuration at intervals until it detects that the Primary Node's configuration has been added successfully. Once it determines it has been successfully added, it alerts the administrator that the federation was successful. If after 5 minutes it does not detect the node in the Deployment Manager's configuration, it gives an error stating that federation did not succeed.

Occasionally, federation actually takes longer than 5 minutes. In this case, simply waiting a few minutes and clicking Federate Node again results in a success message. Other times, the Deployment Manager has to be restarted, and then clicking Federate Node results in a success message. Very rarely, there is another condition that cannot be anticipated by the Sametime System Console that leads to the failure. In these cases, the administrator needs to look at the Primary Node's AddNode.log for additional information to help resolve the issue, and if necessary, contact IBM Support for assistance.

In other extremely rare cases, running the federation from the Sametime System Console results in an error in the AddNode.log, but running the `addNode` command directly successfully federates the node into the Deployment Manager. This is an acceptable workaround if the administrator cannot figure out why the clustering guided activity is failing. Run one of the following commands to federate the node:

```bash
addNode.bat dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses

./addNode.sh dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses
```

After manually running `addNode`, the administrator can use the clustering guided activity for the remainder of the clustering process without any issues. The application recognizes the federated status of the node and proceeds accordingly.

After running the clustering guided activity, the administrator should make sure that all nodes are synchronized before restarting any node agents. In the Integrated System Console, click System Administration > Nodes, and select the nodes you want to synchronize. and then click the Synchronize.

### Troubleshooting a Sametime Community Server

Use the following information to troubleshoot problems with an IBM Sametime Community server.

#### Troubleshooting general issues in the Sametime Community Server

The topics in this section describe how to debug general issues with the IBM Sametime Community server that can be easily reproduced.
Gathering Sametime Community Server general diagnostic data

Collect information for IBM Support to investigate Sametime awareness problems and related issues.

About this task

The recommended trace level for gathering general diagnostic information, \texttt{VP\_TRACE\_ALL=1}, is very verbose, and therefore should only be used in on servers which have available disk space and CPU utilization to spare. If you are enabling trace on a production server which is running near capacity, please contact IBM Support to get more specific diagnostic settings which do not have as high of an impact on system resource.

Follow these instructions to set the trace level, and then reproduce the problem to gather information.

Procedure

1. Stop the Lotus Domino and Sametime Community Server.
2. Remove old log files from the Sametime trace directory.
3. Use a text editor to edit the \texttt{sametime.ini} file, which is located in the Sametime Community Server installation directory (for example: \texttt{C:\Program Files\lotus\domino}). Add the following line to the \texttt{Debug} section to set the trace level:
   \begin{verbatim}
   VP_TRACE_ALL=1
   UCM_SNIF=0
   VP_SNIF=0
   UCM_DELAY_SNIF=0
   VP_DELAY_SNIF=0
   \end{verbatim}
4. Restart the Lotus Domino and Sametime Community Server.
5. Reproduce the problem that you want to troubleshoot, so you can collect diagnostic information.
6. Collect diagnostic information:
   a. Run the following collector utility: \texttt{stdiagzip.bat} located in the Sametime binary folder. For Windows, this is \texttt{C:\Lotus\Domino} by default. The output file is in the following format:
      \texttt{\Trace\stdiags_hostname_MM_DD@hh_mm.zip}
   b. Collect the following data:
      - The \texttt{sametime.log} file - Preserve as much history as possible. Do not remove data from this log.
      - The \texttt{sametime.ini} file
      - The \texttt{communityConfig.txt} file
      - The \texttt{Stlog.nsf} file - Keep this file small, not more then 1M.
      - \texttt{STConfig.nsf}
      - Details of user IDs that were used to reproduce the problem.
      - The exact time and date of the reproduced failure.
      - Client Application type and version that was used to reproduce the problem.
      - If you are troubleshooting a server crash, send all the core dump files which were created at the time of the crash.
      - Any additional details about the deployment, configuration, abnormal behavior, or any other general details that might help IBM Support with the problem investigation.
**What to do next**

After collecting the diagnostic information, any trace which was enabled on the Sametime Community Server should be disabled or reverted back to the default level. Use the STRuntimeDebug tool to enable and disable traces without having to restart the server.

**Controlling the size and content of diagnostic data**

You can set the maximum size file of each trace file and the maximum number of trace files used until the files are recycled. The setting is applicable to the IBM Sametime C++-based Community Service Application.

**Procedure**

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).

2. Add the following lines to the `Debug` section:
   - `ST_TRACEFILE_SIZE=file_size` - Sets the maximum file size of each trace file.
   - `ST_TRACEFILE_CNT=number_of_files` - Set the number of trace files generated per Sametime service application.

   ST_TRACEFILE_SIZE multiplied by ST_TRACEFILE_CNT equals the maximum size of the trace files on the Operating System hard disk per Sametime Community Service Application.

3. And finally, this.

**Example**

If the `sametime.ini` contains the following settings:

- `ST_TRACEFILE_SIZE=10`
- `ST_TRACEFILE_CNT=25`

Then 10 X 25 equals 250, so 250 MB is the maximum disk space each Sametime Service application consumes for the trace files.

**Sametime Community Server log and trace file formats**

The IBM Sametime Community Server log and trace files follow a specific naming format.

**Log files**

For Sametime 8.5 and later, log files are named `Sametime_YYYYMMDD.log`, where YYYYMMDD is the date. The log files are located in the `.../Domino/Trace` folder.

**Note:** For older versions of Sametime, the log file is named `samtime.log` and is located in the main application directory (data directory on Unix).

When the Sametime Community Server starts, a script runs that purges old logs. The script purges `samtime_YYYYMMDD.log` files that were created X number (X is 30 by default) of days ago or more. You can change the number of days by editing the `T_PURGE_LOGSOLDER_THAN` setting in the `sametime.ini` file.

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).

2. Add or edit the following line in the `Control` section:
T_PURGE_LOGS_OLDER_THAN=number_of_days

Trace files

Trace files are logged in the .../Domino/Trace folder. Once a process starts, most of the components in the name of the trace file remain unchanged until the process is restarted. Only the counter part changes. The pattern for generating file names follows this format. The name of the process always displays in the log file. The other components of the format are optional:

<The name of the process>_<date of process startup>_<time of process startup>_<the process id number in the OS>_<trace file counter>

For example, if the trace file is named StResolve_090720_1922_5544_088.txt, then the name has the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Always displays/Optionally displays</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the process</td>
<td>Always</td>
<td>StResolve</td>
</tr>
<tr>
<td>Date of process startup</td>
<td>Optional</td>
<td>090720</td>
</tr>
<tr>
<td>Time of process startup</td>
<td>Optional</td>
<td>1922</td>
</tr>
<tr>
<td>Process id number in the OS</td>
<td>Optional</td>
<td>5544</td>
</tr>
<tr>
<td>Trace file counter</td>
<td>Optional</td>
<td>088</td>
</tr>
</tbody>
</table>

**Sametime Community Server trace files location**

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  - From the Domino program directory, run the stdiagzip.bat file.
  - For example:
    ```
    C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat
    ```

- **AIX/Linux/Solaris**
  - `/local/noteddata> sh stdiagzip.sh`
  - A zip file generated by the stdiagzip script is created in the data_dir/Trace directory

- **IBM i**
  - `call QSAMETIME/STDIAGZIP servername`
  - A zip file generated by the stdiagzip program is created in the data_dir/trace directory

**Gathering Sametime Community Server name change utility diagnostic data**

Collect information for IBM Support to investigate the IBM Sametime name change utility.

**About this task**

Since the trace files require large amounts of disk space, you should leave these settings turned off by default, and only enable them when you need to run the name change utility for special overall organization migrations.

Before you start the name change utility task, follow these instructions to set the trace level for gathering diagnostic information.
Procedure

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory. For example:
   `C:\Program Files\lotus\domino`.
2. Add the following line to the Debug section to set the trace level:
   
   ```
   VP_NCSA_TRACE=1
   VP_LDAP_TRACE=1
   ```
3. Restart the Sametime Community Server.
4. After the name change task finishes, you can collect the diagnostic information:
   - A `namechange_*_.txt` debug log file
   - If you ran a name change task in RESOLVE mode, then a `StResolve_*_.txt` is produced, too.
5. Disable the `sametime.ini` file settings after the utility successfully finishes by setting the values to 0.

NSD Log and core dump file location

When an IBM Sametime Community Services process crashes, an NSD log or core dump file is created with the relevant information about the crash.

The NSD log contains information about the tasks that were running when the process crashed, as well as general system information that may help determine the cause of the crash. The log is stored in the server's `.\data\trace` directory. On Windows, the log is stored in the server's `.\trace` directory. Part of the Sametime Community Components, using Notes API libraries, creates an NSD log in an alternate directory: `.\data\IBM_TECHNICAL_SUPPORT`.

Important: The date in the NSD log file's name is not its creation date, but rather the date when the crashing process was first executed. To find the date when the NSD log was produced, look inside the log or use the file creation date based on the operating system information.

Troubleshooting LDAP in Sametime

See the following article to troubleshoot LDAP problems in IBM Sametime.

About this task

The "Best Practices for using LDAP with Sametime" article in the Sametime wiki contains a table with common problems and resolutions:


Troubleshooting network issues on the Sametime Community Server

The topics in this section describe how to diagnose networking problems that affect performance with the IBM Sametime Community server.

About this task

Some environments are sensitive to network behavior, or use a configuration that is insufficient for the expected Sametime capacity, which may result in the following symptoms:

- Delayed messages are caused by slow network performance. The messages may be one-to-one chats, group chats, and status updates of users.
Lost messages can occur when network slowdowns delay the delivery of messages and they are sent after the intended recipient logs out.

Failure to start a chat can occur when the request to start a chat times out on the recipient's end. The timeout is typically set to 30 seconds.

**Best practices for performance of the Sametime Community Server**

Delays can be caused by insufficient throughput of server-to-server connections. Follow these best practices to improve the throughput between servers.

**About this task**

Occasional delays, especially when data centers from different continents or remote geographies are online and active together, can be caused by large individual messages. If a large message is sent out and the throughput is insufficient, the message can take an unusually long time to be transferred. While one message is being transferred, no other message can be transferred on the same server-to-server connection.

Frequent or sustained delays indicate that the throughput is not high enough between two servers or given servers on remote geographies. In this situation, the delays get progressively longer, until it appears that no messages are being transferred.

Although network bandwidth can be a factor in low throughput, in most production environments, bandwidth is more than sufficient for Sametime. However, high network latency combined with a small TCP send buffer can often result in network delays. In particular, sites with servers in remote geographies may encounter this problem.

Use these best practices to improve throughput.

- All Sametime Community servers and multiplexers (if used) should be located in the same data center. Maintaining a short distance between servers is much more important than the distance between servers and clients.
- If the policy is to deploy servers on remote sites for site redundancy, try to set up sites with very low latency between them. High latency (for example, 250 ms) lowers throughput significantly. Low throughput causes congestion, which in turn causes long delays of 30 seconds or more.
- Here is a simple formula for calculating the throughput of a server-to-server connection:
  \[
  \text{throughput} = \frac{\text{buffersize}}{\text{roundtrip\_latency}}
  \]
  - Buffer size is 8 KB by default on Windows. Sametime. Server-to-server connections default to 64 KB, which is the largest useful size on standard TCP.
  - Estimate the round trip latency by using the `ping` command.

**Improving throughput on Sametime 8.5 servers**

Sametime 8.5 Community Server, as well as hotfixes on top of earlier select releases, allows you to change the default server-to-server buffer size to improve performance. In the `sametime.ini` file, use the following buffer size settings, which match the default settings of Sametime 8.5.1 and later servers.

[Connectivity]
Collecting data about network congestion problems that affect the Sametime Community server

To diagnose network problems that affect performance and stability of the IBM Sametime Community Server, add specific flags related to network traffic to the sametime.ini file. Running the server with these flags allows you to collect data that you can then send to IBM Support for evaluation.

About this task

Follow these steps to add specific data collection flags to the sametime.ini file.

Procedure

1. Open a text editor on the Sametime Community Server.
2. Open the sametime.ini file located in the Sametime Community Server installation directory. For example, the default directory in Windows is C:\program files\lotus\domino.
3. Navigate to the Sametime Community Server's config section. The name is specific to the operating system you're running on.
   - Windows
     [Debug-STCommunity]
   - AIX, Linux, and Solaris
     [Debug-stserver]
   
   Note: If you are troubleshooting a Sametime server running a release earlier than Sametime 8.5, contact IBM Support for the "per-component debug" feature, which is based on SPR#ICAE7QLJJ. This feature provides the Debug-STCommunity or Debug-stserver sections described above.
4. Add one or more of the following flags.

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCM_TRANSFER_RATE_SAMPLE_INTERVAL</td>
<td>The interval, in seconds, of sampling transfer rates of all Sametime TCP connections. A value of 0 indicates no sampling.</td>
<td>Recommended value for investigating delays and slow traffic: 5</td>
</tr>
<tr>
<td>UCM_TRANSFER_RATE_TRACE_ALL_SAMPLES</td>
<td>Transfer rate samples should be printed to debug trace files. A value of 1 indicates samples should be printed.</td>
<td>Recommended value for investigating delays and slow traffic: 1</td>
</tr>
<tr>
<td>Flag</td>
<td>Description</td>
<td>Recommended value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPS_SERVER_TRANSFER_RATE</td>
<td>Setting this flag to a number greater than 0 sends reports of the transfer rates of server-to-server TCP connections to the sametime.log file. The flag is not useful for investigating delays or slow traffic, but rather to get an idea of the transfer rates. A value of 0 indicates no reports. Any other number represents how many times a day you want to generate reports.</td>
<td>In order to get a report once every 3 hours (8 times a day), set it to 8.</td>
</tr>
<tr>
<td>UCM_DELAY_THRESHOLD</td>
<td>The threshold, in seconds, above which data queued for sending and not yet sent is reported as &quot;delayed&quot; in the socket layer. A value of 0 indicates no delay detection in the socket layer.</td>
<td>Recommended value for investigating delays: 10</td>
</tr>
<tr>
<td>UCM_DELAY_SNIFF</td>
<td>When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by UCM_DELAY_THRESHOLD.</td>
<td>This flag is only useful in a few special cases. Recommended value: 0</td>
</tr>
<tr>
<td>VP_DELAY_THRESHOLD</td>
<td>The threshold, in seconds, above which encrypted data queued for sending and not yet sent would be reported as &quot;delayed&quot; in the encryption layer. A value of 0 indicates no delay detection in the encryption layer.</td>
<td>Recommended value for investigating delays: 10</td>
</tr>
<tr>
<td>VP_DELAY_SNIFF</td>
<td>When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by VP_DELAY_THRESHOLD.</td>
<td>This flag is only useful in a few special cases. Recommended value: 0</td>
</tr>
</tbody>
</table>

5. Save the sametime.ini file.
6. Restart the Sametime Community Server.

**What to do next**

When you no longer need to collect the data, set the flags back to 0 and restart the server.

**Troubleshooting network problems on Domino**

Learn about the tools and utilities that you can use when troubleshooting problems on a Sametime Community Server.

**Basic networking knowledge and skills**
Sametime relies on networking to "work" as does Domino.

Use Ping, Telnet, Netstat and IPConfig to verify that tunneling is set up correctly on the network and in DNS.

Use Ipconfig (at the DOS or command prompt) to:
- gather pertinent information for troubleshooting general TCP/IP network problems
- troubleshoot IP issues on DHCP clients.

Use Netstat to determine:
- if an application other than a Domino server task is bound to a specific port
- if there is a network connectivity problem at the network interface or with the physical media of the network
- if the local network segment might be overloaded.

Use Traceroute to determine the physical layout of a network or internetwork.

Use the Ping utility to:
- test connectivity to a host
- gather information for troubleshooting connectivity problems.

Use the Telnet utility to connect to a Domino server and check the status of an application on a well-known port.

Use the NotesConnect utility to determine:
- services running on a machine
- network configuration problems
- if the target host name can be resolved to its IP address

The link below is provided as a reference:
Networking Basics - Key Concepts in Computer Networking

**Troubleshooting a Sametime Proxy Server**

Use the following topics to troubleshoot problems in an IBM Sametime Proxy Server.

**Enabling logging and tracing for a Sametime Proxy Server**

The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.

**Before you begin**

Ensure that the Sametime Proxy Server is running.

**About this task**

Follow these steps to enable tracing on the Sametime Proxy Server.
Procedure

1. Login to the WebSphere Integrated Solutions Console with administrator privileges on port 8601.
   For example: https://yourserver.com:8601/ibm/console
2. Select Troubleshooting > Logs and Trace.
4. Select Diagnostic Trace.
5. Select the Runtime tab.
6. Select Change log level details.
7. Type in the desired log setting, or select the components and levels by expanding the *[All Components] twistie.
8. Enable the "Save runtime changes to configuration as well" checkbox.
   Trace.log will be created in ...\profiles\STPAppProfile\logs\STProxyServer for Windows or /opt/IBM/WebSphere/AppServer/profiles/xxxxSTPPNProfilex/logs/STProxyServer for Linux.

<table>
<thead>
<tr>
<th>Log levels</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>*=info</td>
<td>Enabled by default. All SEVERE, WARNING, and INFO messages will be logged to Systemout.log and Systemerr.log.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.stproxy.</em>=</td>
<td></td>
</tr>
<tr>
<td>all:com.ibm.collaboration.realtime.*=</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>Enables Sametime Proxy related logging to the FINEST level.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.stproxy.</em>=</td>
<td></td>
</tr>
<tr>
<td>all:com.ibm.rtc.servlet.RTCServlet=</td>
<td></td>
</tr>
<tr>
<td>fine:com.ibm.collaboration.realtime.*=</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>Sometimes it is necessary to turn on rtc4web long-poll logging. Use this level to trace the long-poll traffic during the Proxy run and use states.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.</em>=</td>
<td></td>
</tr>
<tr>
<td>all:com.ibm.rtc.collaboration.realtime.*=</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>Turns on all rtc4web logging to the FINEST level. In most cases, com.ibm.rtc.servlet.RTCServlet=fine should be sufficient.</td>
</tr>
</tbody>
</table>

Troubleshooting a Sametime Media Manager

Use the following topics to troubleshoot problems in an IBM Sametime Media Manager.

Setting a diagnostic trace on a Sametime Media Manager server

You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the STMediaServer of if components are stored on different servers, the server component you want to change.
3. Under General Properties, click **Change Log Detail Levels**.
4. In the text box, append the following settings.
   
   For a single server:
   
   ```
   :com.lotus.sametime.telephony.*=all:
   com.ibm.mediaserver.*=all:
   com.ibm.telephony.conferencing.spi.*=all:
   com.ibm.ws.sip.*=all:
   com.lotus.sametime.telephony.sipfocus.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.packetswitch.*=all:
   com.lotus.sametime.telephonymanager.*=all
   com.ibm.ice.*=all
   ```

   For the conference manager only:
   
   ```
   :com.lotus.sametime.telephony.*=all:
   com.ibm.mediaserver.*=all:
   com.ibm.telephony.conferencing.spi.*=all:
   com.ibm.ws.sip.*=all:
   com.lotus.sametime.telephony.sipfocus.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.telephonymanager.*=all
   ```

   For the packet switcher only:
   
   ```
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.packetswitch.*=all
   com.ibm.ice.*=all
   ```

   For the SIP Proxy and Registrar only:
   
   ```
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all
   ```

   5. Check the box to reflect the log settings in the Configuration tab as well.
6. Click **OK**, and then **Save**.
7. Restart the Sametime Media Manager.
8. Monitor the log files in the following locations.
   
   Windows:
   
   ```
   WAS_Install_Root\WebSphere\AppServer\profiles\HostName_Media_deploymentType_Profile_Number\logs
   ```

   Linux:
   
   ```
   /opt/IBM/WebSphere/AppServer/profiles/HostName_Media_deploymentType_Profile_Number/logs
   ```

**Logging and tracing on Sametime Media Manager**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.
For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

**Gathering Sametime Media Manager logs and traces for IBM Support**

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

**About this task**

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

**Procedure**

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   
   For more information, see the following topic in the WebSphere Application Server information center:
   
   Gathering information with the collector tool (deprecated).

2. Run the collector on the IBM Sametime Media Manager server.
   
   Run collector on the WebSphere Application Server profiles.
   
   The profiles are stored in the \profiles directory; for example on Microsoft Windows:
   
   C:\Program Files\ibm\WebSphere\AppServer\profiles
   
   The profile name follows this format:
   
   HostName_Media_deploymentType_Profile_Number
   
   The collector resides in the \bin directory below the profile; for example:
   
   C:\Program Files\ibm\WebSphere\AppServer\profiles\wplicdlvm053MediaPProfile1\bin\collector.bat
   
   The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
   
   HostName_Media_deploymentType_Profile_Number-WASenv.jar
   
   **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. Submit the collector generated log files to IBM support.

**Troubleshooting a Sametime Media Manager using JVM logs**

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.
About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting > Logs and Trace.
2. Click STMediaServer.

   Note: Any configuration changes to the JVM logs that are made to a running IBM Sametime Media Manager do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting video quality

To ensure good quality video in your video-enabled IBM Sametime meeting rooms and Sametime Connect video calls, check your video driver.

Sametime Connect video calls and video-enabled Sametime meeting rooms take advantage of the hardware acceleration available in modern video cards and their associated drivers. If you are experiencing difficulty in establishing video call connections, or experience poor video quality in video in meeting rooms, ensure that you are using a video driver that takes full advantage of your video card's acceleration hardware.

Refer to the A/V Client Support & Requirements section in the system requirements:
http://www.ibm.com/support/docview.wss?rs=477&uid=swg27016451

Troubleshooting Sametime Media Manager component clusters

This section explains how to troubleshoot clusters of IBM Sametime Media Manager components.

Enabling logging and tracing for a Conference Manager cluster

Enable traces and logs for the members in a Conference Manager cluster.
Procedure
1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.lotus.sametime.telephony.**=all:
   com.ibm.mediaserver.**=all:
   com.ibm.telephony.conferencing.spi.**=all:
   com.ibm.ws.sip.**=all:
   com.lotus.sametime.telephony.sipfocus.**=all:
   com.ibm.sip.**=all:
   com.lotus.sametime.telephonymanager.**=all
7. Click Apply.
8. Save your changes by clicking the Save link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

Enabling logging and tracing for a SIP Proxy and Registrar cluster
Enable traces and logs for the members in a SIP Proxy and Registrar cluster.

Procedure
1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all
7. Click Apply.
8. Save your changes by clicking the Save link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

Configuring a Sametime Community Server to allow connections from Conference Manager nodes
Add Conference Manager nodes to the list of Trusted IPs for an IBM Sametime Community Server.

About this task
This task is only necessary if you see the ST_CONNECT_HOST_UNREACHABLE error in the Conference Manager logs, which means that the Community Server is not allowing connections from the Conference Manager nodes. Enable the connection by adding
each Conference Manager node’s IP address to the list of Trusted IPs for the Sametime Community Server.

**Procedure**
1. Log into the Sametime System Console’s Integrated Solutions Console as the WebSphere administrator.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the “Sametime Community Servers” table, click the name of a Community Server.
4. Click the Connectivity tab.
5. Add the Conference Manager nodes to the list of trusted servers:
   a. Under “Trusted Servers” enter the IP address (or host name) of the server where a Conferencing Manager node is hosted.
   b. Click Add.
   c. Repeat for each node in the Conference Manager cluster.
   d. Click OK.
6. Restart the Sametime Community Server.

**Enabling traces and logs for the WebSphere proxy server used by a Media Manager cluster**

Enable traces and logs for an IBM WebSphere proxy server that is used with an IBM Sametime Media Manager cluster.

**About this task**

Both Conference Manager clusters and SIP Proxy and Registrar clusters can use a WebSphere proxy server; this task applies to both clusters.

**Procedure**
1. Log into the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the “Logging and Tracing” table, click the name of a WebSphere proxy server to open its “Logging and Tracing” page.
4. Under “General Properties” click Diagnostic Trace.
5. Under “Additional Properties” click Change Log Detail Levels.
6. In the text box, append the following settings:
   ```
   :com.ibm.ws.sip.*=all
   :com.ibm.ws.proxy.*=all
   ```
7. Click Apply and then save the changes by clicking the Save link in the “Messages” box at the top of the page.

**Troubleshooting a Sametime Meeting Server**

Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server.

**Setting a diagnostic trace on a Sametime Meeting Server**

You can specify how the server handles IBM Sametime Meeting Server log records. You can select a Sametime Meeting Server to enable or disable a system log for the
server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Procedure**

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and trace.
2. Click the Sametime Meeting Server that you want to trace.
3. Under General Properties click Diagnostic Trace
4. Under Additional Properties, click Change Log Detail Levels.
5. In the text box, append the following settings:
   
   
   To get even more detailed traces, use this setting instead:
   
   *=info: com.ibm.rtc.*=all
6. Click Apply, and then Save.
7. Monitor the log file in IBM\WebSphere\AppServer\profiles\HostName_Meeting_deploymentType_Profile_Number\logs

**Logging and tracing on Sametime Meeting Server**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

**Gathering Sametime Meeting Server logs and traces for support**

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

**About this task**

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files,
operating system and Java data, and the presence and level of each software prerequisite.

**Procedure**

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   
   For more information, see the following topic in the WebSphere Application Server information center:
   
   Gathering information with the collector tool (deprecated)

2. Run the collector on the IBM Sametime Meeting Server.
   
   • Run collector on the WebSphere Application Server profiles.
     
     The profiles are stored in the `\profiles` directory; for example on Microsoft Windows:
     
     `C:\Program Files\ibm\WebSphere\AppServer`\profiles
   
   • The collector resides in the `\bin` directory below the profile; for example:
     
     `C:\Program Files\ibm\WebSphere\AppServer\profiles\`\HostName_Meeting_deploymentType_Profile_Number\bin\collector.bat`

   The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:

   `HostName_Meeting_deploymentType_Profile_Number-WASenv.jar`

   **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. Submit the collector generated log files to IBM support.

**Troubleshooting a Sametime Meeting Server using JVM logs**

To start troubleshooting a problem on an IBM Sametime meeting server, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

**About this task**

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

• **SystemOut.log** is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.

• **SystemErr.log** contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived,
files to keep and which of the log files to rollover or archive based by time or size or both.

**Procedure**
1. In the Integrated Solutions Console, click **Troubleshooting --> Logs and Trace**.
2. Click the IBM Sametime Meeting Server.
3. Under General Properties, click **JVM Logs**.

   **Note:** Any configuration changes to the JVM logs that are made to a running Sametime Meeting Server do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the **Runtime** tab, then click **View**.

**Troubleshooting a Sametime Meeting Server cluster**
Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server cluster.

**Troubleshooting WebSphere proxy issues with the Sametime Meeting Server cluster**
You can troubleshoot issues with the IBM WebSphere proxy server used with the IBM Sametime Meeting Server cluster by setting traces and logs.

**Procedure**
1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Troubleshooting > Logs and trace**.
3. In the "Logging and Tracing" table, click the name of a WebSphere proxy server to open its "Logging and Tracing" page.
4. Under "General Properties" click **Diagnostic Trace**.
5. Under "Additional Properties" click **Change Log Detail Levels**.
6. In the text box, append the following settings:
   ```
   com.ibm.rtc.proxy.filter.**=all
   ```
   Based on this output, IBM might recommend other settings.
7. Click **Apply** and then save the changes by clicking the Save link the "Messages" box at the top of the page.
8. Repeat for every WebSphere proxy server used by the cluster.

**Troubleshooting installation or uninstallation**
Use the following topics to troubleshoot problems that occur after installing and uninstalling IBM Sametime servers.

**Troubleshooting a Sametime System Console installation**
To install the IBM Sametime System Console server, the DB2 application user ID must have administrator rights to be able to create and update tables in the database. If the user does not have administrator rights and installation was not successful, follow these steps to create the tables required by the installation program.
**About this task**

Connect to the system console database (for example, STSC). Then enter the `createSchedTable.ddl` command to create additional tables in the database.

**AIX, Linux, or Solaris**

`db2 connect to STSC`  
`db2 -tf createSchedTable.ddl`

**Windows**

`db2cmd`  
`db2 connect to STSC`  
`db2 -tf createSchedTable.ddl`

**Troubleshooting a Sametime Gateway installation**

These steps help you troubleshoot installation problems by describing how you can use a different tablespace name for the database and how you can clean your system of previous installations.

**About this task**

Many installation problems are caused when the installer cannot locate the database or when installing a new instance of Sametime Gateway and a previous installation has not been completely removed from the system. The following steps describe how to use a different tablespace in the database or clean your system of previous installations.

**Procedure**

1. Open the installation log file at `stgw_server_root\logs\install.log.txt`
2. If the log reports an error in finding the DB2 database, check to make sure you are using the tablespace name USERSPACE1. Sametime Gateway expects USERSPACE1 by default. To install using a different tablespace name, use the following command when you run the installer:
   
   `install.bat -VTableSpaceName="tableSpaceName"`
   
   Where `tableSpaceName` is the name of the tablespace that you want the installer to use.
3. To clean your system of previous installations, use the log to find the location of the Install Shield Multiplatform (ISMP) database called the Vital Product Database (VPD). For example, examine this log entry from Windows (formatted to fit on the page):
   
   `(Dec 24, 2009 2:22:22 PM), stGwInstall, com.ibm.rtc.gateway.install.CheckVPDRegistry, msg1, using VPD registry at C:\Program Files\Common Files\InstallShield\Universal\common\Gen2\vpddb\vpd`

   The location of this registry varies from system to system. On windows, VPD is usually found in the `\Program Files\Common Files\InstallShield\Universal\common\Gen2` folder. If a Sametime Gateway server is uninstalled, but an error occurs and the product is not unregistered, the VPD shows that Sametime
Gateway is installed on the system. When a new installation is initiated, and a previously installed Sametime Gateway server is detected, the installer prompts you to upgrade or install a new version, or the installer forces you to install a Deployment Manager server or a Primary Server on the same system. None of these scenarios are desired because there are no Sametime Gateway servers installed on the system.

4. Back up the Gen2 folder. Note that the VPD registry may be used by other programs that are installed with InstallShield, so removing this registry may interfere with other programs. Do not remove the Gen2 folder unless it is absolutely necessary.

5. Remove the original Gen2 folder.

6. If installing on Windows, delete the following left over files:
   - C:\Windows\nifregistry
   - C:\Windows\vpd.properties

7. Start the installation again.

### Registering a Sametime server manually on AIX, Linux, Solaris, and Windows

On IBM AIX, Linux, Sun Solaris, and Microsoft Windows, you can manually register an IBM Sametime server from the console if a problem occurs during the installation process and results in a failure to register the server.

**About this task**

A successful registration on AIX, Linux, Solaris, or Windows automatically registers the following servers from the Sametime System Console:

- Sametime Community Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server

If a problem arises during installation and the server is not successfully registered, follow the instructions in the appropriate topic below to complete the registration:

### Registering a Community Server manually on AIX, Linux, Solaris, and Windows

If automatic registration fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime Community server with the Sametime System Console.

**Before you begin**

The Sametime System Console must be started.

**About this task**

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties
Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's Sametime console directory:
      - **AIX, Linux, Solaris**: The console directory is under the Community
        Server data directory; for example: /opt/IBM/domino85/notesdata/console
      - **Windows**: The console directory is under the Domino directory; for
        example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and
      productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

   **Table 168. console.properties settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
<td>Provide the fully qualified host name of the Sametime System Console server.</td>
</tr>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.
   Only the required values in this file are listed here:

   **Table 169. productConfig.properties settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the Community Server that is being registered.</td>
</tr>
</tbody>
</table>

4. Start the Sametime Community Server.

5. Now register the server:
   a. Run the registerSTServerNode registration utility from the /console directory.
      - **AIX, Linux, Solaris**: registerSTServerNode.sh
• Windows: registerSTServerNode.bat

The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the registration is successful, a console.pid file will be added.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows

If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Before you begin

Verify that the Deployment Manager, the Sametime System Console server, and the Sametime server that you are registering are running.

About this task

This procedure works for the following Sametime servers:
• Sametime Proxy Server
• Sametime Media Manager
• Sametime Meeting Server
• Sametime Advanced

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:
• console.properties
• productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. On the server to be registered, navigate to the InstallLocation/console directory.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.

| SSCHostName       | Provide the fully qualified host name of the Sametime System Console server. |

Chapter 16. Troubleshooting 1223
Table 170. console.properties settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

3. Verify that the following settings in the productConfig.properties file are correct. Modify them as needed before saving and closing the file. You will need to add the passwords.

Table 171. Sametime Proxy Server

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

Table 172. Sametime Media Manager

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

| Note: Remove any values for STCommunityServerHost or STCommunityServerPort in the productConfig.properties file when you are preparing to register a Media Manager with the Packet Switcher component. The Community server is not a prerequisite for Packet Switcher and these values cause registration to fail. |

Table 173. Sametime Meeting Server

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBAppPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
</tbody>
</table>
Table 173. Sametime Meeting Server (continued)

<table>
<thead>
<tr>
<th>WASPassword</th>
<th>Specify the password associated with the WASUserID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

Table 174. Sametime Advanced

<table>
<thead>
<tr>
<th>DBAppPassword</th>
<th>Specify the password associated with the database ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

4. If you are registering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.

5. Now register the server:
   a. Run the registerWASProduct.sh registration utility from the /console directory.
      * AIX, Linux, Solaris: ./registerProduct.sh -federateNode
      * Windows: registerProduct.bat -federateNode

   The utility registers the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the registration is successful, a console.pid file will be added.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Manually removing WebSphere Application Server
You may need to remove WebSphere Application Server manually if it remains on the system after Sametime fails to install or uninstall completely. WebSphere Application Server is installed when you install the following Lotus Sametime servers: Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Gateway.

Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows
Remove WebSphere Application Server on AIX, Linux, Solaris, and Windows manually if it remains on the system after Sametime fails to install or uninstall completely.
Before you begin

Stop all servers associated with the Sametime server in the order shown below. For more information, see “Command reference for starting and stopping servers” on page 487.

1. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
2. Stop the Sametime server.
3. Stop WebSphere Application Server.
4. Stop the Deployment Manager.
5. Close all browsers and command windows that are accessing the server you plan to uninstall.

About this task

If after an attempted Sametime install or uninstall, you have many files and folders left in `was_install_root/profiles/profile_name` or `was_install_root/bin`, run the WebSphere Application Server uninstall program to remove the rest of the files. Remove WebSphere Application Server only if it is not in use by any other server on the system.

Windows

1. From the Microsoft Windows Start menu, select Settings > Control Panel > Add/Remove Programs.
2. Select IBM WebSphere Application Server from the list and click Add/Remove. Click Yes when prompted to remove the server.
3. When the Windows uninstall program completes, click OK to exit the uninstall program.
4. Delete the WebSphere Application Server installation directory (for example, C:\Program Files\IBM\WebSphere).

AIX, Linux, Solaris

1. Go to the WebSphere Application Server installation root folder (for example, /opt/IBM/WebSphere/Appserver).
2. Navigate to the uninstall folder.
3. Run the uninstall command:
   ```
   ./uninstall
   ```
4. After uninstallation completes, delete the WebSphere Application Server installation directory (for example, /opt/IBM/WebSphere/AppServer).

For more information, see Uninstalling the WebSphere Application Server product in the WebSphere Application Server information center.

Manually removing WebSphere Application Server on IBM i

Remove WebSphere Application Server on IBM i manually if you have removed all Sametime servers from the system, and no longer want the program installed.

Before you begin

Stop all servers running on the WebSphere Application Server system. If the server belongs to a cluster, you will also need to stop all node agents in the cluster, and then stop the Deployment Manager. Finally, close all browsers and command windows that may have been accessing the WebSphere Application Server.
About this task

After uninstalling a Sametime server from IBM i, WebSphere Application Server will still be installed on the system. You may choose to uninstall WebSphere Application Server only if it is not in use by any other server on the system.

Stop all java processes. Then follow the steps in the WebSphere Application Server 7 Information Center to remove unneeded WebSphere Application Server software from the system:

Uninstalling the product on IBM i

**Manually removing DB2 data on AIX, Linux, Solaris, and Windows**

If DB2 installation or uninstallation was unsuccessful, you can follow these steps to manually remove DB2 and other files.

About this task

Remove the DB2 software, then remove the rest of the DB2 files and data left on the system.

**Procedure**

1. Remove the DB2 from your operating system. For example, if you are running DB2 on Windows, use the Control Panel, Add/Remove Programs panel and remove the programs.
2. Remove all files in the local /tmp or temp directory.
3. Manually remove user and group information.
   - **Linux**
     - Remove user home directories under /home.
     - DB2 Instance user account: db2admin (or the administrator account specified during installation)
     - DB2 Administration Server (DAS) user account: dasuser1
     - DB2 users group: db2admin (or the same as the DB2 Instance user account name defined by user)
     - DB2 Administration users group: dasadm1
   - **Windows**
     - Remove DB2 users and groups:
     - DB2 Instance user account: db2admin (or the administrator account specified during installation)
     - DB2 Administration Server (DAS) user account: db2admin
     - DB2 users group: DB2USERS
     - DB2 Administration users group: DB2ADMNS
4. Remove these directories for DB2.
   - The directories below show the Windows path. They will differ on Linux.
     - c:\documents and settings\all users\application data\ibm\db2
     - c:\documents and settings\all users\application data\ibm\db2history
     - c:\documents and settings\db2admin
     - c:\documents and settings\install user\application data\ibm\vshet
     - c:\documents and settings\install user\application data\ibm\db2
5. Delete the remaining DB2 directories.

**Unregistering a Sametime server on AIX, Linux, Solaris, or Windows**

On IBM AIX, Linux, Sun Solaris, and Microsoft Windows, you can manually unregister an IBM Sametime server from the console if a problem occurs during the uninstallation process and results in a failure to unregister the server.

**About this task**

A successful unregistration on AIX, Linux, Solaris, or Windows automatically unregisters the following servers from the Lotus Sametime System Console:

- Sametime Community Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server

If a problem arises during uninstallation and the server is not successfully unregistered, follow the instructions in the appropriate topic below to complete the unregistration:

**Unregistering a Sametime Community Server**

To remove an IBM Sametime Community Server from the list of the Sametime System Console's managed servers, run the unregister utility on the server. This step is required before uninstalling a Community Server that you installed without a deployment plan and then registered with the Sametime System Console later using the registration utility. If you installed the server with a deployment plan, unregistering is only needed if you are performing some other activity that requires removal of the product from the console.

**Before you begin**

The Sametime System Console must be started.

**About this task**

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

**Procedure**

1. Back up the `console.properties` and `productConfig.properties` files:
   a. Navigate to the Community Server's Sametime console directory:
      - AIX, Linux, Solaris: The console directory is under the Community Server data directory; for example: `/opt/IBM/domino85/notesdata/console`
      - Windows: The console directory is under the Domino directory; for example: `C:\Lotus\Domino\console`
   b. Make back-up copies (using different names) of the `console.properties` and `productConfig.properties` files.
2. Update the following values in the console.properties file and save the file.

Table 175. console.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
<td>Provide the fully qualified host name of the Sametime System Console server.</td>
</tr>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot; To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile. For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/ AppServerProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to 'true' to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.

Only the required values in this file are listed here:

Table 176. productConfig.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The Dep Name must be the name that was used when you installed: the unique name for this deployment as known by the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the Community Server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Start the Sametime Community Server.

5. Now unregister the server:

a. Run the unregister utility with the following command:
   - AIX, Linux, Solaris: unregisterProductNode.sh
   - Windows: unregisterProductNode.bat

b. As the unregister utility runs, you will be prompted to enter the Location of the notes.ini file. You are only prompted for the notes.ini file location when unregistering the server. Type the full path to the directory containing the notes.ini file (for example, /stserver/data), and press Enter.

The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.
Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233
If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Related reference
“Command reference for starting and stopping servers” on page 487
You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

Unregistering a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced
To unregister an IBM Sametime server from the list of the Sametime System Console’s managed servers, run the unregister utility on the server. You do not normally need to unregister a Sametime server. This step is needed only if there was a problem with the uninstallation or you are performing some other activity that requires removal of the product from the console.

About this task
This procedure works for the following Sametime servers:
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Advanced

Skip this task if you are uninstalling the Sametime System Console.

During this task you will edit the following files; click the topic titles below to see details on each file. You may want to open each topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure
1. Back up the console.properties and productConfig.properties files:
   a. On the server to be unregistered, navigate to the InstallLocation/console directory.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.
2. Update the following values in the console.properties file and save the file.

   Table 177. console.properties settings
   | SSCHostName       | Provide the fully qualified host name of the Sametime System Console server. |
Table 177. `console.properties` settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/STSCAppProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

3. Verify that the following settings in the `productConfig.properties` file are correct. Modify them as needed before saving and closing the file. You will need to add the passwords.

**Table 178. Sametime Proxy Server**

<table>
<thead>
<tr>
<th>WASPassword</th>
<th>Specify the password associated with the WASUserID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The unique descriptive name of the deployment as it was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

**Table 179. Sametime Media Manager**

<table>
<thead>
<tr>
<th>WASPassword</th>
<th>Specify the password associated with the WASUserID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The unique descriptive name of the deployment as it was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

**Table 180. Sametime Meeting Server**

<table>
<thead>
<tr>
<th>DBAppPassword</th>
<th>Specify the password associated with the database ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
</tbody>
</table>
Table 180. Sametime Meeting Server (continued)

<table>
<thead>
<tr>
<th>DepName</th>
<th>The unique descriptive name of the deployment as it was registered with the Sametime System Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

Table 181. Sametime Advanced

<table>
<thead>
<tr>
<th>DBAppPassword</th>
<th>Specify the password associated with the database ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DepName</th>
<th>The unique descriptive name of the deployment as it was registered with the Sametime System Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

4. If you are unregistering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.

5. Now unregister the server:
   a. Run the unregisterWASProduct.sh unregistration utility from the /console directory.
      - **AIX, Linux, Solaris**: ./unregisterWASProduct.sh
      - **Windows**: unregisterWASProduct.bat

   The utility unregisters the server, generating a log file called ConsoleUtility.log and storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.

**Related tasks**

“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 1233

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**Related reference**

“Command reference for starting and stopping servers” on page 487

You may use a command window to start and stop Sametime components running on WebSphere Application Server. To stop servers, you will supply the WebSphere Application Server administrator password that was established when you installed the server.

**Updating the Sametime System Console when server unregistration fails**

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.
About this task

The steps for removing the server’s entry from the Sametime System Console’s database vary with the operating system on which the console runs:

Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Before you begin

Make a note of the product type, host name, install type, and deployment name for the Sametime server you want to remove.

About this task

This utility removes information about a Sametime server from the IBM DB2 database used by the Sametime System Console, effectively unregistering the server. This method is useful when you are unable to complete the unregistration task from the server itself; for example:

- If you have run an uninstall, and received an error message stating that the Sametime System Console could not be contacted to remove the server from the configuration.
- If you experienced a catastrophic server failure and cannot run the uninstallation program or the unregistration utility on that server.
- If you want to force the removal of a server from the Sametime System Console’s topology for some reason and the unregistration utility failed.

Procedure

1. Working on the Sametime System Console server, navigate to the InstallLocation/console directory.
2. Update the following values in the console.properties file before saving and closing the file:

   | SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
   | SSCHTTPPort | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false." |
   | | To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the "HTTP transport port." The default profile name is STSCAppProfile. |
   | SSCUserName | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin. |
   | SSCPASSWORD | Enter the WebSphere Application Server password associated with the SSCUserName. |
3. Run the updateStaleEntry utility:
   a. Open a command window and run the following command:
      • AIX, Linux, Solaris: ./updateStaleEntry.sh -uninstall
      • Windows: updateStaleEntry.bat -uninstall
   b. When prompted, provide the product type, host name, install type, and deployment name for the Sametime server that you are removing from the console's database.
      The utility removes the server from the database and generates the ConsoleUtility.log file, storing it in the console/logs directory.

4. Restart the Sametime System Console.

**Updating the Sametime System Console on IBM i when server unregistration fails**

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**Before you begin**

Make a note of the product type, host name, install type, and deployment name for the Sametime server you want to remove.

**About this task**

This utility removes information about a Sametime server from the IBM DB2 database used by the Sametime System Console, effectively unregistering the server. This method is useful when you are unable to complete the unregistration task from the server itself; for example:

- If you have run an uninstall, and received an error message stating that the Sametime System Console could not be contacted to remove the server from the configuration.
- If you experienced a catastrophic server failure and cannot run the uninstallation program or the unregistration utility on that server.
- If you want to force the removal of a server from the Sametime System Console's topology for some reason and the unregistration utility failed.

**Procedure**

1. Working on the Sametime System Console server, navigate to the /QIBM/UserData/Lotus/stii_ssc/console directory.
2. Update the following values in the console.properties file before saving and closing the file:

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</table>

"Table 183. console.properties settings"
Table 183. `console.properties` settings (continued)

| SSCHTTPPort | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false."
| SSCHTTPPort | To determine the correct HTTP port, open the AboutThisProfile.txt file for the Sametime System Console Application Server Profile and use the setting specified for the "HTTP transport port." The default profile name is STSCAppProfile.
| SSCHTTPPort | On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt
| SSCUserName | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin.
| SSCPassword | Enter the WebSphere Application Server password associated with the SSCUserName.

3. Run the `updateStaleEntry` utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: `QSH`
   b. Navigate to the server's console directory; for example: `cd /stserver/data/console`.
   c. Run the shell script to unregister the cluster: `updateStaleEntry.sh`.
   d. When prompted, provide the product type, host name, install type, and deployment name for the Sametime server that you are removing from the console's database.
   e. When the utility finishes, press F3 to exit QSH. The utility removes the server from the database and generates the `ConsoleUtility.log` file, storing it in the `console/logs` directory.

4. Restart the Sametime System Console.

Log file locations

Use this reference to locate log files for IBM Sametime components.

Collecting the proper files and information helps to expedite problem determination and resolution for IBM Sametime when you are working with IBM Support. Provide the following information:

- A precise description of the issue, error message, and steps to reproduce
- Applicable screen shots of the problem or error message
- Log files pertaining to your problem

Installation Files

Installation log files can be found in the following locations:

- **Windows**
  C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs\Windows 2008
  C:\ProgramData\IBM\Installation Manager\logs
• **AIX/Linux/Solaris**
  `/var/ibm/InstallationManager/logs`
  
  • **Websphere-based application log files** are created on the server's file system for each server's instance.
  
  
  • **IBM i**
  `/QIBM/UserData/LOTUS/stii/logs`
  
  **Sametime System Console**

  Sametime System Console log files can be found in the following locations:

  • **Windows**
    
    C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCDMgrProfile\logs
    C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCAppProfile\logs

  • **AIX/Linux/Solaris**
    
    /opt/IBM/WebSphere/AppServer/profiles/STSCDMgrProfile/logs
    /opt/IBM/WebSphere/AppServer/profiles/STSCAppProfile/logs

  • **IBM i**
    
    /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDMgrProfile/logs
    /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs

  **Sametime Proxy Server**

  Sametime Proxy Server log files can be found in the following locations:

  • **Windows**
    
    C:\Program Files\IBM\WebSphere\AppServer\profiles\STPAppProfile\logs
    C:\Program Files\IBM\WebSphere\AppServer\profiles\STPDMgrProfile\logs

  • **AIX/Linux/Solaris**
    
    /opt/IBM/WebSphere/AppServer/profiles/STPDMgrProfile/logs
    /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile/logs

  • **IBM i**
    
    /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPDMgrProfile/logs
    /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs

  **Sametime Meeting Server**

  Sametime Meeting Server log files can be found in the following locations:

  • **Windows**
    
    C:\Program Files\IBM\WebSphere\AppServer\profiles\STMDMgrProfile\logs
    C:\Program Files\IBM\WebSphere\AppServer\profiles\STMAppProfile\logs

  • **AIX/Linux/Solaris**
    
    /opt/IBM/WebSphere/AppServer/profiles/STMDMgrProfile/logs
    /opt/IBM/WebSphere/AppServer/profiles/STMAppProfile/logs

  • **IBM i**
Sametime Media Manager

Sametime Media Manager log files can be found in the following locations:

- **Windows**
  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSDMgrProfile\logs  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSAppProfile\logs

- **Linux**
  
  /opt/IBM/WebSphere/AppServer/profiles/STMSDMgrProfile/logs  
  /opt/IBM/WebSphere/AppServer/profiles/STMSAppProfile/logs

Sametime Community Server

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  
  From the Domino program directory, run the stdiagzip.bat file.  
  
  For example:
  
  C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat

- **AIX/Linux/Solaris**
  
  /local/notesdata> sh stdiagzip.sh
  
  A zip file generated by the stdiagzip script is created in the data_dir/Trace directory

- **IBM i**
  
  call QSAMETIME/STDIAGZIP servername
  
  A zip file generated by the stdiagzip program is created in the data_dir/trace directory

Sametime clients

The Sametime Connect log files are in the logs directory, which is located under the client workspace directory. For example, logs are located in the following directory on Windows XP:

C:\Documents and Settings\user_name\Application Data\Lotus\Sametime\logs

Logs for the Sametime web audio-visual plugin are stored in the following locations:

- **Microsoft Windows XP**: %APPDATA%\IBM\Lotus\Sametime WebPlayer\  
- **Windows Vista and Windows 7**: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\  
- **Mac OS X**: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/
Related concepts

“Logging and tracing on Sametime Connect” on page 1185
IBM Sametime Connect users can enable tracing on their clients.

Related tasks

“Locating the Sametime Connect workspace” on page 1188
Both IBM Sametime Connect and IBM Lotus Notes store user-specific data, including configuration data, preferences, and trace logs, in a workspace folder on your local hard drive or a network drive. In order to diagnose Sametime Connect issues, you might be asked to update or collect files in your workspace.

Directory conventions

Directory variables are abbreviations for the default installation paths for IBM AIX, Linux, Solaris, IBM i, and Microsoft Windows. This topic defines the directory variable and its matching default installation directory for each supported operating system.

<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
<tbody>
<tr>
<td>was_install_root</td>
<td>AIX</td>
<td>/usr/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/usr/IBM/WebSphere/AppServer7</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt/IBM/WebSphere/AppServer7</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/ProdData/WebSphere/AppServer/V7/ND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/QIBM/ProdData/WebSphere/AppServer7/V61/ND</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer7</td>
</tr>
<tr>
<td>Directory variable</td>
<td>Operating system</td>
<td>Default installation root</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>app_server_root</strong></td>
<td>AIX</td>
<td>/usr/IBM/WebSphere/AppServer</td>
</tr>
</tbody>
</table>
| Root directory for the creation of WebSphere Application Server profile directories. | For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/usr/IBM/WebSphere/AppServer7 |
| Linux and Solaris | /opt/IBM/WebSphere/AppServer |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/opt/IBM/WebSphere/AppServer7 |
| IBM i             | /QIBM/UserData/WebSphere/AppServer/V7/ND |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/QIBM/UserData/WebSphere/AppServer/V7/ND |
| Windows           | [%drive%]:\Program Files\IBM\WebSphere\AppServer |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
[%drive%]:\Program Files\IBM\WebSphere\AppServer7 |
| stSSC_profile_root | All platforms | Primary node  
app_server_root/profiles/STSCAppProfile |
| The Sametime System Console profile directory | Secondary node  
app_server_root/profiles/STSCAppProfile |
| stM_profile_root  | All platforms | Primary node  
app_server_root/profiles/STMAppProfile |
| The Sametime Meeting Server profile directory | Secondary node  
app_server_root/profiles/STMAppProfile |
| stP_profile_root  | All platforms | Primary node  
app_server_root/profiles/STPAppProfile |
| The Sametime Proxy Server profile directory | Secondary node  
app_server_root/profiles/STPAppProfile |
| stMS_profile_root  | All platforms | Primary node  
app_server_root/profiles/STMSAppProfile |
| The Sametime Media Manager profile directory | Secondary node  
app_server_root/profiles/STMSSAppProfile |
| stgw_profile_root | AIX              | /opt/IBM/WebSphere/AppServer/profiles/RTCGW_Profile[1,2,...] |
| Sametime Gateway profile directory  
The default profile directory is incremented by 1 with each additional installation on the machine. | For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/opt/IBM/WebSphere/AppServer7/profiles/RTCGW_Profile[1,2,...] |
|Linux and Solaris | /opt/IBM/WebSphere/AppServer/profiles/RTCGW_Profile[1,2,...] |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/opt/IBM/WebSphere/AppServer7/profiles/RTCGW_Profile[1,2,...] |
| IBM i             | /QIBM/UserData/WebSphere/AppServer/V7/ND/RTCGW_profile |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
/QIBM/UserData/WebSphere/AppServer/V7/ND/RTCGW_profile |
| Windows           | [%drive%]:\Program Files\IBM\WebSphere\AppServer\profiles\RTCGW_Profile[1,2,...] |
| For Sametime Gateway upgrade:  
If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:  
[%drive%]:\Program Files\IBM\WebSphere\AppServer\profiles\RTCGW_Profile[1,2,...] |
<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
<tbody>
<tr>
<td>stgw_server_root</td>
<td>AIX</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/UserData/STgateway/[profile name]</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\STgateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
<tbody>
<tr>
<td>stADV_profile_root</td>
<td>All platforms</td>
<td>Primary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>app_server_root</em>profiles/STADVVPNProfile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secondary node</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>app_server_root</em>profiles/STADVSNProfile</td>
</tr>
</tbody>
</table>
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
5 Technology Park Drive
Westford Technology Park
Westford, MA 01886
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,
modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

### Trademarks

These terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
AIX
DB2
DB2 Universal Database Domino
Domino
Domino Designer
Domino Directory
i5/OS
Lotus
Lotus Notes
Notes
OS/400
Sametime
WebSphere

AOL is a registered trademark of AOL LLC in the United States, other countries, or both.

AOL Instant Messenger is a trademark of AOL LLC in the United States, other countries, or both.

Google Talk is a trademark of Google, Inc, in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.