Sametime
Version 8.5.2

IBM Sametime 8.5.2
Installation, Migration, and Configuration Guide
Note
Before using this information and the product it supports, read the information in “Notices” on page 1693.

Edition notice
First edition (June 2011)
This edition applies to version 8.5.2 of IBM Sametime (program number 5724-J23) and to all subsequent releases and modifications until otherwise indicated in new editions.
© Copyright IBM Corporation 1996, 2011.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

Chapter 1. Overview ........................................ 1
  Accessibility features for Sametime ......................... 1
  What's new in this release? ................................ 2
  What is Sametime? ........................................ 5
    Sametime server architecture ............................. 8
    Sametime System Console ................................ 9
    Sametime Community Server ............................... 10
    Sametime Proxy Server .................................. 10
    Sametime Media Manager .................................. 10
    Sametime Bandwidth Manager .............................. 11
    Sametime TURN Server ................................... 15
    Sametime Meeting Server ................................ 15
    Sametime Gateway ......................................... 16
    Sametime clients ......................................... 18
  PDF library ................................................ 41
  Glossary .................................................. 41

Chapter 2. Planning ........................................ 51
  Skills needed for Sametime administration ................ 51
  Readme .................................................. 53
  System requirements ....................................... 53
  Resources for IBM Sametime Standard and
  Sametime Entry users ....................................... 53
  Downloading Sametime files for installation ............ 53
    Using Passport Advantage to download IBM products .. 56
  Supporting IPv6 addressing in a Sametime deployment .. 60
    Supporting IPv4, IPv6, or both protocols .................. 61
    Enabling support for IPv6 ................................ 62
  Ports used by Sametime servers ............................. 68
  Finding ports for WebSphere Application
  Server-based applications .............................. 78
  Planning deployments with the Sametime Standard
  features you want ....................................... 78
  Deploying instant messaging and presence only .......... 78
  Deploying instant messaging and meetings ................ 79
  Deploying instant messaging, meetings, and web clients .... 79
  Deploying instant messaging, meetings, web clients, audio, and video .... 80
  Deploying instant messaging to external
  messaging communities .................................... 81
  Deploying meetings to external Internet users ......... 85
  Planning the size of your deployment on AIX, Linux, Solaris, or Windows ... 86
    Planning a small deployment on AIX, Linux, Solaris, and Windows ........ 87
    Clustering Sametime servers for high enterprise
    availability ............................................. 88
  Planning for an LDAP directory ......................... 93
  Planning a Community Server installation ............. 96
    Planning for the dedicated Lotus Domino server ....... 97
    Deploying a stand-alone Community Server Mux ....... 98
  Planning a Sametime Media Manager installation
  on Linux or Windows ..................................... 102
    Audio and video considerations ......................... 102
  Planning a Bandwidth Manager installation ............ 105
    Modeling your network topology ......................... 107
  Planning a Sametime TURN Server installation ......... 116
    TURN Server topologies ................................ 116
    Port allocations for NAT traversal ....................... 117
    NAT traversal terms .................................... 118
  Planning for a Sametime Meeting Server installation ... 119
  Planning a Sametime Gateway installation ............ 120
  Planning for migration from an earlier release .......... 123
    Planning server upgrades ................................ 123
    Planning for a mixed-release server environment .... 125
    Planning client upgrades ................................ 126
  Planning for a mixed-license environment of
  Sametime Entry, Sametime Standard, and
  Sametime Advanced servers ................................ 127

Chapter 3. Installing ..................................... 129
  Installing on AIX, Linux, Solaris, and Windows .......... 129
    Installing DB2 on Linux or Windows ...................... 129
  Installing the Sametime System Console .................. 134
  Connecting to an LDAP server ................................ 143
  Installing a Sametime Community Server and
  supporting software ...................................... 154
  Installing a Sametime Proxy Server ....................... 232
  Installing a Sametime Media Manager on Linux or
  Windows .................................................. 258
  Installing a Sametime Bandwidth Manager ............... 320
  Installing Sametime TURN Server ........................ 384
  Installing a Lotus SIP Edge Proxy Server ............... 394
  Installing a Sametime Meeting Server ................... 415
  Installing a Sametime Gateway server .................... 456
  Installing the WebSphere Application Server
  Update Installer ........................................ 575
  Starting and stopping servers in a Sametime
  deployment ............................................... 581
  Uninstalling ............................................. 601
  Installing on IBM i ...................................... 642
    Preparing to install Sametime on IBM i ................ 642
  Installing the Sametime System Console on IBM i .... 644
  Installing a Sametime Community Server and
  supporting software (IBM i) ............................. 663
  Installing a Sametime Proxy Server on IBM i .......... 747
  Installing a Sametime Meeting Server on IBM i ....... 772
  Installing a Sametime Gateway server on IBM i ....... 814
  Installing the WebSphere Application Server
  Update Installer on IBM i ................................ 914
  Starting and stopping servers in a Sametime
  deployment on IBM i ...................................... 917
  Uninstalling on IBM i .................................... 929
  Deploying the Sametime client to users ................... 968
Chapter 1. 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
  - 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 1551. 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 (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 TCSP adapter and optionally an external TCSP 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 1. 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 2. 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>

### Related concepts

“Links to other sites” on page 1666

Links are defined as properties of the sites they connect. A link can be created, configured, or modified from the site configuration screen of either of the sites that it connects within the network managed by IBM Sametime Bandwidth Manager.

### Related tasks

“Configuring sites” on page 1663

In a network managed by IBM Sametime Bandwidth Manager, sites are configured with properties whose settings help determine the bandwidth used for audio and video calls.

### 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” on page 1670.

**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.

Related tasks

“Configuring call rate policies” on page 1667
In an IBM Sametime Bandwidth Manager deployment, you can define call rates to be used during periods of normal utilization, and call rates to be used during periods of peak utilization. Combine these call rates with different classes of users and different locations to create call rate policies.

“Configuring groups for Sametime Bandwidth Manager” on page 1672
Call rate policies can be applied to either endpoints, or to users, within network managed by IBM Sametime Bandwidth Manager. If you choose to use groups, they can be Sametime user groups, groups created specifically for use with bandwidth management, or a mixture of the two.

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 119
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 3. Presence 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 Notes</td>
<td>Embedded Connect</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
<td>Web</td>
</tr>
<tr>
<td>Presence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3. 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></td>
<td></td>
<td>x</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>x</td>
<td>x</td>
<td></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>x</td>
</tr>
<tr>
<td>Selective do not disturb/privacy lists</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></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 3. 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></td>
<td></td>
<td>x</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>x</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4. 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</td>
<td>Embedded</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</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>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Anonymous or “Guest Access”</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</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 4. Instant Messaging feature comparison (continued)

<table>
<thead>
<tr>
<th>Type ahead</th>
<th>Contact Search / Quick Find</th>
<th>Primary Contacts View</th>
<th>Frequent Contacts View</th>
<th>Recent Contacts View</th>
<th>Initiate chats with users not in contact list</th>
<th>User created personal groups and nested groups</th>
<th>Administrator created public contact list groups</th>
<th>Contact List Sorting Options</th>
<th>Contact list scrubber to remove infrequently used contacts</th>
<th>Automatically send email if contact is offline</th>
<th>Secure One-on-one text chat</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>
</tr>
<tr>
<td>Feature</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Multi-party text chat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice and Video</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Integration</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Announcements (to selected users and groups)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></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></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabbed Chat Windows</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display user information and photo in chat window</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display chat partner status in chat window</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rich text formatting</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></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>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emoticon Palettes</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Capture Tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Screen Share</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfer</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4. 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>
<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>
<td>x</td>
</tr>
<tr>
<td>Spell Check</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>Time and Date Stamps</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>Chat History</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 populate recent chat history in chat window</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>Off the record mode / disable transcript save</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>Print Transcript</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 transcript as email</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>Zero-download browser chat client</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 5. Meetings 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>
<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>
<td></td>
</tr>
<tr>
<td>Meetings</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>Reservationless, persistent meeting rooms, available 24 x 7 for participant use</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 Description</td>
<td>IBM</td>
<td>Other 1</td>
<td>Other 2</td>
<td>Other 3</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>Instantly create a Sametime Meeting Room from Sametime Connect Client or browser based Meeting Room Center</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</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></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign and enter meeting rooms from Notes, Outlook invitations</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View your calendar from Sametime Connect with one click access to meeting rooms</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One click access to Meeting rooms you own</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One click access to your recently used Meeting Rooms</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</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>Find Meeting Rooms by owner or room name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set passwords and hide meeting rooms</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous or &quot;Guest Access&quot;</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></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></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control who else can manage room permissions</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite users to meeting by drag and drop from contact list</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser users can participate in meetings without any client download</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photo and list view of attendees</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 5. Meetings feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>IBM Sametime</th>
<th>IBM Lotus Sametime</th>
<th>IBM Lotus Sametime</th>
<th>IBM Lotus Sametime</th>
</tr>
</thead>
<tbody>
<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>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>x</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>x</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>x</td>
</tr>
<tr>
<td>Local, background, high-fidelity file conversion</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table 5. Meetings feature comparison (continued)**

<p>| Control whether users can download documents from meeting library | x | x | x | x |
| Fit to screen view | x | x | x | x |
| Edge-to-edge full screen view | x | x | x | x |
| Presenter tools (highlighter, pointer) | x | x |
| View slide thumbnails during presentation | x | x |
| Create Polls Immediately or Store for Future Use | x | x |
| Immediately share poll results with participants | x | x |
| Screen Capture tool | x | x |
| Paste an item from your clipboard to the meeting library | x | x |
| Share URL’s | x | x | x | x |
| Raise Hand | x | x | x |
| Initiate private chat | x | x | x | x |
| Group discussion | x | x | x | x |</p>
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>IBM Sametime</th>
<th>Microsoft Teams</th>
<th>Zoom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emoticon Support</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Breakout sessions and simultaneously participate in multiple meetings</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Join Call function to enter audio portion of meeting</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Client-side meeting recordings in standard file formats</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Control whether users can record a meeting</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Conferencing Integration/Voice and Video</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>User re-arrangeable interface</td>
<td>x</td>
<td></td>
<td>x</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>
</tr>
<tr>
<td>Detailed Meeting reports</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Historical Meeting Reports</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Table 5. 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>x</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>x</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>x</td>
</tr>
<tr>
<td>Built in failover and clustering</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Zero Download browser meetings client</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Table 6. Voice and Video feature comparison

| Offering | Entry | Entry | Standard | Standard | Standard/Advanced | Advanced | Advanced |
|----------|-------|-------|----------|----------|-------------------|----------|
| Client   | Notes | Connect | Connect | Web | Mobile | Connect | Web |
| Voice and Video | Embedded |         |          |     |        |          |    |
Table 6. Voice and Video feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Vendor 1</th>
<th>Vendor 2</th>
<th>Vendor 3</th>
</tr>
</thead>
<tbody>
<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>x</td>
<td>x</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>x</td>
<td>x</td>
</tr>
<tr>
<td>VoIP and video chats with multiple participants</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>New Administrative controls over the video experience (size, bitrate, quality, and so on)</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Table 6. 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/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>
</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>
</tr>
<tr>
<td>Telephony Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7. 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/Advanced</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
</tr>
</tbody>
</table>

Notes: 
- x: Available
- xx: Not available
Table 7. Community Collaboration feature comparison (continued)

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>IBM</th>
<th>Others</th>
<th>32 Bit</th>
<th>64 Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange presence and chat with Microsoft OCS users through the connectors built into the Sametime Gateway</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Broadcast Community Channels</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Skill Tap</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Polls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Chat</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Announcements</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create FAQs from Broadcast community content</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Persistent Group Chat</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Chats history stored on the server</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Ability to store and share files with others</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

IBM Sametime: Installation, Migration, and Configuration Guide
Table 7. 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>
</tr>
</thead>
<tbody>
<tr>
<td>swarming tools - notifications triggered by keywords or number of participants - drive real time use</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Create FAQs from Persistent Group Chat content</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8. Mobile Access 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</td>
<td>Connect</td>
<td>Connect</td>
<td>Web</td>
<td>Mobile</td>
<td>Connect</td>
<td>Web</td>
</tr>
<tr>
<td>Mobile Access</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></td>
<td>x</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>x</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>x</td>
</tr>
</tbody>
</table>
**Table 8. 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>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple iPhone and iPod Touch (browser)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 9. 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>Client Embedded Connect Connect Web Mobile Connect Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications Enabled Business Processes</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDKs and Toolkits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephony Conferencing Service Provider Interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable Branding Area</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible plug-in model and resource area</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible toolbars, icons and right click menus</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web client customization via style sheets</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Web 2.0 APIs</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>WebSphere Portal</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Table 9. Communications Enabled Business Processes feature comparison (continued)

<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>
</tbody>
</table>
Table 10. Administration and Security feature comparison

<table>
<thead>
<tr>
<th>Service</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>Client Embedded Connect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration and Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sametime System Console</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Integrated Installation Manager</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central policy management of</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>features and user settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-provision client updates</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Serviceability Management</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Security and Encryption</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Chat monitoring and archiving</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related concepts

“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 127

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 11. 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 12. 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 127

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>
<tr>
<td>Features</td>
<td>Connect client</td>
<td>Web client</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<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 statistics 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 36

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 977
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 1005
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
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 (TCSPI) 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
conference by calling each participant. 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 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
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 2. 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 Readme 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.

Downloading Sametime files for installation

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:
   &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
   ```

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:
      &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:

```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
```

Using Passport Advantage to download IBM products

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:

**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.
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:db8:85a3:0:0:8a2e:0370:7334

You may see IPv6 addresses abbreviated, for example:
• 2001:db8:85a3:0:8a2e: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:

   ```
   eth0  Link encap:Ethernet  HWaddr 00:0F:1F:89:8F:D5
   inet addr:192.168.1.100  Bcast:140.171.243.255  Mask:255.255.254.0
   inet6 addr: fe80::20f:1fff:fe89:8fd5/64 Scope:Link
   UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
   RX packets:33386388  errors:0  dropped:0  overruns:0  frame:0
   TX packets:2947979  errors:0  dropped:0  overruns:0  carrier:0
   collisions:0  txqueuelen:1000
   RX bytes:2211978470 (2109.5 Mb)  TX bytes:380978644 (363.3 Mb)
   Base address:0xdf40  Memory:feae0000-feb00000
   lo   Link encap:Local Loopback
   inet addr:127.0.0.1  Mask:255.0.0.0
   inet6 addr: ::1/128 Scope:Host
   UP LOOPBACK RUNNING  MTU:16436  Metric:1
   RX packets:895  errors:0  dropped:0  overruns:0  frame:0
   TX packets:895  errors:0  dropped:0  overruns:0  carrier:0
   collisions:0  txqueuelen:0
   RX bytes:76527 (74.7 Kb)  TX bytes:76527 (74.7 Kb)
   ```

   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**.
Close the "Local Area Connection Properties" dialog box by clicking the Close button.

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.
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 13. Sametime System Console ports

<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>
<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 14. 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 15. 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 16. 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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>Alternate HTTP port (8088)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>This configuration enables the Sametime Community Server to support HTTP tunneling on port 80 by default following the server installation.</td>
</tr>
</tbody>
</table>
### Table 16. 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>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>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>
<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 17. 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>
Table 17. Community Services ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
</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.  
If the 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.  
**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. |
| 80           | If the 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.  
**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. |
### Table 17. Community Services ports (continued)

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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 8082.</td>
</tr>
</tbody>
</table>

### Table 18. Sametime Classic Meetings

<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1533, 8081</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). The Meeting Room client must establish connections with the Meeting Services on the Sametime Community Server (on default port 8081). 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>
<tr>
<td>554</td>
<td></td>
</tr>
</tbody>
</table>
### Sametime Media Manager

The following ports are used on the Sametime Media Manager.

**Table 19. 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 20. 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 21. 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 21. 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 22. 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 23. 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 23. 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 24. 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 STMediaServer 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>Sametime Media Manager</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.
If you plan a small installation of Sametime Entry for instant messaging and presence only and do not plan to migrate to an LDAP directory, you can install Sametime on a single server, as described in the article, Beginners Guide to Sametime Entry 8.5, published on the Sametime wiki.

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.
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 Sametime 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.

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 581

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 232
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 258
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 418
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 server. 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 92
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 197
You can add IBM Sametime Community servers to an existing cluster.

“Clustering Sametime Proxy Servers” on page 242
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 269
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 426
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.

“Installing Gateway servers in a cluster” on page 472
Complete these steps to install a cluster of Sametime Gateway servers in a network
deployment. A cluster is a group of application servers that are managed together
and participate in workload management. A network deployment is a group of nodes
administered by the same cell, and controlled by a Deployment Manager.

Installing Gateway servers in a cluster on IBM i
Complete these steps to install a cluster of Sametime Gateway servers in a network
deployment. A cluster is a group of application servers that are managed together
and participate in workload management. A network deployment is a group of nodes
administered by the same cell, and controlled by a Deployment Manager.

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 232
  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 258
  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 418
  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 232  
  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 258  
  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 418  
  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.
Related tasks
“Creating custom Java classes for searching the LDAP” on page 217
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.
“Upgrading policies from Release 8.5 or 8.5.1” on page 1219
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.

Related reference
“LDAP directory settings” on page 148
Find more details about LDAP settings for the guided activity, “Sametime prerequisite: Connecting to an LDAP server.”

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 88
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)

### Number of Community Services connections

- Each Sametime Community Server can service approximately 100,000 active connections.
- 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.
- 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).

**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 standalone 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 10
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 image. 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 \(150\text{ms end-to-end}\) is normally acceptable in interactive real-time audio video conferencing.

**Note:** As of release 8.5.2, encryption is supported in audio and video conferences.

**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**
- In this release, 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.
- Clients running this release of Sametime can only establish audio and video connections with clients running Release 8.5.1 or later.
- 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 who have not yet upgraded, do not use these new 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.

---

**Planning a Bandwidth Manager installation**

The IBM Sametime Bandwidth Manager works with Sametime Media Manager, controlling bandwidth used in audio and video calls that are handled by the media manager.

You can install the bandwidth manager on an existing Sametime Media Manager server, or on a separate computer. The bandwidth manager client is built into the Sametime Connect client, web client, and embedded client, so its features are installed automatically.

The bandwidth manager is a J2EE SIP application running on IBM WebSphere Application Server. The bandwidth manager communicates directly with the Sametime Media Manager’s SIP Proxy and Registrar component, using it to relay bandwidth constraints to clients using audio and video features. If the deployment additionally includes Sametime Unified Telephony, that application shares the same SIP Proxy and Registrar server to ensure that it can access bandwidth constraints as well.

The bandwidth manager can be installed on a shared server with other applications such as the Sametime Media Manager, or IBM DB2. This type of deployment is useful for purposes such as demos, pilots, or small businesses. Because it is hosted on WebSphere Application Server, the bandwidth manager can share the same instance that the Media Manager uses; however, since both the bandwidth manager and the media manager are SIP applications use the
WebSphere Integrated Solutions Console for management, you would have to resolve port conflicts (for example, by creating separate profiles or virtual host settings).

You can alternatively deploy the bandwidth manager on its own computer so that it does not share resources with other applications. Most production environments would benefit from this distributed approach due to increased reliability, improved performance, and simpler problem determination and system management. In a large-scale deployment, you can install multiple bandwidth managers and cluster them using WebSphere Application Server Network Deployment. A bandwidth manager cluster requires a dedicated Deployment Manager (unlike some other Sametime components, the bandwidth manager does not use the Sametime System Console as its Deployment Manager) and can include up to two instances of the bandwidth manager application. In a horizontal cluster you would deploy one Primary Node and one Secondary Node; in a vertical cluster you would deploy both instances on the same node.

Prerequisite components

The bandwidth manager works with the following components in a Sametime deployment, and requires that these components be deployed first:

- **DB2**
  The bandwidth manager requires DB2 UDB 9.5 or later, with the latest fix packs applied (use the same version used by other Sametime components in this release). You can use the same DB2 server that you install for other Sametime components (console, meeting server, gateway server). You will need DB2 instance owner and administrative credentials during bandwidth manager installation.

- **LDAP directory**
  The bandwidth manager requires an LDAP server to which it has administrative “read/write” access since it looks up, creates, and modifies both users and groups while applying bandwidth management policies. This LDAP server can be any supported LDAP server using the Virtual Member Manager through federated repositories in WebSphere Application Server; use the same LDAP server that is used by the rest of the Sametime deployment. Configuring the WebSphere Application Server LDAP directory for bandwidth manager requires a Bind DN that is a valid LDAP user with administrative privileges.

- **Sametime Media Manager**
  The bandwidth manager works directly with the media manager’s SIP Proxy and Registrar component (use Sametime 8.5.2 or later because the bandwidth manager is not supported in earlier releases). SIP is the only signaling mechanism for describing bandwidth required for a call. The SIP Proxy and Registrar server is configured (force-route) to pass all incoming signals to the bandwidth manager, and to pass outgoing signals from the bandwidth manager go to the intended destination.

- **WebSphere Application Server**
  The bandwidth manager requires WebSphere Application Server Network Deployment version 7.0.0.9 or later (use the same version used by other Sametime components in this release). For simple deployments, you can install the bandwidth manager on the same instance of WebSphere Application Server used for the media manager. If you install the bandwidth manager on the same server as other applications, you should define a separate WebSphere Application Server profile for the bandwidth manager (although virtual hosts may also be used). The WebSphere Application Server must also have Virtual
Member Manager (VMM) installed and enabled, with global administrative and application security enabled for VMM to function properly (although individual application security may be selectively disabled). The WebSphere administrative credentials will be required for the bandwidth manager installation.

**Modeling your network topology**

The first step towards configuring IBM Sametime Bandwidth Manager is to model your network topology. By understanding your network, and the locations that are connected on the network, you can identify the bandwidth bottlenecks where bandwidth constraints are wanted. In this way, you can plan the sites and links that will enable you to place constraints on bandwidth use.

**About this task**

The Sametime Bandwidth Manager models networks using sites and links:

- A *site* represents a physical location on the corporate network, defined by a set of IP ranges. A site can represent an office location, a building, a campus, or even an entire city. The bandwidth manager uses the IP ranges defined for each site to associate endpoints with the site where they are located. This method assumes that IP ranges are unique within the enterprise's network.

- The dedicated line between the two sites is modeled as a direct *link* between these sites. Each link is uniquely defined by the two sites it connects.

**Bandwidth management for unmanaged calls**

Sametime endpoints can call a SIP endpoint not registered with the Sametime SIP Registrar. Such calls are referred to as “unmanaged calls” or calls to “unmanaged endpoints.”

Bandwidth Manager cannot determine the location of the called endpoint until the call is connected. When the call is connected, Bandwidth Manager can then apply bandwidth policies and constraints to future actions such as upgrading to video. The Bandwidth Manager enables an overall configuration policy for such calls that includes:

- Whether to allow such calls to proceed even if they exceed bandwidth capacity or have no route during ICE re-INVITE.

- The bandwidth allocation to apply to such calls
  - Allowing such calls to proceed also affects NAT-traversed calls, even if they are “managed calls” in that initial IP addresses are found for both endpoints.

Bandwidth usage is configured for combinations of sites and links. Modeling your network topology helps you gain a clear overview of the sites on your network, so you can configure the allowable bandwidth and call routing values for the audio and video traffic that passes between them.

**Procedure**

To optimize bandwidth management, you must understand your organization’s network and usage needs. For best results, model your network and settings on paper before you attempt to configure them in the bandwidth manager, by completing the following steps:

1. Map your network out on paper (if possible, use an existing network map as a starting point).
Visualizing the network with a map makes it easier to identify the sites and links you should configure.

2. Define the network’s sites.
   Sites will normally correlate with buildings or cities. The simplest way to determine what should constitute a site for your enterprise is to first identify the bandwidth bottlenecks on your enterprise network. Typically, these will be places where network traffic leaves a building or campus and travels to another building or campus through a wide-area connection. These are the points where you want to control and constrain bandwidth use, so they should determine the sites you create.

3. Define the network’s links.
   A link is a connection between two sites.

4. Define the groups to which call rates will be applied.
   A group consists of a particular class of users and endpoints (such as meeting rooms); for example, high-priority users will probably be allocated a greater amount of bandwidth during calls.

5. Define the network’s call rates.
   A call rate is a policy setting that determines the amount of bandwidth allocated for an audio or video call on a particular link. Call rates are applied to groups of users.

6. Define the network’s reflectors if they are used.
   Reflectors are used to assist in firewall and NAT traversal. Defining reflectors enables Bandwidth Manager to more accurately calculate call routes.

What to do next

Once you have a visual model of your network components plus a clear understanding of the call rates in effect and the different classes of user, you are ready to begin “Configuring Sametime Bandwidth Manager” on page 1661.

Network topology examples

When modeling a network managed by IBM Sametime Bandwidth Manager, it may be helpful to review these examples of different types of networks.

Example 1: Leased lines:

Illustration of a leased-line network managed by IBM Sametime Bandwidth Manager. This example shows how you can model the simplest possible type of network, consisting of only two locations connected through leased lines.

The following figure shows a simple network consisting of two locations connected through leased lines:
If you replace specific users and devices with sites and then connect the sites with links, the resulting network topology model looks like this:

At call setup time, the bandwidth manager figures out the route taken by the media through the modeled network topology, and allocates bandwidth as appropriate along the way. For example, for a call between an endpoint in Site A and an endpoint in Site B, different amounts of bandwidth can be allocated for Site A, for the link between the two sites, and for Site B. The amount of bandwidth allocated is determined by the settings configured for each of the sites and the link connecting them.

Example 2: Clouds:

Illustration of a cloud-based network managed by IBM Sametime Bandwidth Manager. This example shows how you can model a network containing sites that are connected through any-to-any clouds, rather than dedicated links.

Cloud sites offer the following advantages:
- Coupled with the Distance metric, you can see the actual routes that calls take when there are multiple route possibilities.
- They provide an anchor for describing virtual links if physical link sharing is used at your site.

Many common scenarios involve multiple sites that are connected through any-to-any clouds (for instance, MPLS networks). The following figure shows a scenario where 3 sites are connected through a common MPLS (Multiprotocol Label Switching) network:
Each of the sites is represented in the topology model and is defined by a set of IP ranges. In addition, the MPLS cloud is introduced as a separate network in the topology. The WAN access links in each site are modeled as links between that site and the shared cloud. The resulting topology model looks as follows:

Note: Clouds differ from sites in the following three ways:
- They do not have any IP ranges associated with them.
- As a result, they cannot have any endpoints associated with them.
- They do not have any bandwidth constraints associated with them.

Example 3: Virtual circuits between sites:

Illustration of a network, managed by IBM Sametime Bandwidth Manager, that uses virtual circuits (for example, using frame relay, ATM, or VPN technology). In this example, multiple virtual circuits can share the same physical link.

A typical scenario consists of a number of sites (buildings or campus locations) connected through virtual circuits that are routed through any-to-any clouds, as shown in the following figure:
In this scenario, multiple VPN circuits may use the same physical access circuit (for example, a connection to the internet). When modeling VPN circuits, you must do the following:

1. Model the physical links that will carry the VPN circuits. In this example, you must model three physical circuits—one for each site—to the Internet. These physical links will have bandwidth pools associated with them that model the capacity of the physical circuits.

2. Model the VPN links between the various sites as you would any other link between sites. Since they are virtual links, these links do not have any bandwidth constraints of their own; instead, they inherit the bandwidth constraints of the physical links they’re associated with. Administrators model this association by indicating which physical link is used to carry the virtual link.

In summary, the bandwidth constraint of the shared access line is modeled by a single bandwidth pool that is shared by multiple virtual circuits as shown in the following diagram:
Setting the nominal VPN link capacity

In addition to modeling the physical constraints of access links, you may also want to separately constrain how much bandwidth each individual VPN link can use. This prevents any one VPN link from using all of the physical link’s capacity and starving the other VPN links sharing the same circuit. You can set this restriction by specifying the “nominal” VPN link capacity as a percentage of the maximum capacity of the physical link. For example, nominal VPN link capacity may be 80% of the physical capacity, meaning that at least 20% of the physical link capacity is available for other VPN links. By default, the nominal link capacity for all VPN links will be set to 100%, meaning there is no restriction on how much physical bandwidth any one VPN link can use.

Example 4: Mobile users and home users with VPN access:

Illustration of a network managed by IBM Sametime Bandwidth Manager where mobile users and home users access a site using VPN connections.

In this scenario, home users and mobile users establish VPN tunnels to an on-premise VPN concentrator across the internet. The VPN concentrator physically resides in Site A and is accessible from the internet through a bandwidth-constrained access link as shown in the following figure:

The home users have both a private IP address (192.168.1.100 for User 1) and a public IP address (1.1.1.1 for User 1). However, they also have a VPN IP address (10.1.1.10 for User 1). This VPN IP address is associated with the network adapter representing the VPN tunnel, and typically assigned by a DHCP server contacted by the VPN concentrator. For purposes of bandwidth management, only the VPN IP address is relevant.

Modeling this scenario contains two parts:

1. Modeling the sites and links.
2. Modeling the bandwidth constraints.

Modeling the sites and links

First model the sites and links by following these steps:

1. Model the internet (representing home users and mobile users) as a site.
2. Model the VPN concentrator as a site. Site A physically contains the VPN concentrator so in this model, it is labelled Site A.
3. Model the link between the VPN concentrator (Site A) and the internet.
4. Model a VPN site for home users and mobile users.
While home users and mobile users reside on the internet, they cannot actually be associated with the internet site, since the act of establishing a VPN connection typically disables direct internet connectivity. To represent connections from those users, use a separate VPN site instead of the Internet site.

5. Because the VPN concentrator sits in Site A, model a connection between the VPN Site and Site A (the VPN concentrator).

**Modeling the bandwidth constraints**

After modeling the sites and links, model the bandwidth constraints.

1. Model the bandwidth constraint for VPN connections.
   - Because of the tunneled nature of VPN connections, all VPN calls are routed through the VPN concentrator, even calls between two home users (in this example, VPN User 1 and VPN User 2). To correctly model the fact that calls between VPN users require bandwidth on the internet access link, the bandwidth constraint of that link must be associated with the VPN Site itself, rather than with the link between the VPN Site and the user's site.

2. Model the VPN Site as requiring double bandwidth allocation for calls.
   - Calls between two different VPN users traverse the internet-VPN access link twice (once heading towards the VPN concentrator and then a second time back from it. This behavior means that the VPN Site needs to be modeled as a special type of site that requires double bandwidth allocation for calls. In the diagram for the model, the VPN site is shown using concentric circles to indicate its special nature.

3. Make the link between the VPN Site and Site A have unlimited bandwidth.
   - The connection between the VPN Site and Site A does not need to be bandwidth-constrained because the VPN concentrator physically sits within Site A. Traffic within a physical site does not cause bottlenecks and does not require bandwidth management.

**The topology model**

The following figure shows the resulting topology model:

![Topology Diagram](attachment:topology_diagram.png)

**Example 5: NAT Traversal:**

Illustration of a network managed by IBM Sametime Bandwidth Manager where NAT Traversal is in use.
Remote user scenarios

Sametime supports firewall and NAT traversal for the media exchange path for clients. Scenarios for both remote and internally-firewalled users are also supported by the Bandwidth Manager. The Bandwidth Manager supports the following calling scenarios with remote users:
- A remote user (Home user or Business partner) calling another remote user
- A remote user calling users in the enterprise
- A remote user calling users working behind an internal firewall in the enterprise

Internal firewall scenarios

The Bandwidth Manager supports the following calling scenarios with users working behind an internal firewall:
- Internal user calling users in the enterprise
- Internal user calling other users located behind the same internal firewall
- Internal user calling remote users

In this deployment example, administrative policies prevent direct media connections between remote users (Home User 1 and Business Partner 2) and any internal users. To support call scenarios between remote users and internal users, a reflector is deployed in the DMZ to relay the media streams. Additionally, users in Site B (User 5 and User 6) are firewalled from other users in the enterprise and direct media connections are not allowed. To connect with other users, Site B users will require use of the internal reflector. In this scenario where a remote user wants to call an internally firewalled user, the call path requires two reflectors. Therefore, the expected call route between User 6 and Business Partner 3 would be as follows:
Based on these examples, the reflector policies for this enterprise could be summarized as follows:

<table>
<thead>
<tr>
<th>Endpoint Site</th>
<th>Reflector Assigned to Endpoint</th>
<th>Remote Site Accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site B</td>
<td>Internal Reflector</td>
<td>Any other Site</td>
</tr>
<tr>
<td>Internet</td>
<td>DMZ Reflector</td>
<td>Any other Site</td>
</tr>
</tbody>
</table>

If you replace specific users and devices with sites and then connect the sites with links, the resulting network topology model looks like this:

Sametime features that support NAT Traversal

To enable NAT Traversal support, Sametime uses the following features to model the enterprise network and allocate bandwidth to calls accurately.

- **Sametime Connect endpoints use ICE protocol to determine the best media path for each call.**
  
  For discovering the correct endpoints (IP addresses) of clients, the Bandwidth Manager uses several techniques, including inspecting the ICE candidates that are carried in the underlying SIP flows. Part of the ICE protocol is the usage of SIP re-INVITEs by the clients, which serve to inform the Bandwidth Manager about the IP addresses that were actually used for a call (in “c=” SDP attribute). These re-INVITEs enable the Bandwidth Manager to correct the predicted call path if the predicted path was not correct the first time. Bandwidth can be modified better by subsequent re-INVITEs for the same call (upgrade to video, for example).
- **Reflectors in the deployment support call scenarios where a direct connection does not exist.**

  Reflectors are transit sites on a given call's route, for example: Caller site -> Reflector1 site -> Reflector2 site -> Callee site. The existence of reflectors affects route calculation and distance. For accurate route calculation, the Bandwidth Manager needs to know if there are any reflectors used. In order to accurately reflect the route transitions that a given media path takes, the Bandwidth Manager enables the configuration of Reflector Policies.

---

### Planning a Sametime TURN Server installation

The IBM Sametime TURN Server works with Sametime Media Manager, enabling clients to communicate across a NAT or firewall during a multimedia session.

When planning a Sametime audio/video deployment, ask yourself the following questions and then use the answers to help determine the placement of the Sametime Media Server and the TURN server:

- **Do I want to provide audio/video connections between internal (intranet) and external (extranet) users?**

  The Sametime TURN server must be reachable by all clients, as well as by all Sametime servers for which the TURN server provides services. This 'reachability' requirement may dictate that the Sametime Media Server and the TURN server be installed in DMZ area of the enterprise network.

  **Note:** In DMZ deployments, both internal and external clients must be able to resolve the name of the Sametime TURN server to the “proper” IP address, so that your network architecture may direct different IP addresses for internal and external clients. IBM require that you configure the TURN server's identity with a Fully Qualified Domain Name (FQDN), and that you use Domain Name Service (DNS) to provide clients with the proper IP address for their environment.

- **Is my deployment internal-only on a server with a single network IP address?**

  If Sametime audio/video is used between internal users on a flat network (without the use of Network Address Translation), communication occurs directly between clients (“peer-to-peer”) and does not use the Sametime TURN server. If the Sametime TURN server is required due to NAT or heterogeneous network environments between users, you have to install the TURN server on the same subnetwork with the Media Server.

- **Do my clients have multiple IP addresses on multiple subnets?**

  If this is the case, you have to enable the Sametime NAT traversal feature, so the clients will perform the necessary connectivity checks and find a candidate pair on which the media can be sent. If Sametime audio/video is used between internal users on a flat network (without the use of Network Address Translation), communication occurs directly between clients (“peer-to-peer”), and the TURN server address can be set to 0.0.0.0 in SSC, to indicate that allocation of relayed address is not necessary.

---

### TURN Server topologies

There are multiple options for the network topology for the TURN Server.

This example shows a simple topology where multimedia connections can be established between IBM Sametime clients using the Sametime TURN server and ICE:
Port allocations for NAT traversal

The Sametime Connect client will dynamically allocate UDP ports as a result of ICE negotiation.

Ephemeral ports are allocated on clients and are assigned by the client’s operating system. Ephemeral ports are usually in the range of 1024-5000 and are dynamically re-allocated by the operating system as needed. Proper function of the Sametime NAT traversal feature requires open access to UDP ports on both the TURN server and the Media Manager’s Packet Switcher.

Note: UDP is the preferred protocol; TCP should be used only if UDP is not available (for example, due to company policy).

For more information on ports used by a Sametime deployment, see “Ports used by Sametime servers” on page 68.

The following table lists the ports used for NAT traversal on the Sametime TURN Server:

Table 26. Sametime TURN Server ports opened for NAT traversal

<table>
<thead>
<tr>
<th>Default port</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>3478</td>
<td>UDP or TCP, for basic STUN/TURN protocol handling. This port should be reachable by internal and external clients.</td>
</tr>
<tr>
<td>49152 - 65535</td>
<td>UDP, for dynamically allocated packet relay.</td>
</tr>
</tbody>
</table>

The following table lists the ports opened between the Media Manager's Packet Switcher component (which functions as the MCU) and Sametime clients residing on the corporate intranet:
Table 27. Packet Switcher ports opened for internal clients

<table>
<thead>
<tr>
<th>Default port</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>39000</td>
<td>UDP, for audio when the Packet Switcher is operating in a single port mode.</td>
</tr>
<tr>
<td>40000</td>
<td>UDP, for video when the Packet Switcher is operating in a single port mode.</td>
</tr>
<tr>
<td>42000 - 43000</td>
<td>UDP, for audio when the Packet Switcher is operating in multiple ports mode (the default mode).</td>
</tr>
<tr>
<td>46000 – 47000</td>
<td>UDP, for video when the Packet Switcher is operating in multiple ports mode (the default mode).</td>
</tr>
</tbody>
</table>

It is strongly recommended that you use the default values for these ports. These port numbers must not be subject to third-party load balancing, packet rewriting (NAT/PAT), or other network-layer manipulation.

**NAT traversal terms**

When planning to deploy the IBM Sametime TURN Server, it may be helpful to review some terms related to NAT traversal.

**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.

**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.

**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

**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.

**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.

**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.

**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.

**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.

**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.

**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.

---

**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 8.5x 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.


Related concepts

“Sametime Meeting Server” on page 15
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.

Related tasks

“Installing a Sametime Meeting Server” on page 415
Follow the instructions for your operating system to install an IBM Sametime Meeting Server.

Planning a Sametime Gateway installation

Before you begin your installation, consider the size of your deployment, the DB2 database and LDAP server that you will connect to, ports in the firewalls that need to open, hardware requirements, and node names. Review this checklist to prepare for installation.

About this task

Collecting information about servers and ports now will make it easier to supply correct information during the Sametime Gateway installation.

Procedure

1. Read the Sizing Guide and deployment scenarios on the Sametime wiki and refer to the software and hardware requirements as you size your deployment.
2. Talk with the systems administrators in your company who oversee DB2, LDAP, and DNS servers about Sametime Gateway requirements. Make sure everyone in your organization knows that this product requires these services. A well-designed and well-thought out process makes the deployment of new software systems roll out smoother and faster.
3. Consult the network firewall administrator about requirements to open ports in the firewalls. Sametime Gateway is installed in the DMZ between the
internal and external firewalls. See the deployment scenario diagrams to understand the ports that need to be open:

<table>
<thead>
<tr>
<th>Port</th>
<th>Firewall</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1516</td>
<td>Internal</td>
<td>Port to each Sametime community server in the local Sametime community, allowing both inbound and outbound traffic between Sametime Gateway and each community server.</td>
</tr>
<tr>
<td>389 or 636</td>
<td>Internal</td>
<td>Port 389 or 636 (SSL) to LDAP server that services the local Sametime community. <strong>Note:</strong> Port 389 or 636 should be opened for all deployed nodes, including the SIP proxy.</td>
</tr>
<tr>
<td>50000</td>
<td>Internal</td>
<td>Port to DB2 server.</td>
</tr>
<tr>
<td>5269</td>
<td>External</td>
<td>Port to Google Talk and Jabber connections.</td>
</tr>
<tr>
<td>5061</td>
<td>External</td>
<td>Port to external Sametime or AOL communities.</td>
</tr>
<tr>
<td>5060</td>
<td>External</td>
<td>Port to external Sametime communities not using TLS/SSL.</td>
</tr>
<tr>
<td>53</td>
<td>External</td>
<td>Port to external DNS servers to resolve the fully qualified domain name of external community servers.</td>
</tr>
</tbody>
</table>

4. The Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example, the following commands should be able to resolve successfully:

```
nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

5. If you are installing a standalone deployment of Sametime Gateway, what machine will you use?

6. If you plan to configure a cluster, determine what machines and how many you will need before installing the Network Deployment:

<table>
<thead>
<tr>
<th>Node type</th>
<th>Number allowed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Manager</td>
<td>1</td>
<td>You can install the Deployment Manager on its own machine, or on the same machine with primary node and proxy servers.</td>
</tr>
</tbody>
</table>
### Node type

<table>
<thead>
<tr>
<th>Node type</th>
<th>Number allowed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary node</td>
<td>1</td>
<td>You can install the primary node on its own machine, or on the same machine with Deployment Manager and the proxy servers. You can install multiple server instances on each primary node.</td>
</tr>
<tr>
<td>Secondary node</td>
<td>n</td>
<td>Install the secondary node on its own machine, or on the same machine with proxy servers. You can install multiple server instances on each secondary node.</td>
</tr>
<tr>
<td>SIP proxy server</td>
<td>2</td>
<td>If you have a clustered deployment, you must install a SIP proxy server to connect to other Sametime communities, or AOL communities. The best practice is to install proxy servers on a separate machine to isolate the proxy processing from the Sametime Gateway cluster.</td>
</tr>
<tr>
<td>XMPP proxy server</td>
<td>1</td>
<td>If you have a clustered deployment, you must install an XMPP proxy server to connect to a Google Talk or Jabber community.</td>
</tr>
</tbody>
</table>

7. Determine the following items for the DB2 database:

<table>
<thead>
<tr>
<th>What You Need to Know</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database host name</td>
<td>For example: database.server.acme.com</td>
</tr>
<tr>
<td>Port used by the database server</td>
<td>The default port is 50000.</td>
</tr>
<tr>
<td>Name of the database</td>
<td>The default database name is STGW but you can change this by editing the database creation script.</td>
</tr>
<tr>
<td>DB2 application user ID and password</td>
<td>A database user ID that has permission to connect to the DB2 database and read or write records. This is normally the ID you created when you installed DB2.</td>
</tr>
<tr>
<td>DB2 schema owner ID and password</td>
<td>A database user ID for a user who has appropriate permission to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
</tbody>
</table>

8. Determine the Administrative security user ID and password. You are prompted for this ID and password during installation. Use these credentials to log into the Integrated Solutions Console (http://localhost:9060/ibm/console), the administrative interface to WebSphere Application Server.
9. Determine if you plan to connect to your LDAP server when you run the installation wizard, or later. If you require a client side certificate to securely connect to an LDAP server from the Sametime Gateway server, you must configure LDAP using the Integrated Solutions Console after installation. Otherwise, you can connect to your LDAP during the installation process. In either case, you will need this information about your LDAP:

<table>
<thead>
<tr>
<th>LDAP information needed for anonymous access</th>
<th>LDAP information needed for authenticated access</th>
</tr>
</thead>
<tbody>
<tr>
<td>• host name (or IP address)</td>
<td>• host name (or IP address)</td>
</tr>
<tr>
<td>• port</td>
<td>• port</td>
</tr>
<tr>
<td></td>
<td>• bind distinguished name and password</td>
</tr>
<tr>
<td></td>
<td>• base distinguished name (not required for Domino LDAP)</td>
</tr>
</tbody>
</table>

10. What are the node names for the Deployment Manager, primary node, proxy server node, and additional secondary nodes? The installation wizard provides a name that you can change if needed. Node names must be unique and cannot contain spaces or special characters.

11. What is the fully qualified host name or IP address of the Sametime Community Server in your local Sametime community?

12. How will you install Sametime Gateway? You can use an installation wizard, console mode, or silent installation.

   **Note:** If your server runs on IBM i and it is enabled for IPv6 addressing, you must install Sametime Gateway in console mode with input validation disabled, as noted in the installation instructions.

13. Download the installation images and either burn a CD or copy the install images to each machine where you plan to install Sametime Gateway.

14. Sketch a deployment diagram that shows where your load balancer, firewalls, Deployment Manager, primary node, secondary nodes, and proxy servers will be installed related to the hardware. List the node names and host names that you plan to use. Identify where you should check network connectivity and other environmental issues that may interfere with a smooth installation process.

---

**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**

Existing Sametime 8.5 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 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.

- 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 install to 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 client running a variety of releases.

- **Audio/video (A/V) interoperability between releases**
  
  - In this release, 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.
  
  - Clients running this release of Sametime can only establish audio and video connections with clients running Release 8.5.1 or later.
  
  - 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 who have not yet upgraded, do not use these new 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.
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 229

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.

“Disabling or enabling meetings on an IBM i Sametime Standard server” on page 744

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

**Related reference**

“Sametime offering features by client type” on page 18

The features available to users depend on the type of client they use and the Sametime offering installed on their home servers.
Chapter 3. 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 4, “Migrating and upgrading,” on page 1031
Migrate data from a previous version of Sametime and upgrade one or more servers to take advantage of the latest features.

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

© Copyright IBM Corp. 1996, 2011
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\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 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:

&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 --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. 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.

**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.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 129

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.
Linux: 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: 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
```

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 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:
  `! ( ) - . ? [ ] ` _ ` ~`
- **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. 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 584

Related tasks
“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 606
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
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.
   
   \[http://serverhostname.domain:port/ibm/console\]

   For example:
   
   \[http://sametime.example.com:8700/ibm/console\]
   \[https://sametime.example.com:8701/ibm/console\]

   **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`

   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. 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 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.

What to do next

“Connecting to an LDAP server” on page 143

Related tasks

“Starting the Sametime System Console” on page 582

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

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:

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 -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 `servername.domain` with the fully qualified host name of the Sametime System Console server.
   ```
   http://servername.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 93

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 582

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 28. Person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object class</strong></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><strong>LDAP user search base</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy ID for users and groups</strong></td>
<td>Specifies which ID to search for when the administrator selects User ID as the search criteria for managing policies. <strong>UUID</strong> 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.</td>
</tr>
<tr>
<td><strong>Display name</strong></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><strong>Similar name distinguisher</strong></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><strong>Email address</strong></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><strong>Home Sametime server</strong></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><strong>Membership attribute</strong></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 29. 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 &quot;Display Name&quot; 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>

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 30. 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>
</tbody>
</table>
Table 30. Group attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Starting and stopping the Deployment Manager on IBM i” on page 917
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Enabling encryption between Sametime and the LDAP server” on page 1435
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 588
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” on page 149
- “Base Distinguished Name and Filter for Searches” on page 150
- “Collect Person Settings” on page 151
- “Collect Group Settings” on page 153
**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 31. 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>
| 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 31. 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 32. 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 DN</strong></td>
<td></td>
<td>Sample Base distinguished name: <code>dc=example,dc=com</code></td>
</tr>
<tr>
<td>Search Base and Scope</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base Objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base object when searching for person entries:</td>
<td><code>DC=austin,DC=ibm,DC=com</code></td>
<td></td>
</tr>
<tr>
<td>Base object when searching for group entries:</td>
<td><code>DC=austin,DC=ibm,DC=com</code></td>
<td></td>
</tr>
<tr>
<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>
<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 33. 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>
<tr>
<td>Authentication</td>
<td>Allows the user to authenticate with more than one attribute of the user’s</td>
<td>Sample authentication attributes:&lt;br&gt;mail;cn&lt;br&gt;mail;cn;uid&lt;br&gt;Consider an LDAP person entry&lt;br&gt;containing the following attributes:&lt;br&gt;• mail: <a href="mailto:jlock@example.com">jlock@example.com</a>&lt;br&gt;• cn: James Lock&lt;br&gt;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.</td>
</tr>
<tr>
<td>Attributes</td>
<td>entry. Use any of these properties: mail, cn, or uid. The properties must</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be separated by a semicolon (;). Important: For the Meeting Server to work,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the first field of the Authentication attribute must be set to mail and it</td>
<td></td>
</tr>
<tr>
<td></td>
<td>must be listed first.</td>
<td></td>
</tr>
<tr>
<td>Search Attributes</td>
<td>Specifies the fields used for searching the directory for users. The fields</td>
<td>Sample search attributes: mail;cn;uid</td>
</tr>
<tr>
<td></td>
<td>must be separated by a semicolon (;).</td>
<td></td>
</tr>
<tr>
<td>Object Class</td>
<td>Individual users are represented by entries with a unique object class. Enter</td>
<td>The value is set automatically to a default value based on the type of LDAP directory detected.</td>
</tr>
<tr>
<td></td>
<td>the object class attribute used for people in the LDAP schema of the LDAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>directory in your environment. The name of the object class specified in this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>setting to the object class values of each entry to decide whether the entry</td>
<td></td>
</tr>
<tr>
<td>Person attributes</td>
<td>is a person or a group.</td>
<td></td>
</tr>
</tbody>
</table>
Table 33. Collect Person Settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy ID for users and groups</strong></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 <strong>Distinguished Name</strong> 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><strong>Display Name</strong></td>
<td>Displays a user’s name in Sametime user interfaces.</td>
<td>Sample display name: cn</td>
</tr>
<tr>
<td><strong>Similar name distinguisher</strong></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. 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>
<td></td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>Contains the user’s email address in the field.</td>
<td></td>
</tr>
<tr>
<td><strong>Home Sametime Server</strong></td>
<td>Specifies the name of the field within the LDAP person entries that contains the name of each user’s home Sametime server. If you have installed multiple Sametime servers, each user’s person entry in an LDAP directory must contain a field in which a user’s home server is specified. You can either: • Add a new field to the LDAP directory to store the name of each user’s home server. This field must be in the person entry of every Sametime user in the LDAP directory. • Use a field that exists in the person entries of each Sametime user, such as the email address.</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 34. Collect Group Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Class</td>
<td>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.</td>
<td>Microsoft Active Directory group&lt;br&gt;Netscape Directory groupOfUniqueNames&lt;br&gt;Microsoft Exchange 5.5 and Lotus Domino directories groupOfNames&lt;br&gt;SecureWay™ Directory groupOfUniqueNames</td>
</tr>
<tr>
<td>Group Attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td>Displays a group's name in Sametime user interfaces.</td>
<td>Sample display name:&lt;br&gt;cn</td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>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 &quot;description&quot; attribute contains descriptive information about a group. If a search on the name &quot;Marketing&quot; returns two group entries, the information contained in the description attribute (such as &quot;West region&quot; or &quot;East region&quot;) can be used to distinguish between the two groups.</td>
<td>Microsoft Exchange 5.5 Directory info&lt;br&gt;All other directories description</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. 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>
<td>member&lt;br&gt;uniquemember</td>
</tr>
</tbody>
</table>

Related tasks

“Sametime prerequisite: Connecting to an LDAP server” on page 144
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 4, “Migrating and upgrading,” on page 1031
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 1522
This section describes how to configure an IBM Sametime Community Server.

Related tasks
“Connecting to an LDAP server” on page 143
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.
   - **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 like:
     ```bash
     mount /dev/cdrom /cdrom
     ```
   - **Solaris**
     Mount the CD/DVD using a command like:
     ```bash
     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:
   ```bash
   ./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:
      ```java
      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 581
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><strong>Basics tab</strong></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security tab</th>
<th></th>
</tr>
</thead>
</table>

This field must be Primary Domino Directory.

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.
<table>
<thead>
<tr>
<th>Server document field</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>You complete this field during the Lotus Domino server installation. It contains the name of the Sametime administrator. If the name is incorrect, click the arrow to select a name from an address book.</td>
</tr>
<tr>
<td>Internet authentication</td>
<td>The default value is <em>Fewer name variations with higher security</em>, which is better for tighter security.</td>
</tr>
<tr>
<td></td>
<td>Select <em>More name variations with lower security</em> if you use Lotus Domino Directory 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 the list of trusted directories:</td>
</tr>
<tr>
<td></td>
<td>Sametime Development/Lotus Notes 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 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></td>
</tr>
<tr>
<td>Port</td>
<td>This field must be TCPIP. Use uppercase letters.</td>
</tr>
<tr>
<td>Protocol</td>
<td>This field must be TCP.</td>
</tr>
<tr>
<td>Net address</td>
<td>The fully qualified host name for the Lotus Domino server as known by the DNS server.</td>
</tr>
<tr>
<td></td>
<td>The value of this field must be the same as the fully qualified Internet host name on the Basics tab and the host name on the Internet Protocols-HTTP tab. The value cannot be a numeric IP address.</td>
</tr>
<tr>
<td></td>
<td>For example, <code>comptername.domain_name.com</code> or <code>stdom1.example.com</code>.</td>
</tr>
<tr>
<td>Ports - Internet Ports - Web tab</td>
<td></td>
</tr>
<tr>
<td>TCP/IP port number</td>
<td>This field must be 80.</td>
</tr>
<tr>
<td></td>
<td>Before you install the community server, the port number must be set to 80. The TCP/IP port number changes after installation to 8088 automatically if you enable HTTP tunneling.</td>
</tr>
<tr>
<td>TCP/IP port status</td>
<td>This field must be Enabled.</td>
</tr>
<tr>
<td>Server document field</td>
<td>Description and values</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Name &amp; password</td>
<td>This field must be Yes.</td>
</tr>
<tr>
<td>Anonymous</td>
<td>This field must be Yes.</td>
</tr>
<tr>
<td>Internet Protocols - HTTP tab</td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<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, computername.domain_name.com or stdom1.example.com.</td>
</tr>
<tr>
<td>Bind to host name</td>
<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>
<tr>
<td>Allow HTTP clients to browse databases</td>
<td>This field must be set to Yes for portals.</td>
</tr>
<tr>
<td>Home URL</td>
<td>This field is set to stcenter.nsf during Sametime installation.</td>
</tr>
<tr>
<td>DSAPI filter file names</td>
<td>If this field is set to NDOLEXTN (Lotus Domino offline services), remove the value and leave this field blank.</td>
</tr>
<tr>
<td>Internet Protocols - Domino Web Engine tab</td>
<td></td>
</tr>
<tr>
<td>Session authentication</td>
<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 single-server.</td>
</tr>
<tr>
<td>Web SSO configuration</td>
<td>This field is set to LtpaToken during Sametime installation.</td>
</tr>
<tr>
<td>Java servlet support</td>
<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 581
An IBM Sametime deployment is made of up 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 582
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 154

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:

   Explicit_IPv6_address  Fully_qualified_host_name  Short_name
   Explicit_IPv4_address  Fully_qualified_host_name  Short_name

   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:
   - 2001:0DB8:1:2:3:4:5:6  stsyscon.example.com  stsyscon
   - 192.0.2.10  stsyscon.example.com  stsyscon

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
```

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

Related tasks
“Mapping the system console’s host name when IPv4 and IPv6 are enabled” on page 166
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 164
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 582
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,O=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 593

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 164

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
   \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.
1. 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 be 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.

1. Save and close the "Server" document.
2. 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 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
   TCPIPV6=tcp,0,15,0
   tcpip_tcpipaddress=0,Domino_server's_IPv4_address
   TCPIPV6_tcpipaddress=0,Domino_server's_IPv6_address
   ports=tcnip,tcpiipv6

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 35. Accepted values for STLINKS_HOST

<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 36. 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 37. 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:
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:
   ```bash
   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:
#if [ -f /etc/SuSE-release ]; then
#    IBM_JAVA_OPTIONS=-Djava.net.preferIPv4Stack=true
#    export IBM_JAVA_OPTIONS
#fi

4. Save and close the file.
5. Restart the community server.

**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 98

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:
   ```ini
   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 93
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 582
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 machine 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.

VPMX_ASSUME_COMMUNITY_ISFUNC=1
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
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 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:DB8::32:42:54:6</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:29e66</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:DB8::32:42:54:6</td>
</tr>
<tr>
<td>IPv6 explicit address using double-colon notation</td>
<td>3ef0::bee7:994:29e66</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 193

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 195

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 88
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 nnotes.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 “Cluster Directory” and the file name “cldbdir.nsf” 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:
   \n   ST_COMMUNITY_ID=community_name
   \n   For example, the following value names the community sametime.example.com:
   \n   ST_COMMUNITY_ID=sametime.example.com
   \n4. 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 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 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.</td>
</tr>
<tr>
<td></td>
<td>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></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.</td>
</tr>
<tr>
<td></td>
<td><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.</td>
</tr>
<tr>
<td></td>
<td>This configuration enables the Sametime Community Server to support HTTP tunneling on port 80 by default following the server installation.</td>
</tr>
<tr>
<td>Alternate HTTP port (8088)</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 389</td>
<td>The Domino HTTP server listens for HTTPS connections on this port by default.</td>
</tr>
<tr>
<td>Port 443</td>
<td>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

<table>
<thead>
<tr>
<th>Port 9094</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 206 for a discussion on resolving access to this port.</td>
</tr>
</tbody>
</table>

### 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.  
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. |
| 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 | Purpose
--- | ---
Port 8082 | 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.

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:
   
   ```
   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:

```
[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:

```
[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.

**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. 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 **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, you must assign the "DistinguishedName" directory attribute to be the internal ID for Sametime users. Doing so guarantees that Active Directory returns the DistinguishedName attribute in the same case-sensitive and space-sensitive format. Allowing Sametime to use that consistent attribute for the internal userID prevents awareness problems caused by ambiguous internal userIDs.

**About this task**

If you do not assign the "DistinguishedName" directory 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.

**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.

**Mapping the user ID to a unique directory attribute:**

If you map the Sametime user ID to a unique LDAP directory attribute, 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, does not trigger a user ID change when a name changes.

**About this task**

Sametime provides the 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. RESOLVE mode migrates the VpUserInfo.nsf database, from the old user ID to the new user ID.

With this release, IBM Sametime uses the UUID LDAP attribute by default, which ensures ID uniqueness. The UUID for the LDAP directory type can be chosen for the Sametime user ID. Its value will never change.

- Lotus Domino LDAP: dominounid
- IBM Tivoli Directory Server: ibm-entryuuid
If you are upgrading from a previous release, you can map the Sametime user ID to an LDAP directory attribute that is unlikely to change.

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

You change the Sametime LDAP configuration to map the user ID to a directory attribute in the person entry that is not bound to change. This change eliminates the need for running the Name Change tool. The Sametime Community server stores contact and privacy lists in the vpuserinfo.nsf file. Name Change RESOLVE mode migrates that database, from the old user ID to the new user ID.

Note: The old name will still appear in the contact list for users that have previously added them.

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. In case you prefer to use an existing attribute instead of modifying the schema, choose an attribute that is not bound 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

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 lookup 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 is 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, "Mapping the user ID to a unique directory attribute."

- Create a CSV file with the RESOLVE mode indicated.
- Create a name change task.
- 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.

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 each and every user ID in the database against the directory, and replaces the old user ID with the directory user ID. 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.

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."

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."


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 217
   • "Running the name change utility in RESOLVE mode on IBM i" on page 732

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 213.

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 209
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 214.
   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.”
   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 217.

```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";

    // Other code...

}```
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++;
    }
  }
  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
 */
public static boolean isEscapedBinaryValue(String name)
{
    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)
```java
String filter = null;
if (isEscapedBinaryValue(name))
{
    // 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 multiplexor 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 213.

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
      ```

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++;
        }
    }
    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
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 \texttt{sn} specifies each user’s last name.
The LDAP directory attribute \texttt{givenName} specifies each user’s first name.

\textbf{Sample code}

This example takes values from the \texttt{sn} and \texttt{givenName} directory attributes and combines these values into a single display name in the format of \texttt{LastName, FirstName}.

\begin{verbatim}
public class StLdapCustomizedAttributes {

public static String displayName (String givenName, String sn)
{
    String result = sn + ", " + givenName;
    return result;
}

}
\end{verbatim}

\textbf{What to do next}

After writing your Java class, complete the tasks in this section to integrate it into the Sametime Community server.

\textit{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.

\textbf{About this task}

Follow these steps to add the class to the Sametime Community Server.

\textbf{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.

\textbf{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

\textit{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 214
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 1409

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. It's 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.

   ```ini
   [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
   ```
   

   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 127

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 229

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 18

The features available to users depend on the type of client they use and the Sametime offering installed on their home servers.
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 229
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 1626
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 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, 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.

Related concepts

“Configuring a Sametime Proxy Server” on page 1650
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 257
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 582
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.
   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”

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.
Linux: 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:
         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
```

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 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. 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

**Related tasks**

“Guided activity: Preparing to install a Sametime Proxy Server” on page 233

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 582

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 606

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.

**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:
   
   \[ \text{http://serverhostname.domain:port/stwebclient/index.jsp} \]
   
   Replace serverhostname.domain with your server name and add the port number. For example:
   
   \[ \text{http://stproxy1.example.com:9080/stwebclient/index.jsp} \]

   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.
     
     \[ \text{http://serverhostname.domain:8600.ibm/console} \]
     
     8600 is the default port when the Proxy Server is installed as a Cell Profile. For example:
     
     \[ \text{http://stproxy1.example.com:8600.ibm/console} \]

   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 584
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
     \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**
   
   ```bash
   ./IBMIM --launcher.ini silent-install.ini -input response_file -log log_file -acceptLicense
   ```

   **Windows**
   
   ```bash
   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.

   ```bash
   ./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 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.

**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 88

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.

#### Related tasks

“Registering a Sametime Proxy Server on IBM i with the Sametime System Console” on page 753

After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

#### 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 582

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_CONNETCTOR_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:
      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 40. 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>Cluster: 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 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 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
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:
      
      dscontrol service stop
   c. Set the sticky time with the following command:
      
      dscontrol port set `fullyqualifiedhostname`@portnumber stickytime numberofseconds

Where:

- `fullyqualifiedhostname` is the fully qualified host name of the server where IBM Load Balancer runs.
- `portnumber` is the port that will be affected by the new sticky time setting.
- `numberofseconds` 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.

   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.

**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 as a different 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](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 1655
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 582
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.

Linux: 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:
```
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 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**.

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 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. 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 259
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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Managing multiple Packet Switcher nodes in a cluster with the Sametime System Console” on page 320
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:

&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 SSCPPassword 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
     ```
   - **Windows**
     ```
     IBMIM --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.
```bash
./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 `servername.domain` with the fully qualified domain name of the server.
      
      `http://servername.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`
   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, disable IPv6 addressing on that server.

**About this task**

This task is only needed for Media Manager components installed on Windows 2008 server. The Media Manager does not support IPv6 addressing, even when IPv4 addressing is enabled at the same time. Windows 2008 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 88

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 582

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.
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 > Proxy Servers.
   b. In the “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:

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>
<thead>
<tr>
<th></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>
</tbody>
</table>
Table 41. Write down the port numbers used for these settings in every cluster member (continued)

<table>
<thead>
<tr>
<th></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:

Verify that the IBM WebSphere proxy server is listening on the correct ports and is not in conflict with the IBM Sametime server running on the same computer.

Before you begin

This task is only necessary when Sametime and WebSphere proxy server are running on the same computer.

About this task

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 proxy server:
   a. Click Servers > Server Types > WebSphere proxy servers.
   b. In the list of proxy servers, click the node’s WebSphere 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 server:
   a. Click Servers > Server Types > WebSphere proxy servers.
b. In the list of application servers, click the name of the Sametime 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

4. Decide whether the ports are in conflict:
   If you install a WebSphere Proxy Server on an existing Primary Node, the PROXY_SIP_ADDRESS and PROXY_SIPS_ADDRESS will be 5062 and 5063, respectively. Ports are in conflict if either of the following conditions is true:
   - The WebSphere proxy server is listening on ports other than 5062 (PROXY_SIP_ADDRESS) and 5063 (PROXY_SIPS_ADDRESS).
   - The Sametime server is listening on the same ports as the WebSphere proxy 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 to (for example, to 5061), and then click **OK**.
6. Use the Ports table to change the HTTP ports as follows:
   Although the HTTP and HTTPS ports will not be used by the Sametime server (so there will not be a conflict), you still need to make sure they are using the correct values.
a. Click on the HTTP link, change its setting (for example, to 80), and then click OK.
b. Click on the HTTPS link, change its setting (for example, to 443), and then click OK.

7. 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.
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.

Verifying ports for the WebSphere proxy server’s virtual host alias:

On the IBM WebSphere proxy server, verify that the ports specified for the virtual host alias are correct.

About this task

Verify that the virtual host table contains the correct entries for the WebSphere proxy server’s SIP ports, creating or modifying entries as needed.

Procedure

1. On the node where WebSphere proxy server is running, log in to the Integrated Solutions Console as the WebSphere administrator.
2. Click Environment > Virtual Hosts.
3. In the list of hosts, click default_host.
4. Click Host Aliases.
5. Verify the host for port 5060:
   a. If an entry exists for port 5060 and the host name or IP address for the WebSphere proxy server is correct, skip to step 6.
• If an entry exists for port 5060 but specifies an incorrect host name or IP address for the WebSphere proxy server, click Edit, update the entry with the correct information, and then click OK.
• If no entry exists for port 5060, click Add, enter 5060 as the port, leave the host name as *, and then click Apply.

6. Verify the host for port 5061:
• If an entry exists for port 5061 and the host name or IP address for the WebSphere proxy server is correct, skip to step 7.
• If an entry exists for port 5061 but specifies an incorrect host name or IP address for the WebSphere proxy server, click Edit, update the entry with the correct information, and then click OK.
• If no entry exists for port 5061, click Add, enter 5061 as the port, leave the host name as *, and then click Apply.

7. Save the changes by clicking the Save link in the "Messages" box at the top of the page.

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 a 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:
      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 42. 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>
</table>
| Load balancer: loadbal.example.com | Load balancer (Cluster address) | Load balancer (NFA): 192.0.2.15  
Cluster: st-cluster.example.com | Cluster: 192.0.2.0 |
| stconsole.example.com | Deployment Manager  
(Sametime System Console) | 192.0.2.3 |
| svr1.example.com | Primary Node  
(a Sametime server) | 192.0.2.4 |
| svr2.example.com | Secondary Node  
(a Sametime server) | 192.0.2.5 |

**Configuring 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:
   ```
   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 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
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 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:
     ```
     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:
   - **Open a command window on the load balancer server.**
   - **Start the load balancer’s Dispatcher process by clicking Start > Control
     Panel > Administrative Tools > Services. right-click IBM Dispatcher
     (ULB), and then click Start.**
   - **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.
   - **Start the executor function of the dispatcher:**
dscontrol executor start

e. Add the cluster to the service:
\texttt{dscontrol cluster add cluster's\_fully\_qualified\_host\_name}

where \texttt{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}

f. Add the cluster port:
\texttt{dscontrol port add cluster's\_fully\_qualified\_host\_name@port}

where \texttt{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:
\texttt{dscontrol server add cluster\_host@port@primary\_node}
\texttt{dscontrol server add cluster\_host@port@secondary\_node}

where:
- \texttt{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}
- \texttt{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:
\texttt{dscontrol executor add cluster's\_fully\_qualified\_host\_name}

where \texttt{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:
\texttt{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):
\texttt{dscontrol advisor start http 80}

k. Now you can stop the service:
\texttt{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 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 "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 88
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 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 582
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 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 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="wasproxy_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.  

Chapter 3. Installing  301
**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**
        ```sh
        ./startManager.sh
        ```
      - **Microsoft Windows**
        ```bat
        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:
           ```cl
           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 > Proxy Servers.
   b. In the "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 43. 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>
<tbody>
<tr>
<td></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.

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 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:

Verify that the IBM WebSphere proxy server is listening on the correct ports and is not in conflict with the IBM Sametime server running on the same computer.

Before you begin

This task is only necessary when Sametime and WebSphere proxy server are running on the same computer.

About this task

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 proxy server:
   a. Click **Servers > Server Types > WebSphere proxy servers**.
   b. In the list of proxy servers, click the node’s WebSphere 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 server:
   a. Click **Servers > Server Types > WebSphere proxy servers**.
   b. In the list of application servers, click the name of the Sametime 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

4. Decide whether the ports are in conflict:
   If you install a WebSphere Proxy Server on an existing Primary Node, the PROXY_SIP_ADDRESS and PROXY_SIPS_ADDRESS will be 5062 and 5063, respectively. Ports are in conflict if either of the following conditions is true:
   • The WebSphere proxy server is listening on ports other than 5062 (PROXY_SIP_ADDRESS) and 5063 (PROXY_SIPS_ADDRESS).
   • The Sametime server is listening on the same ports as the WebSphere proxy 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 to (for example, to 5061), and then click OK.

6. Use the Ports table to change the HTTP ports as follows:
   Although the HTTP and HTTPS ports will not be used by the Sametime server (so there will not be a conflict), you still need to make sure they are using the correct values.
   a. Click on the HTTP link, change its setting (for example, to 80), and then click OK.
   b. Click on the HTTPS link, change its setting (for example, to 443), and then click OK.

7. 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 a 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:
   \[\text{dm\_install\_root}/config/cells/cell\_name/nodes/node\_name/servers/server\_name\]
   For example:
   \[\text{config/cells/bassMediaCell1/nodes/bassMediaNode1/servers/STMediaServer}\]
2. Modify the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:
      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>
</table>
| Load balancer: loadbal.example.com | Load balancer (Cluster address) | Load balancer (NFA): 192.0.2.15  
Cluster: st-cluster.example.com | Cluster: 192.0.2.0 |
| stconsole.example.com | Deployment Manager (Sametime System Console) | 192.0.2.3 |
| svr1.example.com | Primary Node (a Sametime server) | 192.0.2.4 |

*Table 44. Sample host names and IP addresses for a Sametime cluster with IBM Load Balancer*
Table 44. 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>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 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 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 PREIFHC 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:
   
   \texttt{dscontrol server add \textit{cluster\_host@port@primary\_node}}
   
   \texttt{dscontrol server add \textit{cluster\_host@port@secondary\_node}}

   where:

   \begin{itemize}
   \item \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}
   \item \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}
   \end{itemize}

h. Now start the Load Balancer administration interface with the following command:
   
   \texttt{./lbadmin}

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

4. Continue configuring Load Balancer as follows:
   
   a. Add the cluster to the executor:
      
      \texttt{dscontrol executor add \textit{cluster\_fully\_qualified\_host\_name}}

      where \textit{cluster\_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}

   b. Start the manager:
      
      \texttt{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):
      
      \texttt{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:
   \texttt{dscontrol\ port\ set \textit{fully\_qualified\_host\_name}@port\_number\ stickytime\ number\_of\_seconds}
   \textbf{Where:}
   \begin{itemize}
   \item \textit{fully\_qualified\_host\_name} is the fully qualified host name of the server
     where IBM Load Balancer runs.
   \item \textit{port\_number} is the port that will be affected by the new sticky time setting.
   \item \textit{number\_of\_seconds} is the duration, in seconds, of the time that a client
     should "stick to" the specified port.
   \end{itemize}
   \textbf{For example:}
   \texttt{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 \textbf{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 \textbf{OK}.

\textit{Configuring IBM Load Balancer for the Conference Manager cluster (Windows):}

Configure IBM Load Balancer on a server running Microsoft Windows.

\textbf{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.

\textbf{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.

\textbf{Procedure}

1. Configure the nodes of the cluster.
   \textbf{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 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**.

**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 Bandwidth Manager**

The IBM Sametime Bandwidth Manager is not managed by the Sametime System Console, so you do not use the console to create a deployment plan before installation. Instead, the Bandwidth Manager uses its own installation program, which can install it on a server shared with other applications or on a dedicated server. You can install a single instance of the Bandwidth Manager, or a clustered deployment that includes a Deployment Manager and up to two instances of the Bandwidth Manager.

**About this task**

To ensure proper deployment of the Sametime Bandwidth Manager, follow the instructions in these tasks in the sequence shown here.

**Related tasks**

“Configuring Sametime Bandwidth Manager” on page 1661
Configure the bandwidth manager to control bandwidth usage within a network managed by IBM Sametime Bandwidth Manager, defining sites, links between them, call rates that control bandwidth utilization, and policies that apply the rates to various classes of user.

**Creating a DB2 database for the Bandwidth Manager**

On the IBM DB2 server, create a database to store information used by the IBM Sametime Bandwidth Manager.
Before you begin

You can use the DB2 server that you installed for use with the Sametime System Console, or any DB2 server running DB2 UDB 9.7 Fixpack db2_2.1.102.v20091026.1945 or later. The DB2 server must be installed and running before you attempt to create the Bandwidth Manager's database.

Procedure

1. On the DB2 server, open the DB2 Control Center.
2. Click Selected > Create Database > Standard.
3. In the Database Name field, type the database name, such as BWM_DATA. The name must correspond to the name assigned to the db2.connection.database property in the db2.connection.properties file.
4. Set the page size to 8K; otherwise the installation will fail. Click Next, and then click Next again.
5. On the "Region" screen, change the Code Set to UTF-8, change the Collating Sequence to UCA400_NO, and then click Finish to create the database.
6. Wait for the database creation to finish, confirm that the database was created correctly, and then click Close to exit the DB2 Control Center.

What to do next

Now that the database is ready, proceed to install Sametime Bandwidth Manager.

Installing a Sametime Bandwidth Manager server

Install IBM WebSphere Application Server and IBM Sametime Bandwidth Manager. You can install a single Bandwidth Manager, or create a clustered deployment containing up to two instances of the Bandwidth Manager.

About this task

Unlike other Sametime components, the Sametime Bandwidth Manager does not install with a deployment plan created on the Sametime System Console. Instead, you enter required information as you proceed through the installation program. After installation is complete, you configure and administer the Bandwidth Manager using the Integrated Solutions Console of the WebSphere Application Server instance hosting the Bandwidth Manager.

Installing a stand-alone Bandwidth Manager:

Install a single, stand-alone IBM Sametime Bandwidth Manager and connect to the bandwidth management database and the LDAP directory.

About this task

Use this method to install a single, stand-alone Bandwidth Manager that will not be federated into a cluster. If you anticipate adding another Bandwidth Manager later and want the option of creating a cluster, you should install it as a cluster now and just use a single node until you are ready to expand the deployment. For information on a clustered deployment, see “Installing a cluster of Bandwidth Managers” on page 338.

Downloading the WebSphere Application Server installation package to the stand-alone Bandwidth Manager computer:
Download and extract the IBM WebSphere Application Server installation package to the server where you will install the application.

About this task

This task is only needed when WebSphere Application Server is not already installed on the computer where you want to host the IBM Sametime Bandwidth Manager. Download the WebSphere Application Server installation package from either CD, DVD, or the IBM Passport Advantage site.

Procedure

1. (Linux RHEL only) If you have not done so already, disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).
3. Create a temporary folder called TMP\WAS.
4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command:
      `mount /dev/cdrom /cdrom`
      See your operating system documentation for additional instructions on mounting CDs and DVDs.
   b. From the installation media, copy the WebSphere Application Server installation image to the TMP\WAS folder.
5. If you will install from downloaded packages, download the WebSphere Application Server installation image to the TMP\WAS folder now.
   For the installation package’s part number, see the Sametime Download document. For instructions on how to locate and download the installation package to your server, see Using Passport Advantage to download IBM products.
6. When the installation package has been copied to your server, open a command window and navigate to the TMP\WAS folder.
7. Extract all files to the temporary directory TMP\WAS.

Installing a stand-alone WebSphere Application Server to host the Bandwidth Manager:

Install a stand-alone instance of the version of IBM WebSphere Application Server that comes with Sametime. Install the software on Linux or Microsoft Windows for use with the IBM Sametime Bandwidth Manager.

Before you begin

Sametime Bandwidth Manager must run on WebSphere Application Server 7.0.0.15. Perform this task if the correct version of WebSphere Application Server is not installed on the computer where you want to host the Bandwidth Manager. If you have already installed the correct version of WebSphere Application Server, skip
this task and proceed directly to “Installing WebSphere iFixes on the stand-alone Bandwidth Manager server” on page 326.

About this task

You will make an important decision during this installation: What profile should you use?

During the installation, the WebSphere Application Server Environments screen will prompt you to select a server profile. To install a stand-alone server that will not be federated to a deployment manager, select the Application server profile. This profile stands alone and is administered using its own Integrated Solutions Console. Even if you install an additional instance of this profile, it cannot be used to provide load balancing or failover services; those capabilities require a clustered deployment.

Tip: If you anticipate installing additional application servers at a later time and want to be able to cluster them for high performance, install this server using the Cell (deployment manager + primary node) profile; later you can install additional nodes using the Custom profile, and then configure a cluster. For instructions on installing a Cell profile, use the topic “Installing the deployment manager or cell for the Bandwidth Manager cluster” on page 339.

Procedure

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server where you will install WebSphere Application Server.
   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 (Windows) or as root (IBM AIX, Linux, Solaris).
3. Create a temporary folder called \TMP\WASCD.
4. Do one of the following:
   • If you will install from CD or DVD:
     a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command: mount /dev/cdrom /cdrom
     See your operating system documentation for additional instructions on mounting CDs and DVDs.
   b. Copy the WebSphere Application Server installation image to the \TMP\WASCD folder.
   • If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WASCD folder now.
   For the installation package’s part number, see the Sametime Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   For instructions on locating and downloading the installation package to your server, see Using Passport Advantage to download IBM products.
5. Extract all files into the temporary directory `\TMP\WASCD`.
   When you are done extracting the files, you should have a `\TMP\WASCD\ifpackage` folder with WAS and JDK subfolders inside it.

6. Change to the WAS subfolder and run the `install.exe` command.

7. On the Welcome screen, click Next.

8. On the Software License Agreement screen, review the license agreement, click I **accept both the IBM and the non-IBM terms**, and then click Next.

9. On the System Prerequisites Check screen, verify that your computer satisfies the requirements, and then click Next.
   If you computer does not meet the requirements, stop the installation and configure your system to meet the stated requirements before beginning the installation again.

10. On the Optional Features Installation screen, you can choose to install non-English language packages for the Integrated Solutions Console and for the runtime environment (for example, the wsadmin tool and logging); click Next when you are ready to proceed.

11. On the Installation Directory screen, either accept the default path or **Browse** to select an appropriate location, and then click Next.

12. On the WebSphere Application Server Environments screen, select a server profile:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server</td>
<td>A stand-alone WebSphere Application Server that will not be federated into a cluster.</td>
</tr>
<tr>
<td>Cell</td>
<td>A deployment manager and an application server node, installed and federated on a single computer. Even if you only want a single application server now, a cell profile gives you the option of easily adding additional nodes later so you can create a cluster to provide load balancing and failover. <strong>Note:</strong> A cell is not a cluster. To provide load balancing and failover for high performance, you must additionally configure the cell to operate as a cluster as described later in this documentation.</td>
</tr>
<tr>
<td>Custom</td>
<td>An empty node that is federated to a deployment manager, but is not necessarily installed on the same computer. Use this profile to install a single application server node separately from the deployment manager, or to add nodes to a cell or cluster. After you install the empty node, you must complete a separate task to install the application that it will host (in this case, the Lotus Sametime product), or to configure the node to function as a proxy server for a cluster. Both of these tasks are explained later in this installation documentation.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>One of the following management profiles:</td>
</tr>
<tr>
<td></td>
<td>• A deployment manager with no application server node. Use this profile when you want to install the node on a different computer from the deployment manager.</td>
</tr>
<tr>
<td></td>
<td>• A job manager. You do not need to install a job manager for this deployment.</td>
</tr>
<tr>
<td></td>
<td>• An administrative agent. You do not need to install an administrative agent for this deployment.</td>
</tr>
<tr>
<td>Secure proxy</td>
<td>A WebSphere proxy server, intended for use in the DMZ. This is not the proxy server that you typically install directly in front of a cluster – you do not need to install a secure proxy server at this time. If you configure a cluster, you will have the option of setting up a WebSphere proxy server at that time.</td>
</tr>
<tr>
<td>None</td>
<td>No profile defined during installation. This option requires you to create a profile before you can actually use this new server.</td>
</tr>
</tbody>
</table>

13. **Custom** profile only: When you install an additional application server node, the Federation screen offers you the option of federating the new node to the deployment manager during installation. Do one of the following:
   - Federate the new node during installation:
     a. Fill in the following fields:
     - Deployment manager host name or IP address: Type the fully qualified host name or the IP address of the server hosting the deployment manager.
     - Deployment manager SOAP port number (8879 is the default): Type the SOAP port number on the server hosting the deployment manager.
     - User name: Type the WebSphere administrator user name for the deployment manager (created when you installed the deployment manager).
     - Password: Type the password for the administrator account.
     b. Make sure the deployment manager is running.
     c. Click Next.
   - Choose not to federate now:
     a. Scroll to the bottom of the screen and click **Federate this managed node later using the addNode command**.
     b. Click Next.

14. At the Enable Administrative Security screen, select **Enable administrative security**, create a new WebSphere Application Server administrator account by typing a user name and a password (and confirming the password), and then click Next.
Enabling administrative security provides the authentication of users accessing the WebSphere administration functions, the use of Secure Sockets Layer (SSL) data encryption, and the choice of user account repository (the LDAP directory against which users will be authenticated).

**Note:** In this step you create a single new administrator account; you can create additional administrator accounts later. To avoid conflicts, do not use an account that already resides in the deployment's LDAP server.

15. **Cell** and **Deployment manager** profiles only: When you install a cell or deployment manager profile, the Repository for Centralized Installation Managers screen offers you the option of creating a repository on that server and storing a copy of the WebSphere Application Server installation package, and then later using it to install additional application server nodes remotely by launching the installation from the deployment manager (instead of downloading the installation kit to each computer). Do one of the following:
   - **Create the repository:**
     a. Select **Create a repository for Centralized Installation Managers.**
     b. Accept the default path for the repository or use **Browse** to select another location.
     c. Select **Populate the repository with this installation package.**
     d. Click **Next.**
   - **Choose not to create the repository:**
     a. Deselect all options.
     b. Click **Next.**

16. At the Installation Summary screen, review the installation details. Use the **Back** button to return to earlier screens and make any needed changes, then proceed until you reach this screen once again. When you are ready to run the installation, click **Next.**

   During installation, a progress bar is displayed and the activity is logged to the log file. When the installation is complete, the wizard displays a message indicating whether the installation was successful.

17. Review the message and then click **Finish** to close the installation program.

   If the installation encountered problems, you can review the logs. The `app_server_root/logs/install/log.txt` file and the `app_server_root/logs/manageprofiles/profile_name_create.log` file record installation and profile creation status.

**What to do next**

After you have successfully installed WebSphere Application Server, proceed to the topic on “Installing WebSphere iFixes on the stand-alone Bandwidth Manager server.”

**Installing WebSphere iFixes on the stand-alone Bandwidth Manager server:**

Install the required updates on an IBM WebSphere Application Server.

**About this task**

After you install WebSphere Application Server (any profile), you must add any required updates. Sometimes iFixes are released after a particular version of WebSphere Application Server has been incorporated into Sametime, but before the Sametime product itself was released. When that happens, the iFixes are included
in the Sametime packaging as separate files that must be applied manually using
the WebSphere Update Installer.

**Procedure**

1. Download the package containing the WebSphere iFixes to the computer
   hosting WebSphere Application Server.
2. Install the WebSphere Update Installer as described in Installing the WebSphere
   Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in
   Installing WebSphere Application Server updates.

**Downloading the Bandwidth Manager installation package to the stand-alone Bandwidth
Manager computer:**

Download and extract the IBM Sametime Bandwidth Manager installation package
to the server where you will install the application.

**About this task**

Download the installation package from either CD, DVD, or the IBM Passport
Advantage site.

**Procedure**

1. (Linux RHEL only) If you have not done so already, disable SELinux on any
   RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).
3. Create a temporary folder called \TMP\BWM.
4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled,
      mount it manually with the following command:
      ```
mount /dev/cdrom /cdrom
      ```
      See your operating system documentation for additional instructions on
      mounting CDs and DVDs.
   b. From the installation media, copy the Sametime Bandwidth Manager
      installation image to the \TMP\BWM folder.
5. If you will install from downloaded packages, download the WebSphere
   Application Server installation image to the \TMP\BWM folder now. You can find
   the Bandwidth Manager installation files from the Sametime Media Manager
disk in the Bandwidth Manager subfolder.
   For the installation package's part number, see the Sametime Download
   document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   For instructions on how to locate and download the installation package to
   your server, see Using Passport Advantage to download IBM products.
6. When the installation package has been copied to your server, open a command window and navigate to the \TMP\BWM folder.

7. Extract all files to the temporary directory \TMP\BWM.

**Updating the db2.connection.properties file for the stand-alone Bandwidth Manager:**

Update the db2.connection.properties file included in the IBM Sametime Bandwidth Manager installation package and add settings for your deployment.

**About this task**

The db2.connection.properties file is used during installation to create a new connection to the Bandwidth Manager database hosted on the deployment's IBM DB2 server. Update the file and specify settings for your deployment as explained here.

**Procedure**

1. Navigate to the \TMP\BWM folder containing the extracted installation files.
2. Update the db2.connection.properties file as follows:
   a. Change the properties of the db2.connection.properties file to make it editable if necessary.
      This file was supplied with the Bandwidth Manager installation package and may be set to read-only.
   b. Open the db2.connection.properties file for editing and change the following lines:
      
      ```
      db2.login=DB2_Username
      db2.password=DB2_Password
      db2.connection.address=Host_name
      db2.connection.port=DB2_Port
      db2.schema=Schema_name
      db2.connection.database=Database_Name
      ```

      where:
      - **DB2_Username** and **DB2_Password** are the credentials of the user who created the BWM_DATA database (usually the DB2 instance owner).
      - **Host_Name** can be a short name, fully qualified domain name, or an IP address as long as it is addressable by both the install program and the Bandwidth Manager runtime. A fully qualified domain name is recommended. A short name is also possible to use as long as it is defined in the local hosts file (for example `system32/driver/etc/hosts` on Windows or `/etc/hosts` on Linux.
      - **DB2_Port** is the DB2 server network port. The default is 50000, but change this to the appropriate value if your DB2 server uses a different port.
      - **Schema_name** is the name of the database schema that will be used by the Bandwidth Manager. Typically the default database schema is used, which is named the same as the **DB2_Username**, but the schema must be in uppercase letters. On Linux, the schema name is case sensitive.
      - **Database_Name** is the name you used to create the database, such as BWM_DATA.

      For example:
db2.login=myDB2user
db2.password=myDB2passw0rd
db2.connection.address=db2svr.example.com
db2.connection.port=50000
db2.schema=MYDB2USER
db2.connection.database=BWM_DATA

c. Save and close the file.

Updating the `websphere_configuration.properties` file for the stand-alone Bandwidth Manager:

Update the `websphere_configuration.properties` file included in the IBM Sametime Bandwidth Manager installation package and add settings for your deployment.

About this task

The `websphere_configuration.properties` file is used during installation to configure IBM WebSphere Application Server settings needed by the Bandwidth Manager. Update the file and specify settings for your deployment as explained here.

Procedure

1. Navigate to the `\TMP\BWM` folder containing the extracted installation files.
2. Update the `websphere_configuration.properties` file as follows:
   a. Change the properties of the `websphere_configuration.properties` file to make it editable if necessary.
      This file was supplied with the Bandwidth Manager installation package and may be set to read-only.
   b. Open the `websphere_configuration.properties` file for editing and change the following lines:
      ```
      was.language=Language_abbreviation
      was.node=Node_name
      was.server=Server_name
      was.cell=Cell_name
      was.profilename=Profile_name
      was.home=WAS_install_root
      was.hostname=Host_name
      was.hostport=Host_port
      was.sipport=SIP_port
      was.httpport=HTTP_port
      was.userid=WAS_admin_username
      was.password=WAS_admin_password
      was.db2.driver.path=${WAS_INSTALL_ROOT}/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.102.vBuild_number/driver
      ```
      where:

      - **Language_abbreviation** defines the language to be used for console and log messages produced by the Bandwidth Manager server or administrative interface. This setting does not affect messages that are presented to end users. Use one of the following language abbreviations to choose the language. If the parameter is missing, the default Language is English.
        - `en` (English)
        - `de` (German)
        - `es` (Spanish)
        - `fr` (French)
        - `it` (Italian)
- ja (Japanese)
- ko (Korean)
- pt_BR (Brazilian Portuguese)
- zh (Simplified Chinese)
- zh_TW (Traditional Chinese)

- Node_name, Server_name, Cell_name, Profile_name and are the WebSphere Application Server node, server, cell, and profile names where the Bandwidth Manager application will be installed (the current WebSphere Application Server instance).

- 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 and forward slashes or the installation will fail; for example: C:\PROGRA~1/IBM/WebSphere/AppServer.

- Host_Name is the IP address or the fully qualified domain name of the server where you will install the Bandwidth Manager (the current WebSphere Application Server).

- On an unclustered server, Host_port, SIP_port, and HTTP_port correspond to the values that are used by the target profile in WebSphere Application Server for WC_adminhost, SIP_DEFAULTHOST, and WC_defaulthost, respectively.

  On a clustered node, Host_port and HTTP_port correspond to the values that are used by the Deployment Manager profile in WebSphere Application Server for WC_adminhost and WC_defaulthost, respectively. Find these values in the Integrated Solutions Console by navigating to System Administration > Deployment Manager. In the Additional Properties section, select Ports.

  On a clustered node, SIP Port corresponds to the value used by the target WebSphere Application Server for SIP_DEFAULTHOST. Find this value in the Integrated Solutions Console by navigating to Application Servers > server_name. In the Communications section, select Ports.

- WAS_admin_username and WAS_admin_password are the credentials of the WebSphere administrator (the credentials used for logging in to the Integrated Solutions Console). If administrative security is not enabled, you can omit the credentials.

- ${WAS_INSTALL_ROOT} represents the WebSphere Application Server root installation directory. The install program looks for this exact designation; do not change it.

- Build_number is the build date that corresponds to the JDBC driver build date. To find the correct number, open the WAS-Install-Root/deploytool/itp/plugins folder and locate the folder named com.ibm.datatools.db2_2.0.102.vBuild_number, where Build_number is a 12-digit number.

For example:

```bash
was.language=ja
was.node=myWASnode
was.server=myWASserver
was.cell=myWAScell
was.profilename=AppServerProfile
was.home=C:/PROGRA~1/IBM/WebSphere/AppServer
was.hostname=myWASserver.example.com
```
was.hostport=9060
was.sipport=5060
was.httpport=9080
was.userid=wasadmin
was.password=password
was.db2.driver.path=${WAS_INSTALL_ROOT}/deploytool/ftp/plugins/com.ibm.datatools.db2_2.1.102.v20091026_1945/driver

Save and close the file.

Installing the Bandwidth Manager application on the stand-alone computer:

Install the IBM Sametime Bandwidth Manager application on a computer where IBM WebSphere Application Server is running.

Before you begin

Make sure that the IBM DB2 server is running and the database has been created.

On the server where you will install the Bandwidth Manager, make sure the appropriate IBM WebSphere Application Server instance is running, the installation package has downloaded and extracted, and the necessary files have been modified for your deployment.

Procedure

1. On the server where you will install the Bandwidth Manager, use a command line terminal or prompt, navigate to the \TMP\BwM folder containing the extracted installation files.
2. Run the following command to install the Bandwidth Manager:

   - **Linux**
     
     ```bash
     WAS_install_root/profiles/Profile_name/bin/ws_ant.sh -Dinstall.db=true
     ```
     
     where:
     
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application will be 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:
     
     ```bash
     /opt/IBM/WebSphere/AppServer/profiles/AppServerProfile/bin/ws_ant.sh -Dinstall.db=true
     ```

   - **Microsoft Windows**
     
     ```cmd
     WAS_install_root\profiles\Profile_name\bin\ws_ant.bat -Dinstall.db=true
     ```
     
     where:
     
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application will be 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:
     
     ```cmd
     C:\PROGRA~1\IBM\WebSphere\AppServer\profiles\AppServerProfile\bin\ws_ant.bat -Dinstall.db=true
     ```

When -Dinstall.db is set to true, the install script drops any existing Bandwidth Manager tables and then creates clean tables in the database. If -Dinstall.db is
set to false or is omitted, the install script does not drop or create Bandwidth Manager tables in the database, and any existing data is retained.

**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 installation process may take up to 10 minutes. You may see failures indicated, for example, an indication that a number of SQL commands could not be executed. This is expected behavior, because the installation program script attempts to "drop" (delete) any existing tables in the database without first checking whether the tables actually exist.

*Enabling security for the stand-alone Bandwidth Manager:*

Enable IBM WebSphere Application Server administrative security for the IBM Sametime Bandwidth Manager residing on that server.

**Before you begin**

Set administrative security for the WebSphere Application Server if is not already set. When WebSphere Application Server administrative security is on, you are prompted for the administrator user name and password when you log in to the Integrated Solutions Console.

1. Log in to the Integrated Solutions Console as the WebSphere Application Server administrator.
2. In the navigation tree, click **Security > Global security**
3. Under Available realm definitions, select **Federated Repositories**, then click **Configure**.
4. (Optional) Change the realm name to "LdapRealm".
5. Enter the primary administrator user name, such as `wasadmin` and click **OK**.
6. Enter the primary administrator password, such as "passw0rd" and click **OK**.
7. Click **Save** in the Messages box at the top of the page.
8. On the Global security page, select **Federated Repositories** again, and click **Set as current**.
9. Click **Save** in the Messages box at the top of the page.
10. On the Global security page, select **Enable administrative security**, but do not select **Use Java 2 security to restrict application access to local resources**.
11. Click **Save** in the Messages box at the top of the page.
12. Restart the Bandwidth Manager server to put the changes into effect.

**About this task**

Follow these steps to set administrative security and create an administrator for the Bandwidth Manager server.

**Procedure**

1. Log in to the Integrated Solutions Console as the WebSphere administrator.
2. Disable Java 2 security on local resources:
   a. In the navigation tree, click **Security > Global security**.
b. Under “Java 2 security” deselect the option **Use Java 2 security to restrict application access to local resources**.

c. Click **Apply**, and then click **Save** in the Messages box at the top of the page.

3. Enable access to the Common Object Request Broker Architecture (CORBA) name service for all service groups:
   a. In the navigation tree, click **Environment > Naming > CORBA Naming service groups**.
   b. In the service groups table, click the **EVERYONE** link.
   c. In the in the “General Properties” section, add the following **Roles** by clicking within the list and then using Shift+click to add each role until all are selected:
      - Cos Naming Read
      - Cos Naming Write
      - Cos Naming Create
      - Cos Naming Delete

A selected role appears highlighted.

![CORBA naming service groups](image)

   d. Click **Apply**, and then click **Save** in the Messages box at the top of the page.

4. Create a new user as the Bandwidth Manager administrator. This administrator is not the same as the WebSphere Application Server administrator.
   a. In the navigation tree, click **Users and Groups > Manage Users**.
   b. Click the **Create** button at the top of the users table.
   c. Fill in information for the new administrator:
      - User ID
      - First name
      - Last name
      - Password
      - Confirm password
d. Click the **Create** button at the bottom of the page to generate the new account. Enable administrative security when you are prompted to do so.

e. When the **The user was created successfully** message appears, click the **Close** button.

5. Now add the new administrator to all security roles:

a. In the navigation tree, click **Users and Groups > Administrative user roles**.

b. Click **Add** at the top of the roles table.

c. In the "Roles" list at the top of the page, use Shift+click to add each role until all are selected.

**Tip:** Only the "All Authenticated Users" is required but you should select all roles to ensure that the new administrator has full access to the Bandwidth Manager application.

d. In the "Search and Select Users" section of the page, click the **Search** button (located next to the "Search string" field).

The search results appear in the "Available" list below the field.

e. Select the administrator you created earlier, and click the **Add** button (the right-facing arrow) to add that user to the "Mapped to role" list.

f. Click **OK**, and then click **Save** in the Messages box at the top of the page.

6. Stop and restart the IBM WebSphere Application Server:

a. Open a command window.

b. Change to the profile directory of the WebSphere Application Server hosting the Bandwidth Manager.

c. Run the following commands:

Supply your WebSphere administrative credentials when stopping the server. Be sure the server has fully stopped before starting it again.

**Linux**

```
./stopServer.sh server1 -username was_admin_user -password was_admin_password
```

**Microsoft Windows**

```
./startServer.sh server1
```
Verifying the stand-alone Bandwidth Manager installation:

After completing the basic installation for an IBM Sametime Bandwidth Manager, verify that the installation was successful.

About this task

For best results, you should verify that the Bandwidth Manager installation was successful before you proceed to configure the new server.

Procedure

1. On the computer hosting the Bandwidth Manager, stop and restart the IBM WebSphere Application Server:
   a. Open a command window.
   b. Change to the profile directory of the WebSphere Application Server hosting the Bandwidth Manager.
   c. Run the following commands:
      Supply your WebSphere administrative credentials when stopping the server. Be sure the server has fully stopped before starting it again.
      **Linux**
      ```bash
      ./stopServer.sh server1 -username was_admin_user -password was_admin_password
      ./startServer.sh server1
      ```
      **Microsoft Windows**
      ```cmd
      stopServer.bat server1 -username was_admin_user -password was_admin_password
      startServer.bat server1
      ```

2. Log in to the Integrated Solutions Console as the WebSphere administrator (the credentials used for installing the Bandwidth Manager).

3. Look at the lower left portion of the console (the navigation tree) and verify that a new set of tasks appears, named Sametime Servers.

4. In the navigation tree, click Sametime Servers and verify that the Bandwidth Manager link appears.

5. Click on Bandwidth Manager, then click the Status tab and verify that MediaSessionController, SipFrontend, and at least one BandwidthPoolManager components appear in the table.

What to do next

If the components appear in the table, the installation was successful. Otherwise, the installation failed. If the installation fails, follow these steps to try again:

1. Delete the Bandwidth Manager profile using the following command:
   **Linux:**
   ```bash
   /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -delete -profileName BWMProfile
   ```

2. Create the profile again.

3. Install Bandwidth Manager again using the instructions for Installing the Bandwidth Manager application on the stand-alone computer.

**Important:** Even if the installation was successful, do not click the Start/Rerstart button in the Status table; you must complete the Bandwidth Manager's initial configuration first as explained in the tasks that follow.
Connecting the stand-alone Bandwidth Manager to the LDAP server:

Configure the IBM WebSphere Application Server federated repository for LDAP access.

About this task

The LDAP server must be running when you configure access to it.

Procedure

1. Disable secure access to Virtual Member Manager.
   a. On the server running the Bandwidth Manager module, open the `wimconfig.xml` file.
      Linux
      Standalone server
      `/opt/IBM/WebSphere/AppServer/profiles/Host_name/config/cells\Cell_name/wim/config/wimconfig.xml`
      On a node
      `/opt/IBM/WebSphere/AppServer/profiles/DeploymentManager_name/config/cells\Cell_name/wim/config/wimconfig.xml`
      Windows
      Standalone server
      `C:\Program Files\WebSphere\AppServer\profiles\Host_name\config\cells\Cell_name\wim\config\wimconfig.xml`
      On a node
      `C:\Program Files\WebSphere\AppServer\profiles\DeploymentManager_name\config\cells\Cell_name\wim\config\wimconfig.xml`
   b. Search for the string `isSecurityEnabled` and change the value to `false`.
   c. Save the file.
2. Stop and restart the application server.
3. Log in to the Integrated Solutions Console as the WebSphere administrator.
4. In the navigation tree, click Security > Global security.
5. Locate the "User account repository" sections of the Global Security page.
6. In the Available realm definitions list, select Federated repositories and click the Set as current button.
7. Click Configure button and define settings for the LDAP connection:
   a. On the "Federated Repositories" page, type a descriptive name, such as LdapRealm, in the Realm name field.
   b. In the Primary administrative user name field, type the user name (only the user name itself, not the full distinguished name) of the LDAP server's administrative user. The user must be in the LDAP repository.
   c. Click the Add Base entry to Realm button in the "Repositories in the realm" table.
   d. On the "Repository reference" page, click the Add Repository button.
   e. Under "LDAP server," fill in properties for your LDAP directory:

<table>
<thead>
<tr>
<th>Repository identifier</th>
<th>Type a descriptive name, such as LDAP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory type</td>
<td>Select the LDAP directory used by your deployment.</td>
</tr>
<tr>
<td>Primary host name</td>
<td>Enter the short host name, fully qualified domain name, or IP address of the server where the LDAP directory resides. The fully qualified domain name is recommended.</td>
</tr>
</tbody>
</table>
f. Under "Security," fill in security settings for your LDAP directory:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bind distinguished name</strong></td>
<td>Type the user name and domain name of a user with full permissions to access the LDAP server. Use LDAP canonical name format; cn=administrator, cn=users, o=ibm</td>
</tr>
<tr>
<td><strong>Bind password</strong></td>
<td>Type the password for the LDAP user specified in the <strong>Bind distinguished name</strong> field.</td>
</tr>
<tr>
<td><strong>Login properties</strong></td>
<td>Delete the &quot;uid&quot; string that appears in this field, and leave the field blank.</td>
</tr>
</tbody>
</table>

---

**g.** Click the **Apply** button, and then click the **Save** link in the "Messages" box at the top of the page.

If an error message appears, double-check the settings you entered, particularly the **Bind distinguished name**, and correct the settings as needed.

When the LDAP settings are configured correctly, a web page appears so that you can enter two more distinguished names.

**8.** For both occurrences of the **Base entry distinguished name** field, type the Base search entry, for example, ou=sametime, dc=lotus, dc=com. Then click **OK**.

The "Federated Repositories" page reappears, and you can continue configuring the LDAP connection.

**9.** Click the **Apply** button, and then click the **Save** link in the "Messages" box at the top of the page.

**10.** The Bandwidth Manager server uses the **uid** attribute internally to search for users through the Virtual Member Manager. If the **uid** attribute does not map directly to the corresponding **uid** in the LDAP directory, change the mapping in the wimconfig.xml file to map the **uid** attribute to a different LDAP attribute.

For example, it is common that the Media Manager server uses the **mail** identifier to identify users in the SIP URI, from which Bandwidth Manager extracts user IDs for lookup in the Virtual Member Manager.

The following example maps the Virtual Member Manager **uid** attribute to the LDAP **mail** attribute:

```xml
<config:attributeConfiguration>
    ...
    <config:attributes name="mail" propertyName="uid">
        <config:entityTypes>PersonAccount</config:entityTypes>
    </config:attributes>
</config:attributeConfiguration>
```

**11.** The Bandwidth Manager server uses the **email** attribute in the LDAP directory to look up users in the LDAP directory and assign the correct call rate policy. If your LDAP directory uses a different attribute for users’ email addresses, such as **mail**, **email**, and **emailAddress**, change the mapping in the wimconfig.xml file to map the **email** attribute to a different LDAP attribute.

The following example comments out the default mapping of **samAccountName**.

```xml
<config:attributeConfiguration>
    ...
</config:attributeConfiguration>
```

---
Add the appropriate mapping in the attributeConfiguration section of the wimconfig.xml file. This example maps the uid attribute to the mail attribute.

```xml
<config:attributeConfiguration>
  ...
  <config:attributes name="mail" propertyName="uid">
    <config:entityTypes>PersonAccount</config:entityTypes>
  </config:attributes>
  ...
</config:attributeConfiguration>
```


13. If you have more than one LDAP directory, repeat the previous two steps on all directories.

**Installing a cluster of Bandwidth Managers:**

Install a cluster of IBM Sametime Bandwidth Manager servers using an IBM WebSphere Application Server network deployment.

**About this task**

Use this method to install a multiple Bandwidth Manager servers as a cluster that provides load balancing and failover for improved performance. In this release, a cluster can support two Bandwidth Manager servers.

**Tip:** Even if you do not need two Bandwidth Managers now, you should consider using these clustering instructions to install a cell consisting of a deployment manager and a federated node. This gives you the option of adding another Bandwidth Manager to the cell later, and then configuring the cell to function as a cluster.

*Installing a WebSphere Application Server deployment manager or cell for the Bandwidth Manager cluster:*

Begin a clustered deployment of IBM Sametime Bandwidth Manager by installing a deployment manager, or a cell containing a deployment manager with a federated node, running on IBM WebSphere Application Server.

**About this task**

**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.

*Downloading the WebSphere Application Server installation package to the deployment manager computer:*

Download and extract the IBM WebSphere Application Server installation package to the server where you will install the application.
About this task

This task is only needed when WebSphere Application Server is not already installed on the computer where you want to host the IBM Sametime Bandwidth Manager. Download the WebSphere Application Server installation package from either CD, DVD, or the IBM Passport Advantage site.

Procedure

1. (Linux RHEL only) If you have not done so already, disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).
3. Create a temporary folder called \TMP\WAS.
4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command:
      
      ```
      mount /dev/cdrom /cdrom
      ```
      See your operating system documentation for additional instructions on mounting CDs and DVDs.
   b. From the installation media, copy the WebSphere Application Server installation image to the \TMP\WAS folder.
5. If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WAS folder now.
   For the installation package's part number, see the Sametime Download document. For instructions on how to locate and download the installation package to your server, see Using Passport Advantage to download IBM products.
6. When the installation package has been copied to your server, open a command window and navigate to the \TMP\WAS folder.
7. Extract all files to the temporary directory \TMP\WAS.

Installing the deployment manager or cell for the Bandwidth Manager cluster:

Install an IBM WebSphere Application Server cell on Linux or Microsoft Windows for use with the IBM Sametime Bandwidth Manager. The cell includes a deployment manager and a single federated application node; you can add additional nodes and create a cluster at any time.

About this task

You will make two important decisions during this installation:
• What profile should you use?
  The WebSphere Application Server Environments screen will prompt you to select a server profile. To create a cluster, you must install a deployment manager using one of these options:
- **Cell** profile: In a single operation, install a deployment manager and a federated application server node on the same instance of WebSphere Application Server.

- **Deployment manager** profile: Install only a deployment manager. This option requires you to install at least one federated application server node using the **Custom** profile. Use this profile when you want to install the application server node separately; for example, at a later time or on a different computer.

**Tip:** When creating a cluster, install the deployment manager or cell first, so that additional nodes can be federated to the deployment manager as part of the installation process.

- **Create a Centralized Installation Manager (CIM) repository?**

  The Repository for Centralized Installation Managers screen will prompt you to decide whether to create a CIM repository and store a copy of the installation package in it. Establishing a centralized installation manager repository allows you to create application server nodes on remote servers by launching the installation from the deployment manager. Because the installation program is stored on the deployment manager, you do not have to download it to the remote server. Before selecting this option, review the WebSphere topics Creating and managing Network Deployment cells using the centralized installation manager (CIM) and Considerations when using the centralized installation manager (CIM).

**Procedure**

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server where you will install WebSphere Application Server.
   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 (Windows) or as root (IBM AIX, Linux, Solaris).

3. Create a temporary folder called \TMP\WASCD.

4. Do one of the following:
   - If you will install from CD or DVD:
     a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command: mount /dev/cdrom /cdrom
        See your operating system documentation for additional instructions on mounting CDs and DVDs.
     b. Copy the WebSphere Application Server installation image to the \TMP\WASCD folder.
   - If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WASCD folder now.

For the installation package's part number, see the Sametime Download document at the following web address:

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

For instructions on locating and downloading the installation package to your server, see Using Passport Advantage to download IBM products.
5. Extract all files into the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK subfolders inside it.

6. Change to the WAS subfolder and run the install.exe command.

7. On the Welcome screen, click Next.

8. On the Software License Agreement screen, review the license agreement, click I accept both the IBM and the non-IBM terms, and then click Next.

9. On the System Prerequisites Check screen, verify that your computer satisfies the requirements, and then click Next.

If you computer does not meet the requirements, stop the installation and configure your system to meet the stated requirements before beginning the installation again.

10. On the Optional Features Installation screen, you can choose to install non-English language packages for the Integrated Solutions Console and for the runtime environment (for example, the wsadmin tool and logging); click Next when you are ready to proceed.

11. On the Installation Directory screen, either accept the default path or Browse to select an appropriate location, and then click Next.

12. On the WebSphere Application Server Environments screen, select a server profile:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server</td>
<td>A stand-alone WebSphere Application Server that will not be federated into a cluster.</td>
</tr>
<tr>
<td>Cell</td>
<td>A deployment manager and an application server node, installed and federated on a single computer. Even if you only want a single application server now, a cell profile gives you the option of easily adding additional nodes later so you can create a cluster to provide load balancing and failover. Note: A cell is not a cluster. To provide load balancing and failover for high performance, you must additionally configure the cell to operate as a cluster as described later in this documentation.</td>
</tr>
<tr>
<td>Custom</td>
<td>An empty node that is federated to a deployment manager, but is not necessarily installed on the same computer. Use this profile to install a single application server node separately from the deployment manager, or to add nodes to a cell or cluster. After you install the empty node, you must complete a separate task to install the application that it will host (in this case, the Lotus Sametime product), or to configure the node to function as a proxy server for a cluster. Both of these tasks are explained later in this installation documentation.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management</td>
<td>One of the following management profiles:</td>
</tr>
<tr>
<td></td>
<td>• A deployment manager with no application server node. Use this profile when you want to install the node on a different computer from the deployment manager.</td>
</tr>
<tr>
<td></td>
<td>• A job manager. You do not need to install a job manager for this deployment.</td>
</tr>
<tr>
<td></td>
<td>• An administrative agent. You do not need to install an administrative agent for this deployment.</td>
</tr>
<tr>
<td>Secure proxy</td>
<td>A WebSphere proxy server, intended for use in the DMZ. This is not the proxy server that you typically install directly in front of a cluster – you do not need to install a secure proxy server at this time. If you configure a cluster, you will have the option of setting up a WebSphere proxy server at that time.</td>
</tr>
<tr>
<td>None</td>
<td>No profile defined during installation. This option requires you to create a profile before you can actually use this new server.</td>
</tr>
</tbody>
</table>

13. **Custom** profile only: When you install an additional application server node, the Federation screen offers you the option of federating the new node to the deployment manager during installation. Do one of the following:

   • Federate the new node during installation:
     a. Fill in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment manager host name or IP address</td>
<td>Type the fully qualified host name or the IP address of the server hosting the deployment manager.</td>
</tr>
<tr>
<td>Deployment manager SOAP port number (8879 is the default)</td>
<td>Type the SOAP port number on the server hosting the deployment manager.</td>
</tr>
<tr>
<td>User name</td>
<td>Type the WebSphere administrator user name for the deployment manager (created when you installed the deployment manager).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the administrator account.</td>
</tr>
</tbody>
</table>

   b. Make sure the deployment manager is running.
   c. Click Next.

   • Choose not to federate now:
     a. Scroll to the bottom of the screen and click **Federate this managed node later using the addNode command**.
     b. Click Next.

14. At the Enable Administrative Security screen, select **Enable administrative security**, create a new WebSphere Application Server administrator account by typing a user name and a password (and confirming the password), and then click Next.
Enabling administrative security provides the authentication of users accessing the WebSphere administration functions, the use of Secure Sockets Layer (SSL) data encryption, and the choice of user account repository (the LDAP directory against which users will be authenticated).

**Note:** In this step you create a single new administrator account; you can create additional administrator accounts later. To avoid conflicts, do not use an account that already resides in the deployment’s LDAP server.

15. **Cell and Deployment manager profiles only:** When you install a cell or deployment manager profile, the Repository for Centralized Installation Managers screen offers you the option of creating a repository on that server and storing a copy of the WebSphere Application Server installation package, and then later using it to install additional application server nodes remotely by launching the installation from the deployment manager (instead of downloading the installation kit to each computer). Do one of the following:

   • Create the repository:
     a. Select **Create a repository for Centralized Installation Managers**.
     b. Accept the default path for the repository or use **Browse** to select another location.
     c. Select **Populate the repository with this installation package**.
     d. Click **Next**.

   • Choose not to create the repository:
     a. Deselect all options.
     b. Click **Next**.

16. At the Installation Summary screen, review the installation details. Use the **Back** button to return to earlier screens and make any needed changes, then proceed until you reach this screen once again. When you are ready to run the installation, click **Next**.

   During installation, a progress bar is displayed and the activity is logged to the log file. When the installation is complete, the wizard displays a message indicating whether the installation was successful.

17. Review the message and then click **Finish** to close the installation program. If the installation encountered problems, you can review the logs. The `app_server_root/logs/install/log.txt` file and the `app_server_root/logs/manageprofiles/profile_name_create.log` file record installation and profile creation status.

**What to do next**

After you have successfully installed WebSphere Application Server, proceed to the topic on “Installing WebSphere iFixes on the deployment manager or cell.”

**Installing WebSphere iFixes on the deployment manager or cell:**

Install the required updates on an IBM WebSphere Application Server.

**About this task**

After you install WebSphere Application Server (any profile), you must add any required updates. Sometimes iFixes are released after a particular version of WebSphere Application Server has been incorporated into Sametime, but before the Sametime product itself was released. When that happens, the iFixes are included
in the Sametime packaging as separate files that must be applied manually using the WebSphere Update Installer.

Procedure
1. Download the package containing the WebSphere iFixes to the computer hosting WebSphere Application Server.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

**Installing a WebSphere Application Server node for the Bandwidth Manager cluster:**

Install an IBM WebSphere Application Server node, which you will federate to a cell’s deployment manager prior to configuring a network deployment cluster.

**About this task**

A Bandwidth Manager cluster supports two application server nodes. If you installed a deployment manager using the **Cell** profile, an application server node was already installed on the same computer; you can install up to one additional node for use in the cluster. If you installed the deployment manager with the **Deployment manager** profile, no application server nodes were installed; you must install at least one application server node now using the **Custom** profile.

**Downloading the WebSphere Application Server installation package to the node’s computer:**

Download and extract the IBM WebSphere Application Server installation package to the server where you will install the application.

**About this task**

This task is only needed when WebSphere Application Server is not already installed on the computer where you want to host the IBM Sametime Bandwidth Manager. Download the WebSphere Application Server installation package from either CD, DVD, or the IBM Passport Advantage site.

**Procedure**
1. (Linux RHEL only) If you have not done so already, disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).
3. Create a temporary folder called `\TMP\WAS`.
4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command:
mount /dev/cdrom /cdrom

See your operating system documentation for additional instructions on mounting CDs and DVDs.

b. From the installation media, copy the WebSphere Application Server installation image to the \TMP\WAS folder.

5. If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WAS folder now.

For the installation package’s part number, see the Sametime Download document. For instructions on how to locate and download the installation package to your server, see Using Passport Advantage to download IBM products.

6. When the installation package has been copied to your server, open a command window and navigate to the \TMP\WAS folder.

7. Extract all files to the temporary directory \TMP\WAS.

Installing a node in the Bandwidth Manager cluster:

Install an IBM WebSphere Application Server node on Linux or Microsoft Windows for use with the IBM Sametime Bandwidth Manager. A cluster requires at least one application server node; you can install additional nodes at any time.

Before you begin

Tip: Application server nodes are administered through a deployment manager. Install the deployment manager (or cell) first, so that this new node can be federated to the deployment manager as part of the installation process.

About this task

You will make two important decisions during this installation:

• What profile should you use?

The WebSphere Application Server Environments screen will prompt you to select a server profile. To install an application server node that can be federated to a deployment manager, select the Custom profile.

Note: An application server can be installed as a node or as a stand-alone server. If you are installing an application server and do not want to administer the node using a deployment manager, you should install this server using the Application Server profile instead. For instructions on installing a stand-alone application server, see “Installing a stand-alone WebSphere Application Server to host the Bandwidth Manager” on page 322.

• Federate the node?

The Federation screen will prompt you to decide whether to automatically federate the new node to the deployment manager. When you federate an application server node to the deployment manager, a node agent is created to monitor the application server. The node agent serves as an intermediary between the application server hosted on the node and the deployment manager; all nodes are administered using the deployment manager’s Integrated Solutions Console. If you choose not to federate the new node at this time, you can federate it later with the WebSphere addNode command.

Procedure

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
a. Log in as root on the Linux RedHat server where you will install WebSphere Application Server.
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 (Windows) or as root (IBM AIX, Linux, Solaris).

3. Create a temporary folder called \TMP\WASCD.

4. Do one of the following:
   • If you will install from CD or DVD:
     a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command: mount /dev/cdrom /cdrom
     See your operating system documentation for additional instructions on mounting CDs and DVDs.
     b. Copy the WebSphere Application Server installation image to the \TMP\WASCD folder.
     • If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WASCD folder now.
       For the installation package's part number, see the Sametime Download document at the following web address:
       https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
       For instructions on locating and downloading the installation package to your server, see Using Passport Advantage to download IBM products.

5. Extract all files into the temporary directory \TMP\WASCD.
   When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK subfolders inside it.

6. Change to the WAS subfolder and run the install.exe command.

7. On the Welcome screen, click Next.

8. On the Software License Agreement screen, review the license agreement, click I accept both the IBM and the non-IBM terms, and then click Next.

9. On the System Prerequisites Check screen, verify that your computer satisfies the requirements, and then click Next.
   If your computer does not meet the requirements, stop the installation and configure your system to meet the stated requirements before beginning the installation again.

10. On the Optional Features Installation screen, you can choose to install non-English language packages for the Integrated Solutions Console and for the runtime environment (for example, the wsadmin tool and logging); click Next when you are ready to proceed.

11. On the Installation Directory screen, either accept the default path or Browse to select an appropriate location, and then click Next.

12. On the WebSphere Application Server Environments screen, select a server profile:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server</td>
<td>A stand-alone WebSphere Application Server that will not be federated into a cluster.</td>
</tr>
</tbody>
</table>
| Cell            | A deployment manager and an application server node, installed and federated on a single computer. Even if you only want a single application server now, a cell profile gives you the option of easily adding additional nodes later so you can create a cluster to provide load balancing and failover.  
**Note:** A cell is not a cluster. To provide load balancing and failover for high performance, you must additionally configure the cell to operate as a cluster as described later in this documentation. |
| Custom          | An empty node that is federated to a deployment manager, but is not necessarily installed on the same computer. Use this profile to install a single application server node separately from the deployment manager, or to add nodes to a cell or cluster.  
After you install the empty node, you must complete a separate task to install the application that it will host (in this case, the Lotus Sametime product), or to configure the node to function as a proxy server for a cluster. Both of these tasks are explained later in this installation documentation. |
| Management       | One of the following management profiles:  
• A deployment manager with no application server node. Use this profile when you want to install the node on a different computer from the deployment manager.  
• A job manager. You do not need to install a job manager for this deployment.  
• An administrative agent. You do not need to install an administrative agent for this deployment. |
| Secure proxy     | A WebSphere proxy server, intended for use in the DMZ. This is not the proxy server that you typically install directly in front of a cluster – you do not need to install a secure proxy server at this time. If you configure a cluster, you will have the option of setting up a WebSphere proxy server at that time. |
| None            | No profile defined during installation. This option requires you to create a profile before you can actually use this new server.                                                                                     |

13. **Custom** profile only: When you install an additional application server node, the Federation screen offers you the option of federating the new node to the deployment manager during installation. Do one of the following:  
• Federate the new node during installation:
a. Fill in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment manager host name or IP address</td>
<td>Type the fully qualified host name or the IP address of the server hosting the deployment manager.</td>
</tr>
<tr>
<td>Deployment manager SOAP port number (8879 is the default)</td>
<td>Type the SOAP port number on the server hosting the deployment manager.</td>
</tr>
<tr>
<td>User name</td>
<td>Type the WebSphere administrator user name for the deployment manager (created when you installed the deployment manager).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the administrator account.</td>
</tr>
</tbody>
</table>

b. Make sure the deployment manager is running.

c. Click Next.
• Choose not to federate now:
  a. Scroll to the bottom of the screen and click **Federate this managed node later using the addNode command**.
  b. Click Next.

14. At the Enable Administrative Security screen, select **Enable administrative security**, create a new WebSphere Application Server administrator account by typing a user name and a password (and confirming the password), and then click Next.

   Enabling administrative security provides the authentication of users accessing the WebSphere administration functions, the use of Secure Sockets Layer (SSL) data encryption, and the choice of user account repository (the LDAP directory against which users will be authenticated).

   **Note:** In this step you create a single new administrator account; you can create additional administrator accounts later. To avoid conflicts, do not use an account that already resides in the deployment's LDAP server.

15. **Cell** and **Deployment manager** profiles only: When you install a cell or deployment manager profile, the Repository for Centralized Installation Managers screen offers you the option of creating a repository on that server and storing a copy of the WebSphere Application Server installation package, and then later using it to install additional application server nodes remotely by launching the installation from the deployment manager (instead of downloading the installation kit to each computer). Do one of the following:

   - Create the repository:
     a. Select **Create a repository for Centralized Installation Managers**.
     b. Accept the default path for the repository or use **Browse** to select another location.
     c. Select **Populate the repository with this installation package**.
     d. Click Next.

   - Choose not to create the repository:
     a. Deselect all options.
     b. Click Next.

16. At the Installation Summary screen, review the installation details. Use the **Back** button to return to earlier screens and make any needed changes, then proceed until you reach this screen once again. When you are ready to run the installation, click **Next**.
During installation, a progress bar is displayed and the activity is logged to the log file. When the installation is complete, the wizard displays a message indicating whether the installation was successful.

17. Review the message and then click **Finish** to close the installation program.

If the installation encountered problems, you can review the logs. The `app_server_root/logs/install/log.txt` file and the `app_server_root/logs/manageprofiles/profile_name_create.log` file record installation and profile creation status.

What to do next

After you have successfully installed WebSphere Application Server, proceed to the topic on “Installing WebSphere iFixes on a node.”

**Installing WebSphere iFixes on a node:**

Install the required updates on an IBM WebSphere Application Server.

**About this task**

After you install WebSphere Application Server (any profile), you must add any required updates. Sometimes iFixes are released after a particular version of WebSphere Application Server has been incorporated into Sametime, but before the Sametime product itself was released. When that happens, the iFixes are included in the Sametime packaging as separate files that must be applied manually using the WebSphere Update Installer.

**Procedure**

1. Download the package containing the WebSphere iFixes to the computer hosting WebSphere Application Server.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

**Configuring a cluster of Bandwidth Managers:**

Configure a cluster of IBM Sametime Bandwidth Managers using an IBM WebSphere Application Server network deployment.

**Before you begin**

Before you can configure a cluster, you must federate each application server node in the cell to the deployment manager. If you did not accept automatic federation when you installed the node, you can federate it now using the WebSphere addNode command.

**About this task**

Clustering a deployment improves performance by providing load balancing and failover among the nodes in the deployment. For best results, deploy at least one WebSphere proxy server in front of the cluster to direct traffic to the nodes; if you use multiple proxy servers you can deploy a load balancer to automatically balance resources by distributing communications among the proxy servers.
Setting clocks on the Bandwidth Manager nodes:

Synchronize the system clocks on the IBM Sametime Bandwidth Manager servers to be clustered.

About this task

Complete this task for every node that you will add to the cluster, including all dedicated proxy servers.

Procedure

For each node that will be added to the cluster, set the system clock to exactly the same time as the Deployment Manager’s system clock.

Creating the Bandwidth Manager cluster configuration:

Create the cluster configuration for an IBM Sametime Bandwidth Manager cluster.

About this task

Create the cluster on the computer hosting the deployment manager.

Procedure

1. Start the deployment manager:
   a. On the server hosting the deployment manager, open a command window.
   b. Navigate to the `bin` folder of the deployment manager profile and 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
        ```

2. Start each application server’s node agent:
   a. Navigate to the `bin` folder of the application server node’s profile and run the `startNode` command:
      - Linux
        
        ```
        cd /opt/IBM/WebSphere/AppServer/profiles/Node_profile_name/bin
        startNode.sh
        ```
      - Microsoft Windows
        
        ```
        cd C:\Program Files\WebSphere\AppServer\profiles\Node_profile_name\bin
        startNode.bat
        ```
   b. If you have two nodes, repeat this step for the second node.

3. Log in to the Integrated Solutions Console as the WebSphere administrator.
4. On the navigation tree, click Servers > Clusters > WebSphere application server clusters.
5. On the clusters page, click the New button at the top of the table.
6. On the Create a new cluster page, type a descriptive name for the cluster (for example, BWMcluster), and then click Next.
7. On the Enter basic cluster information page, click Configure HTTP session memory-to-memory replication, and then click Next.
8. On the Create first cluster member page, type a descriptive name for the first
cluster member (for example, BWMserver1), and then click Next.
9. On the Create additional cluster members page, add a second cluster member
(for example, with the name BWMserver2), and then click Create.
10. Click Apply and then click the Save link in the Messages box at the top of the
page.

Restarting and synchronizing nodes in the Bandwidth 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 Bandwidth 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 Bandwidth Manager cluster:

Set up an IBM WebSphere proxy server for use with a cluster of IBM Sametime Bandwidth Managers. The proxy server can be hosted on any node in the cluster or on a dedicated computer; it performs routing and caching tasks for the servers in the cluster.

About this task

Installing a dedicated WebSphere proxy server for the Bandwidth Manager cluster:

Install an IBM WebSphere proxy server node, which you will federate to a cell’s deployment manager prior to configuring a network deployment cluster.

About this task

A cluster uses a WebSphere proxy server to manage routing and caching tasks. You can either enable the proxy server on an existing application server node, or you can install a new proxy server node on a dedicated computer. If you want to enable the proxy server on an existing node rather than install a new proxy server on a dedicated computer, skip this task and proceed directly to “Configuring a WebSphere proxy server for the Bandwidth Manager cluster” on page 358.

Downloading the WebSphere Application Server installation package to the proxy server computer:

Download and extract the IBM WebSphere Application Server installation package to the server where you will install the application.

About this task

This task is only needed when WebSphere Application Server is not already installed on the computer where you want to host the IBM Sametime Bandwidth Manager. Download the WebSphere Application Server installation package from either CD, DVD, or the IBM Passport Advantage site.
**Procedure**

1. (Linux RHEL only) If you have not done so already, disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).

3. Create a temporary folder called \**TMP\WAS**.

4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command:
      ```
      mount /dev/cdrom /cdrom
      ```
      See your operating system documentation for additional instructions on mounting CDs and DVDs.
   b. From the installation media, copy the WebSphere Application Server installation image to the \**TMP\WAS** folder.

5. If you will install from downloaded packages, download the WebSphere Application Server installation image to the \**TMP\WAS** folder now.
   For the installation package's part number, see the Sametime Download document. For instructions on how to locate and download the installation package to your server, see Using Passport Advantage to download IBM products.

6. When the installation package has been copied to your server, open a command window and navigate to the \**TMP\WAS** folder.

7. Extract all files to the temporary directory \**TMP\WAS**.

*Installing a WebSphere proxy server for the Bandwidth Manager cluster:*

Install an IBM WebSphere proxy server on Linux or Microsoft Windows for use with the IBM Sametime Bandwidth Manager. A cluster requires at least one proxy server; you can install additional proxy servers as needed.

**Before you begin**

**Tip**: Proxy server nodes are administered through a deployment manager. Install the deployment manager (or cell) first, so that this new node can be federated to the deployment manager as part of the installation process.

**About this task**

You will make two important decisions during this installation:

- **What profile should you use?**
  The WebSphere Application Server Environments screen will prompt you to select a server profile. To install a proxy server node that can be federated to a deployment manager, select the **Custom** profile.

- **Federate the node?**
The Federation screen will prompt you to decide whether to automatically federate the new node to the deployment manager. When you federate a node to the deployment manager, a node agent is created to monitor it. The node agent serves as an intermediary between the node and the deployment manager; all nodes are administered using the deployment manager's Integrated Solutions Console. If you choose not to federate the new node at this time, you can federate it later with the WebSphere addNode command.

Procedure

1. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server where you will install WebSphere Application Server.
   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 (Windows) or as root (IBM AIX, Linux, Solaris).

3. Create a temporary folder called \TMP\WASCD.

4. Do one of the following:
   - If you will install from CD or DVD:
     a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command: `mount /dev/cdrom /cdrom`
     b. Copy the WebSphere Application Server installation image to the \TMP\WASCD folder.
     c. For the installation package's part number, see the Sametime Download document at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
     d. For instructions on locating and downloading the installation package to your server, see Using Passport Advantage to download IBM products.
   - If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\WASCD folder now.

5. Extract all files into the temporary directory \TMP\WASCD.

6. Change to the WAS subfolder and run the install.exe command.

7. On the Welcome screen, click Next.

8. On the Software License Agreement screen, review the license agreement, click I accept both the IBM and the non-IBM terms, and then click Next.

9. On the System Prerequisites Check screen, verify that your computer satisfies the requirements, and then click Next.

   If your computer does not meet the requirements, stop the installation and configure your system to meet the stated requirements before beginning the installation again.
10. On the Optional Features Installation screen, you can choose to install non-English language packages for the Integrated Solutions Console and for the runtime environment (for example, the wsadmin tool and logging); click Next when you are ready to proceed.

11. On the Installation Directory screen, either accept the default path or Browse to select an appropriate location, and then click Next.

12. On the WebSphere Application Server Environments screen, select a server profile:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server</td>
<td>A stand-alone WebSphere Application Server that will not be federated into a cluster.</td>
</tr>
<tr>
<td>Cell</td>
<td>A deployment manager and an application server node, installed and federated on a single computer. Even if you only want a single application server now, a cell profile gives you the option of easily adding additional nodes later so you can create a cluster to provide load balancing and failover. <strong>Note:</strong> A cell is not a cluster. To provide load balancing and failover for high performance, you must additionally configure the cell to operate as a cluster as described later in this documentation.</td>
</tr>
<tr>
<td>Custom</td>
<td>An empty node that is federated to a deployment manager, but is not necessarily installed on the same computer. Use this profile to install a single application server node separately from the deployment manager, or to add nodes to a cell or cluster. After you install the empty node, you must complete a separate task to install the application that it will host (in this case, the Lotus Sametime product), or to configure the node to function as a proxy server for a cluster. Both of these tasks are explained later in this installation documentation.</td>
</tr>
<tr>
<td>Management</td>
<td>One of the following management profiles:</td>
</tr>
<tr>
<td></td>
<td>• A deployment manager with no application server node. Use this profile when you want to install the node on a different computer from the deployment manager.</td>
</tr>
<tr>
<td></td>
<td>• A job manager. You do not need to install a job manager for this deployment.</td>
</tr>
<tr>
<td></td>
<td>• An administrative agent. You do not need to install an administrative agent for this deployment.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure proxy</td>
<td>A WebSphere proxy server, intended for use in the DMZ. This is not the proxy server that you typically install directly in front of a cluster – you do not need to install a secure proxy server at this time. If you configure a cluster, you will have the option of setting up a WebSphere proxy server at that time.</td>
</tr>
<tr>
<td>None</td>
<td>No profile defined during installation. This option requires you to create a profile before you can actually use this new server.</td>
</tr>
</tbody>
</table>

13. **Custom** profile only: When you install an additional application server node, the Federation screen offers you the option of federating the new node to the deployment manager during installation. Do one of the following:

- Federate the new node during installation:
  a. Fill in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment manager host name or IP address</td>
<td>Type the fully qualified host name or the IP address of the server hosting the deployment manager.</td>
</tr>
<tr>
<td>Deployment manager SOAP port number (8879 is the default)</td>
<td>Type the SOAP port number on the server hosting the deployment manager.</td>
</tr>
<tr>
<td>User name</td>
<td>Type the WebSphere administrator user name for the deployment manager (created when you installed the deployment manager).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the administrator account.</td>
</tr>
</tbody>
</table>
  b. Make sure the deployment manager is running.
  c. Click Next.
- Choose not to federate now:
  a. Scroll to the bottom of the screen and click **Federate this managed node later using the addNode command**.
  b. Click Next.

14. At the Enable Administrative Security screen, select **Enable administrative security**, create a new WebSphere Application Server administrator account by typing a user name and a password (and confirming the password), and then click Next.

Enabling administrative security provides the authentication of users accessing the WebSphere administration functions, the use of Secure Sockets Layer (SSL) data encryption, and the choice of user account repository (the LDAP directory against which users will be authenticated).

**Note:** In this step you create a single new administrator account; you can create additional administrator accounts later. To avoid conflicts, do not use an account that already resides in the deployment's LDAP server.

15. **Cell** and **Deployment manager** profiles only: When you install a cell or deployment manager profile, the Repository for Centralized Installation Managers screen offers you the option of creating a repository on that server and storing a copy of the WebSphere Application Server installation package,
and then later using it to install additional application server nodes remotely by launching the installation from the deployment manager (instead of downloading the installation kit to each computer). Do one of the following:

- Create the repository:
  a. Select **Create a repository for Centralized Installation Managers**.
  b. Accept the default path for the repository or use **Browse** to select another location.
  c. Select **Populate the repository with this installation package**.
  d. Click **Next**.
- Choose not to create the repository:
  a. Deselect all options.
  b. Click **Next**.

16. At the Installation Summary screen, review the installation details. Use the **Back** button to return to earlier screens and make any needed changes, then proceed until you reach this screen once again. When you are ready to run the installation, click **Next**.

During installation, a progress bar is displayed and the activity is logged to the log file. When the installation is complete, the wizard displays a message indicating whether the installation was successful.

17. Review the message and then click **Finish** to close the installation program.

If the installation encountered problems, you can review the logs. The `app_server_root/logs/install/log.txt` file and the `app_server_root/logs/manageprofiles/profile_name_create.log` file record installation and profile creation status.

**What to do next**

After you have successfully installed WebSphere Application Server, proceed to the topic on “Installing WebSphere iFixes on the proxy server for the Bandwidth Manager cluster.”

**Installing WebSphere iFixes on the proxy server for the Bandwidth Manager cluster:**

Install the required updates on an IBM WebSphere Application Server.

**About this task**

After you install WebSphere Application Server (any profile), you must add any required updates. Sometimes iFixes are released after a particular version of WebSphere Application Server has been incorporated into Sametime, but before the Sametime product itself was released. When that happens, the iFixes are included in the Sametime packaging as separate files that must be applied manually using the WebSphere Update Installer.

**Procedure**

1. Download the package containing the WebSphere iFixes to the computer hosting WebSphere Application Server.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.
Configuring a WebSphere proxy server for the Bandwidth Manager cluster:

Configure an IBM WebSphere proxy server to perform routing and caching tasks for a cluster of IBM Sametime Bandwidth Managers.

**Before you begin**

Create a cluster of Sametime Bandwidth Managers running on WebSphere Application Server; start the deployment manager as well as all node agents and application servers in the cluster. If you will configure the proxy server on a dedicated computer, make sure the new proxy server node has been federated to the deployment manager.

**About this task**

A cluster uses 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. You can host a WebSphere proxy server on any node in the cluster but because it uses a lot of system resources, you may want to host it on a dedicated 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 clustering documentation.

**Procedure**

1. If this proxy server is installed on a dedicated computer, set the system clock to exactly the same time as the deployment manager's system clock.
2. Log in to the deployment manager's Integrated Solutions Console as the WebSphere administrator.
3. In the navigation tree, click **Servers > Server Types > WebSphere proxy servers.**
4. In the Proxy servers table, click the **New** button at the top of the table.
5. On the Create a new proxy server entry page, do the following:
   a. In the **Select a node** list, select the node that will host the WebSphere proxy server.
      Be sure to select a node that belongs to the Bandwidth Manager cluster.
   b. Type a descriptive name for the new proxy server (for example, BWMproxy1).
   c. Click **Next**.
6. On the Specify server specific properties page, do the following:
   a. Select both **HTTP** and **SIP** protocols for your cluster.
   b. Select **Generate unique ports**.
   c. Click **Next**.
7. On the Select a server template page, select **proxy_server.foundation** (the WebSphere Default Proxy Server Template), and then click **Next**.
8. On the Confirm new server page, click **Finish**.
9. Click **Apply** and then click the **Save** link in the Messages box at the top of the page.
10. Synchronize the nodes in the cluster:
    a. Click **System Administration > Nodes**.
    b. Select both nodes, and then click **Full Resynchronization**.
11. Assign the new proxy server to the cluster:
   a. In the navigation tree, 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 Bandwidth Manager cluster that you are configuring this WebSphere proxy server to work with.
   c. Click **Apply** and then click **Save** in the Messages box at the top of the page.

12. Now start the new proxy server:
   a. Again in the navigation tree, click **Servers > Proxy Servers**.
   b. On the Proxy Servers page, select the new proxy server from the list.
   c. Click the **Start** button at the top of the table.

---

**Adding ports to the virtual host alias for the Bandwidth Manager cluster:**

After creating a cluster, add the SIP ports of each cluster member to the virtual host alias.

**About this task**

On the cluster's deployment manager, 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.

**Procedure**

1. Determine the ports used by every cluster member:
   a. Log in to the deployment manager's Integrated Solutions Console as the WebSphere administrator.
   b. In the navigation tree, click **Servers > Server Types > WebSphere application servers**.
   c. In the table listing the servers, click the name of the cluster member.
   d. On the Configuration page, look in the Communication section and click **Ports**.
   e. Look in the Ports table and write down the following port settings for use in the next step:

<table>
<thead>
<tr>
<th>Cluster member 1</th>
<th>SIP_DEFAULTHOST</th>
<th>SIP_DEFAULTHOST_SECURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster member 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   f. Repeat this process for every cluster member.

2. Next, determine the ports used by every WebSphere proxy server that operates with this cluster.
   a. Back in the navigation tree, click **Servers > Server Types > WebSphere proxy servers**.
   b. In the table listing proxy servers, click the name of the WebSphere proxy server.
   c. On the Configuration page, look in the Communication section and click **Ports**.
   d. Look in the Ports table and write down the following port settings for use in the next step:
Repeat this process for every WebSphere proxy server used by the cluster.

3. Now add the ports collected in steps 1 and 2 to the deployment manager’s Virtual Hosts table:
   a. In the navigation tree, click Environment > Virtual Hosts.
   b. In the Virtual Hosts table, click the host called default_host.
   c. On the Configuration page, look in the Additional Properties section and click Host Aliases.
   d. In the Host Aliases table, add the ports used by all of the cluster members and proxy servers:
      Remember that you have information on two ports for each cluster member or proxy server; 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 until all of the ports you collected are listed in the table.
   e. Now delete all of the table entries that do not use * as the Host Name.
      Click the check box next to each entry you want to delete; then click the Delete button at the top of the table.
   f. Click Apply and then click the Save link in the Messages box at the top of the page.

4. Synchronize the nodes in the cluster:
   a. Click System Administration > Nodes.
   b. Select both nodes, and then click Full Resynchronization.

*Installing IBM Load Balancer for a Bandwidth 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.
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:
      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 45. 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>Cluster: 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 for a Bandwidth 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.
   a. **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.
   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. 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:
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 Bandwidth 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.
   
   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 `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
   ```

gh. 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.

Installing the Bandwidth Manager on a node:

Install IBM Sametime Bandwidth Manager on an IBM WebSphere Application Server node.

About this task

A Bandwidth Manager cluster supports two nodes; complete this installation and configuration task for each node. Remember, there is no need to install the Bandwidth Manager on a stand-alone Deployment manager profile, but you must install it on the application server node that is hosted in a Cell profile, as well as on any additional node.

Important: When installing and configuring the Bandwidth Manager on an application server node that is hosted on the same computer as a deployment
manager, be sure to work in the node's own profile directory rather than the deployment manager's profile. The node's profile looks like this:

**Linux**

**Microsoft Windows**

*Configuring a connection to the JDBC provider for the Bandwidth Manager:*

To create a connection to the Bandwidth Manager database hosted on the IBM DB2 server, you must configure IBM WebSphere Application Server to use the driver implementation classes that are encapsulated by the Java Database Connectivity (JDBC) provider.

**About this task**

Configuring the JDBC provider involves using the WebSphere Integrated Solutions Console to define a path to the location where the JDBC drivers reside.

**Procedure**

1. On the computer where WebSphere Application Server is installed, open the folder `WAS_install_root/deploytool/itp/plugins`.
   
   `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`.

2. Now locate the subfolder named `com.ibm.datatools.db2_2.0.101.vXXXXXXXXXXX`, where "XXXXXXXXXXX" is a 12-digit number.
   
   This is the path to the JDBC drivers; you will need this information later in step 5.

3. Log in to the WebSphere Integrated Solutions Console and the WebSphere administrator (the ID you created when you installed WebSphere Application Server).

4. Click **Environment tasks > WebSphere variables**.

5. Click on the environment variable called `DB2UNIVERSAL_JDBC_DRIVER_PATH`, and enter the complete path to the drivers you located in step 2 before clicking OK.
   
   The path will be `WAS_install_root/deploytool/itp/plugins/com.ibm.datatools.db2_2.0.101.vXXXXXXXXXXX`, where "XXXXXXXXXXX" is a 12-digit number.

6. Click the **Save** link in the "Messages" box at the top of the page.

7. Restart the server so the change can take effect.

*Downloading the Bandwidth Manager installation package to the node's computer:*

Download and extract the IBM Sametime Bandwidth Manager installation package to the server where you will install the application.

**About this task**

Download the installation package from either CD, DVD, or the IBM Passport Advantage site.
Procedure

1. (Linux RHEL only) If you have not done so already, disable SELinux on any RedHat operating system:
   a. Log in as root on the Linux RedHat server.
   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 (Linux).

3. Create a temporary folder called \TMP\BWM.

4. If you will install from CD or DVD, do the following:
   a. To ensure that the CD or DVD mounts with execution privileges enabled, mount it manually with the following command:
      ```bash
      mount /dev/cdrom /cdrom
      ```
      See your operating system documentation for additional instructions on mounting CDs and DVDs.
   b. From the installation media, copy the Sametime Bandwidth Manager installation image to the \TMP\BWM folder.

5. If you will install from downloaded packages, download the WebSphere Application Server installation image to the \TMP\BWM folder now. You can find the Bandwidth Manager installation files from the Sametime Media Manager disk in the Bandwidth Manager subfolder.
   For the installation package's part number, see the Sametime Download document at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   For instructions on how to locate and download the installation package to your server, see Using Passport Advantage to download IBM products.

6. When the installation package has been copied to your server, open a command window and navigate to the \TMP\BWM folder.

7. Extract all files to the temporary directory \TMP\BWM.

**Updating the db2.connection.properties file for a node:**

Update the db2.connection.properties file included in the IBM Sametime Bandwidth Manager installation package and add settings for your deployment.

**About this task**

The db2.connection.properties file is used during installation to create a new connection to the Bandwidth Manager database hosted on the deployment's IBM DB2 server. Update the file and specify settings for your deployment as explained here.

**Procedure**

1. Navigate to the \TMP\BWM folder containing the extracted installation files.
2. Update the db2.connection.properties file as follows:
   a. Change the properties of the db2.connection.properties file to make it editable if necessary.
This file was supplied with the Bandwidth Manager installation package and may be set to read-only.

b. Open the `db2.connection.properties` file for editing and change the following lines:

```properties
db2.login=DB2_Username
db2.password=DB2_Password
db2.connection.address=Host_name
db2.connection.port=DB2_Port
db2.schema=Schema_name
db2.connection.database=Database_Name
```

where:

- `DB2_Username` and `DB2_Password` are the credentials of the user who created the BWM_DATA database (usually the DB2 instance owner).
- `Host_Name` can be a short name, fully qualified domain name, or an IP address as long as it is addressable by both the install program and the Bandwidth Manager runtime. A fully qualified domain name is recommended. A short name is also possible to use as long as it is defined in the local hosts file (for example `system32/driver/etc/hosts` on Windows or `/etc/hosts` on Linux.
- `DB2_Port` is the DB2 server network port. The default is 50000, but change this to the appropriate value if your DB2 server uses a different port.
- `Schema_name` is the name of the database schema that will be used by the Bandwidth Manager. Typically the default database schema is used, which is named the same as the `DB2_Username`, but the schema must be in uppercase letters. On Linux, the schema name is case sensitive.
- `Database_Name` is the name you used to create the database, such as BWM_DATA.

For example:

```properties
db2.login=myDB2user
db2.password=myDB2passw0rd
db2.connection.address=db2svr.example.com
db2.connection.port=50000
db2.schema=MYDB2USER
db2.connection.database=BWM_DATA
```

c. Save and close the file.

**Updating the `websphere_configuration.properties` file for a node:**

Update the `websphere_configuration.properties` file included in the IBM Sametime Bandwidth Manager installation package and add settings for your deployment.

**About this task**

The `websphere_configuration.properties` file is used during installation to configure IBM WebSphere Application Server settings needed by the Bandwidth Manager. Update the file and specify settings for your deployment as explained here.

**Procedure**

1. Navigate to the `\TMP\BWM` folder containing the extracted installation files.
2. Update the `websphere_configuration.properties` file as follows:
a. Change the properties of the `websphere_configuration.properties` file to make it editable if necessary.
   This file was supplied with the Bandwidth Manager installation package and may be set to read-only.

b. Open the `websphere_configuration.properties` file for editing and change the following lines. These lines apply to any Bandwidth Manager installation.

   ```
   was.language=Language_abbreviation
   was.node=Node_name
   was.server=Server_name
   was.cell=Cell_name
   was.profilename=Profile_name
   was.home=WAS_install_root
   was.hostname=Host_name
   was.hostport=Host_port
   was.sipport=SIP_port
   was.httpport=HTTP_port
   was.userid=WAS_admin_username
   was.password=WAS_admin_password
   was.db2.driver.path=${WAS_INSTALL_ROOT}/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.102.vBuild_number/driver
   ```

   where:
   - `Language_abbreviation` defines the language to be used for console and log messages produced by the Bandwidth Manager server or administrative interface. This setting does not affect messages that are presented to end users. Use one of the following language abbreviations to choose the language. If the parameter is missing, the default Language is English.
     - `en` (English)
     - `de` (German)
     - `es` (Spanish)
     - `fr` (French)
     - `it` (Italian)
     - `ja` (Japanese)
     - `ko` (Korean)
     - `pt_BR` (Brazilian Portuguese)
     - `zh` (Simplified Chinese)
     - `zh_TW` (Traditional Chinese)
   - `Node_name`, `Server_name`, `Cell_name`, `Profile_name` and are the WebSphere Application Server node, server, cell, and profile names where the Bandwidth Manager application will be installed (the current WebSphere Application Server instance).
   - `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 and forward slashes or the installation will fail; for example: `C:\PROGRA~1\IBM\WebSphere\AppServer`.
   - `Host_Name` is the IP address or the fully qualified domain name of the server where you will install the Bandwidth Manager (the current WebSphere Application Server).
   - `Host_port`, `SIP_port`, and `HTTP_port` correspond to the values that are used by the target profile in WebSphere Application Server for `WC_adminhost`, `SIP_DEFAULTHOST`, and `WC_defaulthost`, respectively.
• WAS_admin_username and WAS_admin_password are the credentials of the WebSphere administrator (the credentials used for logging in to the Integrated Solutions Console). If administrative security is not enabled, you can omit the credentials.

• \$[WAS_INSTALL_ROOT] represents the WebSphere Application Server root installation directory. The install program looks for this exact designation; do not change it.

• Build_number is the build date that corresponds to the JDBC driver build date. To find the correct number, open the \$[WAS-Install-Root]/deploytool/itp/plugins folder and locate the folder named com.ibm.datatools.db2_2.0.102.vBuild_number, where Build_number is a 12-digit number.

For example:
was.language=ja
was.node=myWASnode
was.server=myWASserver
was.cell=myWAScell
was.profilename=AppServerProfile
was.home=C:\PROGRA~1\IBM\WebSphere\AppServer
was.hostname=myWASserver.example.com
was.httpport=9060
was.sipport=5060
was.userid=wasadmin
was.password=passw0rd
was.db2.driver.path=${WAS_INSTALL_ROOT}/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.102.v20091026_1945/driver

c. Change the following lines when installing Bandwidth Manager in a cluster.

was.cluster=Cluster_name
proxy.host=Proxy_host_name
proxy.port.http=Proxy_port
proxy.port.sip=Proxy_sip_port
portlet.node=Portlet_node_name

where:

• Cluster_name is the name of the cluster.

• Proxy_host_name is the IP address or the host name of the Proxy server where you will install the Bandwidth Manager (the current WebSphere Application Server).

• Proxy_port and Proxy_sip_port TO BE WRITTEN

• Portlet_node_name TO BE WRITTEN

For example:
was.cluster=
proxy.host=
proxy.port.http=
proxy.port.sip=
portlet.node=

d. Save and close the file.

Installing the Bandwidth Manager application on a node:

Install the IBM Sametime Bandwidth Manager application on a computer where IBM WebSphere Application Server is running.

Before you begin

Make sure that the IBM DB2 server is running and the database has been created. On the server where you will install the Bandwidth Manager, make sure the
appropriate IBM WebSphere Application Server instance is running, the installation package has downloaded and extracted, and the necessary files have been modified for your deployment.

**Procedure**

1. On the server where you will install the Bandwidth Manager, use a command line terminal or prompt, navigate to the \TMP\BWM folder containing the extracted installation files.
2. Run the following command to install the Bandwidth Manager:

   - **Linux**
     
     ```
     WAS_install_root/profiles/Profile_name/bin/ws_ant.sh -Dinstall.db=true
     ```
     
     where:
     
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application will be 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 -Dinstall.db=true
     ```

   - **Microsoft Windows**
     
     ```
     WAS_install_root\profiles\Profile_name\bin\ws_ant.bat -Dinstall.db=true
     ```
     
     where:
     
     - `Profile_name` is the WebSphere Application Server profile name where the Bandwidth Manager application will be 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 -Dinstall.db=true
     ```

     When `-Dinstall.db` is set to true, the install script drops any existing Bandwidth Manager tables and then creates clean tables in the database. If `-Dinstall.db` is set to false or is omitted, the install script does not drop or create Bandwidth Manager tables in the database, and any existing data is retained.

     **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 installation process may take up to 10 minutes. You may see failures indicated, for example, an indication that a number of SQL commands could not be executed. This is expected behavior, because the installation program script attempts to "drop" (delete) any existing tables in the database without first checking whether the tables actually exist.

**Enabling security on a node:**
Enable IBM WebSphere Application Server administrative security for the IBM Sametime Bandwidth Manager residing on that server.

**Before you begin**

Set administrative security for the WebSphere Application Server if it is not already set. When WebSphere Application Server administrative security is on, you are prompted for the administrator user name and password when you log in to the Integrated Solutions Console.

1. Log in to the Integrated Solutions Console as the WebSphere Application Server administrator.
2. In the navigation tree, click **Security > Global security**
3. Under Available realm definitions, select **Federated Repositories**, then click **Configure**.
4. (Optional) Change the realm name to "LdapRealm".
5. Enter the primary administrator user name, such as `wasadmin` and click **OK**.
6. Enter the primary administrator password, such as "passw0rd" and click **OK**.
7. Click **Save** in the Messages box at the top of the page.
8. On the Global security page, select **Federated Repositories** again, and click **Set as current**.
9. Click **Save** in the Messages box at the top of the page.
10. On the Global security page, select **Enable administrative security**, but do not select **Use Java 2 security to restrict application access to local resources**.
11. Click **Save** in the Messages box at the top of the page.
12. Restart the Bandwidth Manager server to put the changes into effect.

**About this task**

Follow these steps to set administrative security and create an administrator for the Bandwidth Manager server.

**Procedure**

1. Log in to the Integrated Solutions Console as the WebSphere administrator.
2. Disable Java 2 security on local resources:
   a. In the navigation tree, click **Security > Global security**.
   b. Under "Java 2 security" deselect the option **Use Java 2 security to restrict application access to local resources**.
   c. Click **Apply**, and then click **Save** in the Messages box at the top of the page.
3. Enable access to the Common Object Request Broker Architecture (CORBA) name service for all service groups:
   a. In the navigation tree, click **Environment > Naming > CORBA Naming service groups**.
   b. In the service groups table, click the **EVERYONE** link.
   c. In the in the "General Properties" section, add the following **Roles** by clicking within the list and then using Shift+click to add each role until all are selected:
      - Cos Naming Read
      - Cos Naming Write
      - Cos Naming Create
• Cos Naming Delete
A selected role appears highlighted.

<table>
<thead>
<tr>
<th>CORBA naming service groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CORBA naming service groups</strong> &gt; <strong>EVERYONE</strong></td>
</tr>
<tr>
<td>Use this page to configure a group with authorization roles (name service). The available group roles, in alphabetical order: CosNaming, authorization policy is enforced only when global role assignment result in a org.omg.CORBA.NO_PERM</td>
</tr>
<tr>
<td><strong>General Properties</strong></td>
</tr>
<tr>
<td>+ Group</td>
</tr>
<tr>
<td>EVERYONE</td>
</tr>
<tr>
<td>+ Role(s)</td>
</tr>
<tr>
<td>Cos Naming Read</td>
</tr>
<tr>
<td>Cos Naming Write</td>
</tr>
<tr>
<td>Cos Naming Create</td>
</tr>
<tr>
<td>Cos Naming Delete</td>
</tr>
<tr>
<td><strong>Apply</strong>  <strong>OK</strong>  <strong>Reset</strong>  <strong>Cancel</strong></td>
</tr>
</tbody>
</table>

d. Click **Apply**, and then click **Save** in the Messages box at the top of the page.

4. Create a new user as the Bandwidth Manager administrator. This administrator is not the same as the WebSphere Application Server administrator.
   a. In the navigation tree, click **Users and Groups** > **Manage Users**.
   b. Click the **Create** button at the top of the users table.
   c. Fill in information for the new administrator:
      - User ID
      - First name
      - Last name
      - Password
      - Confirm password
   d. Click the **Create** button at the bottom of the page to generate the new account. Enable administrative security when you are prompted to do so.
   e. When the **The user was created successfully** message appears, click the **Close** button.

5. Now add the new administrator to all security roles:
   a. In the navigation tree, click **Users and Groups** > **Administrative user roles**.
   b. Click **Add** at the top of the roles table.
   c. In the “Roles” list at the top of the page, use **Shift+click** to add each role until all are selected.

   **Tip:** Only the “All Authenticated Users” is required but you should select all roles to ensure that the new administrator has full access to the Bandwidth Manager application.

d. In the “Search and Select Users” section of the page, click the **Search** button (located next to the “Search string” field).
The search results appear in the “Available” list below the field.

e. Select the administrator you created earlier, and click the Add button (the right-facing arrow) to add that user to the "Mapped to role" list.

f. Click OK, and then click Save in the Messages box at the top of the page.

6. Stop and restart the IBM WebSphere Application Server:

   a. Open a command window.

   b. Change to the profile directory of the WebSphere Application Server hosting the Bandwidth Manager.

   c. Run the following commands:

      Supply your WebSphere administrative credentials when stopping the server. Be sure the server has fully stopped before starting it again.

      **Linux**
      ```
      ./stopServer.sh server1 -username was_admin_user -password was_admin_password
      ./startServer.sh server1
      ```

      **Microsoft Windows**
      ```
      stopServer.bat server1 -username was_admin_user -password was_admin_password
      startServer.bat server1
      ```

Verifying the Bandwidth Manager installation on a node:

After completing the basic installation for an IBM Sametime Bandwidth Manager, verify that the installation was successful.

About this task

For best results, you should verify that the Bandwidth Manager installation was successful before you proceed to configure the new server.

Procedure

1. On the computer hosting the Bandwidth Manager, stop and restart the IBM WebSphere Application Server:
a. Open a command window.
b. Change to the profile directory of the WebSphere Application Server hosting the Bandwidth Manager.
c. Run the following commands:
   Supply your WebSphere administrative credentials when stopping the server. Be sure the server has fully stopped before starting it again.
   **Linux**
   ```bash
   ./stopServer.sh server1 -username was_admin_user -password was_admin_password
   ./startServer.sh server1
   ```
   **Microsoft Windows**
   ```bash
   stopServer.bat server1 -username was_admin_user -password was_admin_password
   startServer.bat server1
   ```
2. Log in to the Integrated Solutions Console as the WebSphere administrator (the credentials used for installing the Bandwidth Manager).
3. Look at the lower left portion of the console (the navigation tree) and verify that a new set of tasks appears, named **Sametime Servers**.
4. In the navigation tree, click **Sametime Servers** and verify that the **Bandwidth Manager** link appears.
5. Click on **Bandwidth Manager**, then click the **Status** tab and verify that **MediaSessionController**, **SipFrontend**, and at least one **BandwidthPoolManager** component appear in the table.

**What to do next**

If the components appear in the table, the installation was successful. Otherwise, the installation failed. If the installation fails, follow these steps to try again:
1. Delete the Bandwidth Manager profile using the following command:
   **Linux**
   ```bash
   /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -delete -profileName BWMProfile
   ```
2. Create the profile again.
3. Install Bandwidth Manager again using the instructions for Installing the Bandwidth Manager application on the stand-alone computer.

**Important:** Even if the installation was successful, do not click the **Start/Restart** button in the Status table; you must complete the Bandwidth Manager's initial configuration first as explained in the tasks that follow.

**Connecting a Bandwidth Manager node to the LDAP server:**

Configure the IBM WebSphere Application Server federated repository for LDAP access.

**About this task**

The LDAP server must be running when you configure access to it.

**Procedure**

1. Disable secure access to Virtual Member Manager.
   a. On the server running the Bandwidth Manager module, open the `wimconfig.xml` file.
   **Linux**
   **Standalone server**
b. Search for the string `isSecurityEnabled` and change the value to false.
c. Save the file.

2. Stop and restart the application server.

3. Log in to the Integrated Solutions Console as the WebSphere administrator.

4. In the navigation tree, click Security > Global security.

5. Locate the "User account repository" sections of the Global Security page.

6. In the Available realm definitions list, select Federated repositories and click the Set as current button.

7. Click Configure button and define settings for the LDAP connection:
   
a. On the "Federated Repositories" page, type a descriptive name, such as LdapRealm, in the Realm name field.
   
b. In the Primary administrative user name field, type the user name (only the user name itself, not the full distinguished name) of the LDAP server's administrative user. The user must be in the LDAP repository.
   
c. Click the Add Base entry to Realm button in the "Repositories in the realm" table.
   
d. On the "Repository reference" page, click the Add Repository button.
   
e. Under "LDAP server," fill in properties for your LDAP directory:

<table>
<thead>
<tr>
<th>Repository identifier</th>
<th>Type a descriptive name, such as LDAP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory type</td>
<td>Select the LDAP directory used by your deployment.</td>
</tr>
<tr>
<td>Primary host name</td>
<td>Enter the short host name, fully qualified domain name, or IP address of the server where the LDAP directory resides. The fully qualified domain name is recommended.</td>
</tr>
</tbody>
</table>

f. Under "Security," fill in security settings for your LDAP directory:

<table>
<thead>
<tr>
<th>Bind distinguished name</th>
<th>Type the user name and domain name of a user with full permissions to access the LDAP server. Use LDAP canonical name format; <code>cn=administrator,cn=users,o=ibm</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind password</td>
<td>Type the password for the LDAP user specified in the Bind distinguished name field.</td>
</tr>
<tr>
<td>Login properties</td>
<td>Delete the &quot;uid&quot; string that appears in this field, and leave the field blank.</td>
</tr>
</tbody>
</table>

g. Click the Apply button, and then click the Save link in the "Messages" box at the top of the page.

If an error message appears, double-check the settings you entered, particularly the Bind distinguished name, and correct the settings as needed.
When the LDAP settings are configured correctly, a web page appears so that you can enter two more distinguished names.

8. For both occurrences of the **Base entry distinguished name** field, type the Base search entry, for example, ou=sametime,dc=lotus,dc=com. Then click **OK**. The "Federated Repositories" page reappears, and you can continue configuring the LDAP connection.

9. Click the **Apply** button, and then click the **Save** link in the "Messages" box at the top of the page.

10. The Bandwidth Manager server uses the **uid** attribute internally to search for users through the Virtual Member Manager. If the **uid** attribute does not map directly to the corresponding **uid** in the LDAP directory, change the mapping in the **wimconfig.xml** file to map the **uid** attribute to a different LDAP attribute.

For example, it is common that the Media Manager server uses the **mail** identifier to identify users in the SIP URI, from which Bandwidth Manager extracts user IDs for lookup in the Virtual Member Manager.

The following example maps the Virtual Member Manager **uid** attribute to the LDAP **mail** attribute:

```xml
<config:attributeConfiguration>
  ...
  <config:attributes name="mail" propertyName="uid">
    <config:entityTypes>PersonAccount</config:entityTypes>
  </config:attributes>
  ...
</config:attributeConfiguration>
```

11. The Bandwidth Manager server uses the **email** attribute in the LDAP directory to look up users in the LDAP directory and assign the correct call rate policy. If your LDAP directory uses a different attribute for users’ email addresses, such as **mail**, **email**, and **emailAddress**, change the mapping in the **wimconfig.xml** file to map the **mail** attribute to a different LDAP attribute.

The following example comments out the default mapping of **samAccountName**.

```xml
<config:attributeConfiguration>
  ...
  <!--
  <config:attributes name="samAccountName" propertyName="uid">
    <config:entityTypes>PersonAccount</config:entityTypes>
  </config:attributes>
  -->
  ...
</config:attributeConfiguration>
```

Add the appropriate mapping in the attributeConfiguration section of the **wimconfig.xml** file. This example maps the **uid** attribute to the **mail** attribute.

```xml
<config:attributeConfiguration>
  ...
  <config:attributes name="mail" propertyName="uid">
    <config:entityTypes>PersonAccount</config:entityTypes>
  </config:attributes>
  ...
</config:attributeConfiguration>
```

12. Close and save the **wimconfig.xml** file.

13. If you have more than one LDAP directory, repeat the previous two steps on all directories.
Verifying the SIP Proxy and Registrar virtual host used by the Bandwidth Manager

Verify that the correct virtual host settings are used by the IBM Sametime Media Manager’s SIP Proxy and Registrar before you configure the IBM Sametime Bandwidth Manager to use that server.

About this task

This task is required once per deployment (for a stand-alone Bandwidth Manager or for a cluster of Bandwidth Managers).

Procedure

1. Log in to the Integrated Solutions Console as the WebSphere administrator on the server hosting the Media Manager’s SIP Proxy and Registrar (for a cluster, use the deployment manager).

2. Determine the port used by the SIP_ProxyRegHOST:
   Make a note of this port number so you can use it later when you configure the Bandwidth Manager to use the SIP Proxy and Registrar.
   a. In the navigation tree, click Servers > Server Types > WebSphere application servers.
   b. On the Status page, click the link for the server hosting the SIP Proxy and Registrar component.
   c. On the Configuration page, locate the Communications section, and then click on Ports.
   d. In the Ports table, locate the SIP_ProxyRegHOST and write down its port value.

3. Verify the SIP Proxy server’s virtual host:
   a. Back in the navigation tree, click Applications > Application Types > WebSphere enterprise applications.
   b. In the Enterprise Applications table, click IBM Lotus SIP Proxy.
   c. On the Configuration page, locate the Web Module Properties section, and then click Virtual hosts.
   d. Verify that the virtual host is set to sip_proxyreg_host.
      If necessary, set it now by clicking sip_proxyreg_host in the list, clicking OK, and then clicking the Save link in the Messages box at the top of the page.

4. Verify the SIP Registrar server’s virtual host:
   a. Back in the navigation tree, click Applications > Application Types > WebSphere enterprise applications.
   b. In the Enterprise Applications table, click IBM Lotus SIP Registrar.
   c. On the Configuration page, locate the Web Module Properties section, and then click Virtual hosts.
   d. Verify that the virtual host is set to sip_proxyreg_host.
      If necessary, set it now by clicking sip_proxyreg_host in the list, clicking OK, and then clicking the Save link in the Messages box at the top of the page.

5. Log out of the Integrated Solutions Console.
Setting up routing from the SIP Proxy and Registrar to the Bandwidth Manager

To ensure that the IBM Sametime Media Manager's SIP Proxy and Registrar routes communications to the IBM Sametime Bandwidth Manager, create a routing rule.

Procedure

1. On the server hosting the SIP Proxy and Registrar component, 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>Record route mode</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>Parallel search mode</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>Add public IP to outgoing request</td>
<td>Always select this option when you Bandwidth Manager is deployed. 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 New to create a new routing rule.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>To define a condition based on the method used for the incoming initial request, choose one or more methods from the list. If you do not select a method, any method is allowed.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source Address</td>
<td>To define a condition based on the originating IP address, select Source Address and define the IP address to be matched. For example, 192.0.2.12 matches a SIP request with the exact IP address of 192.0.2.12.</td>
</tr>
<tr>
<td>Request-URI</td>
<td>The Request URI (Uniform Resource Identifier) identifies the resource, usually the origin server, on which to apply the request. To define a condition based on the Request URI of an incoming initial request, select Request URI and define the Request-URI. For example: .<em>example..</em> matches incoming initial requests with sip:example.com:5060;transport=tcp or sips:subdomain.example.com:5061.</td>
</tr>
<tr>
<td>Contact Header</td>
<td>A contact header identifies the specific originator of the request. To define a condition based on the contact header of the request, select Contact Header and specify the header for the condition. For example: .<em>20100@192.168.0.100:506[01].</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>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>The scheme can be either SIP or SIPS, which is a secure version of SIP. The default is SIP. This field is required.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or the fully qualified host name of the server. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on the server through which requests are routed. This field is optional. If you do not provide a value, the server uses the correct port.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Determines the network transport mechanism to use for sending SIP messages: TCP or TLS. This field is optional. If you do not provide a value, the server supplies a transport protocol. UDP is not supported.</td>
</tr>
</tbody>
</table>

8. Click OK.
9. Restart the SIP Proxy and Registrar.

**Configuring the Bandwidth Manager to use the SIP Proxy and Registrar server**

Configure IBM Sametime Bandwidth Manager to use the Sametime Media Manager's SIP Proxy and Registrar.
About this task

This task is required for both a stand-alone Bandwidth Manager and a cluster of
Bandwidth Managers. Communications between the Bandwidth Manager and the
Media Manager are handled by the SIP Proxy and Registrar.

Procedure

1. Log in to the Bandwidth Manager server's Integrated Solutions Console as the
   WebSphere administrator (in a cluster, use the deployment manager).
2. In the navigation tree, click **Sametime Servers > Bandwidth Manager**.
3. On the Status page, click the **Configuration** tab.
4. Change the **SIP Server URI** field to:
   ```
   [sip|sips]:[SipProxyIPAddress]:ProxyRegistrarHostPort;transport=[tcp]
   ```
   where:
   - You use **sip** for a non-secure port and **sips** for a secure port.
   - **SipProxyIPAddress** is the IP address of the SIP Proxy and Registrar server
     (for a cluster, use the deployment manager's IP address).
   - **ProxyRegistrarHostPort** is the SIP_ProxyRegHOST port number that you
     noted when confirming the SIP Proxy and Registrar virtual host.
   - The transport setting matches the setting that you specified for force-routing
     the SIP Proxy and Registrar.
5. Click **Apply** and then click the **Save** link in the Messages box at the top of the
   page.
6. Restart the Bandwidth Manager server (or cluster):
   - Stand-alone server:
     a. Click the **Status** tab.
     b. On the Status page, click the **Start/R startup** button at the top of the table.
     c. After a few seconds, click the **Refresh** button and verify that all three
        Bandwidth Management components are 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
           ```

Verifying that the Bandwidth Manager can access the LDAP
server

Verify that the IBM WebSphere Application Server administrator can access the
LDAP server used by IBM Sametime Bandwidth Manager.
About this task

After you have disabled security for WebSphere Application Server virtual member manager, you should verify that the administrator can still access the LDAP server. You can verify access by running a quick search against the LDAP directory as explained here.

Procedure

1. On the server hosting the Bandwidth Manager, open the WebSphere Integrated Solutions Console and log in as the WebSphere administrator.
2. On the navigation tree, click Sametime Servers > Bandwidth Manager.
3. On the Status page, click the Groups tab.
4. On the Groups page, click the New button at the top of the Groups table. You will not actually create a new group, but you can use this page to search the LDAP for a user, which will indicate whether you can access the LDAP server.
5. On the New Group page, navigate to the Assign Members section, click the Search By list, and then select User.
6. In the Search field, type a name that you know is stored in the LDAP directory (for example, your own user name). Type either a full user name or a partial user name followed by the * wild card.
7. Click the Search button. If you have a valid connection to the LDAP server, the user information is displayed in a table below the Search fields.

Installing 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. The Sametime TURN Server is available for installing on the Linux or Windows platforms only.

Installing the Sametime TURN Server files

Deploying IBM Sametime TURN Server involves installing a Java Run-time Environment (JRE) plus some additional files. Unlike other Sametime servers, the TURN Server does not require IBM WebSphere Application Server.

Procedure

1. Install IBM JRE 1.6 (or later) on the server. JRE 1.6 is installed with WebSphere Application Server on the Sametime Media Manager and you can copy the jre directory to the TURN server.
2. Create a new directory, where you will install the TURN Server files. For example, on Windows you might call the directory: C:\TURN.
3. Copy the files from SametimeMediaManager/TURN_Server into the new directory. The Sametime TURN Server is packaged with the Sametime Media Manager; you can copy the files from the computer where you downloaded the Media Manager package.
4. If Java is in your system path, skip this step. If Java is not in the system path, edit the run batch file and insert the path to the Java executable. Insert the path right before the “java.exe” reference in the command; for example in the Windows version (run.bat):
   C:\Program Files\Java\jreX.XXX\bin\java.exe
5. Run the batch file to start the TURN Server:
   
   **Linux**
   
   run.sh
   
   **Windows**
   
   run.bat

### Enabling NAT traversal

Enable the NAT traversal feature by editing the `stavconfig.xml` file on the IBM Sametime Media Manager’s Conference Manager component.

#### Procedure

1. On the server hosting the Conference Manager, open the `stavconfig.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.

2. Set the value for `NATTraversalEnabled` to `true`.
   
   For example:
   
   `<configuration lastUpdated="1226425838277" name="NATTraversalEnabled" value="true"/>

3. Save and close the file.

4. If the Conference Manager is clustered, synchronize all nodes in the cluster:
   
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.

   b. Click **Full Resynchronize**.

### Configuring firewalls and opening ports

If the IBM Sametime TURN Server and the Sametime Media Manager are separated from clients by firewalls, you must open ports in the firewalls to enable communications.

#### About this task

Use the information in “Port allocations for NAT traversal” on page 117 to help you determine which ports need to be opened.

### Configuring the Media Manager to use the TURN Server

Configure the IBM Sametime Media Manager to work with the Sametime TURN Server.

#### About this task

On the Sametime System Console, configure the Media Manager to use the new TURN Server.

#### Procedure

1. On the server hosting the Sametime System Console, 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. Locate the "NAT Traversal" section at the bottom of the page.
6. Under "TURN server" fill in one of the following, based on the protocol you are using:
   - UDP: Type the TURN Server's fully qualified domain name (FQDN) in the *Turn Server UDP host name* field (leave it set to "0.0.0.0" if you are not using this protocol).
   - TCP: Type the TURN Server's fully qualified domain name (FQDN) in the *Turn Server TCP host name* field (leave it set to "0.0.0.0" if you are not using this protocol).
7. You can leave the other settings with their default values.
8. Click **OK**.
9. Restart the Sametime Media Manager (not the Sametime System Console) so these changes can take effect.

**Deploying a load balancer with Sametime TURN Servers**

Although IBM Sametime TURN Server cannot be clustered for high availability, you can provide some additional service by deploying multiple TURN Servers with a load balancer to distribute the workload.

**Before you begin**

Before deploying a load balancer, make sure that all of the TURN Servers can communicate with each other (from each server, ping each of the other servers to ensure network reachability).

**Installing IBM Load Balancer for use with Sametime TURN Servers:**

Install IBM Load Balancer to distribute workload among multiple Sametime TURN Servers.

**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:
      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>
</table>
| Load balancer:           | Load balancer               | Load balancer (NFA):
                          loadbal.example.com       | 192.0.2.15                |
| Cluster:                 | (Cluster address)           | Cluster: 192.0.2.0        |
| st-cluster.example.com   |                             |                           |
| stconsole.example.com    | Deployment Manager          | 192.0.2.3                 |
|                          | (Sametime System Console)   |                           |
| svr1.example.com         | Primary Node                | 192.0.2.4                 |
|                          | (a Sametime server)         |                           |
| svr2.example.com         | Secondary Node              | 192.0.2.5                 |
|                          | (a Sametime server)         |                           |

Configuring IBM Load Balancer for use with Sametime TURN Servers:

Configure IBM Load Balancer to direct connections to individual Sametime TURN
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 use with Sametime TURN Servers (Linux):

Configure an IBM Load Balancer on Linux to direct connections to individual
Sametime TURN Servers.
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:
   ```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:
   ```bash
   start usr/bin/autoconf6 " " -A
   ```

**Linux**

Run the following command (you must be logged in as root):
```bash
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:
```bash
ifconfig device inet6 plumb
ifconfig device inet6 address/prefix up
```

**d.** Start the executor function of the dispatcher:
```bash
dscontrol executor start
```

**e.** Add the cluster to the service:
```bash
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:
```bash
stms-cluster.example.com
```

**f.** Add the cluster port:
```bash
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:
```bash
stms-cluster.example.com@80
```

**g.** Add the nodes for which this server will balance workload:
```bash
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:
  ```bash
  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:
  ```bash
  stms-cluster.example.com@80@meetsvr2.example.com
  ```

**h.** Now start the Load Balancer administration interface with the following command:
```bash
./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:
      
      dcontrol 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:
      dcontrol manager start
   c. Start the HTTP advisor for the port you are using (the port you specified in
      the previous steps, typically port 80):
      dcontrol 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:
      dcontrol port set fully_qualified_host_name@port_number sticktime 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:
      dcontrol 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 use with Sametime TURN Servers (Windows):

Configure an IBM Load Balancer on Microsoft Windows to direct connections to individual Sametime TURN Servers.

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 `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@80meetsvr1.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@80meetsvr2.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**.

**Configuring the TURN Server for load balancing**

Create or modify the IBM Sametime TURN Server’s properties file and add settings for use with the load balancer.
Before you begin

Install and configure the load balancer, and define the loopback interface.

About this task

Complete this task on every TURN Server.

Procedure

1. On the computer hosting the TURN Server, locate the TurnServer.properties file and open it for editing.
   This file is stored in the directory where you installed the TURN Server files. If the file does not exist, you can create it now using any text editor.
2. Add the following statements to the file:
   - `turn.loopback.hostname.ipv4=Load_balancer_Loopback_IP`
     The IP address on which requests are sent to the load balancer for the TURN servers (the loopback address in the TURN servers themselves).
   - `turn.local.hostname.ipv4=TURN_Server_local_IP`
     The physical IP address of the host where the TURN Server will be listening for client connections. This a real IP address of the host computer, not the loopback address.
   - `turn.allocation.hostname.ipv4=TURN_Server_local_IP`
     The IP address where the TURN server should allocate the relayed ports. In most cases this IP address will be the same as the `turn.local.hostname.ipv4` value.
   - `turn.redirect.hostname.ipv4=TURN_Server_external_IP`
     The IP address where the TURN server should redirect the initial client requests coming from the load balancer. In most cases this IP address will be the same as the `turn.local.hostname.ipv4` value but in some cases where the physical IP address of the TURN server is not directly accessible by the clients (such as a private address), use the address that is accessible for the clients.
   - `turn.public.hostname.ipv4=TURN_Server_reflexive_IP`
     The IP address that the TURN server should publish as the allocated IP address. In most cases this IP address will be the same as the `turn.local.hostname.ipv4` value but in some cases where the physical IP address of the TURN server is not directly accessible such as a private address), this address will specify the NAT reflexive address that is accessible.

Note: Note that the `turn.local.hostname.ipv4` and the `turn.redirect.hostname.ipv4` (if specified) IP addresses should be open in the firewall on the same port to ensure that clients can connect to the TURN Server using the specified addresses.
3. Save and close the file.
4. Restart the TURN Server so the changes can take effect.
5. Repeat these steps on each additional TURN Server.

Installing a Lotus SIP Edge Proxy Server

The IBM Lotus SIP Edge Proxy is a SIP Application installed over a WAS server. Since there is no specific installer for the IBM Lotus SIP Edge Proxy server, you can
use the SIP Proxy/Registrar installer and then perform manual steps in order to adjust the environment to the Lotus SIP Edge Proxy.

**Deploying Lotus SIP Edge Proxy Server in a stand alone environment**
You can install the IBM Lotus SIP Edge Proxy in a stand alone environment.

**Before you begin**

The host names for the SIP Proxy/Registrar, Conference Manager, Packet Switcher, and Community Server must be all different. The Proxy/Registrar host name should be the local host, and the others should be different from the Proxy/Registrar host name and also from each other. For example:

- Proxy/Registrar host name: pr1.example.com
- Conference Manager host name: cf1.example.com
- Packet Switcher host name: ps1.example.com (it cannot be host name cf1.example.com since this is the Conference Focus host name)

**Procedure**

1. Start the Media server installer.
2. Deselect the **Use Sametime System Console to install** option.
3. Select **Stand alone (Cell and Primary nodes)** installation type.
4. To avoid installing the Conference Manager and the Packet Switcher applications on the Edge Proxy's machine, enter the following values in the **common configuration** page. Each name must be unique, as described in the "Before you begin" section above:
   - For the **SIP Proxy/Registrar Server Host Name** field, enter the local machine's host name.
   - For the **Conference Manager Host Name** and **Packet Switcher Host Name** fields, enter a different host name (not the local host name).

   **Note:** The Edge Proxy does not require a Community Server. Due to installer limitations, you should still enter a value in the **Community Server Host Name** field. This value must be a resolvable host name, but the Community Server should not be installed in this host.
   - For the **Community Server Host Name** field, enter a resolvable host name.
5. Click **Validate**.
6. In the next page, select the **Configure LDAP after the installation** option.
7. Click **Next** until completion.
8. In the WebSphere Application Server administrative console, browse to **Applications > Websphere Enterprise Applications**.
9. Uninstall the following applications:
   - IBM Lotus SIP Proxy
   - IBM Lotus SIP Registrar
   - SSC connector
10. If the Conference Manager and the Packet Switcher applications are installed too, uninstall them.
11. Download the latest SIP Edge Proxy application from the STIAV installation package. The package is in a subdirectory called **SIPEdgeProxy**.
12. Download the **fe.zip** file and unzip it to a temporary directory.
13. In the administrative console, browse to Applications > Websphere Enterprise Applications.
14. Click Install.
15. Specify the fully qualified path to the SIP Edge proxy application file (EdgeProxyAppI.ear).
16. Click Next until you reach the Map modules to servers page. Be sure to verify that the application is installed on the correct server.
17. Click Apply.
18. Click Next until you reach the last wizard page and then click Finish.
19. Save the changes by clicking the Save link in the Messages box at the top of the page.

Configuring SIP ports:

To set up ports for the IBM Lotus SIP Edge Proxy, an administrator needs to determine the SIP ports used for the SIP Proxy/Registrar and ensure that the Lotus SIP Edge Proxy listens on these same ports.

About this task

The Lotus SIP Edge Proxy must listen on the same ports as the SIP Proxy/Registrar. To determine the SIP ports used by the SIP Proxy/Registrar, log in to SIP Proxy/Registrar ISC administrative console.

Find the SIP Proxy/Register ports in a stand alone environment:

Procedure
1. Click Servers > WebSphere application servers.
2. Click <server name>.
4. Look in the Ports table and record the following port settings for use in the next step:
   - SIP_ProxyRegHOST
   - SIP_ProxyReg_SECURE

Find the SIP Proxy/Register ports in a clustered environment:

Procedure
1. Click Servers > WebSphere proxy servers.
2. Click <proxy name that sits in front of the SIP Proxy/Registrar cluster>.
4. Look in the Ports table and record the following port settings for use in the next step:
   - PROXY_SIP_ADDRESS
   - PROXY_SIPS_ADDRESS

Change the SIP Edge proxy SIP ports:

Procedure
1. Log in to the Lotus SIP Edge Proxy ISC administrative console
2. Click Servers > WebSphere application servers.
3. Click <server name>.
4. Under Communications, click Ports.
5. Ensure that SIP_ProxyRegHOST and SIP_ProxyReg_SECURE ports do not have the same values as the SIP ports used by the SIP Proxy/Registrar. Change to different values if needed.

6. Click SIP_DEFAULTHOST

7. Type in the Port field the value of the non-TLS port used by the SIP Proxy/Registrar (SIP_ProxyRegHOST or PROXY_SIP_ADDRESS) and then click OK.

8. Click SIP_DEFAULTHOST_SECURE.

9. Type in the Port field the value of the TLS port used by the SIP Proxy/Registrar (SIP_ProxyReg_SECURE or PROXY_SIPS_ADDRESS) and then click OK.

10. Save your changes by clicking the Save link

11. Change the corresponding ports in the virtual host setting.

12. Click Environment > Virtual Hosts.

13. Click default_host.


15. Click the "*" link for the corresponding SIP port and change it to the port value used by the SIP Proxy/Registrar.

16. Remember that you have information on two ports.

17. Save your changes.

Additional settings:

Procedure

1. Click Servers > WebSphere application servers and then perform the following steps:
   a. In the administrative console, browse to Security > Global security > Web and SIP security > general settings
   b. Make sure that the Use available authentication data when an unprotected URI is accessed option is deselected.

2. In the administrative console, browse to: Servers > WebSphere Application Server > server name > SIP Container Settings (under "Container settings") > SIP Container > Custom properties and set the following property:
   - Name: com.ibm.ws.sip.sent.by.host
   - Value: <the FQDN of SIP Edge Proxy server>

   Note: This property may be already exists after the installation. If it does, make sure that its value is the Lotus SIP Edge Proxy host name.

3. In the administrative console, browse to Servers > WebSphere Application Server > server name > SIP Container Settings (under "Container settings") > SIP Container > Custom properties and remove the com.ibm.ws.sip.security.trusted.iplist property

   Note: The sections detailed in steps 4 and 5 are relevant only if you setup LDAP server during the installation process. If you selected the Configure LDAP after the installation option as mentioned in step 5 under "Installing the SIP Edge Proxy" do not perform steps 4 and 5.

4. In the administrative console, browse to Security > Global security > Configure and remove the entry that points to the LDAP repository.

5. In the administrative console, browse to Security > Global security > Configure > Manage repositories and remove the entry that points to the LDAP repository
Modifying Lotus SIP Edge Proxy settings in the edge-proxy.xml file:

An administrator can edit the edge-proxy.xml file manually to modify IBM Lotus SIP Edge Proxy server configuration settings.

Before you begin

Since there are no SSC administrative pages for the Lotus SIP Edge Proxy configuration, any configuration updates must be performed manually by editing the edge-proxy.xml file.

Procedure

1. On the Lotus SIP Edge Proxy deployment manager's machine, open the edge-proxy.xml file located in the `<dm profile>/config/cells/<cell>/applications/EdgeProxyApp1.ear/deployments/EdgeProxyApp1/EdgeProxyWeb.war/WEB-INF/` directory.
   - The authoritativeProxy section contains the hostname, port, and transport of the SIP Proxy/Registrar:
     - Specify the SIP port used for TCP.
     - Specify the SIP port used for TLS.
   - The edgeProxy section contains the hostname, port, and transport of the Lotus SIP Edge Proxy:
     - Specify the SIP port used for TCP.
     - Specify the SIP port used for TLS.
   - The authProxySourceAddr section specifies the address of the SIP Proxy/Registrar. When the Lotus SIP Edge Proxy receives stand-alone or initial requests, it determines the remote address from which the request was received. If the remote address does not match the SIP Proxy/Registrar address, the request is sent to the SIP Proxy/Registrar for further processing. Supported values: IP address, regular expression that matches the SIP Proxy/Registrar address (for example, "10.10.102.14 | 10.10.102.16").

   For example (settings for TCP):
   ```xml
   <authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5060" authProxyTransport="tcp" authProxySourceAddr="10.10.102.14"/>
   ```
   For example (settings for TLS):
   ```xml
   <authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5061" authProxyTransport="tls" authProxySourceAddr="10.10.102.14"/>
   ```

   Note: Use the same transport as for Media Manager components. For example, if the CF is configured to use TLS, set the authProxyTransport attribute to TLS as well.

2. After editing, copy the changed file to `<dm-profile>/config/cells/<cell-name>/nodes/<node>/servers/<server>`.

3. Synchronize all of the nodes in the cell as follows:
   a. Log into the Deployment Manager, and then click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.

Replacing the default certificate used by the Lotus SIP Edge Proxy:
To avoid the problem of IBM Sametime clients rejecting the certificate issued for the IBM Lotus Edge Proxy server, an administrator needs to replace the default certificate on the Lotus SIP Edge Proxy so that it contains the SIP Proxy/Registrar’s FQDN.

**About this task**

These instructions are for the default certificate, which is meant for internal communications (not meant to act as a CA). Sametime clients verify that the certificate was issued for the SIP Proxy/Registrar. In a Lotus SIP Edge Proxy deployment, the client opens a TLS connection to the Lotus SIP Edge Proxy resulting in the client receiving a certificate issued for the Lotus SIP Edge Proxy server. This certificate will be rejected by the client.

**Procedure**

1. Log in to WebSphere Application Server administrative console where the Lotus SIP Edge Proxy is installed.
2. Click Security > SSL certificate and Key management > Manage endpoint security configurations.
3. Expand Inbound and click the node where the Lotus SIP Edge Proxy is installed.
4. Click Manage Certificates.
5. Click Create chained certificate.
6. Complete the form. Specify an alias (such as, sip-pr-cn-cert), common name (FQDN of the SIP Proxy/Registrar), organization for the new certificate (IBM), and country (US).
7. Click OK and Save.
8. On the Manage endpoint security configurations page, click the node again, and then click Manage Certificates to view the old and new certificates.
9. Select the old certificate and click Replace.
10. Select the new certificate and select the Delete old certificate and the Delete old signers options.
11. Click OK and Save.
12. Stop and restart all WebSphere application server processes.

**Exchanging certificates between the Lotus SIP Edge Proxy and the SIP Proxy/Registrar servers:**

If you configured to use TLS between the IBM Lotus SIP Edge proxy and the SIP Proxy/Registrar, then you need to exchange certificates between two servers.

**About this task**

These instructions are for the default certificate. This certificate is meant for internal communications (not meant to act as a CA). Exchange the root certificates between the servers so that you can change the personal certificate without any impact to communication between the SIP edge proxy and the SIP Proxy/Registrar servers. Follow the instructions below to extract the root certificate from the SIP Edge Proxy:
**Procedure**

1. In WebSphere Application Server administrative console hosting the SIP Edge Proxy, click **Security > SSL certificates and key management > Key stores and certificates**.
2. Select **CellDefaultTrustStore**.
3. Click **Signer certificates**.
4. Select the root certificate (with default alias).
5. Click **Extract**.
6. Specify the file name and click **OK**.
7. Copy the extracted certificate to a location where the SIP Proxy/Registrar can retrieve the file from.

**Import the Lotus SIP Edge Proxy’s root certificate into the SIP Proxy/Registrar:**

**About this task**

Follow the instructions below to import the Lotus SIP Edge Proxy’s root certificate into the SIP Proxy/Registrar:

**Procedure**

1. In WebSphere Application Server administrative console hosting the Lotus SIP Edge Proxy, click **Security > SSL certificates and key management > Key stores and certificates**.
2. Select **CellDefaultTrustStore**.
3. Click **Signer certificates**.
4. Click **Add**.
5. In the **Alias** field, type a description for the certificate (such as, sip-edge-proxy-root-cert). In the **File name** field, enter the path to the certificate file.
6. Click **OK** and **Save**.
7. Stop and restart all WebSphere Application Server processes hosting the SIP Proxy/Registrar. The instructions for importing the SIP Proxy/Registrar server’s root certificate into the Lotus SIP Edge Proxy server are similar.

**Installing the Lotus SIP Edge Proxy in a cluster**

Installing the IBM Lotus SIP Edge Proxy in a cluster requires setting up primary and secondary nodes.

**Installing the primary node:**

**Procedure**

1. Start the Media server installer.
2. Deselect the **Use Lotus Sametime System Console to install** option.
3. Select **Stand alone (Cell and Primary nodes)** installation type.
4. To avoid installing the Conference Manager and the Packet Switcher applications on the Lotus SIP Edge SIP Proxy’s machine, enter the following values in the **common configuration** page:
   - For the **SIP Proxy/Registrar Server Host Name** field, enter the local machine's host name.
   - For the **Conference Manager Host Name** and **Packet Switcher Host Name** fields, enter a different host name (not the local host name).
   - For the **Community Server Host Name** field, enter a resolvable host name.
Note: The Lotus SIP Edge Proxy does not require a Community Server. Due to installer limitations, you should still enter a value in the Community Server Host Name field. This value must be a resolvable host name, but the Community Server should not be installed in this host.

5. Click Validate.
6. In the next page, select the Configure LDAP after the installation option.
7. In the WebSphere Application Server administrative console, browse to Applications > Websphere Enterprise Applications.
8. Uninstall the following applications:
   - IBM Lotus SIP Proxy
   - IBM Lotus SIP Registrar
9. If the Conference Manager and the Packet Switcher applications are installed, uninstall them too.
10. Click Next until installation finishes.

Installing the secondary node:
Procedure
1. Start the Media server installer.
2. Deselect the Use Lotus Sametime System Console to install option.
3. Select the Secondary node installation type, and provide the Deployment Manager host name, user ID, and password details under Specify the settings of the Deployment Manager section.
4. To avoid installing the Conference Manager and the Packet Switcher applications on the Lotus SIP Edge SIP Proxy's machine, enter the following values in the common configuration page:
   - For the SIP Proxy/Registrar Server Host Name field, enter the local machine's host name.
   - For the Conference Manager Host Name and Packet Switcher Host Name fields, enter a different host name (not the local host name).
   - For the Community Server Host Name field, enter a resolvable host name.

   Note: The Lotus SIP Edge Proxy does not require a Community Server. Due to installer limitations, you should still enter a value in the Community Server Host Name field. This value must be a resolvable host name, but the Community Server should not be installed in this host.

5. Click Validate.
6. Click Next until installation finishes.
7. Repeat steps 1-6 in order to install additional nodes.

Installing the Lotus SIP Edge Proxy Application:
Install the IBM Lotus SIP Edge Proxy application and adjust your firewall settings.

Procedure
1. Download the latest Lotus SIP Edge Proxy application from this location (for example, https://lotusrelease.notesdev.ibm.com/daily/WorkplaceKits/STR8.5.2/STR8.5.2/repository/st-sip/).
3. Unzip into a temporary directory.
4. In the Deployment Manager's administrative console, browse to Applications > Websphere Enterprise Applications.
5. Click **Install** and specify the fully qualified path to the SIP Edge proxy application file (EdgeProxyApp.ear).

6. Click **Next** until you reach the **Map modules to servers** page.

7. Select to install the application on the following scope:
   WebSphere:cell=<cell_name>, node=<node_name>, server=<server_name>
   Where:
   - Cell name is the Edge Proxy cell name.
   - Node name is the Primary node name.
   - Server name is the name of the server installed on the Primary node.

8. Click **Apply**.

9. Click **Next** until you installation wizard completes and then click **Finish**.

10. Save the changes by clicking the **Save** link in the Messages box at the top of the page.

**Adjusting firewall settings using the SSC:**

**About this task**

Since the Lotus SIP Edge Proxy server is behind a firewall, open the appropriate ports in order to be able to install a cluster using SSC (Sametime System Console). The ports that must be opened in the Edge Proxy cell machine are as follows:

**Table 47. Ports to be opened**

<table>
<thead>
<tr>
<th>Description</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSC to Edge PN</td>
<td>SSC IP</td>
<td>Ephemeral port</td>
<td>Edge PN IP</td>
<td>Edge PN: - SOAP DMGR port - SOAP Node Agent port - WC_defaulthost port - WC_defaulthost_secure port - Edge HTTP port - Edge HTTPS port</td>
<td>TCP</td>
</tr>
<tr>
<td>SSC to Edge SN</td>
<td>SSC IP</td>
<td>Ephemeral port</td>
<td>Edge PN IP</td>
<td>Edge SN: - SOAP DMGR port - SOAP Node Agent port - WC_defaulthost port - WC_defaulthost_secure port - SOAP connector port - Edge HTTP port - Edge HTTPS port</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Table 47. Ports to be opened (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge PN to SSC</td>
<td>Edge PN IP</td>
<td>Ephemeral port</td>
<td>SSC IP</td>
<td>SSC: - SOAP</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DMGR port -</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WC_defaulthost</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>port - WC_defaulthost</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>port - SSC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SSL port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS port</td>
<td></td>
</tr>
</tbody>
</table>

Where:
- The SOAP DMGR port can be found in the WebSphere Application Server administrative console under System administration > Deployment manager > ports > SOAP_CONNECTOR_ADDRESS.
- The SOAP Node Agent port can be found in the WebSphere Application Server administrative console under System administration > Node agents > node name > ports > SOAP_CONNECTOR_ADDRESS.
- The WC_defaulthost port can be found in the WebSphere Application Server administrative console under System administration > Node agents > node name > ports > SOAP_CONNECTOR_ADDRESS.
- The WC_defaulthost_secure port can be found in the WebSphere Application Server administrative console under System administration > Node agents > node name > ports > SOAP_CONNECTOR_ADDRESS.
- The SOAP connector port can be found in the Edge SN machine under <WAS_HOME>/profiles/<dmgr_profile>/logs/AboutThisProfile.txt. Look for the Management SOAP connector port.
- The Edge Proxy HTTP and HTTPS ports can be found in the Edge machine under <WAS_home>/profiles/<STMS_profile_name>/log/AboutThisProfile.txt. Look for the HTTP transport port and HTTPS transport port.
- The SSC HTTP and HTTPS ports can be found in the SSC machine under <WAS_home>/profiles/<STSC_profile_name>/logs/AboutThisProfile.txt. Look for the HTTP transport port and HTTPS transport port.

Registering Lotus SIP Edge Proxy nodes with Sametime System Console:

Register the IBM Lotus SIP Edge Proxy nodes with SSC by editing the console.properties and productConfig.properties files.

Procedure
1. Run Sametime System Console (SSC) on a separate machine.
2. On the Lotus SIP Edge Proxy machine, browse to `<WAS_home>/MediaServerCell/console` and open the following files for editing:
   - `console.properties`
   - `productConfig.properties`

3. For `console.properties`, edit the following entries:
   - `SSCHostName=<SSC_host_name>`
   - `SSCHTTPPort=<SSC_http_port>`
   - `SSCUserName=<SSC_username>`
   - `SSCPassword=<SSC_password>`

4. For `productConfig.properties`:
   a. Edit the following entries:
      - `DepName=<unique_deployment_name>`
      - `WASUserID=<Edge_proxy_was_username>`
      - `ComponentName=SIPEdgeProxy`
   b. Add the following lines:
      - `SIPEdgeProxyHost=<edge_proxy_host_name>`
      - `SIPEdgeProxyPort=<edge_proxy_http_port>`
      - `SIPEdgeProxyTransportProtocol=TCP`
   c. Make sure that the `STCommunityServerHost` and `STCommunityServerPort` parameters in the `productConfig.properties` file have no values.

   **Note:** The `productConfig.properties` file also includes also the following parameters: `ConferenceFocusHost`, `AVPacketSwitcherHost`, `ConferenceFocusPort`, and `AVPacketSwitcherPort`. The values for these parameters will be the values entered during installation for the **Conference Manager Host Name** and **Packet Switcher Host Name** fields. Do not set these parameters; it will not affect the Lotus SIP Edge Proxy registration process.
   d. Make sure that all other parameters are correct.

5. Open the command prompt and browse to `<WAS_home>/MediaServerCell/console`.


7. When the utility prompts for the type of component to register, enter 4 for the Lotus SIP Edge Proxy. If the registration is successful, `console.pid` will be generated in the same location of the utility. Also, the `ConsoleUtility.log` will be generated, which will have all the details.

**Creating the Lotus SIP Edge Proxy cluster:**

Use the Sametime System Console to create the IBM Lotus SIP Edge Proxy cluster.

**Procedure**

1. Open SSC, and browse to **Sametime System Console > Sametime Guided Activities > Cluster WebSphere Application Server**.
2. In the **WebSphere Application Server Clustering Guided Activity** page click **Next**.
3. In the **Select Product to Cluster** page select **Sametime Media Manager (Edge Proxy)** product.
4. In the next screen, select to create a new cluster, and provide the cluster name.
5. In Deployment Manager page, select the Edge Proxy Primary node, and click Next.
6. In the next screen, click the Create Cluster button.
7. Add more cluster members as needed.
8. Create the WebSphere Proxy server. Follow these instructions to create the WAS Proxy and bind it to the Lotus SIP Edge Proxy cluster: Setting up a WebSphere proxy server for the cluster

Configuring ports for the Lotus SIP Edge Proxy cluster:
You need to configure the a unique set of SIP access ports for the IBM Lotus SIP Edge Proxy cluster.

About this task
On the cluster's Deployment Manager, update the default_host virtual host with a unique set of SIP access ports.

Tip Print this page and use the table to record the port settings as you look them up in steps 1 and 2.

Table 48. Printable table to record ports on

<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>
</tbody>
</table>

Procedure
1. Determine the ports used by every cluster member as follows:
   a. In the Deployment Manager’s Integrated Solutions Console, click Servers > Server Types > WebSphere application servers.
   b. In the table listing the servers, click the name of the cluster member.
   c. This displays the cluster member's Configuration page.
   d. On the Configuration page, look under Communication, and expand Ports.
   e. Look in the Ports table and write down the following port settings for use in the next step:
      - SIP_DEFAULTHOST
      - SIP_DEFAULTHOST_SECURE
   f. Repeat this process for every cluster member.
2. Determine the ports used by every WebSphere proxy server within this cluster as follows.
   a. In the Deployment Manager’s 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.
   c. This displays the cluster member's Configuration page
   d. On the Configuration page, look under Communication, and expand Ports.
   e. Look in the Ports table and write down the following port settings for use in the next step:
3. Add the ports used by all the cluster members and all of the WebSphere proxy servers to the Deployment Manager’s Virtual Hosts table as follows:
   a. 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.
   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).
   e. Remember that you have information on two ports for each cluster member.

   Note: If a port is already listed in the table, you do not need to add it again.
   f. To add a port, click New at the top of the table.
   g. In the Host Name field, type *.
   h. In the Port field, enter a port from your list and click OK.
   i. Repeat this for the two ports for every cluster member (unless a port is already listed in this table).
   j. 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 Delete at the top of the table.
   k. Save the changes by clicking the Save link in the Messages box at the top of the page.

4. Synchronize all of the nodes as follows:
   a. Still working on the Deployment Manager, click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.

**Setting FQDN on WAS Proxy:**

To enforce the WAS SIP proxy to advertise its FQDN, you need to configure WAS proxy’s transport chains.

**About this task**

By default, WAS proxy advertises its IP address in SIP header fields. To enforce the WAS SIP proxy to advertise its FQDN instead, you need to configure WAS proxy’s transport chains as follows:

**Procedure**

1. In the SIP Edge proxy’s Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers.
2. In the table listing the servers, click the name of the proxy server.
4. Click PROXY_SIPS_ADDRESS port.
5. In the Host field enter the FQDN of the host where the WAS proxy is running and then click OK.
6. Click PROXY_SIP_ADDRESS port.
7. In the Host field enter the FQDN of the host where the WAS proxy is running and then click OK.
8. Save the changes by clicking the Save link in the Messages box at the top of the page.
9. Repeat the process to set FQDN on all WAS proxies that operate with Lotus SIP Edge Proxy cluster.

Additional settings:

Procedure

1. In the administrative console, browse to Security > Global security > Web and SIP security > general settings and ensure that the Use available authentication data when an unprotected URI is accessed option is deselected.
2. For each server in the cluster: In the administrative console, browse to: Servers > WebSphere application servers > <server_name> > SIP Container Settings (under "Container Settings") > SIP Container > Custom properties and set the following property:
   Name: com.ibm.ws.sip.sent.by.host Value: <the FQDN of SIP Edge Proxy server>

   Note: If the property is already listed in the table, you do not need to add it again. In this case, ensure that the value is set to the Lotus SIP Edge Proxy host name.

3. In the administrative console, browse to: Servers > WebSphere application servers > <server_name> > SIP Container Settings (under "Container Settings") > SIP Container > Custom properties and remove the com.ibm.ws.sip.security.trusted.iplist property.

   Note: Steps 4 and 5 are relevant only if you set up LDAP server during the installation process. If you selected the Configure LDAP after the installation option (as mentioned in the "Installing the SIP Edge Proxy" section), you should not perform steps 4 and 5.

4. In the administrative console, browse to Security > Global security > Configure and remove the entry that points to the LDAP repository.
5. In the administrative console, browse to: Security > Global security > Configure > Manage repositories and remove the entry that points to the LDAP repository.

Updating the edge-proxy.xml file:

About this task

The Lotus SIP Edge Proxy application has a configuration file, edge-proxy.xml, that you can modify.

Procedure

1. On the Edge Proxy Deployment Manager machine, open the edge-proxy.xml file located in <dm-profile>/config/cells/<cell>/applications/EdgeProxyApp1.ear/deployments/EdgeProxyApp1/EdgeProxyWeb.war/WEB-INF/ for editing.
   - The authoritativeProxy section contains the hostname, port, and transport of the SIP Proxy/Registrar.
     - For a clustered SIP Proxy/Registrar specify the hostname and SIP port used by the WAS proxy that operates with the SIP Proxy/Registrar's cluster.
- Specify the SIP port used for TCP.
- Specify the SIP port used for TLS.

- The edgeProxy section contains the hostname, port, and transport of the Lotus SIP Edge Proxy. For a clustered SIP Edge proxy specify the hostname and SIP port used by the WAS proxy that operates with the Lotus SIP Edge proxy’s cluster.
  - Specify the SIP port used for TCP.
  - Specify the SIP port used for TLS.

- The authProxySourceAddr specifies the address of the SIP Proxy/Registrar. When the Lotus SIP Edge Proxy receives stand alone or initial requests, it determines the remote address from which the request was received. If the remote address does not match the SIP Proxy/Registrar address, the request is sent to the SIP Proxy/Registrar for further processing. Supported values: IP address, regular expression that matches the SIP Proxy/Registrar address (such as, "10.10.102.14 | 10.10.102.16"). For example (settings for TCP):

```xml
<authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5060" authProxyTransport="tcp" authProxySourceAddr="10.10.102.14"/></edgeProxy>
```

For example (settings for TLS):

```xml
<authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5061" authProxyTransport="tls" authProxySourceAddr="10.10.102.14"/></edgeProxy>
```

**Note:** Use the same transport as for Media Manager components. For example, if the CF is configured to use TLS, set the authProxyTransport attribute to TLS as well.

2. Copy the changed file to `<dm-profile>/config/cells/<cell-name>/nodes/<node>/servers/<server>` (in a clustered environment copy the file to all the servers under DMGR profile).

3. Synchronize all of the nodes in the cell.
   a. Log in to the Deployment Manager, and then click System Administration > Nodes.
   b. Select all nodes in the cluster.
   c. Click Full Resynchronize.

**Modifying Lotus SIP Edge Proxy settings in the edge-proxy.xml file:**

An administrator can edit the edge-proxy.xml file manually to modify IBM Lotus SIP Edge Proxy server configuration settings.

**Before you begin**

Since there are no SSC administrative pages for the Lotus SIP Edge Proxy configuration, any configuration updates must be performed manually by editing the edge-proxy.xml file.

**Procedure**

1. On the Lotus SIP Edge Proxy deployment manager's machine, open the edge-proxy.xml file located in the `<dm profile>/config/cells/<cell>/applications/EdgeProxyApp1.ear/deployments/EdgeProxyApp1/EdgeProxyWeb.war/WEB-INF/` directory.
   - The authoritativeProxy section contains the hostname, port, and transport of the SIP Proxy/Registrar:
     - Specify the SIP port used for TCP.
     - Specify the SIP port used for TLS.
• The edgeProxy section contains the hostname, port, and transport of the Lotus SIP Edge Proxy:
  – Specify the SIP port used for TCP.
  – Specify the SIP port used for TLS.
• The authProxySourceAddr section specifies the address of the SIP Proxy/Registrar. When the Lotus SIP Edge Proxy receives stand-alone or initial requests, it determines the remote address from which the request was received. If the remote address does not match the SIP Proxy/Registrar address, the request is sent to the SIP Proxy/Registrar for further processing. Supported values: IP address, regular expression that matches the SIP Proxy/Registrar address (for example, "10.10.102.14 | 10.10.102.16").
For example (settings for TCP):
  \ `<authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5060" authProxyTransport="tcp" authProxySourceAddr="10.10.102.14"/>` /
  \ `<edgeProxy...`
For example (settings for TLS):
  \ `<authoritativeProxy authProxyHost="authhost.example.com" authProxyPort="5061" authProxyTransport="tls" authProxySourceAddr="10.10.102.14"/>` /
  \ `<edgeProxy...`

Note: Use the same transport as for Media Manager components. For example, if the CF is configured to use TLS, set the authProxyTransport attribute to TLS as well.

2. After editing, copy the changed file to `<dm-profile>/config/cells/<cell-name>/nodes/<node>/servers/<server>.

3. Synchronize all of the nodes in the cell as follows:
   a. Log into the Deployment Manager, and then click **System Administration > Nodes.**
   b. Select all nodes in the cluster.
   c. Click **Full Resynchronize.**

Replacing the default certificate used by Lotus SIP Edge Proxy:

To avoid the issue of IBM Sametime clients rejecting the certificate issued for the IBM Lotus Edge Proxy server, an administrator needs to replace the default certificate on the Lotus SIP Edge Proxy so that it contains the SIP Proxy/Registrar's FQDN.

About this task

These instructions are for the default certificate, which is meant for internal communications (not meant to act as a CA). Sametime clients verify that the certificate was issued for the SIP Proxy/Registrar. In a Lotus SIP Edge Proxy deployment, the client opens a TLS connection to the Lotus SIP Edge Proxy resulting in the client receiving a certificate issued for the Lotus SIP Edge Proxy server. This certificate will be rejected by the client.

Procedure

1. Log in to the WebSphere Application Server ISC administrative console where the SIP edge proxy is installed.
2. Click **Security > SSL certificate and key management > Manage endpoint security configurations.**
3. Expand **Inbound** and select the node where the WAS proxy that operates with the SIP Edge proxy cluster is installed.
4. Click **Manage Certificates.**
5. Click **Create chained certificate.**
6. Complete the form. Specify an alias (for example, sip-pr-cn-cert), common name (FQDN of the SIP Proxy/Registrar), organization for the new certificate (IBM), country (US).

7. Click OK and Save.

8. On the Manage endpoint security configuration page, click the node again, and then click Manage certificates to view the old and new certificates.

9. Select the old certificate and click Replace.

10. Select the new certificate and select the Delete old certificate and Delete old signers check boxes.

11. Click OK and Save.

12. Stop and restart all WebSphere Application Server processes

Exchanging certificates between WAS SIP proxy servers:

If you configured to use TLS between the SIP Edge proxy and the SIP Proxy/Registrar, then you need to exchange certificates between two servers.

About this task

These instructions are for the default certificate. This certificate is meant for internal communications (not meant to act as a CA). Exchange the root certificates between WAS SIP proxy servers so that you can change the personal certificate without any impact on communication between the Lotus SIP Edge Proxy and the SIP Proxy/Registrar servers.

Procedure

1. Follow these instructions to extract the root certificate from the WAS SIP proxy server that operates with the Lotus SIP Edge Proxy cluster:
   a. In the WebSphere Application Server administrative console hosting the WAS SIP proxy server that operates with the Lotus SIP Edge Proxy cluster, click Security > SSL certificate and key management > Key stores and certificates.
   b. Select CellDefaultTrustStore.
   c. Click Signer certificates.
   d. Select the root certificate (with default alias).
   e. Click Extract.
   f. Specify the file name and click OK.
   g. Copy the extracted certificate to a location from which the WAS SIP proxy server that operates with the SIP Proxy/Registrar cluster can retrieve the file.

2. Follow these instructions to import the Lotus SIP Edge Proxy's root certificate into the SIP Proxy/Registrar:
   a. In the WebSphere Application Server administrative console hosting the WAS SIP proxy that operated with SIP Proxy/Registrar, click Security > SSL certificate and key management > Key stores and certificates.
   b. Click Security > SSL Certificates and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.
   c. Click Add.
   d. In the Alias field, type a description for the certificate (for example, sip-edge-proxy-root-cert). In the File name field, type the path to the certificate file.
e. Click OK.
f. Click Save.
g. Stop and restart all WebSphere Application Server processes hosting the SIP Proxy/Registrar.

Note: The instructions for importing the SIP Proxy/Registrar server’s root certificate into the Lotus SIP Edge Proxy server are similar.

Configuring the Lotus SIP Edge Proxy with a Load Balancer:

Configure the IBM Lotus SIP Edge Proxy that sits in front of Media Manager components in a load-balancing environment.

About this task

1.1

Procedure
1. Create a user-defined SIP port from the application server's administrative console as follows:
   a. Log into the ISC administrative console.
   b. Click Servers > WebSphere proxy servers > proxy-name.
   c. Under Communications, click Ports.
   d. Create a non-secure SIP port.
   e. Click New.
   f. Select User-defined Port.
   g. In Specify Port Name field enter PROXY_SIP_ADDRESS_LB.
   h. Enter a value for the Host field. This is the virtual IP (cluster address) that is configured on your load balancer.
   i. In the Port field enter the non-secure SIP port value (such as, 5060). This value corresponds to the port through which the load balanced servers are configured to accept traffic.
   j. Click OK and save the changes
   k. Return to the Ports screen.
   l. To create a secure SIP port click New.
   m. Select User-defined Port.
   n. In the Specify Port Name field enter PROXY_SIPS_ADDRESS_LB.
   o. Enter a value for the Host field. This is the virtual IP (cluster address) that is configured on your load balancer.
   p. In the Port field type the secure SIP port value (such as, 5061). This value corresponds to the port through which the load balanced servers are configured to accept traffic.
   q. Click OK and save the changes. Repeat for each WebSphere Proxy Server. Note that all proxy servers that operate with a particular cluster, must use the same SIP ports.

2. Modify the Lotus SIP Edge Proxy Server transports from the administrative console as follows:
   a. Log into the ISC administrative console.
   b. Click Servers > WebSphere proxy servers > proxy-name.
c. Under **Proxy Settings**, click **SIP Proxy Server Settings** > **SIP proxy server transports**.

d. Modify the transport chain for TLS by clicking **SIPS_PROXY_CHAIN**.

e. Click TCP inbound channel under **Transport Channels**.

f. From the **Port** drop-down list select **PROXY_SIPS_ADDRESS_LB**.

g. Click **OK** and save the changes.

h. Return to the **SIP proxy server transports** screen.

i. Modify the transport chain for TCP by clicking **SIP_PROXY_CHAIN**.

j. Click TCP inbound channel under **Transport Channels**.

k. From the **Port** drop-down list select **PROXY_SIP_ADDRESS_LB**.

l. Click **OK** and save the changes.

m. Return to the SIP proxy server transports screen.

n. Modify the transport chain for UDP by clicking **UDP_SIP_PROXY_CHAIN**.

o. Click UDP inbound channel under **Transport Channels**.

p. From the **Port** drop-down list select **PROXY_SIP_ADDRESS_LB**.

q. Click **OK**, save the changes, and repeat for each WebSphere Proxy Server.

3. Modify Lotus SIP Edge Proxy settings as follows:

a. Log into the ISC administrative console.

b. Click **Servers** > **WebSphere proxy servers** > **proxy-name**.

c. Under Proxy Settings, click **SIP Proxy Server Settings** > **SIP proxy settings**.

d. Under **Container facing network** interface, enter the WebSphere SIP Proxy IP address in the following fields (physical IP address of the machine where the WebSphere SIP Proxy is installed):

- UDP interface
- TCP interface
- TLS interface

e. Move to the **Load balancer health checking** section. These settings can be used for defining WebSphere SIP Proxy Load Balancer Health checking.

f. For **Load balancer members, IP address 1**, enter the Load balancer IP address (the physical IP address of the machine where the Load Balancer is installed).

g. For **SIP health check method name**, enter **OPTIONS**.

h. Save the changes by clicking the **Save** link and repeat for each WebSphere Proxy Server.

---

**Adding ports to the virtual host alias:**

Add ports to the sip_proxyreg_host virtual host for the IBM Lotus SIP Edge Proxy.

**About this task**

These instructions are for a SIP Proxy/Registrar cluster. The instructions for a Conference Focus and SIP Edge proxy clusters are the same with one exception – instead of the sip_proxyreg_host virtual host, the ports should be added the default_host virtual host). Add **PROXY_SIP_ADDRESS_LB** and **PROXY_SIPS_ADDRESS_LB** ports to the sip_proxyreg_host virtual host. However, if a port is already listed in the table, you do not need to add it again.
Procedure
1. Log in to the Integrated Solutions Console.
2. Click Environment > Virtual Hosts.
3. In the Virtual Hosts table, click the host called sip_proxyreg_host. This displays the Configuration page for the sip_proxyreg_host.
5. In the Host Aliases table, add the PROXY_SIP_ADDRESS_LB and PROXY_SIPS_ADDRESS_LB ports (the SIP ports you created). To add a port:
   a. Click the New button at the top of the table.
   b. In the Host Name field, type *.
   c. In the Port field, type a port from your list.
   d. Click OK.
   e. Repeat this for the two ports (unless a port is already listed in this table).
6. Save the new port settings to the master configuration.

What to do next
Adding trusted IP addresses to the SIP Proxy and Registrar. On each server in the SIP Proxy/Registrar cluster, add the virtual IP address (cluster address) of the load balancer that operates with the Conference Focus cluster to the trusted IP list.

Updating the stavconfig.xml file:
Update the stavconfig.xml files on the Packet Switcher and the Conference Manager nodes.

About this task
The stage needs to be set just so.

Procedure
1. On the servers hosting the Deployment Manager of Conference Manager and Packet Switcher, navigate to the following directory: `<dm_install_root>/config/cells/cell_name/nodes/node_name/servers/server_name`
2. In a text editor, open the stavconfig.xml file and modify the following settings if needed:

<table>
<thead>
<tr>
<th>Settings in stavconfig.xml</th>
<th>Description of settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConferenceServerHost</td>
<td>The virtual IP/cluster address that is configured on your load balancer used by the Conference Focus cluster</td>
</tr>
<tr>
<td>ConferenceServerPort</td>
<td>The values of the PROXY_SIP_ADDRESS_LB (TCP) or PROXY_SIPS_ADDRESS_LB (TLS) depending on the transport protocol. These are the ports you configured in when you created SIP Ports for the WebSphere proxies that sit in front of the Conference Manager cluster.</td>
</tr>
<tr>
<td>SIPProxyServerHost</td>
<td>The virtual IP/cluster address that is configured on your load balancer used by the SIP Proxy/Registrar cluster.</td>
</tr>
</tbody>
</table>
### Settings in stavconfig.xml

<table>
<thead>
<tr>
<th>Settings in stavconfig.xml</th>
<th>Description of settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPProxyServerPort</td>
<td>The values of the PROXY_SIP_ADDRESS_LB (TCP) or PROXY_SIPS_ADDRESS_LB (TLS) depending on the transport protocol. These are the ports you configured in when you created SIP Ports for the WebSphere proxies that sit in front of the SIP Proxy/Registrar cluster.</td>
</tr>
<tr>
<td>SIPProxyServerTransportProtocol</td>
<td>TCP or TLS.</td>
</tr>
</tbody>
</table>

3. Synchronize all nodes in the Deployment Manager that manages the component as follows:
   a. In the Deployment Manager's Integrated Solutions Console, click **System Administration > Nodes**.
   b. Select all nodes.
   c. Click **Full Resynchronize**.

4. Restart all WebSphere processes for the changes to take effect.

**Configuring loopback address:**

Ensure that you set up a loopback address with the IP address of the (virtual IP) for your operating system on each of the machines where the Lotus SIP Edge Proxy is installed.

**About this task**

See the Load Balancer Administration Guide for more details. For example, use the following instructions for Windows 2003 (these instructions are taken from the WebSphere 7.0. information center)

**Procedure**

1. Click **Start** and then click **Control Panel**.
2. If you have not done so already, add the **MS Loopback Adapter Driver**.
3. Click **Add Hardware**, which launches the Add Hardware Wizard.
4. Click **Next**.
5. Select **Yes, I have already connected the hardware** and then click **Next**.
6. If the MS Loopback Adapter is in the list, it is already installed. Click **Cancel** to exit.
7. If the MS Loopback Adapter is not in the list, select **Add a New Device** and then click **Next**.
8. To select the hardware from a list for the **Find New Hardware** panel, click **No** and then click **Next**.
9. Select **Network Adapters** and then click **Next**.
10. On the **Select Network Adapter** panel, select **Microsoft** in the **Manufacturers** list, then select **Microsoft Loopback Adapter**.
11. Click **Next** and then click **Next** again to install the default settings (or select **Have Disk**, then insert the CD to install from there).
12. Click **Finish** to complete installation.
13. From the **Control Panel**, click **Network and Dial-up Connections**.
14. Select the connection with **Device Name** Microsoft Loopback Adapter.
15. Select Properties from the drop-down.
16. Select Internet Protocol (TCP/IP), then click Properties.

17. Click **Use the following IP address**. Fill in **IP address** with the cluster address, and **Subnet mask** with the subnet mask of the back-end server.

   **Note:** Do not enter a router address; use the localhost as the default DNS server.

18. Make sure the loopback adapter is listed in the correct order as described:
   a. Open the **Network Connections** panel.
   b. Find **Advanced > Advanced Settings**.
   c. In the Connections box on the Adapters and Bindings tab, make sure Loopback adapter is listed after Local Area Connection and move the Loopback adapter if the order is not correct. It is essential that the physical IP address appears as the first entry in the list (instead of the virtual IP address).
   d. Change the order if required.

### 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, 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.

### Related tasks

- “**Configuring a Sametime Meeting Server**” on page 1675
- 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 129
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 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 582
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 257

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 582

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.

**Linux:** 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
      ```
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 installation package name for this server.

1. **Operating System**

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

5. Click Install IBM Sametime Meeting Server and click Launch IBM Sametime Meeting Server 8.5.2 installation.

6. 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.

7. 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. 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 581
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 606
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.

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://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_nameSTMAppProfile1 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**
     ```bash
     ./IBMIM --launcher.ini silent-install.ini
     --record response_file -log log_file -acceptLicense
     ```
   
   - **Windows**
     ```bash
     IBMIMc --launcher.ini silent-install.ini --record 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.

   ```bash
   ./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

“Clustering Sametime servers for high enterprise availability” on page 88
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.

Related tasks

“Registering a Sametime Meeting Server on IBM i with the Sametime System Console” on page 782
After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

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 582
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**.
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.
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 582

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 Manger’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.

---

**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 in 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 > 
      \textit{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 > 
      Proxy Servers.
   b. In the "Proxy Servers" page, select the new proxy server from the list.
   c. Click the Start button above the list of proxy servers.

\textit{Enabling the WebSphere proxy server to cache dynamic content:}

Optionally configure an IBM WebSphere proxy server to cache dynamic content.

\textbf{Before you begin}

Configure a WebSphere proxy server for use with a cluster of Sametime Meeting 
Servers, and then start the WebSphere proxy server.

\textbf{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.

\textbf{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 "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.
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.

\textit{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.
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:
      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 49. 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 in a Meeting 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:
   ```
   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:
      ```
      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:

```bash
ifconfig device inet6 plumb
ifconfig device inet6 address/prefix up
```

d. Start the executor function of the dispatcher:

```bash
dscontrol executor start
```
e. Add the cluster to the service:

```bash
dscontrol cluster add cluster'sFullyQualifiedHost_name
```
where `cluster'sFullyQualifiedHost_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:

```bash
stms-cluster.example.com
```
f. Add the cluster port:

```bash
dscontrol port add cluster'sFullyQualifiedHost_name@port
```
where `cluster'sFullyQualifiedHost_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:

```bash
stms-cluster.example.com@80
```
g. Add the nodes for which this server will balance workload:

```bash
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:

```bash
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:

```bash
stms-cluster.example.com@80@meetsvr1.example.com
```
h. Now start the Load Balancer administration interface with the following command:

```bash
./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:

```bash
dsserver stop
dscontrol executor stop
dsserver start
dscontrol executor start
./lbadmin
```

4. Continue configuring Load Balancer as follows:

a. Add the cluster to the executor:

```bash
dscontrol executor add cluster'sFullyQualifiedHost_name
```
where `cluster'sFullyQualifiedHost_name` is the fully qualified host name that you assigned to the cluster when you installed the load balancer; for example:
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:
   
   ```
   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 PREFIFIC 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 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 LTTPA 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 1618
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 1581
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, "stmsNNNNNNNNNNNNN", 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
     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

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 1618

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 1581

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 a Sametime Gateway server
Plan a deployment and install IBM DB2 and then one or more Sametime Gateway
servers.

What to do next
After installation, you can perform other required and optional configuration tasks
for Sametime Gateway.
• Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Configure LDAP for Sametime Gateway (IBM i)
• Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Connect servers to Sametime Gateway (IBM i)
• Set up SSL
• Other optional configuration steps

Related tasks
“Configuring a Sametime Gateway” on page 1679

Configure one or more IBM Sametime Gateway servers.

Creating a DB2 database for Windows, Linux, AIX, and Solaris
Create the database tables and schema needed by Sametime Gateway. These steps
assume that you already have installed DB2 on the same machine on which you
are now creating the database. If the machine on which you installed DB2 is
named STGW, follow the steps in this procedure to change the name of the database
in the database creation script. The default database name, STGW, cannot be the
machine name.

Before you begin
The Sametime Gateway installation package includes a database creation script,
which creates the database. Follow the steps below to unpack the installation
compressed file and extract the contents before you run the script.

Expected state: DB2 is installed and running.
Procedure

1. From the installation media, copy the Sametime Gateway installation image for your operating system to a temporary directory on the DB2 server node:
   The part numbers for each product are available at the following Web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
   • Windows:
     \TMP\SametimeGateway\part_number.exe
   • Linux, AIX, or Solaris:
     /TMP/SametimeGateway/part_number.tar

2. Open a command window and navigate to the temporary directory.

3. Unzip the installation image to the /TMP/SametimeGateway folder.

4. Log in to the operating system using the DB2 administrator account created when you installed DB2.

5. On the node where you will be creating the database Sametime Gateway, open a command window and type one of the following commands:
   • Windows:
     db2cmd
   • Linux or AIX:
     . /db2adminHomeDir/sqllib/db2profile
     Note the period (.) and space before /db2adminHomeDir/sqllib/db2profile.
   • Solaris:
     . /db2adminHomeDir/sqllib/db2profile

6. If the host name on which you installed DB2 is named STGW, or if you need to change the database name to something other than STGW, or if your database administrator wishes to specify tablespace options, complete the following substeps, otherwise skip this step.
   a. Using a text editor, open createDb.sql.
   b. Replace every instance of STGW with a new database name that is eight characters or less.
   c. If desired, you may edit the tablespace file locations for your specific environment to be somewhere other than the default location.
   d. Save the file.

7. In the DB2 window, navigate to this directory:
   \TMP\SametimeGateway\database\db2

8. Type the following command to create the database:
   db2 -tvf createDb.sql > createDbOut.txt
   If you edited the createDb.sql file, inspect the createDbOut.txt file to be sure that all commands executed correctly.

9. Stop and then restart the database using the following commands:
   a. db2stop
   b. db2start

Installing Sametime Gateway

Install an IBM Sametime Gateway server. This section provides procedures for installing a single server and installing a cluster of servers. When installing a cluster, you install a Deployment Manager server, SIP and XMPP proxy servers, a primary server, and at least one additional server on its own machine. You can
install the primary server and Deployment Manager on the same machine, or each on its own machine. For better performance, install the SIP and XMPP proxy servers on their own machine; however, they can share a machine with other components of the cluster if necessary.

**Before you begin**

Before installing Sametime Gateway, verify that the fully qualified domain name of the external endpoint is externally resolvable by the domain name server, and is not set in the "hosts" file. When you install a single Gateway server, the external endpoint is the computer hosting the Gateway server. When you install a cluster, the external endpoint is the computer hosting the SIP and XMPP proxy servers.

**About this task**

Unlike other Sametime components, the Sametime Gateway does not install with a deployment plan created on the Sametime System Console. Instead, you enter required information as you proceed through the installation program. Once the installation is complete, you will register the Gateway with the Sametime System Console; from then on, you will administer the Gateway server from the System Console, just like all the other Sametime components.

**What to do next**

After installation, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

**Installing a single Gateway server:**

Choose to install a single Sametime Gateway server on Windows, AIX, Linux, Solaris, or IBM i.

**Installing a single server on Windows:**

Complete these steps to install Sametime Gateway as a single server on Windows, to create an administrative user ID for WebSphere Application Server, and to connect to an LDAP server. This installation program installs WebSphere Application Server and Sametime Gateway. If you need to install an additional Sametime Gateway server later, follow the procedure for installing servers in a cluster.

**Before you begin**

Expected state: DB2 is installed. The DB2 database is created and DB2 is running.

Information on downloading packages for Sametime is located at the following Web address:

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

1. Log in as the Windows administrator on the server where you will install Sametime Gateway.
2. Create the temporary file folder \TMP\WASCD.
3. From the installation media, copy the WebSphere Application Server installation image WAS_part_number.exe to the folder \TMP\WASCD.
4. Open a command window and navigate to the folder \TMP\WASCD.
5. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK folders inside the ifpackage folder.
6. From the installation media, copy the Sametime Gateway installation image part_number.exe to the \TMP folder.
7. Extract the files in part_number.exe. This step creates the folder \TMP\SametimeGateway.
8. Navigate to the \TMP\SametimeGateway folder containing the extracted files.
9. Open a command window and type the following command:
   • For wizard mode: install.bat
   • For console mode: install.bat -console

Attention: If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   install.bat -V BypassWasInfoCheck=true

Because your input will not be verified during installation, you should take extra care when typing values.
10. Select the language for the installation wizard and click OK. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.
11. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click Next to proceed with the installation.
12. Select Standalone server and then click Next.
13. Type or click Browse to select the path to where you extracted the WebSphere Application Server installation files from the CD. Do not use quotation marks. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use C:\\TMP\WASCD\ifpackage but do not use C:\\TMP\WASCD\ifpackage\WAS or C:\\TMP\WASCD\ifpackage\JDK.
14. Click Next to see the default directory path where WebSphere Application Server will be installed is displayed. To change the installation location of WebSphere Application Server, click Browse and select a desired location, or type a new path.
15. Click Next to see node, cell, and host name profile information provided by the installer. If the supplied information is correct, click Next.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, acmeNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, acmeCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.acme.com. Note: If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section &quot;Host name considerations&quot; in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
</tbody>
</table>

16. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters:

;*!?=./|+&'`[]%^`

17. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

18. Click **Next** to enter database properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
</tbody>
</table>
19. Click **Next** to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schema password</strong></td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

20. Select an LDAP host name from list of **Registered host names and ports in your domain**, or select **Other** and enter a host name or IP address in the **Host name** field. The default port number is 389. Click **Next**.

21. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymous access</strong></td>
<td>Select this option if you don't need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.</td>
</tr>
<tr>
<td><strong>Authenticated access</strong></td>
<td>Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.</td>
</tr>
</tbody>
</table>

22. Enter the **Bind distinguished name (DN)** and **Bind password**. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:

- **Bind distinguished name:**
  
  `uid=ldapadmin,cn=users,l=shipley,st=kansas,c=us,ou=example,o=medical,DC=EXAMPLE,DC=COM`

- **Bind password:**
  
  `C@pital1`

23. Click **Next**. Choose a base distinguished name from the list of **Suggested base distinguished names in your LDAP** or enter a base DN in the **Base distinguished name** field. The base distinguished name indicates the starting...
point for LDAP searches of the directory service. For example, for the bind
distinguished name given as an example in the previous step, you can specify
the base DN as: DC=EXAMPLE,DC=COM. For authorization purposes, this field is
case sensitive. This panel is not shown if you are connecting to Domino
LDAP.

24. Click Next to see the Sametime Gateway installation summary. You can
review the installation summary settings and, if necessary, click Back to make
changes.

25. Click Install to begin copying files. A progress bar is displayed and the
activity is logged to the Sametime Gateway log file. This installation takes
about 10 minutes to complete. When the installation is complete, the wizard
displays a message indicating a successful installation.

26. Read the summary and click Finish. To view the installation log, click View
log file or open the log file at stgw_server_root\logs\installlog.txt.

Installing WebSphere iFixes for Sametime Gateway:

Install required IBM WebSphere Application Server updates on the IBM Lotus
Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere
Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime
Gateway server.

   The iFixes are included in the following package: IBM WebSphere V7.0.0.3
   iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
   Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere
   Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in
   Installing WebSphere Application Server updates.

Installing a single server on AIX, Linux, or Solaris:

Complete these steps to install a single Sametime Gateway server on an AIX,
Linux, or a Solaris machine, to create an administrative user ID for WebSphere
Application Server, and to connect to an LDAP server. This installation requires
installing the WebSphere Application Server Network Deployment edition, even if
you are installing a single server. If you need to create a cluster of Sametime
Gateway servers later, follow the procedure for installing a cluster of servers using
the wizard.

Before you begin

Expected state: DB2 or the DBMS Administration Client is installed. The DB2
database is created and DB2 is running.

Information on downloading packages for Sametime is located at the following
Web address:
AIX, Linux, and Solaris: If you are installing using the GUI mode, the full X11 desktop environment is required.

About this task

The Sametime Gateway install wizard deploys both the WebSphere Application Server and the Sametime Gateway server application in one installation.

Procedure

1. Log in as root on the server where you will install Sametime Gateway.
2. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Open the /etc/selinux/config file for editing.
   b. Locate the SELINUX setting.
   c. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
3. Create the temporary file folder /TMP/WASCD.
4. From the installation media, copy the WebSphere Application Server installation image for your operating system to /TMP/WASCD.
5. Open a command window and navigate to the directory /TMP/WASCD.
6. Run the following command to uncompress the files:
   ```bash
gunzip -c part_number.tar.gz | tar -xvf -
```
   When you are done extracting the files, you should have the following folder:
   /TMP/WASCD/ifpackage
   Verify that you have WAS and JDK folders inside the ifpackage folder.
7. From the installation media, copy the Sametime Gateway installation image part_number.tar to the temporary directory /TMP.
8. Navigate to the /TMP directory and uncompress the following file:
   ```bash
   unzip part_number.tar
   ```
   This creates the folder /TMP/SametimeGateway.
9. Navigate to the /TMP/SametimeGateway directory and type the following command:
   ```bash
   install.sh -console
   ```
   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   ```bash
   install.sh -console -V BypassWasInfoCheck=true
   ```
   Because your input will not be verified during installation, you should take extra care when typing values.
10. Select the language to be used for the installation and click OK. The Sametime Gateway Welcome screen is displayed.
11. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed with the installation.

12. Select **Standalone server**, and then click **Next**.

13. Type or click **Browse** to select the path to where you extracted the WebSphere Application Server installation files from the CD. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/WAS` or `/TMP/WASCD/ifpackage/JDK`.

14. Click **Next** to see the default directory path where WebSphere Application Server will be installed is displayed. To change the installation location of WebSphere Application Server, click **Browse** and select a desired location, or type a new path.

15. Click **Next** to see node, cell, and host name profile information provided by the installer. If the supplied information is correct, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td>Logical name for the node. For example, exampleNode.</td>
</tr>
<tr>
<td><strong>Cell</strong></td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCell.</td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
</tbody>
</table>

**Note:** If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section “Host name considerations” in the WebSphere Application Server information center topic, Creating an application server profile.

16. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: `;*!?<>|+&'`\][]^`

17. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

18. Click **Next** to enter properties required by DB2:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

19. Click Next to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP now</td>
<td>Select if you want to set up a connection between Sametime Gateway and LDAP that does not need an SSL connection. You will need to know the host name and port of the LDAP server.</td>
</tr>
<tr>
<td>Configure LDAP after the installation</td>
<td>Select this option if you need to set up an SSL connection with LDAP, or if you do not know the host name and port number used by LDAP. If you are installing Sametime Gateway outside the firewall and the LDAP directory is located inside the firewall, choose this option, and skip to step 23.</td>
</tr>
</tbody>
</table>

20. Select an LDAP host name from list of Registered host names and ports in your domain, or select Other and enter a host name or IP address in the Host name field. The default port number is 389. Click Next.

21. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous access</td>
<td>Select this option if you don’t need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Authenticated access</td>
<td>Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.</td>
</tr>
</tbody>
</table>

22. Enter the **Bind distinguished name (DN)** and **Bind password**. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:

- **Bind distinguished name:**
  
  `uid=ldapadmin,cn=users,l=shipley,st=kansas,c=us,ou=example,o=medical,DC=EXAMPLE,DC=COM`

- **Bind password:**
  
  `C@pital1` 

23. Click **Next**. Choose a base distinguished name from the list of **Suggested base distinguished names in your LDAP** or enter a base DN in the **Base distinguished name** field. The base distinguished name indicates the starting point for LDAP searches of the directory service. For example, for the bind distinguished name given as an example in the previous step, you can specify the base DN as: `DC=EXAMPLE,DC=COM`. For authorization purposes, this field is case sensitive. This panel is not shown if you are connecting to Domino LDAP.

24. Click **Next** to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click **Back** to make changes.

25. Click **Install** to begin copying files. A progress bar is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

26. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`

**Installing WebSphere iFixes for a stand-alone Sametime Gateway server:**

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.
**Adding a stand-alone Sametime Gateway 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.

**Starting a single server:**

This section explains how to start a standalone Sametime Gateway server. Skip these steps if you are setting up a cluster.
About this task

Single server configurations must have the Sametime Gateway server running to access the Integrated Solutions Console, while a Sametime Gateway cluster must have the Deployment Manager running to access the Integrated Solutions Console. Do not start Sametime Gateway at this time if you are creating a cluster of Sametime Gateway servers.

Procedure

1. Log in to the server machine as a user with administrative privileges.
2. Navigate to the Sametime Gateway profile directory that contains binaries:
   
   stgw_profile_root\bin

3. Type the following command to start Sametime Gateway. Note that RTCGWServer is case-sensitive.

   AIX, Linux, and Solaris
   
   ./startServer.sh RTCGWServer

   Windows
   
   startServer.bat RTCGWServer

   IBM i
   
   startServer RTCGWServer

Connecting to a DB2 database from a stand-alone Sametime Gateway server:

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 582

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

**Sametime prerequisite: Connecting to a DB2 database from a stand-alone Sametime Gateway server:**

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.

Registering a new Gateway server with the System Console:

After installing an IBM Sametime Gateway 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

Before you register the server, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the server that you want to connect to the console, follow these steps to update properties files and run the registration utility.

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

- console.properties
- productConfig.properties

Procedure

1. On the Sametime Gateway server, navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.

2. Make backup copies (using different names) of the console.properties and productConfig.properties files.

3. Update the console.properties file with the following values, and then save and close the file.
**Table 50. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>

4. In the productConfig.properties file, set the value of **isFederated** to true for a primary or secondary node. The registration utility cannot run without this value. Verify that the other settings are correct, modifying them as needed before saving and closing the file.

5. Run the registration utility:
   - **AIX, Linux, Solaris:** registerProduct.sh
   - **Windows:** registerProduct.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 will also be generated.

6. Start the Sametime Gateway server, if it is not already running.

**Optional network configuration:**

After you complete your IBM Sametime Gateway installation, you can optionally modify some network configuration settings.

**Configuring network interface cards to simulate a NAT:**

This optional procedure describes how to you can simulate a Network Address Translator (NAT) to provide additional security by using two Network Interface Cards (NICs), one for an internal IP address facing the Sametime community server, and the other for an external IP address facing the Internet. This procedure applies to standalone Sametime Gateway deployments only. If you use this configuration, you must update the default host using the Integrated Solutions Console.
Before you begin

The procedure applies to single server installations only. If you have a cluster of Sametime Gateway servers, and you want to set up two Network Interface Cards, install the NICs on the proxy server node in the cluster. The proxy server node is smart enough to handle incoming and outgoing addresses on two different IP addresses without additional configuration.

About this task

Perform these steps to configure multiple NIC support in a single server installation. When Sametime Gateway has two IP addresses, one external facing and one internal facing, sometimes the Sametime Gateway sends subscribe requests such that the external community is instructed to respond back to the internal IP address. To ensure that Sametime Gateway sends the external IP address instead of the internal IP, perform the following configuration steps:

Procedure

1. Log into Integrated Solutions Console.
2. Click Servers > Application servers.
3. Click RTGWServer.
4. Under Communications, click Ports.
5. Click SIP_DEFAULTHOST.
6. In the Host field, type the external IP address; for example: 192.0.2.10
7. Click SIP_DEFAULTHOST_SECURE.
8. In the Host field, type the external IP address. For example: 192.0.2.10
9. Click Apply, then Save.
10. Restart the Sametime Gateway server.

Installing Gateway servers in a cluster:

Complete these steps to install a cluster of Sametime Gateway servers in a network deployment. A cluster is a group of application servers that are managed together and participate in workload management. A network deployment is a group of nodes administered by the same cell, and controlled by a Deployment Manager.

About this task

Sametime Gateway supports cluster members on multiple nodes across many nodes in a cell, with nodes either coexisting on the same hardware, or running on dedicated systems. A network deployment is made up of a Deployment Manager,
which manages the cell, SIP and XMPP proxy servers, a primary node, a primary server (primary cluster member), and, if needed, one or more secondary cluster members. You expand the cluster by adding additional cluster members either on existing nodes, or by adding a new secondary node and then adding the member to the new node.

Note the following restrictions:

- All of the cluster components (deployment manager, nodes, proxies) must be deployed in the same LAN.
- Deploying components over a WAN is not supported.
- Placing a firewall between two components is not supported (even if the firewall is configured to allow the relevant traffic).
- When fronting the WebSphere Application Server SIP Proxies with a load balancer, the load balancer must be able to communicate with the proxies in Layer 2, using MAC forwarding. IP forwarding (Layer 3) is not supported.

Before you begin, upgrade existing Sametime Gateway servers to the current release before you install new servers.

Except in the case of IBM i, the Sametime Gateway install wizard deploys both WebSphere Application Server and the Sametime Gateway server application in one installation.

**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.

**Related concepts**

“Clustering Sametime servers for high enterprise availability” on page 88

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.

**About network deployments:**

A network deployment is a distributed WebSphere environment. Unlike a stand-alone environment that contains only one application server node, a network deployment contains many application server nodes that can distribute the workload of Sametime Gateway applications across several physical systems. The purpose of a network deployment is to provide a topology that is scalable and has load balancing and failover capabilities.

Typically, a network deployment contains one node per physical computer. This is not a requirement. Nodes are logical groupings of application servers, so you can have more than one node installed on a physical system. For performance reasons, most installations have only one cluster member per node, since each cluster member creates its own JVM footprint.

In a network deployment, all nodes are federated into the deployment manager’s cell. The deployment manager serves to manage the deployment. A Deployment Manager is nothing more than a node that is responsible for administering a cell.
In Sametime Gateway, the only things configured on the Deployment Manager node are a few minor cell level attributes, and the Sametime Gateway administrative portlet plugin extensions. Sametime Gateway application files all run on the cluster member application servers.

The primary node is basically the same thing as a standalone node installation, minus a few cell level configurations that will be trumped by the Deployment Manager’s configuration. The primary node contains all the applications and WebSphere Application Server components that are required to run Sametime Gateway. When you install a primary node, you create a server instance called RTCGWServer. This server instance is cloned for use with all secondary nodes across the cluster. There can only be one primary Sametime Gateway node installed in any network deployment, because applications can only be added to the cell from one node. In the Sametime Gateway network deployment, the primary node also configures the database server.

The secondary nodes are WebSphere Application Server placeholders that can run additional cluster members (servers created as clones of the primary server). When you install a secondary node for Sametime Gateway, the installation creates a node and default server instance, as well as some node level WebSphere Application Server attributes such as data sources, WebSphere variables, and shared library definitions. A network deployment of Sametime Gateway can contain as many secondary nodes as your environment needs.

Installing the Deployment Manager:

Install the Deployment Manager on its own machine, or on the same machine as the primary node. Installing the Deployment Manager on the same machine as the primary node provides the efficiency of multiple Java Virtual Machines and takes advantage of a fast CPU. If you are installing the Deployment Manager on the same machine with an existing primary node from a previous release, upgrade the primary node to the present release before installing the Deployment Manager.

Installing the Deployment Manager on Windows:

Install the Deployment Manager on the same machine as the primary server, or on a separate machine. The installation program also creates a non-SSL connection to LDAP.

Before you begin

Expected state: The DB2 server is installed, the DB2 database has been created, and DB2 is running.

Information on downloading packages for Sametime is located at the following Web address:

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

About this task

You can install the Deployment Manager and the primary server on the same machine, or each on its own machine. Additional nodes must be installed on their own machines.
Procedure

1. Log in as the Windows administrator on the server where you will install Sametime Gateway.
2. Create two temporary file folders: \TMP\WASCD and \TMP\SametimeGateway.
3. From the installation media, copy the WebSphere Application Server installation image `part_number.exe` to the folder \TMP\WASCD.
4. Open a command window and navigate to the folder \TMP\WASCD.
5. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK folders inside the ifpackage folder.
6. Extract the files in Sametime Gateway installation image `part_number.exe` to the \TMP\SametimeGateway folder.
7. Open a command window and navigate to the \TMP\SametimeGateway folder. Type the following command:
   - For wizard mode: `install.bat`
   - For console mode: `install.bat -console`

**Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   
   `install.bat -V BypassWasInfoCheck=true`

Because your input will not be verified during installation, you should take extra care when typing values.

8. Select the language for the installation wizard and click OK. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.
9. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click Next to proceed with the installation.
10. Select Deployment Manager, and then click Next.
11. Type or click Browse to select the path to where you extracted the WebSphere Application Server installation files from the CD. Do not use quotation marks. The directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `C:\TMP\WASCD\ifpackage` but do not use `C:\TMP\WASCD\ifpackage\WAS` or `C:\TMP\WASCD\ifpackage\JDK`.

12. Click Next to see the default directory path where WebSphere Application Server will be installed is displayed. To change the installation location of WebSphere Application Server, click Browse and select a desired location, or type a new path.
13. Click Next to see node, cell, and host name profile information provided by the installer. If the supplied information is okay, click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, exampleDMNode.</td>
</tr>
</tbody>
</table>
14. Create a user ID and password for logging into the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters:

\[;!*?/\!<@]+\&'"[]%^\]

15. Click Next to see the default directory path where Sametime Gateway will be installed. To change the location, click Browse and select a desired location, or type a new path.

16. Click Next to enter properties required by DB2:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

17. Click Next to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP now</td>
<td>Select if you want to set up a connection between Sametime Gateway and LDAP that does not need an SSL connection. You will need to know the host name and port of the LDAP server. If you select this option, continue with the next step.</td>
</tr>
</tbody>
</table>
Configure LDAP after the installation
Select this option if you need to set up an SSL connection with LDAP, or if you do not know the host name and port number used by LDAP. If you are installing Sametime Gateway outside the firewall and the LDAP directory is located inside the firewall, choose this option.
If you select this option, skip to step 21.

If you selected Configure LDAP now, complete the next four steps. Otherwise, proceed to Step 22.

18. Select an LDAP host name from list of Registered host names and ports in your domain, or select Other and enter a host name or IP address in the Host name field. The default port number is 389. Click Next.

19. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

Anonymous access
Select this option if you don't need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.

Authenticated access
Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.

20. Enter the Bind distinguished name (DN) and Bind password. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:
   • Bind distinguished name:
     uid=ldapadmin, cn=users, l=shipley, st=kansas, c=us, ou=sales, o=medical, DC=EXAMPLE, DC=COM
   • Bind password:
     C@pital1

21. Click Next. Choose a base distinguished name from the list of Suggested base distinguished names in your LDAP or enter a base DN in the Base distinguished name field. The base distinguished name indicates the starting point for LDAP searches of the directory service. For example, for the bind distinguished name given as an example in the previous step, you can specify the base DN as: DC=EXAMPLE, DC=COM. For authorization purposes, this field is case sensitive. This panel is not shown if you are connecting to Domino LDAP.

22. Click Next to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click Back to make changes.

23. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes
about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

24. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/install.log.txt`.

25. To test the Deployment Manager installation and ensure that LDAP settings are correct, log into the Deployment Manager node as a user with administrative privileges.

26. Navigate to the `stgw_profile_root/bin` directory.

27. Start the Deployment Manager with the following command:
   ```
   startManager.bat
   ```

28. Log in into the Integrated Solutions Console using the administrative user ID and password that you created.

29. Test the LDAP connectivity. Click **Users and Groups > Manage users**.

30. Verify that you can search and retrieve users in your LDAP directory.

31. Leave the Deployment Manager node running as you install other nodes in the cluster.

---

**Installing WebSphere iFixes for the deployment manager in a Sametime Gateway cluster (Windows):**

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

---

**Adding a Sametime Gateway cluster’s deployment manager (Windows) 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 Deployment Manager on AIX, Linux, or Solaris:**

Complete these steps to install the Deployment Manager server on AIX, Linux, or Solaris. Install the Deployment Manager on the same machine as the primary server, or on its own machine. The installation program also creates a non-SSL connection to LDAP.

**Before you begin**

Expected state: DB2 or the DBMS Administration Client is installed. The DB2 database is created and DB2 is running.

Information on downloading packages for Sametime is located at the following Web address:

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

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

Note that there are special naming rules for each node and cell that are part of a cluster. When installing each node, the node name and the cell name must be unique across all machines. *No two nodes can have the same cell name.* Later, when you federate each node into the cluster, the cell name is automatically changed to the Deployment Manager's cell name.

The installation wizard installs an instance of WebSphere Application Server and an instance of Sametime Gateway.

Procedure

1. Log in as `root` on the server where you will install Sametime Gateway.
2. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Open the `/etc/selinux/config` file for editing.
   b. Locate the `SELINUX` setting.
   c. Change its value to either `disable` or `permissive`.
   d. Save and close the file.
   e. Restart the Linux server.
3. Create the temporary file folder `/TMP/WASCD`.
4. From the installation media, copy the WebSphere Application Server installation image for your operating system to `/TMP/WASCD`.
5. Open a command window and navigate to the directory `/TMP/WASCD`.
6. Run the following command to extract the files:
   ```
   gunzip -c part_number.tar.gz | tar -xvf -
   ```

   When you are done extracting the files, you should have a
   `/TMP/WASCD/ifpackage` folder with WAS and JDK folders inside the ifpackage
   folder.
7. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the `/TMP` folder.
8. Unzip the files in `part_number.tar`. This step creates the folder
   `/TMP/SametimeGateway`.
9. In the DB2 profile window, navigate to the `/TMP/SametimeGateway` directory, and execute the following command:
   • `. /install.sh` (wizard installation)
   • `. /install.sh -console` (console installation)

   **Attention:** If one or more of the domain addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   ```
   install.sh -V BypassWasInfoCheck=true
   ```

   Because your input will not be verified during installation, you should take extra care when typing values.
10. Select the language for the installation wizard and click **OK**. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.
11. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed with the installation.

12. Select **Deployment Manager**, and then click **Next**.

13. The WebSphere Application Server installation directory dialog is displayed. Type the root to the path where you copied the WebSphere Application Server installation files from the CD. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/WAS` or `/TMP/WASCD/ifpackage/JDK`.

14. Click **Next** to see the default directory path where WebSphere Application Server will be installed is displayed. To change the installation location of WebSphere Application Server, click **Browse** and select a desired location, or type a new path.

15. Click **Next** to see node, cell, and host name profile information provided by the installer. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, exampleDMNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleDMCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section &quot;Host name considerations&quot; in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
</tbody>
</table>

16. Create a user ID and password for logging into the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: 

`;!?"/\|+&'[]^`  

17. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

18. Click **Next** to enter properties required by DB2:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

19. Click **Next** to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP now</td>
<td>Select if you want to set up a connection between Sametime Gateway and LDAP that does not need an SSL connection. You will need to know the host name and port of the LDAP server. If you select this option, continue with the next step.</td>
</tr>
<tr>
<td>Configure LDAP after the installation</td>
<td>Select this option if you need to set up an SSL connection with LDAP, or if you do not know the host name and port number used by LDAP. If you are installing Sametime Gateway outside the firewall and the LDAP directory is located inside the firewall, choose this option. If you select this option, skip to step 23.</td>
</tr>
</tbody>
</table>

If you selected **Configure LDAP now**, complete the next four steps. Otherwise, proceed to Step 24.

20. Select an LDAP host name from list of Registered host names and ports in your domain, or select Other and enter a host name or IP address in the Host name field. The default port number is 389. Click Next.

21. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous access</td>
<td>Select this option if you don’t need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.</td>
</tr>
<tr>
<td>Authenticated access</td>
<td>Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.</td>
</tr>
</tbody>
</table>
22. Enter the **Bind distinguished name (DN)** and **Bind password**. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:
   - Bind distinguished name:
     
     \[ uid=ldapadmin, cn=users, l=shipley, st=kansas, c=us, ou=sales, o=medical, DC=EXAMPLE, DC=COM \]
   - Bind password:
     
     Capital1

23. Click **Next**. Choose a base distinguished name from the list of **Suggested base distinguished names in your LDAP** or enter a base DN in the **Base distinguished name** field. The base distinguished name indicates the starting point for LDAP searches of the directory service. For example, for the bind distinguished name given as an example in the previous step, you can specify the base DN as: \[ DC=EXAMPLE, DC=COM \]. For authorization purposes, this field is case sensitive. Note that this panel is now shown if you are connecting to Domino LDAP.

24. Click **Next** to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click **Back** to make changes.

25. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

26. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at \[ stgw_server_root/logs/installlog.txt \]

27. To test the Deployment Manager installation and ensure that LDAP settings are correct, log into the Deployment Manager node as a user with administrative privileges.

28. Navigate to the \[ stgw_profile_root/bin \] directory.

29. Start the Deployment Manager with the following command:

   \[ ./startManager.sh \]

30. Log in into the Integrated Solutions Console using the administrative user ID and password that you created.

31. Test the LDAP connectivity. Click **Users and Groups > Manage users**.

32. Verify that you can search and retrieve users in your LDAP directory.

33. Leave the Deployment Manager node running as you install other nodes in the cluster.

**What to do next**

You have installed the Deployment Manager server.

**Note:** Do not start the server at this time (skip step 3 – restart the server – in the steps below).

*Installing WebSphere iFixes for the deployment manager in a Sametime Gateway cluster (AIX, Linux, Solaris):*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.
About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Adding a Sametime Gateway cluster’s deployment manager (AIX, Linux, Solaris) 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 primary node:

Install a primary node for a cluster. You can install the primary node and the Deployment Manager on the same machine. Installing the primary node on the same machine as the Deployment Manager provides the efficiency of multiple Java Virtual Machines and takes advantage of a fast CPU. If you are installing the primary node on the same machine with an existing Deployment Manager from a previous release, upgrade the Deployment Manager to the present release before installing the primary node.

Installing the primary node on Windows:

Complete these steps to install the primary node of a Sametime Gateway cluster on Windows. You can install both the primary node and Deployment Manager on the same machine.

Before you begin

Expected state: DB2 or the DBMS Administration Client is installed. The DB2 database is created and DB2 is running. The Deployment Manager is installed and running.

Information on downloading packages for Sametime is located at the following Web address:

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

About this task

The following steps show the installation of a primary node on a separate machine from the Deployment Manager. If you are installing the primary node on the same system as the Deployment Manager, you do not have to copy the WebSphere Application Server media to the server. Instead, the install program reuses the shared binaries that are installed with the Deployment Manager.

Procedure

1. Log in as the Windows administrator on the server where you will install Sametime Gateway.
2. Complete the following substeps only if you are installing the primary node on its own machine. If you plan to install the primary node on the same machine as the Deployment manager, skip to step 3.
   a. Create two temporary file folders: \tmp\WASCD and \tmp\SametimeGateway.
   b. From the installation media, copy the WebSphere Application Server installation image part_number.exe to the folder \tmp\WASCD.
   c. Open a command window and navigate to the folder \tmp\WASCD.
d. Extract all files to the temporary directory `\TMP\WASCD`. When you are done, you should have a `\TMP\WASCD\ifpackage` folder with WAS and JDK folders inside the `ifpackage` folder.

e. Extract the files in the Sametime Gateway installation image `part_number.exe` to the `\TMP\SametimeGateway` folder.

3. Navigate to the `\TMP\SametimeGateway` folder.

4. Type the following command:
   - For wizard mode: `install.bat`
   - For console mode: `install.bat -console`

**Attention:** If one or more of the domain addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:
   
   `install.bat -V BypassWasInfoCheck=true`

Because your input will not be verified during installation, you should take extra care when typing values.

5. Select the language for the installation wizard and click **OK**. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

6. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed with the installation.

7. **Primary Node** is selected as the installation type by default; however, sometimes the default selection is not captured. To ensure you really install a Primary Node:
   
   a. Select any other installation type.
   
   b. Then select **Primary Node** as the installation type.

8. Check the node name, cell name, and host name that are supplied by the installer. Make sure that the cell and node names do not match the cell and node names you used when installing the Deployment Manager. Choose a unique node name and cell name for this installation. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>The logical name for the node. For example, <code>exampleNodePrimary</code>.</td>
</tr>
<tr>
<td>Cell</td>
<td>A name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, <code>exampleCellPrimary</code>.</td>
</tr>
</tbody>
</table>
9. Type the administrative user ID and password used to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same user ID and password that you created when you installed the Deployment Manager. The user ID must not exist in the LDAP directory.

10. Click Next to see the default directory path where Sametime Gateway will be installed. To change the location, click Browse and select a desired location, or type a new path.

11. Type the required information for the database as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td></td>
<td>Note: If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section &quot;Host name considerations&quot; in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

12. Click Next to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click Back to make changes.

13. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes
about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

14. Read the summary and click Finish. To view the installation log, click View log file or open the log file at stgw_server_root\logs\installlog.txt

*Installing WebSphere iFixes for the primary node (Windows) in a Sametime Gateway cluster:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Adding the Sametime Gateway cluster’s primary node (Windows) to the Sametime Community Server’s trusted IPs:*

Whenever you install a server that communicates with a community server, you must add the new server’s IP address to the community server.

**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 primary node on AIX, Linux, or Solaris:

Install the primary node of a Sametime Gateway cluster on Windows. You can install both the primary node and Deployment Manager on the same machine.

Before you begin

Expected state: DB2 or the DBMS Administration Client is installed. The DB2 database is created and DB2 is running. The Deployment Manager is installed and running.

Information on downloading packages for Sametime is located at the following Web address:

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

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

About this task

The Sametime Gateway install wizard deploys both the WebSphere Application Server and the Sametime Gateway server application in one installation.

Procedure

1. Log in as root on the server where you will install Sametime Gateway.
2. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Open the /etc/centos/config file for editing.
   b. Locate the SELINUX setting.
   c. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
3. If you are not installing the primary node on the Deployment Manager machine, complete the following sub steps:
   a. Create the temporary file folder /TMP/WASCD.
   b. Open a command window and navigate to the folder /TMP/WASCD.
   c. Extract all files to the temporary directory /TMP/WASCD. When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.
   d. Run the following command to extract the files:
      ```
gunzip -c part_number.tar.gz | tar -xvf -
```
      When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.

4. From the installation media, copy the Sametime Gateway installation image part_number.tar to the temporary directory /TMP/SametimeGateway.

5. Extract the following file to the /TMP/SametimeGateway folder:
   ```
tar -xvf part_number.tar
```

6. Navigate to the temporary directory /TMP/SametimeGateway and type one of the following commands:
   - For wizard mode: ./install.sh
   - For console mode: ./install.sh -console

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:
   ```
./install.sh -V BypassWasInfoCheck=true
```

   Because your input will not be verified during installation, you should take extra care when typing values.
   This command installs WebSphere Application Server 6.1 and Sametime Gateway. The Language Selection dialog is displayed.

7. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.

8. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.

9. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.

10. **Primary Node** is selected as the installation type by default; however, sometimes the default selection is not captured. To ensure you really install a Primary Node:
   a. Select any other installation type.
   b. Then select **Primary Node** as the installation type.

11. If you are installing the primary node on the Deployment Manager, the installation wizard recognizes that an instance of Sametime Gateway is on the same machine. The new installation for the primary node adds a profile to WebSphere Application Server. Click **Next**, and then click **Next** again.

12. Check the node name, cell name, and host name that are supplied by the installer. Make sure that the cell and node names *do not* match the cell and
node names you used when installing the Deployment Manager. Choose a unique node name and cell name for this installation. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td>Logical name for the node. For example, exampleNodePrimary.</td>
</tr>
<tr>
<td><strong>Cell</strong></td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCellPrimary.</td>
</tr>
</tbody>
</table>
| **Host name**| Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com  
**Note:** If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section “Host name considerations” in the WebSphere Application Server information center topic, Creating an application server profile. |

13. Type the administrative user ID and password used to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. You created these credentials when you installed the Deployment Manager. The user ID must not exist in the LDAP directory.

14. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

15. Type the required information for DB2 as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td><strong>Database name</strong></td>
<td>The name of the database that you created. If you used the default database name, type $STGW. Case does not matter.</td>
</tr>
<tr>
<td><strong>Application user ID</strong></td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td><strong>Application password</strong></td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td><strong>Schema user ID</strong></td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

16. Click **Next** to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click **Back** to make changes.

17. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

18. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`.

*Installing WebSphere iFixes for the primary node (AIX, Linux, Solaris) in a Sametime Gateway cluster:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Adding the Sametime Gateway cluster’s primary node (AIX, Linux, Solaris) to the Sametime Community Server’s trusted IPs:*

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.

**Federating the primary node into the cell:**

After you create the primary node you must add the primary node to the Deployment Manager’s cell.

**Federating the primary node into the cell on Windows:**

Add the primary node to the Deployment Manager's cell. Adding the primary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager’s Integrated Solutions Console. You will not be able log into the primary node's Integrated Solutions Console after this step.

**Before you begin**

Expected state: the Deployment Manager is running.
About this task

Procedure

1. Make sure that the system clocks on the Deployment Manager and the primary
node are within five minutes of each other and set for the same timezone.
   Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the primary node to make sure the
host name is resolvable.
3. On the primary node, open a command window and navigate to the
   `stgw_profile_root\bin` directory. If the Deployment Manager and the primary
node are installed on the same machine, the default profile directory is
   RTCGW_Profile1 (not RTCGW_Profile).
4. Run the following command to add the primary node to the Deployment
   Manager’s cell:
   ```
   addNode.bat DM_hostname DM_port_number -includeapps
   ```
   Where `DM_hostname` is the host name of the Deployment Manager server. For
   example:
   ```
   addNode.bat gateway_dm.example.com 8879 -includeapps
   ```
   Port 8879 is the default port on which the Deployment Manager listens.

   **Note:** If you are upgrading the server, the Deployment Manager, the default
   port on which the Deployment Manager listens changes after the upgrade. The
   list of default ports can be found under `stgw_profile_root\logs\AboutThisProfile.txt`
   of the deployment manager profile. To verify which port is
   used by the Deployment Manager for SOAP communication, open **System
   Administration > Deployment manager > Ports** and note the value of
   `SOAP_CONNECTOR_ADDRESS`.

5. When prompted, provide the Deployment Manager’s administrative user ID
   and password.
   Wait for the operation to complete before proceeding. Look for a success
   message similar to the following when complete:
   ```
   Node MyserverNodePrimary has been successfully federated.
   ```

6. To verify that the primary node has joined the Deployment Manager’s cell, log
   into the Integrated Solutions Console using your administrative user ID and
   password and click **Servers > Application servers**. Make sure you can see the
   primary node’s information.
   If you already logged in, you must log out and then log in again before you
   can see changes.

Federating the primary node into the cell on AIX, Linux, and Solaris:

Add the primary node to the Deployment Manager’s cell on AIX, Linux, or Solaris
platforms. Adding the primary node to the cell allows a central point of
administration for the network deployment by using the Deployment Manager’s
Integrated Solutions Console. You will not be able log into the primary node’s
Integrated Solutions Console after this step.

Before you begin

Expected state: the Deployment Manager is running.
Procedure

1. Make sure that the system clocks on the Deployment Manager and the primary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the primary node to make sure the Deployment Manager host name is resolvable.

3. On the primary node, open a command window and navigate to the \stgw_profile_root\bin directory.

4. Run the following command to add the primary node to the Deployment Manager's cell:

   ```
   ./addNode.sh DM_hostname DM_port_number -includeapps
   ```

   Where DM_hostname is the host name of the Deployment Manager server. For example:

   ```
   ./addNode.sh gateway_dm.example.com 8879 -includeapps
   ```

   **Note:** After upgrading, the default port on which the Deployment Manager listens is changing. The list of default ports can be found under \stgw_profile_root\logs\AboutThisProfile.txt of the deployment manager profile (for example, RTCGW_Profile).

5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

   Node MyserverNodePrimary has been successfully federated.

   Port 8879 is the default port on which the Deployment Manager listens.

6. To verify that the primary node has joined the Deployment Manager's cell, log into the Integrated Solutions Console using your administrative user ID and password and click **Servers > Application servers**. Make sure you can see the primary node's information.

   If you already logged in, you must log out and then log in again before you can see changes.

**What happens when you federate the primary node into the cell?:**

When you federate the primary node into the Deployment Manager's cell, the primary node's original configuration is backed up. This means that you can remove the primary node from the Deployment Manager at a later time, and you can restore the profile configuration to the state it was in before federation.

The primary node's scope changes to include the Deployment Manager's cell. Before federation, the scope of the RTCGWServer was:

```
cell:<PrimaryCell>/node:<PrimaryNode>/server:RTCGWServer
```

After federation, the scope of the server is the following:

```
cell:<Deployment Manager Cell>/node:<PrimaryNode>/server:RTCGWServer
```

When you federate, the Integrated Solutions Console of the primary node is disabled because you will be using the Integrated Solutions Console from the Deployment Manager. The primary node inherits all the cell level configuration data from the Deployment Manager. Any information you can see through the Deployment Manager's Integrated Solutions Console is now stored in XML on the primary node, so it is accessible from any application. The applications that were...
installed to RTCGWServer are now included on the RTCGWServer in the Deployment Manager's cell. If you attempt to federate another node that contains these same applications, they are excluded.

Because the LDAP configuration and your credentials as the WebSphere Application Server administrative user in the Deployment Manager are defined at the cell level, this data overwrites the security settings of the primary node. The Deployment Manager's settings apply to the primary node. If you remove the primary node from the cell, the primary node's original security configuration are restored.

When you federate the primary server into the cell, a single server of Sametime Gateway can be managed by a Deployment Manager. You can actually run a real environment and configure your Sametime communities just as you would in a standalone server environment. What is lacking is failover and load balancing capabilities. In order to add those features, you need to add a secondary node and create a cluster in the later steps.

*Installing additional nodes in a cluster:*

Depending upon your capacity requirements, install secondary nodes as needed.

*Installing a secondary node on Windows:*

Complete these steps to install a secondary node on Windows that will be part of a cluster of Sametime Gateway servers.

**About this task**

A secondary node for the cluster must be installed on its own machine and cannot be installed on the same machine as the primary server or the Deployment Manager.

Information on downloading packages for Sametime is located at the following Web address:

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

**Procedure**

1. Log in as the Windows administrator on the server where you will install Sametime Gateway.
2. Create two temporary file folders: `\TMP\WASCD` and `\TMP\SametimeGateway`.
3. From the installation media, copy the WebSphere Application Server installation image `part_number.exe` to the folder `\TMP\WASCD`.
4. Open a command window and navigate to the folder `\TMP\WASCD`.
5. Extract all files to the temporary directory `\TMP\WASCD`. When you are done extracting the files, you should have a `\TMP\WASCD\ifpackage` folder with WAS and JDK folders inside the ifpackage folder.
6. Extract the files in the Sametime Gateway installation image `part_number.exe` to the `\TMP\SametimeGateway` folder.
7. Open a command window and type the following command:
   - For wizard mode: `install.bat`
   - For console mode: `install.bat -console`
Attention: If one or more of the domain addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6–related issue with the installer:

\`install.bat -V BypassWasInfoCheck=true\`

Because your input will not be verified during installation, you should take extra care when typing values.

8. Select the language for the installation wizard and click **OK**. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

9. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed with the installation.

10. Select **Secondary node**, and then click **Next**.

11. Type or click **Browse** to select the path to where you extracted the WebSphere Application Server installation files from the CD. Do not use quotation marks. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `C:\TMP\WASCD\ifpackage` but do not use `C:\TMP\WASCD\ifpackage\WAS` or `C:\TMP\WASCD\ifpackage\JDK`.

12. Click **Next** to see the default directory path where WebSphere Application Server will be installed is displayed. To change the installation location of WebSphere Application Server, click **Browse** and select a desired location, or type a new path.

13. Click **Next** to see node, cell, and host name profile information provided by the installer. Make sure that the cell and node names do not match the cell and node names that you used when installing the Deployment Manager or the primary node, or any previously created secondary nodes. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, gwNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, gwCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section &quot;Host name considerations&quot; in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
</tbody>
</table>

14. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same
administrative user ID and password that you created when installing the Deployment Manager and primary node. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters:  
;!*"/<>`\]['^`

15. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

16. Click **Next** to enter database properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

17. Click **Next** to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click **Back** to make changes.

18. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

19. Read the summary and click **Install**.

To view the installation log, click **View log file** or open the log file at `stgw_server_root\logs\installlog.txt`

*Installing WebSphere iFixes for the secondary node (Windows) in a Sametime Gateway cluster:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.

   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Adding the Sametime Gateway cluster’s secondary node (Windows) to the Sametime Community Server’s trusted IPs:

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 a secondary node on AIX, Linux, or Solaris:
Complete these steps to install a secondary node on AIX, Linux, or Solaris that will be part of a cluster of Sametime Gateway servers.

**Before you begin**

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

**About this task**

A secondary node for the cluster must be installed on its own machine and cannot be installed on the same machine as the primary server or the Deployment Manager.

Part numbers are listed at the following Web address:

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

**Procedure**

1. Log in as root on the server where you will install Sametime Gateway.
2. (Linux RHEL only) Disable SELinux on any RedHat operating system:
   a. Open the `/etc/selinux/config` file for editing.
   b. Locate the SELINUX setting.
   c. Change its value to either disable or permissive.
   d. Save and close the file.
   e. Restart the Linux server.
3. Create the temporary file folder `/TMP/WASCD`.
4. From the installation media, copy the WebSphere Application Server installation image for your operating system to `/TMP/WASCD`.
5. Open a command window and navigate to the directory `/TMP/WASCD`.
6. Run the following command to uncompress the files:
   
   ```
   gunzip -c part_number.tar.gz | tar -xvf -
   ```

   When you are finished extracting the files, you should have a `/TMP/WASCD/ifpackage` folder with WAS and JDK folders inside the ifpackage folder.
7. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the temporary directory `/TMP/SametimeGateway`.
8. In the DB2 profile window, navigate to the temporary directory `/TMP`.
9. Unzip the following file to the `/TMP/SametimeGateway` folder:
   
   ```
   unzip part_number.tar
   ```
10. Navigate to the folder `/TMP/SametimeGateway` and type one of the following commands:
    • For wizard mode: `. /install.sh`
    • For console mode: `. /install.sh -console`
Attention:  If one or more of the domain addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

```
install.sh -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

The Language Selection dialog is displayed.

11. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.

12. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.

13. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.

14. Select **Secondary node** as the type of installation, and then click **Next**.

15. The WebSphere Application Server 6.1 installation directory dialog is displayed. Type the root to the path where you copied the WebSphere Application Server installation files from the CD. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/WAS` or `/TMP/WASCD/ifpackage/JDK`.

16. Click **Next** to continue with the installation. The WebSphere Application Server Location dialog is displayed. If you wish to change the location for the installation of WebSphere Application Server, click **Browse** and select the desired location.

17. Click **Next** to see node, cell, and host name profile information provided by the installer. Make sure that the cell and node names do not match the cell and node names that you used when installing the Deployment Manager or the primary node, or any previously created secondary nodes. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td>Logical name for the node. For example, gwNode.</td>
</tr>
<tr>
<td><strong>Cell</strong></td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, gwCell.</td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com. Note: If the server where you are installing has multiple NICs/IPv/DNS names, or for more information about considerations in choosing a host name, read the section &quot;Host name considerations&quot; in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
</tbody>
</table>
18. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same administrative user ID and password that you created when installing the Deployment Manager and primary node. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters:

;*!"'<>^&\]

19. Click **Next** to see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

20. Click **Next** to enter database properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td><strong>Database name</strong></td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td><strong>Application user ID</strong></td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td><strong>Application password</strong></td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

21. You can review the installation summary settings and if necessary click **Back** to make changes.

22. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating the successful installation of the Sametime Gateway and WebSphere Application Server products.

23. Read the summary and click **Finish** to complete the installation. Do not start the server or first steps at this time.

*Installing WebSphere iFixes for the secondary node (AIX, Linux, Solaris) in a Sametime Gateway cluster:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
The iFixes are included in the following package: IBM WebSphere V7.0.0.3
iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere
Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in
Installing WebSphere Application Server updates.

Adding the Sametime Gateway cluster’s secondary node (AIX, Linux, Solaris) to the
Sametime Community Server’s trusted IPs:

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.
Federating secondary nodes into the cell:

Add secondary nodes to the Deployment Manager's cell to create a network deployment of Sametime Gateway servers.

About this task

In this release, a Sametime Gateway cluster can support only two nodes: one Primary Node and one Secondary Node.

Federating a secondary node on Windows into the cell:

Add a secondary node to the Deployment Manager's cell. Adding secondary nodes to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

Before you begin

Expected state: the Deployment Manager is running.

Procedure

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.

3. On the secondary node, open a command window and navigate to the stgw_profile_root\bin directory.

4. Run the following command to add a secondary node to the Deployment Manager's cell. Note the omission of the -includeapps qualifier.

   ```
   addNode.bat DM_hostname DM_port_number
   ```

   Where `DM_hostname` is the host name of the Deployment Manager server. For example:

   ```
   addNode.bat gateway_dm.example.com 8879
   ```

   Port 8879 is the default port on which the Deployment Manager listens.

   **Note:** To verify which port is used by the Deployment Manager for SOAP communication, open System Administration > Deployment manager > Ports and note the value of SOAP_CONNECTOR_ADDRESS.

5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

   ```
   Node Machine22NodeSecondary has been successfully federated.
   ```

6. For each additional secondary node, repeat the preceding steps.

7. Restart the Deployment Manager by typing the following commands. Wait for the first command to finish before starting the Deployment Manager:

   ```
   stopManager
   startManager
   ```
What to do next

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers.”

Federating a secondary node on AIX, Linux, and Solaris into the cell:

Add a secondary node to the Deployment Manager's cell. Adding a secondary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

Before you begin

Expected state: the Deployment Manager is running.

Procedure

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.
3. On secondary node, open a command window and navigate to the stgw_profile_root\bin directory.
4. Run the following command to add a secondary node to the Deployment Manager's cell. Note the omission of the -includeapps qualifier.
   ```bash
   ./addNode.sh DM_hostname DM_port_number
   ```
   Where **DM_hostname** is the host name of the Deployment Manager server. For example:
   ```bash
   ./addNode.sh gateway_dm.example.com 8881
   ```
5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:
   ```
   Node Machine22NodeSecondary has been successfully federated.
   ```
6. For each additional AIX, Linux, or Solaris secondary node, repeat the preceding steps.
7. Restart the Deployment Manager by typing the following commands on the Deployment Manager machine. Wait for the first command to finish before starting the Deployment Manager:
   ```bash
   ./stopManager.sh
   ./startManager.sh
   ```

What to do next

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers.”

Creating a cluster and proxy servers:
Create a Sametime Gateway cluster, install proxy servers, and then configure the proxy servers to use the cluster. Set up node replication only if you need high availability and failover, and then start the cluster.

About this task

Starting a cluster involves starting the Deployment Manager, starting the node agents on all the nodes, and then starting the servers, including the proxy servers, on each node.

Creating the cluster:

Create a new cluster of Sametime Gateway servers by running the Cluster Configuration Wizard. If you are upgrading an existing Sametime Gateway cluster, you can skip this step because there is no need to create a new cluster.

Before you begin

Expected state: the Deployment Manager is running and nodes are stopped.

About this task

The instructions that follow describe steps for setting up a horizontal cluster, the most common cluster configuration. The primary node already has the primary server installed, so no additional server is needed on that computer. To add servers to the horizontal cluster, create one cluster member for each secondary node (computer).

Procedure

1. On the Deployment Manager, open a command window, navigate to the `stgw_server_root\config` directory, and run the following command:
   - AIX, Linux, and Solaris
     ```bash
     ./configwizard.sh
     ```
   - Windows
     ```bat
     configwizard.bat
     ```
   - IBM i
     ```bash
     configwizard.sh
     ```
   
   **Note:** To run this program in console mode (instead of using the graphical interface), add the `-console` argument to the command line; for example:
   ```bash
   configwizard.bat -console
   ```

2. View the Welcome page and click **Next**.

3. For each secondary node, do the following:
   a. Select a secondary node from the **Node** drop down list and type a unique name in the **Server Name** field.
   b. Click **Add Member**.

4. When you have finished adding the secondary nodes, click **Next**.

5. Type the **Schema user ID** and **Schema password** for the database. These credentials have appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID for the database.
6. Read the summary and click **Configure**. When finished, you can view the configuration log at You can review the configuration wizard log at `stgw_server_root/logs/configwizard.log`.

7. Restart the Deployment Manager with the following commands:
   - **AIX, Linux, and Solaris**
     ```bash
     ./stopManager.sh -username wasadmin_username -password wasadmin_password
     ./startManager.sh
     ```
   - **Windows**
     ```
     stopManager.bat -username wasadmin_username -password wasadmin_password
     startManager.bat
     ```
   - **IBM i**
     ```
     stopmanager -username wasadmin_username -password wasadmin_password
     startManager
     ```

8. Complete the following steps on every node in the cluster, including the primary node:
   a. Log in to the node's operating system.
   b. Navigate to the `stgw_profile_root\bin` directory.
   c. Start the node agent on the node with the following command:
      - **AIX, Linux, and Solaris**
        ```bash
        ./startNode.sh
        ```
      - **Windows**
        ```
        startNode.bat
        ```
      - **IBM i**
        ```
        startNode
        ```

      **Note:** During installations, the Node agent on primary and secondary servers may be loaded, and issuing a `startnode` command may result in the error: "Conflict detected on port 8878. Likely causes: a) An instance of the server nodeagent is already running b) some other process is using port 8878." If this occurs you can confirm the nodeagent status by running the command `serverstatus nodeagent` from the `stgw_profile_root\bin` directory. When prompted, supply the Sametime Gateway administrator credentials. Verify that the nodeagent is running (the status will read, "The Node Agent "nodeagent" is STARTED). If the agent is running, continue to the next step.

9. When all the node agents are started, verify that the cluster configured properly by performing the following steps:
   a. Log into the Integrated Solutions Console using your administrative user ID and password on the Deployment Manager machine.
   b. Click **Servers > Clusters**, and verify that `SametimeGatewayCluster` appears in the table.
   c. Click `SametimeGatewayCluster`, and then under Additional properties, click **Cluster members** to view the cluster members that you created.

**Creating a vertical Gateway cluster by adding servers to existing nodes:**

In an IBM Sametime deployment, create a vertical cluster of Sametime Gateway servers by installing additional servers onto existing nodes.
Add cluster members to an existing node to create a vertical cluster.

Procedure
1. On the cluster's Deployment Manager, log in to the IBM WebSphere Application Server's Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Clusters > WebSphere application server clusters > SametimeGatewayCluster > Cluster members.
3. Add a new cluster member as follows:
   a. In the list of cluster members, click the New button.
   b. Type a name for the new cluster member; for example: Node1RTCWGServer2.
   c. Select the node where you want to install this new cluster member.
   Tip: To see which servers the nodes are hosted on, use another tab to navigate to: System Administration > Nodes.
   d. Leave the remaining settings alone so that they use their default values.
   e. Click Add Member.
   f. Click Next.
   g. At the "Step 3: Summary" screen, click Finish.
4. Click Save.
5. Complete the following tuning procedures for each newly created server:
   a. Setting thread pool values
   b. Setting the JVM garbage collection policy
   c. Setting log files size and rotation
6. Repeat steps 1 through 5 for each additional server that you want to add to an existing node.

Connecting a Sametime Gateway cluster to the 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 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 582

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

*Sametime prerequisite: Connecting a Sametime Gateway cluster to the 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.

Installing SIP and XMPP proxy servers:

SIP and XMPP proxy servers act as the initial point of entry for messages that flow into and out of the enterprise. Both types of proxies are capable of securing the transport, using secure sockets layer (SSL), and the content, using various authentication and authorization schemes.

Before you begin

Expected state: DB2, LDAP, and Sametime Gateway servers are installed.

About this task

A SIP proxy server facilitates automatic load balancing, affinity matching, and failover for a cluster of Sametime Gateway servers. The enterprise’s public SIP fully qualified domain name leads to the SIP proxy host, either directly, or through an IP sprayer that load balances incoming traffic to multiple proxies.

You must set up a Sametime Gateway cluster with at least one node before creating and federating SIP proxy servers. While you can install these proxy servers on an IBM Sametime Gateway node, it is recommended that you install them on a separate machine to isolate the proxy processing from the Sametime Gateway cluster. After you set up a Lotus Sametime Gateway cluster and a SIP proxy server, you can add external communities to Sametime Gateway. All of this information is set in the Sametime Gateway Web administration console (also available through the Sametime System Console after the Gateway is registered).

For network security, IBM recommends that you install the XMPP and SIP proxy server node and the Sametime Gateway cluster in the network DMZ. Installing the SIP proxy in the DMZ by itself is not a supported configuration because it places a
firewall device between that server and the Sametime Gateway cluster. All of these components should be able to communicate freely which each other without traversing through a firewall device.

*Installing a SIP and XMPP proxy server on Windows:*

The SIP and XMPP proxy servers are the first point of contact, after the firewall, for messages that flow into and out your enterprise. Install the proxy servers for both standalone or network deployment installations of Sametime Gateway. IBM recommends that you install a SIP and XMPP proxy server on its own node.

**About this task**

The XMPP and SIP proxy server node installation creates a WebSphere Application Server node with two application servers installed. One server is a generic SIP proxy server provided by WebSphere Application Server, and the other is a standard application server onto which is installed the XMPP proxy application. The node does not function until it is federated into a Sametime Gateway cell.

Information on downloading packages for Sametime is located at the following Web address:

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

**Procedure**

1. Create two temporary file folders: \TMP\WASCD and \TMP\SametimeGateway.
2. From the installation media, copy the WebSphere Application Server installation image *part_number*.exe to the folder \TMP\WASCD.
3. Open a command window and navigate to the folder \TMP\WASCD.
4. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK folders inside the ifpackage folder.
5. From the installation media, copy the Sametime Gateway installation image *part_number*.exe to the \TMP folder.
6. Extract the files in *part_number*.exe to the \TMP\SametimeGateway folder.
7. Navigate to the \TMP\SametimeGateway folder.
8. Type the following command:
   • For wizard mode: *install.bat*
   • For console mode: *install.bat -console*

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   
   *install.bat -V BypassWasInfoCheck=true*

   Because your input will not be verified during installation, you should take extra care when typing values.
9. Select the language for the installation wizard and click **OK**. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.
10. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed with the installation.

11. If you are installing the proxy server on its own computer instead of on an existing Sametime Gateway node, complete the following sub steps:
   a. Select **SIP and XMPP proxy servers**, and then click **Next**.
   b. The WebSphere Application Server installation directory dialog is displayed. Type the root to the path where you copied the WebSphere Application Server installation files from the CD. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `\TMP\WAS\ifpackage` but do not use `\TMP\WAS\ifpackage\WAS` or `\TMP\WAS\ifpackage\JDK`.
   c. Click **Next** to continue with the installation. The WebSphere Application Server Location dialog is displayed. If you wish to change the location for the installation of WebSphere Application Server, click **Browse** and select the desired location.

12. If you are installing the proxy servers on an existing Sametime Gateway node, the installation wizard recognizes that an instance of Sametime Gateway is on the same machine. The new installation for the proxy servers adds a profile to WebSphere Application Server. Click **Next**.

13. Check the node name, cell name, and host name that are supplied by the installer. Make sure that the cell and node names **do not** match the cell and node names you used when installing the Deployment Manager. Choose a unique node name and cell name for this installation. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, <code>acmeNodeProxy</code>.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, <code>acmeCellProxy</code>.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: <code>proxy.acme.com</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section “Host name considerations” in the WebSphere Application Server information center topic.</td>
</tr>
</tbody>
</table>

14. Type the administrative user ID and password used to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same user ID and password that you created when you installed the Deployment Manager. The user ID must not exist in the LDAP directory. Click **Next**.
15. If you are installing the proxy servers on their own machine, you now see the
default directory path where Sametime Gateway will be installed. To change
the location, click Browse and select a desired location, or type a new path.

16. Click Next to see the Sametime Gateway installation summary. You can
review the installation summary settings and, if necessary, click Back to make
changes.

17. Click Install to begin copying files. A progress screen is displayed and the
activity is logged to the Sametime Gateway log file. This installation takes
about 10 to 20 minutes to complete. When the installation is complete, the
wizard displays a message indicating a successful installation.

18. Read the summary and click Finish. To view the installation log, click View
log file or open the log file at stgw_server_root\logs\installlog.txt

What to do next

Note: If you start the SIPProxyServer instance now and log into the Integrated
Solutions Console, you cannot view the SIPProxyServer instance. After you
federate the node in the next procedure, you will see the SIPProxyServer instance.

Installing WebSphere iFixes for the SIP proxy server (Windows) in a Sametime
Gateway cluster:

Install required IBM WebSphere Application Server updates on the IBM Lotus
Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere
Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime
Gateway server.
   - The iFixes are included in the following package: IBM WebSphere V7.0.0.3
   iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
   Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere
Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in
Installing WebSphere Application Server updates.

Installing a SIP and XMPP proxy server on AIX, Linux, or Solaris:

The SIP and XMPP proxy servers are the first point of contact, after the firewall,
for messages that flow into and out your enterprise. To set up a Sametime
Gateway deployment, install a SIP and XMPP proxy server on its own node.

About this task

Information on downloading packages for Sametime is located at the following
Web address:

https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
**AIX, Linux, and Solaris:** If you are installing using the GUI mode, the full X11 desktop environment is required.

**Note:** Multiple XMPP proxies configuration are not currently supported; only one XMPP proxy instance can be configured and run. The installer installs a XMPP proxy instance with every SIP proxy installation, but you must configure only one XMPP proxy in the cell and in the IP sprayer.

**Procedure**

1. Create the temporary file folder `/TMP/WASCD`.
2. Open a command window and navigate to the folder `/TMP/WASCD`.
3. Extract all files to the temporary directory `/TMP/WASCD`. When you are done extracting the files, you should have a `/TMP/WASCD/ifpackage` folder with WAS and JDK folders inside the `ifpackage` folder.
4. Run the following command to uncompress the files:
   ```
   gunzip -c part_number.tar.gz | tar -xvf -
   ```

   When you are done extracting the files, you should have a `/TMP/WASCD/ifpackage` folder with WAS and JDK folders inside the `ifpackage` folder.
5. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the temporary directory `/TMP`.
6. Unzip the following file:
   ```
   unzip part_number.tar
   ```

   This step creates the folder `/TMP/SametimeGateway`.
7. Navigate to the temporary directory `/TMP/SametimeGateway` and type one of the following commands:
   - For wizard mode: `/install.sh`
   - For console mode: `/install.sh -console`

   This command installs WebSphere Application Server and Sametime Gateway. The Language Selection dialog is displayed.
8. Select the language to be used for the installation and click OK. The Sametime Gateway Welcome screen is displayed.
9. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.
10. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click Next to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.
11. Select **SIP and XMPP proxy servers**, and then click Next.
12. If you are installing the proxy servers on their own machine, complete the following sub steps:
   a. The WebSphere Application Server installation directory dialog is displayed. Type the root to the path where you copied the WebSphere Application Server installation files from the CD. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/WAS` or `/TMP/WASCD/ifpackage/JDK`.

---

514 IBM Sametime: Installation, Migration, and Configuration Guide
b. Click **Next** to continue with the installation. The WebSphere Application Server Location dialog is displayed. If you wish to change the location for the installation of WebSphere Application Server, click **Browse** and select the desired location.

14. If you are not installing the proxy servers on their own machine, the installation wizard recognizes that an instance of Sametime Gateway is on the same machine. The new installation for the SIP and XMPP proxy servers adds a profile to WebSphere Application Server. Click **Next**, and then click **Next** again.

15. Check the node name, cell name, and host name that are supplied by the installer. Make sure that the cell and node names do not match the cell and node names you used when installing other Sametime Gateway servers. Choose a unique node name and cell name for this installation. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, exampleNodeProxy.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCellProxy.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com. Note: If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section “Host name considerations” in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
</tbody>
</table>

16. Type the administrative user ID and password used to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the credentials that you created when you installed the Deployment Manager. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: ;\!/\<\=\+\&\'\[\]%$^,

17. Click **Next**. If you are installing the proxy servers on their own machine, you now see the default directory path where Sametime Gateway will be installed. To change the location, click **Browse** and select a desired location, or type a new path.

18. Click **Next** to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click **Back** to make changes.

19. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.
20. Read the summary and click Finish. To view the installation log, click View log file or open the log file at \texttt{stgw\textunderscore server\textunderscore root/logs/installlog.txt}

What to do next

Note: If you start the SIPProxyServer instance now and log into the Integrated Solutions Console, you cannot view the SIPProxyServer instance. After you federate the node in the next procedure, you will see the SIPProxyServer instance.

Installing WebSphere iFixes for the SIP proxy server (AIX, Linux, Solaris) in a Sametime Gateway cluster:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Guidelines for using multiple SIP or XMPP proxy servers:

In enterprise deployments with high traffic from the public Internet, install multiple SIP or XMPP proxy servers with a Sametime Gateway cluster. Then front these proxy servers with an IP sprayer to ensure load balancing and high availability. Configure the IP sprayer to balance connections coming in from the Internet between the proxy servers.

About multiple XMPP proxy servers

This release does not support multiple XMPP proxy server configurations. Although the installer will install an XMPP proxy server instance with every SIP proxy server installation, configure only one XMPP proxy server in the cell and in the IP sprayer.

Follow these guidelines for setting up multiple proxy servers to work with an IP sprayer with Sametime Gateway.

Installing the proxy server nodes

1. Install each SIP or XMPP proxy server’s node on its own host.
2. Federate and configure the additional proxy servers as additional nodes.

Setting up traffic forwarding via the IP sprayer
The IP sprayer is typically a hardware-based load balancer. Ask your network administrator for help setting it up and configuring it.

When communicating with public external communities (such as AOL), the Sametime Gateway SIP/XMPP Proxy servers inspect the IP source address of incoming IP packets, and compare these IP addresses to a list of well known IP addresses associated with the external public communities. To ensure a connection can be complete, the original source IP address must be retained as it passes through the IP sprayer (passthrough mode). The IP sprayer should not replace the IP address of the incoming IP packets with its own (IP sprayer) IP address.

The TCP/IP connection between the proxy servers and an external Internet server may remain open for very long periods of time. Be sure that there are no TCIP/IP inactivity timeout intervals set up for TCP-aware devices that the connection is tunneled through.

**Monitoring proxy server availability**

Ask your network administrator to set up the IP sprayer to check the availability of each proxy server every two seconds, by making sure that the following TCP/IP ports are available.

- **SIP proxy servers**: Ports 5060/5061
- **XMPP proxy servers**: Port 5269

If the proxy server is unavailable, the IP sprayer should suspend spraying new TCP connections until the proxy server becomes available again.

**Federating the proxy server node into the cell:**

After you install the SIP and XMPP proxy server node, you must federate the node into the Deployment Manager’s cell so that the proxy server becomes part of the cluster.

**Before you begin**

Expected state: The Deployment Manager is running.

**About this task**

To federate or add the proxy server node into the cell, you run the `addnode` command on the proxy server node and specify the hostname of the Deployment Manager.

**Procedure**

1. Log into the proxy server node’s operating system.
2. **IBM i only**: On the command line, run the STRQSH (Start Qshell) command.
3. Synchronize the system clocks on the Deployment Manager and the proxy node so that they are within five minutes of one another and are set for the same time zone.
   
   Federation fails if the clocks are not synchronized within five minutes of each other.
4. On the proxy server node, open a command window and navigate to the `stgw_profile_root\bin` directory.
5. **IBM i** only: Run the following command to obtain the
`SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number
as you will need it to add nodes to the cluster:

dspwasinst

6. Run the following command to add the proxy server node to the Deployment
Manager's cell:

**AIX, Linux, and Solaris:**

```
./addNode.sh DM_server_host_name DM_port_number -includeapps
```

**Windows**

```
addNode.bat DM_hostname DM_port_number -includeapps
```

**IBM i:**

```
addNode DM_server_host_name DM_SOAP_port -username WAS_Admin_user_name_on_DM
-password WAS_Admin_password_on_DM
```

where:

- **DM_server_host_name** is the resolvable host name of the Deployment
  Manager.
- **DM_SOAP_port** is the port that the Deployment Manager's SOAP port is
  listening on.
- **WAS_Admin_user_name_on_DM** is the user ID of the WebSphere Application
  Server administrator account on the Deployment Manager.
- **WAS_Admin_password_on_DM** is the password associated with the
  WebSphere Application Server administrator account.

For example:

```
addNode gateway_dm.example.com 8879 -includeapps -username wasadmin -password waspassword
```

7. When prompted, provide the Deployment Manager’s administrative user ID
and password. Wait for the operation to complete before proceeding. Look for a
success message similar to the following when complete:

`Node MyProxyNode has been successfully federated.`

8. Verify that the proxy servers are installed correctly:

   a. Log into the Integrated Solutions Console.
      
      If you already logged in, you must log out and then log in again before you
      can see changes.
   
   b. Click **Servers > Server Types > WebSphere proxy servers**. You should see
      the SIP proxy server.
   
   c. Click **Servers > Server Types > WebSphere application servers**. You should
      see the XMPP proxy server.

**Configuring a SIP proxy server:**

Configure the Session Initiation Protocol (SIP) proxy server for a cluster of IBM
Sametime Gateway servers. There is no need to configure external domains in the
SIP proxy server; this is done through the Sametime Gateway configuration.

**Before you begin**

Set up a cluster with at least one secondary node and install the SIP and XMPP
proxy servers on the same physical hardware as a Deployment Manager, primary
node, or secondary node, or install the proxy servers on separate hardware. The
SIP and XMPP installation creates a new profile for the SIP and XMPP proxy
servers.
About this task

After you finish setting up a SIP proxy server, you’ll have a port number. You provide the port number in combination with the domain name of the node on which the SIP proxy server runs to external servers to connect to your Sametime Gateway.

Assigning the SIP proxy to work with the Sametime Gateway cluster:

Assign the SIP proxy server to function with the IBM Sametime Gateway cluster.

Procedure
1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers**.
2. In the "WebSphere proxy servers" page, click the **SIPProxyServer** link corresponding to the proxy server you want to update.
3. Click **SIP Proxy server settings > SIP Proxy settings**.
4. From the drop down list, select the Sametime Gateway cluster name.
5. Click **OK**, then click **Save**.

Configuring the SIP Proxy server to listen on ports 5060 and 5061:

Configure the IBM Sametime Gateway cluster's SIP Proxy server to listen on ports 5060 and 5061.

Before you begin

Configure a cluster of Sametime Gateway servers.

About this task

Public instant messaging providers require you to accept connections on ports 5060 and 5061, so you will need to confirm that the SIP Proxy server's host name is resolvable and is listening on these ports. If the cluster's SIP Proxy server is installed on a node that is already hosting Sametime Gateway, and the SIP Proxy server is not already listening on ports 5060 and 5061, reconfigure the port settings as follows:

Procedure
1. Determine which ports the SIP Proxy server is currently listening on:
   a. On the cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
   b. Click **Servers > WebSphere proxy servers > SIPProxyServer > Ports**.
   c. Check the listening ports for the following names:
      • PROXY_SIP_ADDRESS
      • PROXY_SIPS_ADDRESS
      If PROXY_SIP_ADDRESS listens on port 5060 and PROXY_SIPS_ADDRESS listens on port 5061, you can skip the rest of this task. Otherwise, proceed to the next step to change the port settings.
2. Determine whether any servers share the IP address and host name with the SIP Proxy server.
   If another server shares the IP address and host name, change the default host port settings for that server to avoid a conflict with the SIP Proxy server.
a. Still on the Deployment Manager, click **Server > Server Types > WebSphere application servers**.

b. Check whether any servers use the same IP address and host name as the SIP Proxy server.

c. If a server does share the IP address and host name, check its port settings for the following names:
   - SIP_DEFAULTHOST
   - SIP_DEFAULTHOST_SECURE

d. If SIP_DEFAULTHOST is not set to 5060 and SIP_DEFAULTHOST_SECURE is not set to 5061, skip to step 3.

e. If ports 5060 and 5061 are already in use, change those settings now by setting:
   - SIP_DEFAULTHOST to port 5080
   - SIP_DEFAULTHOST_SECURE to port 5081

f. Save your changes to the master configuration by clicking **Save** when prompted.

3. Now reset the SIP ports on the SIP Proxy server to use ports 5060 and 5061:
   a. On the Deployment Manager, click **Servers > WebSphere proxy servers > SIPProxyServer > Ports**.

b. Change the port settings for the following names:
   - PROXY_SIP_ADDRESS to port 5060
   - PROXY_SIPS_ADDRESS to port 5061

   c. Save your changes 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. Select the **Synchronize nodes** option before clicking the **Save** button.

*Configuring the correct network address for the SIP Proxy:*

If the SIP proxy server has multiple network addresses, use these instructions to configure the one that the Sametime Gateway uses to contact the SIP Proxy. If the SIP proxy server has one network address, you can skip this task.

**Before you begin**

Follow these steps to determine which address to configure:

Start the SIP Proxy server. Then from the Sametime Gateway server, issue `telnet` commands to each of the network addresses the SIP Proxy uses. Use `telnet` commands to attempt to connect to the SIP Proxy machine. For example, with network addresses of 127.0.0.1 and 127.0.0.2, run the following commands:

- `telnet 127.0.0.1`
- `telnet 127.0.0.2`

Make a note of the address that you connected with successfully.

**About this task**

Follow these steps to configure the network address.
Procedure
1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers.
2. In the "WebSphere proxy servers" page, click the SIPProxyServer link corresponding to the proxy server you want to update.
3. Click SIP Proxy server settings > SIP Proxy settings.
4. For the network address that the SIP Proxy server listens on, supply the host name or IP address for the following three fields:
   - UDP interface
   - TCP interface
   - TLS interface (UDP port should be left as an asterisk (*))
5. Click OK, then click Save.

Creating a virtual host for the SIP proxy:

Create virtual host definitions for ports 5060 and 5061.

Procedure
1. To identify the SIP proxy port number in the proxy server table, click the name of the SIP proxy server that you created.
2. Under Proxy Settings, select SIP proxy server settings > SIP Proxy server transports.
3. Make a note of the port number defined for SIP_PROXY_CHAIN and SIPS_PROXY_CHAIN. The port number in combination with the domain name of the node on which the SIP proxy server runs is needed for configuring external servers to connect to your Lotus Sametime Gateway server.
4. Now move to the Environment section if the Integrated Solutions Console.
5. Click Virtual Hosts > default_host > Host Aliases > New.
6. Verify the virtual host definitions for 5060/5061. If the virtual host is not defined, define the new alias as follows:
   a. Add * to the Host Name field.
   b. Add 5060 or 5061 to the Port field.
   c. Click OK.
   d. Click Save.
   The additional Virtual Host entry is needed if the default ports are not added during installation. Port 5060, however, only covers non-TLS installs. For secure setups, the following entry may also need to be added: *:5061

Create custom properties for the SIP proxy server:

Define custom properties for the SIP proxy server.

About this task

Define custom properties that will instruct the SIP proxy server to do the following:
- Return the "503 Service Unavailable" message when the server is down, rather than the default error "404 Page not found" message.
- Accept messages that do not contain a forwarding header.
Procedure
1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers > your new SIP proxy**.
2. Click **SIP Proxy server settings > SIP Proxy settings > Custom properties**.
3. Create a custom property to set up the "503 Service Unavailable" message text:
   a. Click **New**.
   b. Enter the following information:
   
<table>
<thead>
<tr>
<th>Name</th>
<th>lsnLookupFailureReasonPhrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Service Unavailable</td>
</tr>
</tbody>
</table>
   
   c. Click **OK**.
4. Create the custom property to define the error code to be displayed with the new message:
   a. Click **New**.
   b. Enter the following information:
   
<table>
<thead>
<tr>
<th>Name</th>
<th>lsnLookupFailureResponseCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>503</td>
</tr>
</tbody>
</table>
   
   c. Click **OK**.
5. Create another custom property to accept messages without a forwarding header:
   a. Click **New**.
   b. Enter the following information:
   
<table>
<thead>
<tr>
<th>Name</th>
<th>maxForwardsHeaderRequired</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>False</td>
</tr>
</tbody>
</table>
   
   c. Click **OK**.
6. Click **Save** to save all of the new custom properties.

### Tuning the SIP proxy server used by a Sametime Gateway cluster:

This sections describes the steps for tuning a SIP proxy.

**About this task**

Tune the JVM garbage collection policy for the SIP proxy server as follows:

**Procedure**
1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers > SIPProxyServer**.
2. Perform the following instructions for each of the sip proxies in the list:
   a. Select a proxy server by clicking it in the list.
   b. Under **Server Infrastructure**, click **Java and Process management > Process Definition**.
   c. Under **Additional Properties**, click **Java Virtual Machine**.
   d. In the **Initial Heap Size** field, enter 600.
   e. In the **Maximum Heap Size** field, enter 600.
f. In the **Generic JVM arguments** field, enter the following value as one continuous line:

```-Xmx60m -Xgcpolicy:gencon -Xgc:noAdaptiveTenure,tenureAge=8,
stdGlobalCompactToSatisfyAllocate -Xtgc:parallel```

g. Click **OK**, and click **Save** to save changes to the master configuration.

**Configuring the Gateway cluster and SIP proxy for a NAT environment:**

Configure a cluster of IBM Sametime Gateway servers to operate in a NAT (Network Address Translation) environment. The NAT environment configuration requires that the SIP Proxy’s external Fully Qualified DNS Name (FQDN), as known to external communities, be the same as its internal FQDN.

**Before you begin**

Traversing a NAT environment is a known issue in the SIP domain. There are several ways to solve this issue, while some of them have been formed as IETF standard (RPORT, STUN and ICE), others have been formed as proprietary solutions. So what is the problem? Some of the SIP communication parameters contain the Fully Qualified DNS Name (FQDN) or the IP address, and the port, but a SIP device deployed in a NAT environment does not know how it will be seen from the internet because the NAT device translates the IP address. The SIP message will contain IP address and port – which are not accessible from the internet. There are several paradigms to solve this issue:

- **SIP Friendly NAT device** – NAT devices that can analyze a SIP message and then replace the IP address and ports listed inside of it. This solution does not support encrypted SIP communication such as TLS.
- **IETF Standard** – a method using a standardized protocol such as RPORT, STUN, or ICE.

Currently, the IBM WebSphere SIP infrastructure does not provide a solution to this problem because it does not support any of the IETF standards. Therefore, any SIP application deployed on WebSphere has to develop its own solution. The solution provided here assumes that you have the following elements in your deployment:

- A clustered environment, with one or more clustered servers.
- A SIP proxy server federated to the cluster.
- All cluster members (including the SIP proxy server) are deployed within the same subnet.
- A static NAT is defined in the NAT or firewall; the public IP address should be mapped to the SIP proxy server’s internal IP address.

**About this task**

The following diagram illustrates the NAT environment that this solution was designed for:
Limitations:

- Only static NAT is supported
- A single SIP proxy deployment was tested; a multiple-SIP proxy deployment was never tested but can be applied with the same setting.
- Single-server deployment is not supported, but a clustered deployment which contains only one server is supported.

Procedure

1. Map a fully qualified domain name to the public IP address serving the Sametime Gateway.
   This FQDN will be used when registering the Gateway for provisioning with AOL, as well as in the SRV record used for communicating with Google.

2. Install the SSL certificate.
   The CN name for the certificate should be the one defined as FQDN mapped to the public IP in step 1. For example, the diagram above uses the FQDN gw.ibm.com. For information on requesting the certificate, see Creating a certificate request.

3. Define a custom property to map the cluster FQDN for traversing the NAT:
   Define a custom property to enable communications in a NAT (Network Address Translation) environment. Traversing NAT is a known issue for the SIP domain; defining the "FQDN" custom property for Sametime Gateway is a workaround for this issue. Before beginning, make sure the following requirements have been satisfied:
   - A static NAT should be defined in the NAT or Firewall (only static NATs are supported).
   - The public IP address should be mapped to the SIP proxy internal IP address.
   - A fully qualified domain name must be mapped to the public IP address serving the Sametime Gateway.
   This FQDN will be used when registering the Sametime Gateway for provisioning with AOL, as well as the SRV record used for communicating with Google.
a. Log in to the Integrated Services Console as a Sametime Gateway administrator.

b. Click System administration > Cell > Custom Properties.

c. Click New and enter information for the new custom property:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>com.ibm.sametime.gateway.fqdn</td>
</tr>
<tr>
<td>Value</td>
<td>Type your fully qualified domain name.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the new property.</td>
</tr>
</tbody>
</table>

d. Click Apply, and then click OK.

e. Perform a full synchronize with the nodes:

1) In the Deployment Manager’s Integrated Solutions Console, click System administration > Nodes.

2) Click Full Resynchronize.

f. Restart all Sametime Gateway nodes.

For example, If you set the custom property to gw.ibm.com (and the port is set to 5070), the INVITE SDP would look like this:

```
v=0
o=- 0 0 IN IP4 gw.ibm.com
s=session
ice=IN IP4 gw.ibm.com
a9=0 0
m=audio 5070 RTP/SAVP 0
m=video 5070 RTP/SAVP 0
```

4. Enable the SIP Proxy IP Sprayer as follows:

a. In the Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers.

b. In the list of proxy servers, click the link for your SIP proxy server to open its Configuration page.

c. Click SIP Proxy server settings > SIP Proxy settings > Custom properties.

d. Define the TLS IP Sprayer by clicking New, adding the following settings, and then clicking OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tls.IPSprayer.host</td>
<td>The SIP Proxy server’s external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>tls.IPSprayer.port</td>
<td>The port used by the IP sprayer for TLS encrypted communications; for example: 5061</td>
</tr>
</tbody>
</table>

e. Optionally define a TCP IP Sprayer by clicking New, adding the following settings, and then clicking OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp.IPSprayer.host</td>
<td>The SIP Proxy server’s external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>tcp.IPSprayer.port</td>
<td>The port used by the IP sprayer for TCP communications; for example: 5060</td>
</tr>
</tbody>
</table>

f. Optionally define a UDP IP Sprayer by clicking New, adding the following settings, and then clicking OK.
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp.IPSprayer.host</td>
<td>The SIP Proxy server's external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>udp.IPSprayer.port</td>
<td>The port used by the IP sprayer for UDP communications; for example: 5060</td>
</tr>
</tbody>
</table>

- g. Click **Save**.
- h. Restart the SIP proxy server.
- i. Restart the cluster.

**Configuring the XMPP proxy server:**

Configure the XMPP proxy server to allow Google Talk, and other XMPP-based instant messaging systems to flow to and from the Sametime Gateway.

**Before you begin**

Expected state: the SIP and XMPP proxy server node is installed and federated into the cell. A Sametime cluster has been installed. The Deployment Manager is started.

**Procedure**

1. On the Deployment Manager node, log into the Integrated Solutions Console.
2. Click **Servers > Application Servers** and select the **XMPPProxyServer** from the list.
3. Click **Ports**.
4. Click **New** to add a port.
5. Select **User-defined Port**.
6. Type **XMPP_INTERNAL_PORT** in the **Specify port name** field.
7. In the **Host name** field, type the IP address of the machine on which XMPPProxyServer is installed.
8. In the **Port** field, type 5271.

A note about ports:

- **XMPP_INTERNAL_PORT** is used for listening to traffic from the proxy server.

  If the XMPPProxy and XMPPServer are installed on the same physical computer, they will attempt to listen to the same default value of XMPP_INTERNAL_PORT which is 5271. As a result, the proxy will listen to the incoming connections from the server, and the server will listen to the proxy. In order to break this endless loop, set XMPP_INTERNAL_PORT to another value for the proxy (for example, 5272).

- **XMPP_SERVER_ADDRESS** port is used on the proxy server itself to listen to traffic from an external community.

  The XMPP_SERVER_ADDRESS port (5269) is unrelated to the "port 5269" value that appeared on the XMPP community page when you created the community. That community page port refers to the port that the external community is listening on, and is used when Sametime Gateway performs a DNS-SRV record lookup.

  If you need to change a default port, click **Application Servers > Server Name** and, under the 'Communications' section, click **Ports**.
9. Click OK and Save.
10. In the Integrated Solutions Console, click System administration > Cell.
12. Create Name and Value pairs for the Sametime Gateway cluster, XMPP proxy node name, and XMPP proxy server name. Type the names and values as they are spelled out in the table below. For XMPP proxy node name, substitute the name of the node on which the XMPP proxy resides.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>STGW_CLUSTER_NAME</td>
<td>SametimeGatewayCluster</td>
</tr>
<tr>
<td>XMPP_PROXY_NODENAME</td>
<td>XMPP proxy node name</td>
</tr>
<tr>
<td>XMPP_PROXY_SERVERNAME</td>
<td>XMPPProxyServer</td>
</tr>
</tbody>
</table>

13. Click Apply and Save after you type each pair. When you are done, you will have a table that looks something like this:

What to do next

Next, you must configure a class loader and a shared library for the XMPP proxy server.

Configuring XMPP proxy server shared library:

You configure an XMPP proxy server shared library by defining the shared library, create a class loader to XMPP proxy server, and associating the new shared library with the XMPP proxy server.

Procedure
1. Define a shared library for the XMPP Proxy server:
   a. Click Environment > Shared libraries in the console navigation tree.
   b. Change the scope of the collection table to the following:
      Node=[XMPPPROXY_NODE_NAME], Server=XMPPProxyServer
   c. Click Apply.
   d. Click New.
e. In Name field type GatewayLib.
f. In Classpath field type the following:
   
   C:/PROGRA~1/IBM/WEBSPH~1/STGATE~1/rtc_gw_lib

   where the path represents the install location of WebSphere Application Server. The folder names in the path cannot contain any blank spaces.
g. Click OK, and then click Save.

2. Create a class loader to the XMPP proxy server.
   a. Click Servers > Server Types > WebSphere application servers > XMPPProxy.
   b. Click Java and Process Management > Class loader.
   c. Click New.
   d. Choose the parent first class loader.
   e. Click OK, and then click Save.

3. Associate the new shared library with the XMPP proxy class loader you created.
   a. Click the class_loader_ID you created.
   b. Click Shared library references to access the Library reference page.
   c. Click Add.
   d. Make sure GatewayLib is selected in the list.
   e. Click OK and then click Save.

4. Restart the XMPP proxy server.

Setting up node replication and failover for the cluster:

This optional procedure sets up node replication to provide high availability and fail-over support for the cluster. If one member of the cluster goes down, other nodes can continue to process the SIP request. Use this procedure only if you require high availability and fail-over support.

Before you begin

Before you begin, you must install IBM Sametime Gateway on each node, add the nodes to a cluster, and then start the cluster and the SIP proxy server.

Enabling high availability uses additional memory which reduces your server's session capacity. For more information about enabling high availability, see the IBM Sametime Gateway sizing guide in the Sametime wiki:

http://www-10.lotus.com/ldd/stwiki.nsf/dx/IBM_Lotus_Sametime_Gateway_8.5.08.5.1_sizing_guidelines

About this task

Sametime Gateway offers a comprehensive high availability (HA) solution. High availability means an environment that doesn't have a single point of failure, and therefore prevents the users from losing presence awareness in the event of a Gateway server instance failure.

Replication domains
A SIP cluster with replication and failover can consist of many server instances. Each replication domain contains a set of two servers. Therefore, the number of replication domains needed is half the number of server instances. You need to create a new replication domain for each pair of Sametime Gateway instances (deployment manager and proxy server do not count). For example: if you have eight Sametime Gateway instance, you will be creating four replication domains. In case one server instance fails, the remaining server instance begins servicing the replicated SIP sessions of the failed instance. Therefore, IBM recommends that you pair server instances that are NOT likely to fail at the same time. For example, you should not pair server instances if both are running on the same physical host.

Procedure
1. Validate that the environment is ready:
   a. Click **Servers > clusters** and verify that the Sametime Gateway cluster is started and the status is green.
   b. Click **Servers > Proxy Servers** and verify that the SIP proxy is started and the status is green.
   c. Click **SIP proxy > SIP Proxy Server Settings > SIP proxy settings** and verify that the cluster in the drop down box is the same Sametime Gateway cluster defined in the previous step.
2. Create your new replication domains:
   a. Click **Environment > Replication Domains**, and then click **New**. Note: Disregard the GatewayCache. This is the DynaCache used to propagate the configuration across the cluster, and is not used for SIP session replication.
   b. Type a name for the new replication domain. For example: SIPRD1.
   c. Under **Number of Replicas**, select **Entire Domain** so that the SIP session is replicated to both Gateway instances, and click **OK**.
   d. Repeat the above process for each replication domain you wish to create.
3. Assign replication domains to server instances:
   a. Click **Servers > Application Servers**, and then select a member of the cluster.
   b. Under Container Settings, click **Session management**.
   c. Under Additional Properties, click **Distributed environment settings**.
   d. Under Distributed sessions, click **Memory-to-memory replication**. The distributed session option will become enabled once configured.
   e. Under Replication domain, select one of the replication domains that you created in previous steps. Remember, each replication domain must be assigned to exactly two server instances.
   f. In the **Replication mode** field, select **Both client and server**, then click **OK**, and **Save**. Memory to memory replication is now enabled for this member of the cluster.
   g. Repeat the previous step for each member of the cluster.

Starting a cluster:

When starting a cluster for the first time, you must start the Deployment Manager, node agents, and then all Sametime Gateway servers in the cluster.

Before you begin

Before begin these steps, you must install Sametime Gateway on each node, federate the nodes into the cell, run the Cluster Configuration Wizard, and then set
up SIP and XMPP proxy servers for your cluster.

About this task

In the steps that follow, you start the Deployment Manager in a command window so that you can log in to the Integrated Solutions Console and complete the remaining steps. After the Deployment Manager is started, you can view the Integrated Solutions Console pages. However, you cannot view the Sametime Gateway administration pages until you start at least one node agent and the Sametime Gateway server on that node.

Procedure

1. Log in to the Deployment Manager node as a user with administrative privileges.
2. Open a command window (QShell session on IBM i) and navigate to the `stgw_profile_root\bin` directory
3. If not already started, start the Deployment Manager with the following command:
   - **AIX, Linux, and Solaris**
     ```
     ./startManager.sh
     ```
   - **Windows**
     ```
     startManager.bat
     ```
   - **IBM i**
     ```
     startManager
     ```
4. Log in to one of the Sametime Gateway nodes.
5. Open a command window (QShell session on IBM i) and navigate to the `stgw_profile_root\bin` directory.
6. Start the node agent with the following command.
   - **AIX, Linux, and Solaris**
     ```
     ./startNode.sh
     ```
   - **Windows**
     ```
     startNode.bat
     ```
   - **IBM i**
     ```
     startNode
     ```
7. Log in to the other nodes, except the Deployment Manager node, and repeat the previous steps to start the node agent on each node.

Stopping and starting the Deployment Manager:

This topic describes how to stop and start the Deployment Manager.

Procedure

1. Log in to the Deployment Manager node as a user with administrative privileges.
2. Open a command window (QShell session on IBM i) and navigate to the `stgw_profile_root\bin` directory
3. Stop the Deployment Manager. Use the administrative user ID and password that you created when you installed the Deployment Manager. Note that you do not have to provide the username and password qualifiers in the command; you can wait to be prompted and then enter your credentials. Type the following commands:
Stopping and starting the node agents:

This topic describes how to stop and start the node agents. Typically, you stop and start a node agent by logging onto a node and running the stop node or start node command. If they are stopped, you must start the node agents from nodes themselves.

Procedure

1. Log in to one of the Sametime Gateway nodes.
2. Open a command window (QShell session on IBM i) and navigate to the `stgw_profile_root\bin` directory.
3. Stop the node agent with the following command:
   - **AIX, Linux, and Solaris**
     ```
     ./stopNode.sh
     ```
   - Windows
     ```
     stopNode.bat
     ```
   - **IBM i**
     ```
     stopNode
     ```
4. Start the node agent with the following command.
   - **AIX, Linux, and Solaris**
     ```
     ./startNode.sh
     ```
   - Windows
     ```
     startNode.bat
     ```
   - **IBM i**
     ```
     startNode
     ```
5. Log in to the other nodes, except the Deployment Manager node, and repeat the previous steps to stop and start the node agent on each node.

What to do next

You can also use the Deployment Manager Integrated Solutions Console to stop node agents:

1. Make sure the Deployment Manager is running and log into the Integrated Solutions Console on the Deployment Manager node.
2. Click **System Administration > Node agents**.
3. Select all node agents, and then click **Stop**.

Stopping and starting a cluster:

Complete these steps to stop and start a cluster of Sametime Gateway servers from the Integrated Solutions Console.
Before you begin

Expected state: the Deployment Manager, node agents, and all servers in the
cluster are started.

About this task

You must restart the cluster when you add, delete, or change a community.

Procedure

1. Log into the Integrated Solutions Console on the Deployment Manager server
    as a user with administrative privileges.
2. Click **Servers > Clusters**.
3. Select the Sametime Gateway cluster, and click **Stop**, and wait for the cluster to
    stop.
4. Click **Servers > Clusters**.
5. Select the Sametime Gateway cluster, and click **Start**.
6. Click **Servers > Proxy servers**.
7. Select the SIP proxy server and click **Start** if it is not already started.
8. Click **Servers > Application servers**.
9. Select the XMPP proxy server and click **Start** if it is not already started.

Stopping and starting servers in a cluster:

This topic describes how to stop or start individual servers or nodes in a cluster.

Procedure

1. Log into the Integrated Solutions Console on the Deployment Manager server
    as a user with administrative privileges.
2. Click **Servers > Application Servers**.
3. If you want to stop a server, select the application server's check box and click **Stop**.
4. If you want to start a server, select the application server's check box and click **Start**.

Stopping and starting a single server:

Complete these steps to stop and start a single Sametime Gateway server in a
single server environment.

Procedure

1. Log in to the server machine as a user with administrative privileges.
2. Open a command window and navigate to the Sametime Gateway profile
directory that contains binaries: `stgw_profile_root\bin`
3. Type the following command to stop the Sametime Gateway server. Note that
   **RTCGWServer** is case-sensitive, and that on all the stopserver commands, you are
   prompted to enter your administrative user ID and password that you created.
   - **Windows:**
     `stopserver.bat RTCGWServer`
   - **Linux, AIX, or Solaris:**
     `./stopserver.sh RTCGWServer`
4. Type the following command to start Sametime Gateway.

- **IBM i:**
  ```
  startServer RTCGWServer
  ```
- **Windows:**
  ```
  startserver.bat RTCGWServer
  ```
- **Linux, AIX, or Solaris:**
  ```
  ./startserver.sh RTCGWServer
  ```
- **IBM i:**
  ```
  startServer RTCGWServer
  ```

*Starting the SIP and XMPP proxy servers:*

The XMPP and SIP proxy server node is different from other Sametime Gateway node installation types in that it contains more than one server. Based on the type of traffic you expect to have in your environment (SIP or XMPP), you can start or stop the appropriate proxy server instance on the node. This removes the need to define a proxy server for each type of protocol. If you require the XMPP proxy functionality only, then start the XMPPProxyServer only. If you need SIP proxy functionality only, then start the SIPProxyServer only. If you need both, start both.

**About this task**

<table>
<thead>
<tr>
<th>Instant Messaging System</th>
<th>Proxy Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime</td>
<td>SIP</td>
</tr>
<tr>
<td>AOL Instant Messenger</td>
<td>SIP</td>
</tr>
<tr>
<td>Office Communications Server</td>
<td>SIP</td>
</tr>
<tr>
<td>Google Talk</td>
<td>XMPP</td>
</tr>
<tr>
<td>Jabber</td>
<td>XMPP</td>
</tr>
</tbody>
</table>

Before you start the SIP and XMPP proxy servers, you must add nodes to the cluster, create the cluster, set up a SIP and XMPP proxy server, and then start the cluster.

**Procedure**

1. On the Deployment Manager node, log in to the Integrated Solutions Console.
2. Choose **Servers > Clusters**.
3. Verify that the cluster status is **Started** (shown with a green arrow).
4. Click **Servers > Proxy servers**.
5. Select the **SIP proxy server** and click **Start**.
6. Choose **Servers > Applications servers**.
7. Select the **XMPP proxy server** and click **Start**.

*Registering a new Gateway cluster with the System Console:*

After installing the IBM Sametime Gateway cluster 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**

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

**About this task**

Working from the cluster's Deployment Manager, follow these steps to update properties files and run the registration utility to register the cluster with the System Console.

**Note:** Run this utility only on the Deployment Manager; do not register individual nodes because they will be registered automatically during the cluster registration.

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

- console.properties
- productConfig.properties

**Procedure**

1. On the Deployment Manager, navigate to the `stgw_server_root/console` directory.

   **Note:** If a cluster's Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager's profile.

2. Make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

3. Update the Deployment Manager's `console.properties` file:

   a. Open the file for editing.
   b. Update the file with the following values:

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</table>

Table 52. `console.properties` settings for the Deployment Manager
Table 52. *console.properties* settings for the Deployment Manager (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. For example, on Windows the path is: 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>


c. Verify that the remaining settings are appropriate for the Deployment Manager.

d. Save and close the file.

4. Update the Deployment Manager's *productConfig.properties* file:

   a. Open the file for editing.
   
   b. Update the file with the following values:

   Only the required values in this file are listed here:

Table 53. *productConfig.properties* settings for the Deployment Manager

<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>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBindAnonymous</td>
<td>Change to &quot;true&quot; only if you are allowing anonymous access to the LDAP server.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server for server connections (the default is 1516).</td>
</tr>
</tbody>
</table>


c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

5. Update the Primary Node's productConfig.properties file on the Deployment Manager server:
   a. Navigate to the app_server_root/profiles/DMPProfile/config/cells/DMCell/nodes/PNnode directory.
   b. Open the file for editing.
   c. In the DepName setting, provide a descriptive name for the Primary Node deployment; it must be a unique deployment name on the Sametime System Console.
   d. Set the value of isFederated to true for a primary or secondary node. The registration utility cannot run without this value.
   e. Verify that the remaining settings are appropriate for the Primary Node.
   f. Save and close the file.

6. Update the Secondary Node's productConfig.properties file on the Deployment Manager server:
   a. Navigate to the app_server_root/profiles/DMPProfile/config/cells/DMCell/nodes/SNnode directory.
   b. Open the file for editing.
   c. In the DepName setting, provide a descriptive name for the Secondary Node deployment; it must be a unique deployment name on the Sametime System Console.
   d. Set the value of isFederated to true for a primary or secondary node. The registration utility cannot run without this value.
   e. Verify that the remaining settings are appropriate for the Secondary Node.
   f. Save and close the file.

7. Run the registration utility:
   b. Run the utility:
      - AIX, Linux, Solaris: registerProduct.sh
      - Windows: registerProduct.bat
   c. When the utility prompts for the cluster's name, type the name and press Enter.

The utility registers the cluster, as well as each node, 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.

8. Start the Sametime Gateway cluster, if it is not already running.

Performing a silent installation:

IBM Sametime Gateway can be installed silently using a response file. You can either generate your own response file by installing using the install wizard, or by editing the default response file that is provided.

Performing a silent installation on Windows:

IBM Sametime Gateway can be installed silently using a response file. You can either generate your own response file by installing using the install wizard, or by editing the default response file that is provided.
Before you begin

Information on downloading packages for Sametime is located at the following Web address:

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

About this task

A response file is a text file that contains all the options that would normally be specified in the installation dialogs. Silent installation is useful in situations where automation is desired.

To perform a silent installation, you have to create a new response file or edit the existing response file that is included with the product. On the root of the Sametime Gateway installation CD is a fully-documented response file: installresponse.txt. Follow these steps to copy this file to the machine and edit it with values appropriate for your environment, or to create a response file based on a real installation.

Note: The installation program installs both WebSphere Application Server and Sametime Gateway.

Procedure

1. From the installation media, copy C17KCML.exe, the Sametime Gateway installation image, to a temporary directory \TMP on the machine where you will be installing Sametime Gateway, then extract the files.
2. Open a command window.
3. Navigate to the directory where you copied and extracted the installation files: \TMP\SametimeGateway
4. Record a response file by typing the following command. This will perform an installation and generate a response file:
   ```
   install.bat -options-record response_file
   ```
   where response_file is an absolute path to the response file to be generated. For example:
   ```
   install.bat -options-record C:\TMP\SametimeGateway\gatewayOptions.txt
   ```
5. Once a response file is created, either by modifying the installresponse.txt file included with the installer, or by generating your own response file, open a command window.
6. Type the following command to use the response file that you created:
   ```
   install.bat -options response_file -silent
   ```

What to do next

Upon completion of the installation, control will return to the command window. Validation or installation errors are logged to the installation log file. Open the log file at stgw_server_root\logs\installlog.txt.

Note: Generating response files using the -options-record option puts clear text passwords in the response file.

Adding a Sametime Gateway server (Windows) to the Sametime Community Server’s trusted IPs:
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.

6. Click OK.
7. Restart the community server for the change to take effect.

Performing a silent installation on AIX, Linux, or Solaris:

IBM Sametime Gateway can be installed silently using a response file. You can either generate your own response file by installing using the install wizard, or by editing the default response file that is provided.

Before you begin

Information on downloading packages for Sametime is located at the following Web address:
About this task

A response file is a text file that contains all the options that would normally be specified in the installation dialogs. Silent installation is useful in situations where automation is desired.

To perform a silent installation, you have to create a new response file or edit the existing response file that is included with the product. On the root of the Sametime Gateway installation CD is a fully-documented response file: installresponse.txt. Copy this file to the machine and edit it with values appropriate for your environment, or complete the following steps to create a response file based on a real installation.

Note: The installation program installs both WebSphere Application Server and Sametime Gateway.

Procedure
1. From the installation media, copy CI7KBML.tar, the Sametime Gateway installation image, to a temporary directory /TMP on the machine where you will be installing Sametime Gateway, then uncompress the files.
2. Open a command window and type the following command to source the DB2 profile:

   . /db2adminHomeDir/sql1ib/db2profile

   Note the period (.) and space before /db2adminHomeDir/sql1ib/db2profile.
3. Navigate to the directory where you copied and extracted the installation files: /TMP/SametimeGateway
4. Record a response file by typing the following command. This will perform an installation and generate a response file:

   . /install.sh -options-record response_file

   where response_file is an absolute path to the response file to be generated. For example, in Windows:

   . /install.sh -options-record TMP/SametimeGateway/gatewayOptions.txt
5. Once a response file is created, either by modifying the installresponse.txt file included with the installer, or by generating your own response file, open a command window.
6. Type the following command to install using the response file:

   . /install.sh -options response_file -silent

What to do next

Upon completion of the installation, control will return to the command window. Validation or installation errors are logged to the installation log file. Open the log file at stgw_server_root/logs/installlog.txt.

Note: Generating response files using the -options-record option puts clear text passwords in the response file.

Adding a Sametime Gateway server (AIX, Linux, Solaris) to the Sametime Community Server's trusted IPs:
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.

Configuring LDAP for Sametime Gateway

Configure Sametime Gateway to use the LDAP directory used by the local Sametime environment. If you did not connect to LDAP when you installed Sametime Gateway, or you did connect to LDAP but now want to create a secure connection, use these procedures. Sametime Gateway must look up names and groups in the LDAP directory to grant users and groups access to external communities.
About this task

Use Sametime Gateway with virtually any LDAP directory that is supported by Sametime and the WebSphere Application Server environment. Sametime Gateway deployment does not require changes to existing directory structures. It’s recommended that you configure the same LDAP directory that is used by the Sametime community server. You can use a separate LDAP directory, but information between the two LDAP directories must be replicated and identical.

Note: The use of an LDAP directory is not required for Sametime Gateway, but it lets you implement an access control list (ACL) that controls which users and groups can access, and be accessed from, external communities. If you do not want to configure the use of an LDAP directory at this time, you can skip the procedure. If you later decide to start using an LDAP directory for Sametime Gateway, you can configure the interaction at that time.

Be sure to read the first topic below before setting up your LDAP directory:

LDAP and access to external and internal users:

Sametime Gateway works with the LDAP user registry used by your local Sametime community so that you can assign local users permission to access members in external and clearinghouse communities. For local users to chat with and share presence with a member of an external community, two events must happen: you must assign the local user to the external community and the external community administrator must assign the external community member access to your Sametime community.

You can use Sametime Gateway with virtually any LDAP directory that is supported by Sametime or the WebSphere Application Server environment. Sametime Gateway deployment does not require changes to existing directory structures. When you configure WebSphere Application Server to use an LDAP user registry, you are identifying to Sametime Gateway the LDAP directory that houses members of the local Sametime community. As an administrator, you look up names and groups in the LDAP directory and assign them capabilities when accessing an external community.

Using LDAP, you can assign users and group to capabilities such as instant messaging or presence or both when assigning users and groups access to an external community. Sametime Gateway displays group names, user names (short names), and user e-mail addresses. Groups do not have e-mail addresses.

Access to internal and external communities

When you assign a local user from your LDAP directory access to an external community, you provide, at the local level, permission for that local user to exchange instant messages with potentially all members of an external community. You cannot give the user permission to subscribe to some members of the external community because you cannot control who in the external community has access to the local user. If the administrator in an external community assigns all members in the external directory access to your local community, your local Sametime user can subscribe to all members of the external community and all external community members can subscribe to your user.

As an administrator, you cannot set access for external users because there is no way for you to configure access in external directories. External users can only
have instant messaging and presence with the members of your local community for whom you have assigned access. The only people who can be subscribed to by external users are the users and groups who have been granted access by you.

For example, if local user John has not been granted access to external community, and external user Mary subscribes to John's presence, Mary will never receive a response because local user John does not have the rights to send a response. Any subscription requests from an external user is blocked by the Sametime Gateway because the local user is not granted access to subscribe to the external community.

**Configuring LDAP for a single server on AIX, Linux, Solaris, and Windows:**

IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use a Lightweight Directory Access Protocol (LDAP) user registry that contains members of the local Sametime community. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

**Before you begin**

Expected state: Administrative security is enabled. The Deployment Manager is running.

**Procedure**

1. If not already started, start Sametime Gateway:
   a. Open a command window.
   b. Navigate to the Sametime Gateway profile directory that contains binaries:
      `rtcgw_profile_root\bin`
   c. Type the following command. Note that RTCGWServer is case-sensitive.
      **AIX, Linux, and Solaris**
      ```sh```
      ./startServer.sh RTCGWServer
      ```
      **Windows**
      ```bat```
      startServer.bat RTCGWServer
      ```
   2. Ensure that the enterprise LDAP server is running.
   3. Complete the following sub steps to connect to connect to LDAP over SSL, otherwise skip this step. 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.
      a. From the Integrated Solutions Console, select **Security > SSL Certificates and key management**, then select **Key stores and certificates**.
      b. Click **NodeDefaultTrustStore**.
      c. Click **Signer certificates**.
      d. Click **Add**.
      e. In the **Alias** field, type a description for the certificate, whether it's self-signed or a public CA.
      f. In the **File name** field, type the path to the certificate file. For example, `c:\certname.cer`.
      g. Click **Apply** and then **Save**.
   4. From the Integrated Solutions Console, select **Security > Global Security**.
5. Make sure the Enable administrative security and Enable application security options are selected.
6. In the Available realm definitions, select Federated repositories.
7. Click Set as current.
8. Click Configure.
9. Click Add base entry to the Realm.
10. On the next screen, click Add Repository...
11. Type a logical name for the repository in the Repository Identifier field. The identifier can be any value, as long as it's unique within the cell.
12. Select the type of LDAP server to use from the Type list. If you have an IBM Lotus Domino Version 7.0 server, select IBM Lotus Domino Version 6.5 as your LDAP type.
13. Enter the fully qualified host name of the LDAP server in the Primary Host field. You can enter either the IP address or domain name system (DNS) name.
14. Enter the LDAP server port number in the Port field. The host name and the port number represent the realm for this LDAP server in the WebSphere Application Server cell. The default value is 389.
15. Optionally, enter the bind DN name in the Bind distinguished name field. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. Leave this field blank to connect to the LDAP server anonymously.
16. Optionally enter the password corresponding to the bind DN in the Bind password field. Leave this field blank to connect to the LDAP server anonymously.
17. Specify the Login properties when setting up the repository. The cn, uid, and mail are common login property values. If your LDAP server uses a login property other than uid, you must change the value to match your user prefix.
18. Click Apply, and then click Save.
19. In the Distinguished name of a base entry that uniquely identifies this set of entries in the realm field, type the base DN of your choice such as "o=myLDAPRealm" or "o=defaultWIMLDAPBasedRealm". This DN is for internal WebSphere Application Server use only and is used to identify a set of entries when returning search results.
20. In the Distinguished name of a base entry in this repository field, type the DN of the base entry within the directory to begin searches. Leave this field blank to start LDAP searches at the root of your LDAP repository, or if you have a Domino LDAP, which always begins searches at the root of the directory. An example of a DN for the base entry in a repository:
   dc=IBM,dc=COM
21. Click Apply, and then click Save.
22. Use a text editor and open wimconfig.xml. The directory path that follows is all on one line but represented here on two lines for printing:
   app_server_root\profiles\RTCGW_Profile\config\cells\cell_name\wim\config\wimconfig.xml
   Replace cell_name with the name of your cell.
23. Now find the LDAP repository type in the config:repositories element:
   <config:repositories>
   <config:repositories xsi:type="config:LdapRepositoryType">
   Add the following line to the <config:attributeConfiguration> element block:
   
   Chapter 3. Installing 543
<config:externalIdAttributes name="unique_attribute"
syntax="attribute_syntax"/>

where unique_attribute is the unique LDAP attribute that you want to use and
attribute_syntax identifies the syntax. Include the syntax attribute only if the
syntax is something other than a type of string.

For example, to use a string called dominounid, edit the wimconfig.xml file to
include the following element:

<config:externalIdAttributes name="dominounid"/>

If the attribute was not a string, you would identify its syntax as well. For
example:

<config:externalIdAttributes name="GUID" syntax="octetString"/>

The following are some examples of commonly used unique attributes for
different some flavors of LDAP:

- Domino LDAP: dominounid
- IDS: ibm-entryuuid
- Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

24. Save the file. Note: the dominounid attribute was introduced in Lotus
Domino 6.5.4 and 7.0. In some cases this attribute may not appear in the
schema database or on the Server Configuration document (LDAP tab). This
can occur when the administration server for the Domino domain is version
6.5.3 or lower. The Administration server controls the creation of the Schema
database, as well as which attributes are available for anonymous queries
through the Configuration document. To resolve the issue, the Administration
server should be upgraded to Domino version 6.5.4 or above. In addition,
while a particular Domino LDAP may not require to bind, binding is
necessary to retrieve the dominounid attribute. Any bind user would be
acceptable, read only is fine.

25. Stop and then restart the Sametime Gateway server:

  a. Navigate to the directory that contains binaries: rtcgw_profile_root\bin
  b. Type the following commands, depending on your operating system, to
     stop and then start Sametime Gateway. You must use the user name and
     password that you provided when you enabled administrative security to
     stop the server. Wait for the stopserver command to finish before
     executing the startserver command. Note that RTCGWServer is
case-sensitive.

     AIX, Linux, and Solaris
     ./stopServer.sh RTCGWServer -username username -password password
     ./startServer.sh RTCGWServer

     Windows
     stopServer.bat RTCGWServer -username username -password password
     startServer.bat RTCGWServer

26. log into the Integrated Solutions Console.

27. Select Users and Groups > Manage Users.

28. Click Search to verify that you can search your LDAP directory. If your LDAP
    functionality is enabled, you should see a list of users on the screen.

29. Click a user name and make sure you can see the user's content. You can
    verify group names as well.
30. Copy the script: \texttt{stgw\_server\_root/config/adminscripts/rtcgw\_vmm.jacl} to \texttt{app\_server\_root/bin}.

31. Open a separate command window and navigate to \texttt{app\_server\_root/bin}.

32. Run the following command:
\begin{verbatim}
wsadmin -username \textit{username} -password \textit{password} -f rtcgw\_vmm.jacl
\end{verbatim}

Where \textit{username} is the administrative user ID that you use to log into the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. For example:
\begin{verbatim}
wsadmin -username wasadmin -password gateway4u -f rtcgw\_vmm.jacl
\end{verbatim}

This script will place the default file repository of the WebSphere Application Server at the bottom of listed \texttt{config/repositories} tags of \texttt{wimconfig.xml}, so it is searched after the newly created repository.

33. Stop and then restart the Sametime Gateway server:
   a. Navigate to the directory that contains binaries: \texttt{rtcgw\_profile\_root/bin}
   b. Type the following commands, depending on your operating system, to stop and then start Sametime Gateway. You must use the user name and password that you provided when you enabled administrative security to stop the server. Wait for the \texttt{stopserver} command to finish before executing the \texttt{startserver} command. Note that RTCGWServer is case-sensitive.
      - \textbf{AIX, Linux, and Solaris}
        \begin{verbatim}
        ./stopServer.sh RTCGWServer -username \textit{username} -password \textit{password}
        ./startServer.sh RTCGWServer
        \end{verbatim}
      - \textbf{Windows}
        \begin{verbatim}
        stopServer.bat RTCGWServer -username \textit{username} -password \textit{password}
        startServer.bat RTCGWServer
        \end{verbatim}

34. The remaining optional steps apply to an LDAP server that is not a Domino LDAP directory. By default, Sametime uses \texttt{mail} as the attribute in an LDAP record to search for users. If your LDAP directory uses a different attribute, you can change Sametime to use that attribute instead. For example, if you want to change Sametime to instead use the attribute \texttt{displayName}, complete the following steps:
   a. Use a Lotus Notes client on the Sametime server to open the Sametime Configuration database (\texttt{stconfig.nsf}).
   b. Click \textbf{File} > \textbf{Database} > \textbf{Open} and select the Local server.
   c. Select the Sametime Configuration database (\texttt{stconfig.nsf}).
   d. Click \textbf{Open}.
   e. In the right pane of the Configuration database, locate the LDAP server entry in the \textbf{Form Name} column of the Configuration.
   f. Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the \textbf{Last Modified Date} column. The date represents the last time the LDAP server document was modified.
   g. To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
   h. When the LDAP Server document opens, double-click the document to put it in edit mode.
   i. Search and replace \texttt{mail} with \texttt{displayName}.
Search filter for resolving person names: (&(objectclass=organizationalPerson) (|(uid=%s*)(givenname=%s*)(sn=%s*)(mail=%s*)))

Search filter to use when resolving a user name to a distinguished name: (&(objectclass=organizationalPerson) (|(uid=%s)(givenname=%s)(sn=%s*)(mail=%s*)))

"Attribute of the person entry that defines the person's email address" mail

j. Save your changes and then restart the Domino server.
k. On the Sametime Gateway server that is connected to LDAP, use a text editor and open the following file:

rtcgw_profile_root\config\cells\<cell_name>\wim\config\wimconfig.xml

l. Add the following line under the other configuration attributes:

<config:attributes name="displayName" propertyName="mail"/>

For example:

<config:attributeConfiguration>
  <config:externalIdAttributes name="dominounid" />
  <config:attributes name="userPassword" propertyName="password" />
  - <config:attributes name="cn" propertyName="displayName">
  - <config:attributes name="displayName" propertyName="mail"/>
   <config:entityTypes>Group</config:entityTypes>
  </config:attributes>
  - <config:attributes name="cn" propertyName="cn">
   <config:entityTypes>Group</config:entityTypes>
  </config:attributes>
  <config:propertiesNotSupported name="businessAddress" />
</config:attributeConfiguration>

m. Save the file.
n. Stop and restart the Sametime Gateway server.

Related tasks
“Configuring LDAP for a cluster on IBM i” on page 885
The IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use the Lightweight Director Access Protocol (LDAP) user registry that contains members of the local Sametime community. These steps include information for setting up a connection to LDAP using a self-signed certificate. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

Configuring LDAP for a cluster on AIX, Linux, Solaris, and Windows:

The IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use the Lightweight Director Access Protocol (LDAP) user registry that contains members of the local Sametime community. These steps include information for setting up a connection to LDAP using a self-signed certificate. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

Before you begin

Expected state: the Deployment Manager and node agents are started. The servers are stopped. Administrative security is enabled.
Procedure

1. Log in to the Deployment Manager node as a user with administrative privileges. Make sure you have an enterprise LDAP server that contains members of the local Sametime community and the LDAP server is running.

2. Complete the following sub steps to connect to LDAP over SSL, otherwise skip this step. If your LDAP server is using a public CA, 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.

   a. From the Integrated Solutions Console, select Security > SSL Certificates and key management, then select Key stores and certificates.
   b. Click CellDefaultTrustStore.
   c. Click Signer certificates.
   d. Click Add.
   e. In the Alias field, type a description for the certificate, whether it's self-signed or a public CA.
   f. In the File name field, type the path to the certificate file. For example, c:\certname.cer.
   g. Click Apply and then Save.


4. Make sure the Enable administrative security and Enable application security options are selected.

5. In the Available realm definitions, select Federated repositories.

6. Click Set as current.

7. Click Configure.

8. Click Add base entry to the Realm...

9. On the next screen, click Add Repository...

10. Type a logical name for the repository in the Repository Identifier field. The identifier can be any value, as long as it is unique within the cell.

11. Select the type of LDAP server to use from the Type list. If you have a Lotus Domino Version 7.0 server, select IBM Lotus Domino Version 6.5 as your LDAP type.

12. Enter the fully qualified host name of the LDAP server in the Primary Host field. You can enter either the IP address or domain name system (DNS) name.

13. Enter the LDAP server port number in the Port field. The host name and the port number represent the realm for this LDAP server in the WebSphere Application Server cell. The default value is 389.

14. Optionally, enter the bind DN name in the Bind distinguished name field. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. Leave this field blank to connect to the LDAP server anonymously.

15. Optionally, enter the password corresponding to the bind DN in the Bind password field. Leave this field blank to connect to the LDAP server anonymously.

16. Specify the Login properties when setting up the repository. The cn, uid, and mail are common login property values. If your LDAP server uses a login property other than uid, you must change the value to match your user prefix.

17. Click Apply, and then click Save.

18. In the Distinguished name of a base entry that uniquely identifies this set of entries in the realm field, type the base DN of your choice such as
"o=myLDAPRealm" or "o=defaultWIMLDAPBasedRealm". This DN is for internal WebSphere Application Server use only and is used to identify a set of entries when returning search results.

19. In the **Distinguished name of a base entry in this repository** field, type the DN of the base entry within the directory to begin searches. Leave this field blank to start LDAP searches at the root of your LDAP repository, or if you have a Domino LDAP, which always begins searches at the root of the directory. An example of a DN for the base entry in a repository:
   \[ dc=IBM,dc=COM \]

20. Click **Apply**, and then click **Save**.


22. On the Deployment Manager, use a text editor and open \[ wimconfig.xml \]. The directory path that follows is all on one line but represented here on two lines for printing:
   \[ app_server_root/profiles/RTCGW_Profile/config/cells/cell_name/wim/config/wimconfig.xml \]

The cell name is the name of your cell.

23. Find the configLdapRepository section:
   \[ </config:repositories>\]

24. Within that section, find the config:attributeConfiguration element block.

25. Add a line for config:externalIdAttributes if one does not already exist, using one of the following formats.
   - Add this line if the ID attribute has a default syntax type of string.
     \[ <config:externalIdAttributes name="unique_attribute"/> \]
     where unique_attribute is the unique LDAP attribute that you want to use.
     The following example adds a string called dominounid:
     \[ <config:externalIdAttributes name="dominounid"/> \]
   - Add this line if the ID attribute has a syntax type other than string.
     \[ <config:externalIdAttributes name="unique_attribute" syntax="attribute_syntax"/> \]
     where unique_attribute is the unique LDAP attribute that you want to use and attribute_syntax identifies the syntax. You must include the syntax attribute only if the syntax is a type other than string.
     The following example adds an octetString attribute called GUID, which is the Novell eDirectory attribute:
     \[ <config:externalIdAttributes name="GUID" syntax="octetString"/> \]

The following are some examples of commonly used unique attributes for different flavors of LDAP:
- Domino LDAP: dominounid
- IDS: ibm-entryuuid
- Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

26. Save the file.

27. Navigate to the rtcgw_profile_root/bin directory.

28. 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 created when you enabled administrative security. Type the following commands:
AIX, Linux, and Solaris
./stopManager.sh -username \username -password password
./startManager.sh

Windows
stopManager.bat -username \username -password password
startManager.bat

29. Synchronize your changes to all nodes in the cluster. Click **System Administration > Nodes**.

30. Select all nodes in the cluster, then click **Full Resynchronize**.

31. Restart the node agents.
   a. Log into the Integrated Solutions Console on the Deployment Manager node.
   b. Click **System Administration > Node agents**.
   c. Select all node agents, and then click **Restart**.

32. Choose **Servers > Clusters**.

33. Select the Sametime Gateway cluster and click **Start**. Verify that the cluster status is started. (shown with a green arrow).

34. Select **Users and Groups > Manage Users**.

35. Click **Search** to verify that you can search your LDAP directory. If your LDAP functionality is enabled, you should see a list of users on the screen.

36. Click a user name and make sure you can see the user's content. You can verify group names as well.

37. Copy the following script:
   from:
   stgw_server_root/config/adminscripts/rtcgw_vmm.jacl
   to the Deployment Manager node:
   app_server_root/bin

38. Open a command window and navigate to **app_server_root/bin**.

39. Run the following command:
   wsadmin -username \username -password password -f rtcgw_vmm.jacl
   Where **\username** is the administrative user ID that you use to log into the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. For example:
   wsadmin -username wasadmin -password gateway4u -f rtcgw_vmm.jacl

This script will place the default file repository of the WebSphere Application Server at the bottom of listed **config:repositories** tags of wimconfig.xml, so it is searched after the newly created repository.

40. In the DB2 window on the Deployment Manager node, 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. Type the following commands:

AIX, Linux, and Solaris
./stopManager.sh -username \username -password password
./startManager.sh

Windows
stopManager.bat -username \username -password password
startManager.bat

41. Restart the node agents.
   a. Log into the Integrated Solutions Console on the Deployment Manager node.
b. Click **System Administration** > **Node agents**.
c. Select all node agents, and then click **Restart**.

42. Choose **Servers** > **Clusters**
43. Select the Sametime Gateway cluster and click **Start**. Verify that the cluster status is started. (shown with a green arrow).

44. The remaining optional steps apply to an LDAP server that is not a native internal Domino directory. Complete these steps to change the default attribute of the person entry that defines the person's email address in

```
app_server_root\profiles\RTC Gateway_Profile \config\cells\cell_name\wim\config\wimconfig.xml
```

The default attribute is **mail**. If you want to change the default attribute to **displayName**, complete the following steps:

a. Use a Lotus Notes client on the Sametime server to open the Sametime Configuration database (stconfig.nsf).
b. Click **File** > **Database** > **Open** and select the Local server.
c. Select the Sametime Configuration database (stconfig.nsf).
d. Click **Open**.
e. In the right pane of the Configuration database, locate the LDAP server entry in the **Form Name** column of the Configuration.
f. Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the **Last Modified Date** column. The date represents the last time the LDAP server document was modified.
g. To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
h. When the LDAP Server document opens, double-click the document to put it in edit mode.
i. Search and replace **mail** with **displayname**.

```
Search filter for resolving person names:((objectclass=organizationalPerson) (((uid=%s*)(givenname=%s*)(sn=%s*)(mail=%s*)))
```

Search filter to use when resolving a user name to a distinguished name:

```
(&objectclass=organizationalPerson)((uid=%s)(givenname=%s)(sn=%s)(mail=%s))
```

"Attribute of the person entry that defines the person's email address" **mail**
j. Save your changes and then restart the Domino server.
k. On the Sametime Gateway server that is connected to LDAP, use a text editor and open the following file:

```
app_server_root\profiles\RTC Gateway_Profile
\config\cells\cell_name\wim\config\wimconfig.xml
```
l. Add the following line under the other configuration attributes:

```
<config:attributes name="displayName" propertyName="mail"/>
```

For example:

```
<config:attributeConfiguration>
<config:externalIdAttributes name="dominounid"/>
<config:attributes name="userPassword" propertyName="password"/>
<config:attributes name="cn" propertyName="displayName">
<config:attributes name="displayName" propertyName="mail"/>
<config:entityTypes>Group</config:entityTypes>
</config:attributes>
<config:attributes name="cn" propertyName="cn">
<config:entityTypes>Group</config:entityTypes>
</config:attributes>
<config:propertiesNotSupported name="businessAddress"/>
</config:attributeConfiguration>
```
m. Save the file. Note: the **dominounid** attribute was introduced in Lotus Domino 6.5.4 and 7.0. In some cases this attribute may not appear in the
schema database or on the Server Configuration document (LDAP tab). This can occur when the administration server for the Domino domain is version 6.5.3 or lower. The Administration server controls the creation of the Schema database, as well as which attributes are available for anonymous queries through the Configuration document. To resolve the issue, the Administration server should be upgraded to Domino version 6.5.4 or above. In addition, while a particular Domino LDAP may not require to bind, binding is necessary to retrieve the `dominounid` attribute. Any bind user would be acceptable, read only is fine.

n. Stop and restart the Deployment Manager, the node agents and Sametime Gateway servers.

Results

You are now ready to set up SSL on a cluster.

Related tasks

“Configuring LDAP for a single server on IBM i” on page 881
IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use a Lightweight Directory Access Protocol (LDAP) user registry that contains members of the local Sametime community. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

**Connecting servers to Sametime Gateway**

To complete IBM Sametime Gateway setup, you connect servers to the Sametime Gateway by performing some configuration steps on the local Sametime server, adding the local community to the Sametime Gateway, registering your Sametime Gateway server with AOL so that Sametime Gateway can connect to the AOL clearinghouse, and then, after you complete your registration, adding the AOL clearinghouse community to the Sametime Gateway. Finally, you want to note the port numbers so you can provide these ports to external communities.

**Opening ports in the firewalls:**

Open specific ports in the internal and external firewalls to allow messages to flow to and from the Sametime Gateway server in the DMZ to the local Sametime community, and to permit access to LDAP and DB2. In addition, verify that the external firewall allows inbound and outbound connections to and from specific IP addresses. Make sure any kind of SIP fixup or SIP inspection is disabled in your firewall settings.

**About this task**

A Sametime Gateway server or cluster is normally deployed in the DMZ, which is the zone between the internal and external firewalls. Work with your network firewall administrator to open ports in the internal firewall to allow Sametime Gateway to connect to the local Sametime community servers, LDAP, and DB2. You also need to open ports in the external firewall to allow Sametime Gateway to connect with external communities.
You can deploy a Network Address Translator (NAT) between local Sametime community servers and a Sametime Gateway. However, deploying a NAT device between Sametime Gateway and the Internet is not supported when trying to connect Sametime Gateway to AOL or TLS-encrypted SIP-based external communities. While there are SIP-aware NAT devices, they are not sufficient because AOL communities require secure SIP (SSL/TLS) communication, and a NAT device would not be able to decrypt and translate the packets for proper operation. NAT has no affect on the XMPP protocol, so exchanges using Google Talk over XMPP are always permitted to pass through a NAT-enabled firewall that is between Sametime Gateway and the Internet.

**Procedure**

1. Open the following ports in the internal firewall:
   - Port 1516 on the internal firewall to each Sametime community server in the local Sametime community, the Sametime Gateway will be the one creating the TCP connection to the destination IP at destination port 1516.
   - Port 389 on the internal firewall to the LDAP directory, or port 636 if LDAP access is over SSL.
   - Port 50000 on the internal firewall to a DB2 server.

2. Open the following ports on the external firewall as needed:
   - Port 5269 on the external firewall to Google Talk and non-secured XMPP.
   - Port 5270 on the external firewall to secured XMPP.
   - Port 5061 on the external firewall to external Sametime or AOL communities using a secure TLS/SSL connection.
   - Port 5060 on the external firewall to an external Sametime community (only if using a non-TLS/SSL connection).
   - Port 53 on the external firewall to external DNS servers to resolve the fully qualified domain name of external community servers.

3. Verify that the external firewall allows inbound and outbound connections to and from the following IP addresses:
AOL: 64.12.162.248, 205.188.153.55

1. For Google Talk, update your firewall rules to allow inbound and outbound traffic on the list of IP ranges supported by Google Talk.

**Note:** The list of supported IP ranges for connecting Google Talk changes periodically. For the current list of IP ranges, see List of supported Google Talk IP ranges for use with Sametime Gateway.

In the command window, type:
nslookup talky.l.google.com

Then type:
nslookup talkz.l.google.com

For example:
C:\>nslookup talky.l.google.com

Name: talky.l.google.com
Addresses: 74.125.47.125, 74.125.65.125, 74.125.155.125, 209.85.137.125
209.85.163.125, 209.85.229.125, 216.239.51.125, 64.233.169.125, 72.14.203.125
72.14.247.125

C:\>nslookup talkz.l.google.com

Non-authoritative answer:
Name: talkz.l.google.com

The talky.l.google.com addresses are for connections that are incoming from the enterprise to Google. The talkz.l.google.com addresses are for connections that are incoming from Google to the enterprise.

4. Make sure that the Sametime Gateway server can resolve a reverse lookup on each of the Google IP addresses.

You can verify this by substituting each IP address into the following command:

:C:\>nslookup
> 209.85.163.125
Server: Unknown
Address: 129.42.250.40

Name: el-in-f125.google.com
Address: 209.85.163.125

**Connecting the local Sametime Community Server to Sametime Gateway:**

Complete these steps to prepare and then add your local Community Server to Sametime Gateway.

**Managing trusted IP addresses for Sametime Gateway:**

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.

**Specifying the mail attribute for LDAP person records:**

If your Sametime servers are configured to use an LDAP server that is not a native internal Domino directory, you must specify the attribute in an LDAP record that contains the user’s email address. This setting is required because SIP entities are identified by their email addresses.

**Procedure**

1. From the Sametime server home page, click the **Administer the Server** link to open the Sametime Administration Tool.
2. Choose **LDAP Directory - Basics**.
3. In the **Basics settings for server** drop-down list, select the LDAP server.
4. In the **Attribute of a person entry that defines the person's email address** setting, type the attribute that your LDAP directory uses to hold the user’s email address. Default attribute names include the following:
   - Type **mail** (default) if your LDAP directory is a Domino Directory, IBM Directory Server, or Sun ONE Java System Directory Server.
• Type userPrincipalName (default) if you are using Microsoft Active Directory.
5. Click Update.
7. In the search filter for resolving person names, update the search filter to contain the attribute specified in step 4 above. For example, if the LDAP directory uses the mail attribute, then update the search filter to include the mail attribute. For example:
   (&(objectclass=organizationalPerson)(|(cn=%s*)(givenname=%s*)(sn=%s*)(mail=%s*)))
8. Click Update and restart the server for the change to take effect.

Allowing local Sametime clients to add external users to Contact Lists:

Complete these steps to allow your Sametime clients to add external users to Contact Lists.

About this task

Follow these steps to change policies to allow users to add external contacts.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. In the Instant Messaging tab, select the policy you want to change and click Edit.
5. In the Chat section select "Allow user to add external users using Sametime gateway communities."
6. Click OK.

Results

After you complete these steps, users will see an External Contact check box on the Add New Contact dialog. To add an external contact, users type the external user's email address (name@domain), select External Contact, and then click Add.

Disabling the Sametime SIP Gateway on the local Sametime server:

To use Sametime Gateway with a local Sametime server version 6.5.1 or 7.0, you must disable the Sametime SIP Gateway application.

Procedure

1. Windows: Disable the Sametime SIP Gateway application by completing the following steps:
   a. Click Start > Programs > Administrative tools > Services.
   b. Right click on ST SIP Gateway and click Stop.
   c. Right click on ST SIP Gateway and click Properties.
   d. In the Startup type drop-down list, select Disabled.
   e. Click OK.
   f. Restart the Sametime server.
2. **AIX, Solaris, IBM i**: Disable the Sametime SIP Gateway application by completing the following steps:
   a. Open a command window. On IBM i, run the STRQSH (Start Qshell) command.
   b. Navigate to \lotus\domino.
   c. Use a text editor and open the StCommLaunch.dep file.
   d. Delete the following line from the file:
      - **AIX and Solaris**:
        ```
        SERVERAPP ST SIP Gateway,ST Community,SOFT
        ```
      - **IBM i**:
        ```
        SERVERAPP StGateway,StCommunity,SOFT
        ```
   e. Save the file.
   f. Restart the Sametime server.

**Adding a local Community Server to Sametime Gateway:**

Connect a local Sametime Community Server or Sametime community cluster to Sametime Gateway to enable Sametime users to have instant messaging with external users.

**Before you begin**

Before you can add a local Sametime server to Sametime Gateway, make sure you've completed the preceding steps:

- Opened port 1516 on the internal firewall to the local Sametime community server. If the Sametime community is clustered, you opened port 1516 to each of the Sametime community servers, allowing both inbound and outbound traffic between Sametime Gateway and each community server.
- Configured the Sametime server to trust the IP addresses of Sametime Gateway servers.
- Disabled the legacy Sametime SIP Gateway on the Sametime community server.
- Allowed local Sametime clients to add external users to Contact Lists.

**Important**: You can only connect one gateway to a community; otherwise the awareness and chat features may not work properly. Likewise, you can connect only one local Sametime community to Sametime Gateway. You must add the local community to Sametime Gateway before you add external communities.

**About this task**

**Expected state:**

- **Single server**: the Sametime Gateway server is started.
- **Cluster**: the Deployment Manager is started, and the node agent and Sametime Gateway servers are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a logical name for the local community such as **Sametime Users**.
4. In the **Community Type** field, select **Local**.

5. In the **Domains** field, type the domain names in which users are found in the local community.

   **Notes:**
   - Wildcards are not supported in this field, you must type each complete domain name.
   - Each domain name must access the same user directory. For example: acme.com, us.acme.com, fr.acme.com, and uk.acme.com must all be linked by a common user directory to be in the community. Obtain this information from the system administrator of the local Sametime community.
   - If you plan to connect to Google Talk or other XMPP communities, all the domains listed must have an existing SRV record. See the instructions in Connecting to Google talk community. If even a single listed domain does not have an SRV record, the Google community cannot connect.

6. In the **Translation Protocol** field, select **VP**.

7. Provide the **Host name** that Gateway connects to when it reads the overall configuration of the Community Servers. Depending on the size of your deployment, Sametime Gateway connects to either a single Sametime Community Server or a virtual IP address if you have one configured one for routing to multiple Community Servers.

   Type the appropriate host name.
   - **One Sametime Community Server**
     Enter the server’s host name.
   - **Multiple Community Servers (in a distributed or clustered environment)**
     Enter the host name of a Virtual IP (VIP) configured to route to an available Community Server at all times. This is a bootstrapping phase, in which the Gateway connects to the Community Server the VIP is currently pointing to so it can read the cluster configuration information. This information contains the list of Community Server host names. The Gateway then closes the connection to the VIP and begins connecting to each of the Community Servers directly instead.

   **Note:** Do not enter the host name of a MUX or IP sprayer that Sametime clients connect to.

8. Set the **Port** to 1516. The **transport protocol** is automatically set to TCP (Transmission Control Protocol).

9. Click **OK**.

10. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.

### Related tasks

“Connecting to a Google Talk community” on page 563
IBM Sametime Gateway users can exchange instant messages with the Google Talk community over the Extensible Messaging and Presence Protocol, or XMPP. To communicate with the Google Talk community, you must first set up a DNS service (SRV) record and publish it to DNS so that Google Talk users and local Sametime users can discover each other and establish a connection. This topic instructs you to create a DNS SRV record first, and then add Google Talk as an external community.

### Connecting to instant messaging communities:
Add instant messaging communities such as the AOL clearinghouse, AOL Instant Messenger, Google Talk, XMPP, and Office Communications Server to Sametime Gateway.

About this task

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.

Note: Sametime client users must use the Sametime client version 7.5 or later when exchanging instant messages and presence information with public instant messaging providers such as AOL Instant Messenger, Office Communications Server, and Google Talk. Pre-7.5 clients are not licensed to connect with public instant messaging providers. The Sametime server will check and disable the Add external user checkbox if a client of a lower version is used. It is the responsibility of the Sametime Gateway administrator to comply with the licensing agreement.

Registering your Sametime Gateway with AOL:

The IBM Sametime Provisioning Application enables you to set up interoperability with certain public instant messaging services such as AOL. The application prompts you for relevant information, validates your organization’s entitlement to use IBM Sametime Gateway, provides the information to the instant messaging service, and notifies you when you have been added by the service.

Before you begin

Attention: The Sametime Gateway host name’s public DNS registration is required before creating the provisioning request; otherwise public external provider might fail during the provisioning request.

The procedure for registering your Sametime Gateway depends on how you acquired Sametime Standard or Sametime Advanced:

If you used IBM Passport Advantage:

If you acquired licenses for IBM Sametime Standard or Sametime Advanced using the IBM Passport Advantage website, then register your IBM Sametime Gateway directly using the Sametime Provisioning Application.

Before you begin

Before you begin, collect the following information:

- The primary contact for your site. The primary contact is the person who is entering into the Passport Advantage or Passport Advantage Express® contractual relationship with IBM on behalf of your company. IBM communicates directly with this person on issues such as Agreement modification and so forth. This person may be a procurement or purchasing professional.
• Your Passport Advantage site number.
• Your Sametime Gateway name. This can be any name that you assign to Sametime Gateway.
• Your Sametime Gateway host name.
• Your Sametime Gateway port number.
• Your Sametime Gateway SSL certificate common name.
• Your Sametime Gateway SSL certificate issuer (VeriSign, Comodo, Thawte, and so on).
• An email address for you to be notified when provisioned.
• The Sametime community domains that you want to expose to the instant messaging service.

Procedure
2. Type your IBM ID and password:
   • If you do not have an IBM ID and password, click the register link. You receive your web identity when you complete the registration.
   • If your web identity is not affiliated with a Passport Online Advantage site, you will be redirected to a self-nomination site where you should use the information you collected before starting this procedure. Unless you know you are the primary contact for your site, please select No when prompted "I believe I am the Primary Contact for this Site." Once you have completed the self-nomination form, the Primary Contact for your site must process the form. When you receive a self-nomination approval by email, go to http://www.ibm.com/software/lotus/sametime/federation and start the provisioning process.

Once your web identity is verified, the system checks whether you are a Sametime customer that is entitled to deploy the Sametime Gateway.
3. If you are entitled to deploy Sametime Gateway, enter the information needed by the instant messaging service.
4. Submit the provisioning form. After the instant messaging service receives your information and adds your site, you will receive an email notification from IBM that you have been provisioned. This can take up to seven business days.
5. Before accessing a public instant messaging service through the Sametime Gateway, you are required to agree to the terms of service or end-user license agreement for such public instant messaging services and IBM is not a party to any such agreement.

If you did not use IBM Passport Advantage:

If you did not acquire licenses for IBM Sametime Standard or Sametime Advanced through IBM Passport Advantage, then register your IBM Sametime Gateway by emailing the required information to the provided address. For example, if you are an IBM Business Partner or have purchased IBM Sametime Standard for Cisco Unified Communications from Cisco or an authorized Cisco reseller, you must use this procedure.

Before you begin

Send the information below to the following email address: sametime@us.ibm.com:
Registration Code:
- Registration code
  This is available on the Sametime for Cisco Unified Communications software DVD. If you are an IBM Business Partner, you can get this code from your Business Partner representative.

Technical information:
- Gateway host name (the fully qualified domain name of your gateway; for example: stgateway.company.com)
- The port on which you want to accept incoming TLS/SIP requests (port 5061 is used by default)
- Gateway certificate common name
- Gateway certificate issuer
- SIP realm to be used (for example: company.com)
- Do you wish to be provisioned for AOL AIM?
- Do you wish to participate in the AOL Clearing House?

Contact information:
- Company Name
- ID or Order # (If IBM Business Partner, use Partnerworld ID #; otherwise, use Order #)
- Contact first/last name
- Contact email address
- Contact telephone number
- Contact instant messaging address (optional)

Connecting to an AOL community:
Set up a connection by choosing either the AOL instant messenger community or the AOL clearinghouse community, but not both. The AOL clearinghouse is a superset of the AOL instant messenger community.

Before you begin
You must set up SSL prior to connecting to an AOL community.

About this task
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.

Connecting to the AOL clearinghouse community:
Use this procedure to add the AOL clearinghouse community to IBM Sametime Gateway. The AOL clearinghouse connects your Sametime users to a wide
community that includes AOL, ICQ, iChat, and other users from AOL Enterprise Federation Partner communities, including external Sametime communities. Connect to the AOL clearinghouse community or the AOL community, but not both, as the former is a superset of the latter.

Before you begin

You must set up SSL prior to connecting to an AOL clearinghouse community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

Note: IBM recommends that you do not configure both the AOL clearinghouse and the AOL 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.

Before you add the AOL clearinghouse community, you must establish the local community, and use the provisioning application to register your Sametime with AOL Public Instant Messaging Services.

About this task

Expected state:

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. In the table that lists communities, click New.
3. In the Name field, type a logical name for the new clearinghouse community.
4. In the Community Type field, select Clearinghouse.
6. In the Host Name field, type the following:
   `sip.oscar.aol.com`
7. In the Port field, type the port number. The default port is 5061.
8. Because AOL clearinghouse requires a secure connection, the Transport protocol is set to TLS, so there is nothing to do.
9. Click OK to save the new community.
10. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click Assign local users to this community to assign users access to the AOL clearinghouse community.
11. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.
12. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.
   a. Click Custom Properties to include additional IP addresses for AOL Instant Messenger servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from AOL. The Custom properties link is available only after the community is saved.
   b. In the Route properties field, set the maximum sessions for instant messaging or presence for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway.
   c. Select the check box to disable the route to the community.
   d. Click the Translation Protocol link to set custom properties for the translation protocol. The Custom properties links are available only after the community is saved.

What to do next


Connecting to the AOL Instant Messenger community:

Use this procedure to add the AOL Instant Messenger community to IBM Sametime Gateway so that your users can exchange instant messages and presence with AOL Instant Messenger users. Add the AOL community only if you have not added the AOL clearinghouse community because the AOL clearinghouse is a superset of the AOL community.

Before you begin

You must set up SSL prior to connecting to an AOL clearinghouse community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```bash
nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

Note: IBM recommends that you do not configure both the AOL clearinghouse and the AOL 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.

You must establish the local community first before adding an external community.

About this task

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.
Procedure

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a logical name for the new community such as AOL IM.
4. Under **Community Type**, select **External**.
5. In the **Domains** field, type: aol.net, corp.aol.com, aol.com
6. In the **Translation Protocol** list, select **SIP for AOL**.
7. In the **Host Name** field, type sip.oscar.aol.com.
8. In the **Port** field, type a port number. The default port is 5061.
9. In the **Transport protocol** field, TLS (Transport Layer Security) is already selected.
10. Click AOL IM from the list to edit the connection properties.
11. Click **OK** to save the new community.
12. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign local users access to the external community.
13. Click **Assign local users to this community** to assign local users access to the external community. This link is inoperable until you first save the new external community.
14. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.
15. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.
   a. Click **Custom Properties** to include additional TCP/IP addresses for AOL Instant Messenger servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from AOL. When setting up the community for the first time, the **Custom properties** links are available only after the community is saved.
   b. In the **Route properties** field, set the maximum sessions for instant messaging or presence for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If **Route properties** are not visible, you must connect to a local community first.
   c. Select the check box to disable the route to the community.
   d. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.

**What to do next**


**Connecting to a Google Talk community:**

IBM Sametime Gateway users can exchange instant messages with the Google Talk community over the Extensible Messaging and Presence Protocol, or XMPP. To communicate with the Google Talk community, you must first set up a DNS service (SRV) record and publish it to DNS so that Google Talk users and local
Sametime users can discover each other and establish a connection. This topic instructs you to create a DNS SRV record first, and then add Google Talk as an external community.

Before you begin

**Note:** IBM cannot guarantee the availability of the instant messaging federation with GoogleTalk. Sametime Gateway is fully dependent on GoogleTalk's service availability.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```bash
nslookup talkz.l.google.com
nslookup 64.12.162.248
nslookup -type=SRV -class=all _xmpp-server._tcp.google.com
```

Make sure all domains you specified in the internal community are not registered with "Google Apps." To determine whether a domain is registered with Google Apps, see the IBM Technote Unable to establish awareness with Google Talk users through the Sametime Gateway.

Your firewall rules should be set up as described in the "GoogleTalk" section of the topic, “Opening ports in the firewalls” on page 551.

About this task

Work with your network administrator to set up a DNS SRV record for each domain defined in your internal community using the following format:

```
_xmpp-server._tcp.domain name. IN SRV priority weight port target.
```

For example:

```
```

<table>
<thead>
<tr>
<th>SRV record format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain name</td>
<td>Wild cards are not allowed. Note that the domain name must end with a period. The domain name must match the domain name that you used when you added the local Sametime server to the Sametime Gateway.</td>
</tr>
<tr>
<td>priority</td>
<td>Priority determines the proxy query order when used in an Sametime Gateway cluster. With multiple SRV records, lower values are queried first.</td>
</tr>
<tr>
<td>weight</td>
<td>Weight determines proportionally how often a proxy is queried when you have multiple SRV records of similar priority in a cluster. Higher values are queried more often. So, a weight of 20 would be queried twice as often as one of 10. A weight of 30 would be queried three times as often as one of 10.</td>
</tr>
<tr>
<td>port</td>
<td>The port on which this service is found. Use port 5269.</td>
</tr>
<tr>
<td>target</td>
<td>Fully qualified host name of the machine running the Sametime Gateway. Note that the target must end with a period. For example: sttest.lotus.com.</td>
</tr>
</tbody>
</table>

Expected state: the Sametime Gateway single server or cluster is started
Procedure

1. Create an individual DNS SRV record (_xmpp-server._tcp) for each domain name that you will support.
   For example, you might support two local domain names, called lotus.com and ibm.com®. For each of the domain names you want to support, you must create an individual DNS SRV record. The records will be identical except for the domain name field's value.

2. Verify that the DNS SRV record that you added to DNS is correct by using the nslookup command:
   a. Open a command window and run nslookup.
   b. Type `set type=SRV`.
   c. Type `set class=IN`.
   d. Search the _xmpp-server.tcp record using the supported domains added in the previous step.
   Using the example above, you enter `_xmpp-server._tcp.lotus.com` and repeat the searching for `_xmpp-server._tcp.ibm.com`. Using lotus.com, the full command and returned value appears as follows:
   ```
   nslookup>set type=SRV
   >set class=IN
   >_xmpp-server._tcp.lotus.com.
   ```
   Make sure the correct hostname of the Sametime Gateway server and IP address are returned. The following is an example only:
   ```
   Server: sbydns01.srv.ibm.com
   Address: 9.0.4.1
   
   Non-authoritative answer:
   _xmpp-server._tcp.lotus.com SRV service location
   priority = 5
   weight = 0
   port = 5269
   svr hostname = sttest.lotus.com
   lotus.com nameserver = wtf-ns1.lotus.com
   lotus.com nameserver = wtf-ns2.lotus.com
   lotus.com nameserver = ns0.lotus.com
   sttest.lotus.com internet address = 129.42.249.45
   >
   ```

3. In the Integrated Solutions Console, click Sametime Gateway > Communities.

4. In the table that lists communities, click New.

5. In the Name field, type Google Talk.

6. Under Community Type, select External.

7. In the Domains field, type:
   ```
   gmail.com
   ```

8. Select XMPP as the Translation Protocol.

9. Ignore the host name. XMPP uses the Fully qualified domain name of the host as specified in the target field of the DNS SRV record instead.

10. In the Port field, type 5269.

11. In the Transport protocol field, select TCP. TCP is the only transport protocol for Google Talk.

12. Click OK to save the new community.
13. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click Assign local users to this community to assign local users access to the external community. By default all users can access the external community.

14. The following sub steps are optional:
   a. In the Route properties field, set the maximum sessions for instant messaging or presence for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If Route properties are not visible, you must connect to a local community first.
   b. Select the check box if you ever need to disable the route to the community.
   c. Click the Translation Protocol link to set custom properties for the translation protocol. The Custom properties links are available only after the community is saved.

15. Restart the Sametime Gateway server.

What to do next

Google's IP addresses associated with talky.l.google.com and talkz.l.google.com change occasionally. Google typically adds new IP addresses to DNS at least a week before the Google Talk service starts using them, but occasionally the IP address changes can be seen immediately, potentially causing service disruptions. There are various products that monitor DNS addresses for changes. See these search results for DNS monitoring tools available. Work with your network administrator to actively monitor DNS and update the firewall rules to accommodate new IP addresses.


Related tasks
   “Adding a local Community Server to Sametime Gateway” on page 556

Connect a local Sametime Community Server or Sametime community cluster to Sametime Gateway to enable Sametime users to have instant messaging with external users.

Connecting to an Office Communications Server community:

Connect to a Office Communications Server community so that your users can exchange instant messages with Microsoft Communicator users.

Before you begin

You must establish the local community first before adding an Office Communications Server community. Please also note that setting SSL is a prerequisite for connecting to an Office Communications Server community.

Remember that the IBM Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
nslookup [OCS Edge Server]
```
Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure
1. In the Integrated Solutions Console, click **Sametime > Gateway Communities**
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a logical name for the new community.
4. Under Community Type, select **External**.
5. In the **Domains** field, type the domain names of the Office Communications Server community. For example: `ocs.example.com`.
6. Select **SIP for OCS** as the translation protocol.
7. In the **Host Name** field, type the host name or the IP address of the OCS Edge Server.
8. In the **Port** field, type a port number. The default port is 5061.
9. In the **Transport protocol** field, **TLS** (Transport Layer Security) is already selected.
10. Click **OK** to save the new community.
11. Create a new custom property.
   - Single server: Click **Servers > WebSphere application servers > RTCGWServer**. Under Server Infrastructure, expand **Administration** and select **Custom properties**. Click **New**.
   - Clustered server: Click **System administration > Cell**. Under Additional properties, select **Custom properties**. Click **New**.
12. In the **Name** field type `com.ibm.sametime.gateway.fqdn`.
13. In the **Value** field, type the fully qualified domain name of the Sametime gateway (or the SIP Proxy server in a clustered environment). For example: `stgw.example.com`.
14. Click **OK** to save the new custom property.
15. Click **New** again.
16. In the **Name** field type `com.ibm.sametime.gateway.port`.
17. In the **Value** field type the gateway's port. For example: 5061.
18. Click **OK** to save this new custom property.
19. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users and capabilities** to assign users access to the external community.
20. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.
21. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.
   a. Click **Custom Properties** to include additional host names for OCS edge servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from Office Communications Server. When setting up the community for the first time, the Custom properties links are available only after the community is saved.
Connecting to an XMPP community:

IBM Sametime Gateway users can exchange instant messages with an XMPP community over the Extensible Messaging and Presence Protocol, or XMPP. To communicate with an XMPP community, you must first set up a DNS service (SRV) record and publish it to DNS so that users and local Sametime users can discover each other and establish a connection. This topic instructs you to create a DNS SRV record first, and then add XMPP domains as an external community.

Before you begin

You must set up SSL and establish the local community first before adding the XMPP community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

About this task

Expected state:

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure

1. Create an individual DNS SRV record (_xmpp-server._tcp) for each domain name that you will support.
   
   For example, you might support two local domain names, called lotus.com and ibm.com. For each of the domain names you want to support, you must create an individual DNS SRV record. The records will be identical except for the domain name field’s value.

2. Verify that the DNS SRV record that you added to DNS is correct by using the `nslookup` command:
   
   a. Open a command window and run `nslookup`.
   b. Type `set type=SRV`.
   c. Type `set class=IN`.
   d. Search the _xmpp-server.tcp record using the supported domains added in the previous step.

   Using the example above, you enter `<xmpp-server._tcp.lotus.com>` and repeat the searching for `<xmpp-server._tcp.ibm.com>`. Using lotus.com, the full command and returned value appears as follows:

   ```
   nslookup>set type=SRV
   >set class=IN
   >_xmpp-server._tcp.lotus.com.
   ```

   Make sure the correct hostname of the Sametime Gateway server and IP address are returned. The following is an example only:

   ```
   Server: sbydns01.srv.ibm.com
   Address: 9.0.4.1
   ```
3. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.

4. In the table that lists communities, click **New**.

5. In the **Name** field, type a logical name for the new community.

6. Under **Community Type**, select **External**.

7. In the **Domains** field, type the domains provided by the XMPP community. **Attention:** Wildcards are not supported in this field, you must type each complete domain name.

8. Select **XMPP** as the translation protocol.
   When you select XMPP as your protocol, the **Host Name** field defaults to "Localhost" as its value while Sametime Gateway resolves the domain value that you entered in step 5; once the domain is resolved, an appropriate value is entered automatically into the **Host Name** field.

9. In the **Port** field, the default port is 5269.

10. In the **Transport protocol** field, select **TCP** (Transmission Control Protocol) or **TLS** (Transport Layer Security).

11. Click **OK** to save the new community.

12. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign local users access to the external community.

13. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.

14. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.
   a. Click **Custom Properties** to include additional host names for XMPP servers. Sametime Gateway uses these IP addresses to determine which XMPP requests originate from this community. Note that the **Custom properties** link is available only after the community is saved.
   b. In the **Route properties** field, set the maximum sessions for **instant messaging** or **presence** for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If **Route properties** are not visible, you must connect to a local community first.
   c. Select the check box to disable the route to the community.
   d. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.
What to do next


Managing external watching:

The Sametime server allows an external watcher, or user who has someone on his or her contact list that is unaware of being watched, to conduct this activity; however, this capability can be disabled.

Configuring user consent

Instant messaging users from commercial IM providers such as Google can watch the status of internal Sametime users unless the server is configured to manage this functionality. This functionality can be managed through the ‘user consent’ feature. When the server is configured to require permission from the Sametime user, the Sametime user sees a pop-up window on his screen, asking for permission for the external user to watch the Sametime user’s status. The Sametime user can give consent, or not.

To require the external IM watcher to gain permission of the ‘watched’ person, follow these steps:
1. Open the sametime.ini file.
2. In the [Config] section, add:
   
   AWARENESS_EXTERNAL_NEED_PERMISSION=1

3. Shut down and restart the Sametime server to effect the change.

By default, the configuration flag is set to 0.

When the server is configured to require permission from the Sametime user, the Sametime user sees a popup window requesting permission for the external user to watch the Sametime user's status. The Sametime user can approve or decline.

Connecting to external Sametime communities:

Connect to external Sametime communities by working, if necessary, with an administrator from an external community to prepare the external Sametime server and by then adding the external Sametime community to your list of communities.

Preparing external Sametime servers:

This topic presents general information on steps needed to configure Sametime servers versions 6.5.1 or 7.0 that exist in external communities. Work with the external community’s administrator to prepare the legacy Sametime server for Sametime Gateway communications. For example, if your local Sametime server is a member of widgets.com, and you want to connect to an external Sametime 6.5.1 server at acme.com, you may want to know the steps required to set up the external Sametime server to have instant messaging and presence with your Sametime Gateway.
Procedure

1. If the external community’s Sametime server is version 6.5.1, or 7.0, the external community must enable the Sametime SIP Gateway on the server. See the chapter “Enabling the SIP Gateway” in the Sametime Server Administration Guide.

2. The latest patches and Cumulative Fix Packs must be installed on the external community’s Sametime server. Go to Sametime Product Support to download the latest support files for the external Sametime server.

Adding external Sametime communities:

Add an external Sametime community to IBM Sametime Gateway. You connect to a Sametime community by specifying domains in the external community, selecting a translation protocol, and setting the host name, port, and transport protocol for the external community.

Before you begin

You must add the local Sametime community first before adding an external community. In addition, if you are not connecting to a Sametime 7.5 or later server using its own Sametime Gateway, be sure that the external Sametime 6.5.1 or 7.0 server has the Sametime SIP Gateway enabled. Finally, confirm that the external Sametime server and Sametime Gateway have the latest fixes installed.

About this task

Expected state:

- Single server: the local Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and a Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.

2. In the table that lists communities, click New.

3. In the Name field, type a name for the new community.

4. Under Community Type, select External.

5. In the Domains field, type the Fully qualified domain names in which users are found in the external community. Each domain name must access the same user directory. For example: acme.com, us.acme.com, fr.acme.com, and uk.acme.com must all be linked by a common user directory to be in the community. Obtain this information from the system administrator in the external community.

6. Select a Translation Protocol:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use SIP for Sametime Gateway for connections to Sametime Gateway versions 7.5 or later communities.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>Use SIP for legacy Sametime Gateway for Sametime versions 7.0 or 6.5.1 communities.</td>
</tr>
</tbody>
</table>
7. In the **Host Name** field, type the name of the external real-time communication server such as ExampleServer1.com, for example.

**Note**: If the host name is an IPv6–format network address, set an explicit address here; do not use an abbreviated address (no brackets, no leading zeroes). For example, all of these IPv6–format network addresses are equivalent, but only the first form is accepted:
- `1:2:0:0:6:7:8 [acceptable]`
- `1:2:6:7:8 [do not use this abbreviated format]`
- `01:2:0:0:006:0007:8 [do not use leading zeroes]`

8. In the **Port** field, type the port number (the default port number is 5061). The port you use is dependent on the **Transport protocol** you select in the next step:
- TLS uses port 5061
- TCP uses port 5060

9. In the **Transport protocol** field, select **TLS** (Transport Layer Security) or **TCP** (Transmission Control Program or TCP/IP). If you select TLS as the protocol, you must set up SSL with a certificate signed by a Certificate Authority and exchange trusted certificates with the external community.

10. Click **OK** to save the new community. Note that you can’t assign users to the community until you save the community.

11. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign local users access to the external community.

12. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

13. The following steps are optional:
   a. In the **Route properties** field, set the maximum sessions for **instant messaging** or **presence** for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If **Route properties** are not visible, you must connect to a local community first.
   b. Select the check box to disable the route to the community.
   c. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.
   d. Click **Custom Properties** to set additional properties for the community. The **Custom properties** links are available only after the community is saved.

**Preventing communication with external communities:**

You can prevent external users from communicating with a particular IBM Sametime community by creating an exclusion list. The Sametime Gateway server will deny external communication requests for users hosted on all servers and clusters specified on the list.

**Before you begin**

This feature requires you to define a Home Server (cluster) for all users within the targeted community, so that the Sametime Gateway server can determine whether
the user belongs to a community on the exclusion list. For information on defining a user's Home Server, see Forcing users to connect to a home server.

About this task

An exclusion list is a list of clusters (for a stand-alone Sametime server, the cluster name is the server name) deployed within a local Sametime community; you define the list as a Sametime Gateway custom property. Use the exclusion list to prohibit external users from communicating with users in a community hosted on one of the specified clusters. Subscribe (awareness) and chat (instant messaging) requests from all external users to the local users hosted on the clusters listed on the exclusion list, will be rejected by the Sametime Gateway server. You enable this feature with the custom property called "Sametime community exclusion list".

For example, suppose the Example Corporation has two distributed Sametime clusters, called eu.acme.com (Europe) and usa.acme.com (USA). In addition, Sametime Gateway is installed on gw.acme.com.

On the Sametime Gateway server (gw.acme.com), there is an exclusion list containing "eu.acme.com" – this prevents the Sametime Gateway server from connecting to any servers in the eu.acme.com cluster. When an external user (outside of Example Corporation; for example, on AOL) adds a user hosted on eu.acme.com to her contact list, the subscribe request is routed to the Sametime Gateway server, which denies the request because it cannot access users in that cluster. In this example, the usa.acme.com cluster does not appear on the exclusion list, so the external user can access people in that cluster.

Follow these steps to define an exclusion list. For details see Adding custom properties.

Procedure

1. Log in to the Integrated Services Console as a Sametime Gateway administrator.
2. Click Sametime Gateway > Communities.
3. Select the local community for which you want to define an exclusion list.
4. In the Name field, type: Sametime community exclusion list as the name of the new property.
5. In the Value field, type the list of excluded servers and clusters.
   Type the server names and cluster names as a list using any of these characters to separate names:
   • comma ,
   • semicolon ;
   • space
   Cluster names must appear as defined in the Cluster Document; for more information, see "Creating a cluster document in the Configuration database". Standalone server names must appear as they are defined in the sametime.ini file's VPS_NAME property (for example, CN=st1/O=acme).
6. Click OK.
7. Restart the Sametime Gateway server so your changes can take effect. If the server was previously connected to Sametime servers that are now excluded, restart those servers as well.

Providing a port number to external communities:
The procedures describe how to obtain and update the port number that the SIP container uses to communicate with external communities. You want to provide the port number to external communities so they can use the same port. You may also need to change the TLS port number that Sametime Gateway uses.

Providing a port number to external communities for single server installations:

These steps describe how to obtain and update the port number that the SIP container uses to communicate with external communities. You want to provide the port number to external communities so they can use the same port. You may also need to change the TLS port number that the Sametime Gateway uses.

Before you begin

This procedure assumes that you have installed the Sametime Gateway.

About this task

A standalone Sametime Gateway server uses a SIP container port that is, by default, 5061 for Transport Layer Security (TLS). Therefore, if an external community wants to connect to Sametime Gateway, the external community must define port 5061. Check the `SIP_DEFAULTHOST_SECURE` parameter to verify the TLS port for the SIP container service.

Expected state: the Sametime Gateway server is started.

Procedure

1. To obtain the port number used by a single Sametime Gateway server, in the Integrated Solutions Console:
   a. Click Servers > Application servers > server_name, where server_name is the name of the Sametime Gateway server.
   b. Under Communication, click Ports.
   c. Look for the port number in `SIP_DEFAULTHOST_SECURE` and make a note of this number.

2. Check that the port number is added to the Default Virtual Host. The port is added default but you may need to update the default virtual host if you make changes to the ports:
   a. Click Environment > Virtual Hosts > default_host > Host Aliases.
   b. Click New and type a new port number if the port does not exist.
   c. Click OK, and then Save, and Save again.

What to do next

Now you can provide a port number to external communities.

Providing port numbers to external communities for clusters:

These steps describe how to obtain and update port numbers that the SIP and XMPP proxy servers uses to communicate with external communities. You want to provide the port numbers to external communities so they can use the same port. You may also need to change the TLS/SSL port number Sametime Gateway uses.
Before you begin

This procedure assumes that you have installed Sametime Gateway, have created a cluster, and have installed and configured a SIP and XMPP proxy server.

About this task

By default, the SIP proxy uses port 5061 over TLS/SSL, and the XMPP proxy server uses port 5269 for SSL and non-SSL connections.

Expected state: the Deployment Manager is started.

Procedure

1. To obtain the port numbers used by the Sametime Gateway cluster:
   a. In the Integrated Solutions Console, click **Servers > Proxy servers > SIPProxyServer**.
   b. Under Communication, click **Ports**.
   c. Look for the port number in **PROXY_SIPS_ADDRESS** and make a note of this number.

2. Click **Application Servers > Server Name** and, under the Communications section, click **Ports** to view the port number for **XMPP_SERVER_ADDRESS**. Make a note of this number.

3. Check that the ports are added to the Default Virtual Host. The port is added by default but you may need to update the default virtual host if you make changes to the port:
   a. Click **Environment > Virtual Hosts > default_host > Host Aliases**.
   b. Click **New** and type a new port number if the port does not exist.
   c. Click **OK**, and then **Save**, and **Save** again.

What to do next

The port number in combination with the DNS name of the node on which the SIP and XMPP proxy servers run is needed for configuring external instant messaging communities to connect to your Sametime Gateway.

Adding external contacts to the Sametime Connect Contacts List:

After you install and configure Sametime Gateway, and add an external community or clearinghouse community, your users can add external contacts to their Sametime Contact List. Give these instructions to your Sametime users so they will know how to add external contacts to their Contact List.

Procedure

1. In the Sametime Connect client, click **File > Add > Contact**.
2. Select the **Add external user by email address** check box.
3. Type the external contact’s email address.
4. Select an existing group, or type a new group name, in the **Add to group** field.
5. Click **Add**

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:
         &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

4. Extract the package to the local fixes directory you created.
5. In the UpdateInstallers subdirectory of the package you extracted, extract the updatemanager package for your platform.
6. Navigate to the directory where you extracted the Update Installer and run the install program.
   AIX, Linux, or Solaris
   ./install
   Windows
   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:
&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
```

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 588.
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 588.

**Results**

To verify which updates have been installed, run the `versionInfo` command from the `was_install_root/bin` directory.

**Linux**

```bash
./versionInfo.sh -maintenancePackages > version.txt
```

**Windows**

```bash
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 575

Use the WebSphere Application Server Update Installer to add required software updates.

**Preparing to install Sametime Advanced**

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** > **Install Sametime Advanced Server**.
Related tasks
“Starting the Sametime System Console” on page 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Guided activity: Preparing to install Sametime Advanced
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 up of 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
     ./stopManager.sh -username admin_user -password admin_password
     ```
   - **Windows**
     ```
     startManager.bat
     stopManager.bat -username admin_user -password admin_password
     ```
   - **IBM i**
     ```
     startManager dmgr
     stopManager -username admin_user -password admin_password
     ```

**Related tasks**

“Starting and stopping WebSphere Application Servers on Windows” on page 587
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 588
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**
     ```bash
     ./startNode.sh
     ./startServer.sh STConsoleServer
     ```
   - **Windows**
     ```bat
     startNode.bat
     startServer.bat STConsoleServer
     ```
   - **IBM i**
     ```bash
     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 582
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Adding trust for certificate authorities used by external communities” on page 1463
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 1465
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 1466
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 1469
“Setting up Sametime Gateway to use a new certificate” on page 1470
Set up IBM Sametime Gateway server to use the new certificates.

Related reference

“Command reference for starting and stopping servers” on page 588
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 582
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.

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

   For example:

   http://sametime.example.com:8700/ibm/console
   https://sametime.example.com:8701/ibm/console

   **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`

   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. 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 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.

**What to do next**

“Connecting to an LDAP server” on page 143

**Related tasks**

“Starting the Sametime System Console” on page 582

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

**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:
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 68

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 581
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 587
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 598
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                      |
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>Media Manager</td>
<td>Linux only:</td>
</tr>
<tr>
<td></td>
<td><code>.startNode.sh</code></td>
</tr>
<tr>
<td></td>
<td><code>.startServer.sh STMediaServer</code></td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td><code>.startNode.sh</code></td>
</tr>
<tr>
<td></td>
<td><code>.startServer.sh RTCGWServer</code></td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td><code>.startNode.sh</code></td>
</tr>
<tr>
<td></td>
<td><code>.startServer.sh STAdvancedServer</code></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><code>.stopServer.sh STConsoleServer</code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-password password</code></td>
</tr>
<tr>
<td>Meeting Server</td>
<td><code>.stopServer.sh STMeetingServer</code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopServer.sh STMeetingHttpProxy</code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-password password</code></td>
</tr>
<tr>
<td>Proxy Server</td>
<td><code>.stopServer.sh STProxyServer </code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-password password</code></td>
</tr>
<tr>
<td>Media Manager</td>
<td><code>.stopServer.sh STMediaServer</code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-password password</code></td>
</tr>
<tr>
<td>Sametime Gateway</td>
<td><code>.stopserver.sh RTCGWServer </code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-password password</code></td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td><code>.stopServer.sh STAdvancedServer</code></td>
</tr>
<tr>
<td></td>
<td><code>-username username -password password</code></td>
</tr>
<tr>
<td></td>
<td><code>.stopNode.sh -username username</code></td>
</tr>
<tr>
<td></td>
<td><code>-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 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</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>
<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 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</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>
</tbody>
</table>
Table 58. Stop server commands for Windows (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<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 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 581
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 582
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.
“Starting and stopping WebSphere Application Servers on Windows” on page 587
Use the Start Programs menu in Microsoft Windows to start or stop any Sametime servers running on WebSphere Application Server.

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 1240
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 597

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`
Learn how to start and stop a Sametime Community Server running on AIX, Linux, or Solaris.

Starting Domino and a Sametime Community Server on AIX, Linux, or Solaris:

Follow these instructions to start a Sametime Community Server 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

Related concepts

“Considerations for AIX, Linux, and Solaris” on page 597
If you install IBM Sametime on an IBM AIX, Linux, or Sun Solaris server, you should be aware of some special behaviors.

Running a Sametime server as a background process on AIX:

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
   ```

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
   fi
   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.

   Note that the path in your deployment might be different. Each line that starts with `wasservice.exe` should be on one line in your batch file.

   ```
   cd \Program Files\IBM\WebSphere\AppServer\bin
   set PROFILE_PATH=C:\ProgramData\IBM\WebSphere\AppServer\profiles
   wasservice.exe -add ConsoleServerDM -serverName dmgr -profilePath 
   "%PROFILE_PATH%\STSCDMgrProfile" -logRoot "%PROFILE_PATH%\STSCDMgrProfile\logs\dmgr"
   " -username wasadmin -password password 
   
   wasservice.exe -add ConsoleServerNodeAgent -servername nodeagent -profilePath 
   "%PROFILE_PATH%\STSCAppProfile" -logRoot "%PROFILE_PATH%\STSCAppProfile\logs\nodeagent"
   " -username wasadmin -password password 
   
   wasservice.exe -add ConsoleServerPrimaryNode -servername STConsoleServer -profilePath 
   "%PROFILE_PATH%\STSCAppProfile" -logRoot "%PROFILE_PATH%\STSCAppProfile\logs\STConsoleServer"
   " -username wasadmin -password password 
   
   wasservice.exe -add ProxyServerDM -servername dmgr -profilePath 
   "%PROFILE_PATH%\STPDmgrProfile" -logRoot "%PROFILE_PATH%\STPDmgrProfile\logs\dmgr"
   " -username wasadmin -password password 
   ```
wasservice.exe -add ProxyServerNodeAgent -serverName nodeagent -profilePath "%PROFILE_PATH%\STPAppProfile" -logRoot "%PROFILE_PATH%\STPAppProfile\logs\nodeagent" -username wasadmin -password password "
wasservice.exe -add ProxyServerPrimaryNode -serverName STProxyServer -profilePath "%PROFILE_PATH%\STPAppProfile" -logRoot "%PROFILE_PATH%\STPAppProfile\logs\STProxyServer" -username wasadmin -password password "
wasservice.exe -add MeetingServerDM -serverName dmgr -profilePath "%PROFILE_PATH%\STMDMgrProfile" -logRoot "%PROFILE_PATH%\STMDMgrProfile\logs\dmgr" -username wasadmin -password password "
wasservice.exe -add MeetingServerNodeAgent -serverName nodeagent -profilePath "%PROFILE_PATH%\STPAppProfile" -logRoot "%PROFILE_PATH%\STPAppProfile\logs\nodeagent" -username wasadmin -password password "
wasservice.exe -add MeetingServerProxy -serverName STMeetingHttpProxy -profilePath "%PROFILE_PATH%\STPAppProfile" -logRoot "%PROFILE_PATH%\STPAppProfile\logs\STMeetingHttpProxy" -username wasadmin -password password "
wasservice.exe -add MeetingServerPrimaryNode -serverName STMeetingServer -profilePath "%PROFILE_PATH%\STPAppProfile" -logRoot "%PROFILE_PATH%\STPAppProfile\logs\STMeetingServer" -username wasadmin -password password "
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 "

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:

PROFILE_PATH=C:\ibm\WebSphere\AppServer\profiles

wasservice.exe -add MediaServerDM -serverName dmgr -profilePath "%PROFILE_PATH%\zeta-stmeetMeetingDMProfile1" -logRoot "%PROFILE_PATH%\zeta-st851MeetingDMProfile1\logs\dmgr"

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 587

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.

**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 61. 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: <code>C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</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 62. 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 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 reference**

“Command reference for starting and stopping servers” on page 588

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 63. `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>
</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 64. `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 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.

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 588.
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
- 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 605

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 588.
   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 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 588.
   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 a Sametime Bandwidth Manager server on Linux or Windows:

610 IBM Sametime: Installation, Migration, and Configuration Guide
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`.

   For example:
   
   `/opt/IBM/WebSphere/AppServer/profiles/AppServerProfile/bin/ws_ant.sh uninstall`

   **Microsoft Windows**
   
   ```bash
   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\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 stavconfig.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.
   
   ```
   <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:

**Related tasks**

"Uninstalling all Sametime servers in a cluster on IBM i" on page 952

Use the instructions in this section to remove and uninstall a cluster of Sametime server on IBM i.

**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 625

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.

| SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |

Table 65. console.properties settings
Table 65. 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 “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 66. 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 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 reference
“Command reference for starting and stopping servers” on page 588
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 629

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 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.

**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>SSCHostName</th>
<th>Type the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</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. 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. 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.

   **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 588.
   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
• 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 605
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 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 588.
   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 588.
   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:
Table 69. 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 SSCSSEnabled 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>
</tbody>
</table>

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 581
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, UserName 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>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>
</tbody>
</table>
Table 70. 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>

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>
<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 reference

“Command reference for starting and stopping servers” on page 588
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 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:
<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Type the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>Type the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is “false.”</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>SSCUserName</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>SSCPassword</td>
<td>Type the IBM WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

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>SSCHostName</th>
<th>Type the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</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 <code>AboutThisProfile.txt</code> 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>SSCUserName</td>
<td>Type the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is <code>wasadmin</code>.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Type the IBM WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

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 72. 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 73. 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.

**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 xmi:id="DataReplicationDomain_1286203735111" name="stCellDRS"/>
```

In the example below, this is the multi-broker statement in bold face before the last line.

```xml
  <multibroker:DataReplicationDomain xmi:id="DataReplicationDomain_1285353668677" name="CsCellDRS">
    <defaultDataReplicationSettings 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 xmi:id="DataReplicationDomain_1286203735111" name="stCellDRS"/>
</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 588.
   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
- 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 605

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 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**
     ```sh
     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:
     ```sh
     /opt/IBM/WebSphere/AppServer/profiles/AppServerProfile/bin/ws_ant.sh uninstall
     ```
   - **Microsoft Windows**
     ```bat
     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 588.
   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 588.
   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 the /tmp folder and are named `db2setup.log`, `db2setup.hist`, 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-ES-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-ES-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.

---

**Installing on IBM i**

Install and configure prerequisites, then install IBM Sametime servers and complete basic server configuration.

This section contains information about system requirements, Sametime prerequisites, server installation and required configuration tasks to do after installation.

**Related concepts**
- Chapter 4, “Migrating and upgrading,” on page 1031

Migrate data from a previous version of Sametime and upgrade one or more servers to take advantage of the latest features.

**Preparing to install Sametime on IBM i**

Follow these steps to prepare IBM i for Sametime server installations.

**Preparing to create the Sametime database schemas and tables on IBM i**

The IBM Sametime System Console, Sametime Meeting Server, and the Sametime Gateway Server use databases to store data. Verify that the schemas do not already exist.

**Before you begin**

Decide on which system you will install the Sametime System Console, the Sametime Meeting Server, the Sametime Gateway Server, and their databases. On IBM i, they can all be on the same system or different systems. However, if you plan to install either the Sametime System Console or the Meeting Server on IBM i, both servers and the databases must be on IBM i.

**About this task**

The Sametime System Console requires two database schemas with these specific names: SSC and POLICY. The Meeting server requires these two database schemas: MTG and POLICY. The servers share the POLICY schema. Typically, you will create all of the schemas on the same system.
A schema cannot be created on a particular system LPAR if an IBM i library already exists with that name. Use these WRKLIB commands to determine if a library already exists with these names.

WRKLIB SSC

WRKLIB POLICY

WRKLIB MTG

If there is such a library and it was not created by Sametime, you must resolve the conflict by removing or renaming the libraries. Alternatively, the schemas can be created on a different IBM i system LPAR.

**Creating a user profile to own the database schemas on IBM i**

Follow these steps to create a user profile to own the database schemas for the Sametime System Console and the Sametime Meeting Server.

**About this task**

On the system where you plan to create the database schemas, create a user profile to be the database owner. The profile that you create can have a user class of *USER and does not require any special authorities.

If you plan to create the schemas for the System Console and the Meeting Server on the same system, use the same user profile for all of the schemas.

**Verifying authority to install and set up Sametime on IBM i**

The administrator who installs and sets up IBM Sametime must sign on to the system with a user profile that has the required authorities. Before installing, verify that the user profile you plan to use has the required special authorities.

**About this task**

The IBM i security officer has the required authorities to install and set up Sametime. If you are not the security officer, use the Display User Profile (DSPUSRPRF) command to determine if your user profile has the required authorities by following these steps.

**Procedure**

1. Type the following IBM i command:
   
   ```
   DSPUSRPRF user_id
   ```

2. Press the **PAGE DOWN** key and look for the special authority field to display the special authorities for the user profile. Verify that you have the necessary authorities for installing the Sametime software.
   
   - All object access (*ALLOBJ)
   - Security administration (*SECADM)

3. Verify that you have the necessary authorities to add the Sametime Community Server to an IBM i Domino Server.
   
   - All object access (*ALLOBJ)
   - System configuration (*IOSYSCFG)
   - Job control (*JOBCTL)
Results

If your user profile does not have the required authorities, either ask the security officer to install and set up the Sametime server or add the required authorities to your user profile.

Installing the Sametime System Console on IBM i

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.

Preparing the console installation file on IBM i

Follow these steps to customize the response.properties file to prepare for installing the Sametime System Console on IBM i.

Before you begin

You should have completed the preparation steps in "Preparing to install Sametime on IBM i."

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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
2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the cd shell command, specifying the fully qualified path to the installation package directory; for example:
      cd /MySametimePackages
   c. Run the following shell command, specifying the name of the .zip file:
      ajar -x name_of_installation_package
3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image; for example:
   /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc/licenses
   For DVD:
   /qopt/volume_ID/IBMi/stii_ssc/licenses
4. Navigate to the program image directory; for example:
   /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc
   For DVD:
   /qopt/volume_ID/IBMi/stii_ssc
5. Make a copy of the ssc.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.
6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   • For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces. 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.
   • For the database.db.user.id and database.db.user.password settings in the properties file, specify the user profile and password you created to be the owner of the Sametime System Console database schemas.
   • Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

Example

“Default console installation file for IBM i”

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Default console installation file for IBM i:

The response.properties file contains settings used to install or upgrade a Sametime System Console on IBM i.

The default content for the response.properties file for installing the Sametime System Console follows:

```
# Sametime 8.5.2 System Console Server Installation Properties file for IBM i
#
# Preparing to Install
#
# This file is used for either installing a new Sametime 8.5.2 System Console or
# upgrading a Sametime System Console to Sametime 8.5.2.
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime System Console on IBM i and
# running the installation program.
```
The Information Center is available online from the Lotus Sametime documentation library:


License Acceptance

By changing the silentInstallLicenseAcceptance property in this response file to "true", you agree that you have reviewed and agree to the terms of the IBM International Program License Agreement accompanying this program, which is located at CD_ROOT\IBM\stii_ssc\licenses.

If you do not agree to these terms, do not change the value or otherwise download, install, copy, access, or use the program and promptly return the program and proof of entitlement to the party from whom you acquired it to obtain a refund of the amount you paid.

Valid values for silentInstallLicenseAcceptance:
- true - Accept the license terms and continue with product installation.
- false - Decline the license terms and do not install the product.

silentInstallLicenseAcceptance=false

Installation Type

Set this value to the type of installation you wish to perform. The setting determines the WAS nodes that are created during installation.

Valid values for install.type:
- Cell - (default) Cell installation, recommended for new deployments. Creates both a deployment manager node and a primary application server node with the Sametime System Console installed. The primary node is federated into the deployment manager's cell. If the cell installation already exists, both the deployment manager node and the primary application server node are upgraded.

install.type=Cell

Websphere Settings

These values are used when configuring the Websphere Application Server nodes.

stwas.was.hostname - (required) For new installs, specify the fully qualified hostname that your WAS server will use. For upgrades, specify the fully qualified hostname of the existing WAS server.

stwas.was.admin.id - (required) For new installs, specify the user ID that you will use to log into the Deployment Manager's Integrated Solutions Console once security is enabled. This name must not exist as a user in any LDAP directory that you plan to connect to the server. For upgrades, specify the user ID that you use to log into the Deployment Manager's Integrated Solutions Console.

stwas.was.admin.password - (required) The password associated with the user ID specified for 'stwas.was.admin.id'

stwas.was.hostname=
stwas.was.admin.id=
stwas.was.admin.password=
# STATIC Websphere Settings
#
# These settings are used by the installer to control how Websphere is configured
# during installation. The values have been set specifically for installing the
# Sametime System Console Server.
# DO NOT CHANGE this settings unless instructed to do so by IBM Support.
#
### DO NOT CHANGE ###
stwas.was.installlocation=/QIBM/ProdData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.profilelocation=/QIBM/UserData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.dmprofile.default=STSCDMgrProfile
stwas.was.serverprofile.default=STSCAppProfile
stwas.was.snserverprofile.default=STSCSNAppProfile
stwas.was.appserver=STConsoleServer
### DO NOT CHANGE ###

# Database Settings
#
# These settings define the database used for the Sametime System Console.
# For new installations, they control how the database resources are configured
# in the Websphere Application Server.
# For upgrades, they allow the installer to connect to the database resources.
#
# database.db.hostname - (required) The fully qualified hostname of the system
# where the database is running.
# database.db.user.id - (required) The user ID that will be used when making a
# connection to the database.
# database.db.user.password - (required) The password for the user ID specified
# by database.db.user.id.
#
database.db.hostname=
database.db.user.id=
database.db.user.password=

# STATIC Database Settings
#
# These settings are used by the installer to control how database connections are
# configured during installation. The values have been set specifically for
# installing the Sametime System Console Server.
# DO NOT CHANGE these settings unless instructed to do so by IBM Support.
#
### DO NOT CHANGE ###
database.db.type=db2_iseries
database.db.name=STSC
database.db.port=50000
### DO NOT CHANGE ###

# End of File

Creating the System Console database schemas and tables on IBM i
Run the script to create the database schema for the IBM Sametime System
Console on IBM i.

Before you begin
You should have prepared the console installation file as described in “Preparing
the console installation file on IBM i.”
About this task

On the IBM i system where you will install the Sametime System Console, follow these steps to create the database schema and tables:

Procedure

1. Log in with a user profile that has *ALLOBJ and *SECADM special authorities. These authorities are required to create the database schemas. The database schemas will be created on the system specified in your copy of the ssc.default.response.properties file and owned by the user profile specified in the file.

2. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH

3. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:
   
   cd /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc
   
   For DVD:
   
   cd /qopt/volume_ID/IBMi/stii_ssc

4. If the SSC schema does not already exist on the system, run the following shell command to create the required database schemas and tables. The command also creates the POLICY schema if it does not exist.
   
   setupDB_ssc.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file

5. When the script completes, press F3 to exit QSH.

Results

If the database schema creation was not successful, look at the script log for more information about what occurred during the attempt. Fix the problem, then try running the script again. The script log is stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

ssc_dbsetupyyyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

ssc_dbsetup_20091215_0307.log

Related tasks

“Preparing to install Sametime on IBM i” on page 642

Follow these steps to prepare IBM i for Sametime server installations.

Installing the console on IBM i

Run the install script to set up the IBM Sametime System Console on IBM i.

Before you begin

If you intend to install from a downloaded image, you should have downloaded the console server installation package. For all installations, you should have completed the preparation steps. The database schemas required for the System Console (SSC and POLICY) should already exist.
**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 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.

**About this task**

Follow these steps to install the Sametime System Console and WebSphere Application Server.

**Procedure**

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the **WRKSYSVAL** command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   ```
   QSH
   ```
4. Run the `cd` shell command, specifying the fully qualified path to the installation kit directory; for example:
   ```
   /MySametimePackages/SametimeSystemConsole/IBM/stii_ssc
   ```
   For installing from DVD:
   ```
   cd /qopt/volume_ID/IBM/stii_ssc
   ```
5. Start the Sametime System Console installation with the following shell command:
   ```
   install_ssc.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file
   ```
   When the script completes, a summary of the results is displayed. Make a note of the URL for connecting to the Integrated Solutions Console. The "Admin port" displayed is the port you must use when logging in to the system console.
6. Press F3 to exit QSH.

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

```
/QIBM/UserData/Lotus/stii/logs
```

The log name contains the date and time in this form:

```
install_STCONSOLE_yyyymmd_hhmm.log
```

For example, this log was created at 3:07 A.M. on December 15, 2009:

```
install_STCONSOLE_20091215_0307.log
```
Related tasks
“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Increasing the WebSphere Application Server usage limit for running Sametime on IBM i
Use the Change License Information command to allow an unlimited number of users for the WebSphere Application Server installation. Changing the usage limit in this manner is acceptable provided you are in compliance with the terms of your Sametime license and are only using WebSphere Application Server for running Sametime.

About this task
If you install more than one Sametime server that uses WebSphere Application Server on the same system, this task only needs to be done once. Following the recommended installation sequence, the first server that uses WebSphere Application Server is the Sametime System Console. Other servers that use WebSphere Application Server are the Sametime Meeting Server, Sametime Proxy Server, and Sametime Gateway.

Procedure
1. Sign on to the system with a user profile that has *ALLOBJ special authority.
2. From any IBM i command line, run the following command (on one line):
   CHGLICINF PRDID(5733W70) LICTRM(V7) FEATURE(5102) USGLMT(*NOMAX) THRESHOLD(*USGLMT)

Results
The usage limit is changed to *NOMAX.

If the following message is displayed, type G.
CPA9E1B: Usage limit increase must be authorized.
   Press help before replying (C G)

After you respond to the CPA9E1B message, you must respond to the same message on the QSYSOPR message queue:
1. Run the DSPMSG QSYSOPR command to see the message in the QSYSOPR message queue.
2. When the message is displayed, type G.

Logging in to the Sametime System Console on IBM i
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.
   http://serverhostname.domain:port.ibm/console
   For example:
http://sametime.example.com:8700/ibm/console
https://sametime.example.com:8701/ibm/console

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

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. 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 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.

What to do next

“Connecting to an LDAP server” on page 143

Related tasks

“Starting the Sametime System Console” on page 582
When started, the Sametime System Console runs as a task in the WebSphere
Application Server administrative console.

Connecting to an LDAP server (IBM i)

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 93
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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Sametime prerequisite: Connecting to an LDAP server (IBM i)
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 74. 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.</td>
</tr>
<tr>
<td>Policy ID for users and groups</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>Display name</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 Similar name distinguisher due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td>Similar name distinguisher</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>Email address</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>
</tbody>
</table>
Table 74. Person attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 75. 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 76. 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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Starting and stopping the Deployment Manager on IBM i” on page 917
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Enabling encryption between Sametime and the LDAP server” on page 1435
Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

Related reference

“LDAP directory settings” on page 148
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 588
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 (IBM i)

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 659
- “Collect Person Settings” on page 660
- “Collect Group Settings” on page 662

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>
<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 77. 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><strong>Anonymous access</strong></td>
<td>Select this type of access only if you are certain all attributes are</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>accessible when the Sametime server binds to the LDAP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anonymous bind operations must be able to search on a unique ID attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specific to the LDAP server in use. Use these attributes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lotus Domino LDAP: dominounid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IBM Directory Server: ibm-entryuuid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory: objectguid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Novell eDirectory: guid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sun ONE: nsuniqueid</td>
<td></td>
</tr>
<tr>
<td><strong>Deployment Name for</strong></td>
<td>Specified a name that you provide to this LDAP connection for easy reference.</td>
<td>Sample deployment name: ST_LDAP</td>
</tr>
<tr>
<td><strong>this LDAP connection</strong></td>
<td>It does not need to map to any existing server name or value. It is an easy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>way to identify this object when you reference it in the future.</td>
<td></td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>Enter the fully qualified domain name of the LDAP server or Network</td>
<td>Sample host name: ldap1.example.com</td>
</tr>
<tr>
<td></td>
<td>Dispatcher serving the LDAP servers that you want to connect to. Do not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>use an IP address or a short host name.</td>
<td></td>
</tr>
<tr>
<td><strong>Port of the LDAP server</strong></td>
<td>The port number is the one on which the LDAP server listens for TCP/IP</td>
<td>Default 389</td>
</tr>
<tr>
<td></td>
<td>connections. The default port for LDAP access is TCP/IP port 389.</td>
<td></td>
</tr>
</tbody>
</table>
Table 77. 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</td>
<td>If you have selected <strong>Authenticated Access</strong>, 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 <strong>Anonymous Access</strong>, 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>
<tr>
<td>Password</td>
<td></td>
<td></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 78. 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>Detected LDAP Base DNs</td>
<td>For stconfig.nsf, edit the ldapserver document as follows:</td>
<td>Sample Base distinguished name: dc=example, dc=com</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>LDAP user search base</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>Configure advanced LDAP settings</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 79. 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 79. Collect Person Settings (continued)*
Table 79. 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 <strong>Distinguished Name</strong> 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. 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>
<td></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. If you have installed multiple Sametime servers, each user's person entry in an LDAP directory must contain a field in which a user's home server is specified. You can either: • Add a new field to the LDAP directory to store the name of each user’s home server. This field must be in the person entry of every Sametime user in the LDAP directory. • Use a field that exists in the person entries of each Sametime user, such as the email address.</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 80. 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 |
| 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     | 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 144
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 (IBM i)

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 4, “Migrating and upgrading,” on page 1031
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 1522
This section describes how to configure an IBM Sametime Community Server.

Related tasks
“Connecting to an LDAP server” on page 143
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 on IBM i
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.

Preparing the TCP/IP Environment on IBM i:
Your Sametime Community Server must be configured to use one or more specific TCP/IP addresses so that it will not attempt to share TCP/IP ports with any other HTTP servers on your system.

About this task
This section guides you through the process of verifying your TCP/IP configuration, making changes if necessary to resolve conflicts between servers, and gathering the TCP/IP information that you will need to configure your Sametime server.

Verifying host table entries for IBM i:
IBM Sametime provides a list of host table entries that are already defined on your server.

About this task
To verify your host table entries, follow these steps:

Procedure
1. From any IBM i command line, type the following command and press Enter:
   `CFGTCP`
2. On the Configure TCP/IP display, select option 10 to work with TCP/IP Host Table entries.
3. Record each host name and the corresponding TCP/IP address, as you may need this information later.
4. If your Sametime deployment will support IPv6 addressing, make sure that the IPv6 address is mapped to the server's host name in this table. If you will
support both IPv4 and IPv6 addressing, then each format should be mapped to
the host name to ensure that connections of both types are enabled.

Verifying configuration of existing IBM i Domino servers:

IBM Sametime provides which TCP/IP addresses are currently being used by your
Domino servers.

About this task

Note: If you do not have any Domino servers configured on your system, you can
skip this section.

To determine which TCP/IP addresses are currently being used by your Domino
servers, follow these steps after verifying that you have started your Domino
servers.

Procedure

1. From an IBM i command interface, sign on to your server.
2. Verify the current TCP/IP addresses for each Domino server by entering the
   following command:
   WRKDOMCSL servername
3. From the Domino Console display, type the following command and press
   Enter:
   sh port tcpip
4. Press F5 to refresh the screen.
   a. If the server is using only one TCP/IP address, you will see a specific
      TCP/IP Local Address listed using port 1352. For example, 10.1.2.3:1352.
   b. If the server is using all active TCP/IP addresses, you will see *:1352
      displayed as the Local Address rather than a particular TCP/IP address.
5. Record the results for each Domino server, as you will use this information
   later.

Selecting a TCP/IP address for your IBM i Sametime server:

Determine which TCP/IP addresses are already defined on your system and
decide which address you will use for your IBM Sametime server. You will also
need to determine whether you need to define additional TCP/IP addresses to
avoid conflicts between servers.

About this task

Follow these steps to select a TCP/IP address for the server.

Procedure

1. First determine which TCP/IP addresses are currently defined for your system.
   a. From any IBM i command line, type the following command and press
      Enter:
      CFGTCP
   b. On the Configure TCP/IP display, select option 1 to Work with TCP/IP
      interfaces and display a list of the currently defined TCP/IP interfaces.
2. Verify that each of the TCP/IP addresses you recorded when you looked at the
   Host Table or ran the 'sh port tcpip' command is currently defined.
3. Verify that the system has enough TCP/IP addresses defined so that you can assign at least one for the exclusive use of each of the following:
   - Your Sametime server
   - Each existing Domino server
   - Each instance of the IBM HTTP server running on your system
4. Contact your network administrator to assign additional TCP/IP addresses and host names if needed.
5. Ensure that the new host names are also added to your Domain Name Server (DNS).
6. Select the TCP/IP address you will assign to your Sametime server.
7. Decide which TCP/IP addresses should be assigned to each existing Domino server and each instance of the IBM HTTP server.
   Record this information, as you will use it later to ensure that existing servers are properly bound to specific IP addresses so that their port usage does not conflict with your Sametime server.

Adding a TCP/IP address on IBM i:

To configure an additional TCP/IP address for IBM i, complete this task.

About this task

If you did not need to assign additional TCP/IP addresses, you can skip this topic.

Procedure

1. From any IBM i command line, type the following command and press Enter:
   
   CFGTCP

2. Select option 1 to work with TCP/IP interfaces.
3. On the Work with TCP/IP Interfaces display, type a 1 in the Opt column and press Enter to add a TCP/IP interface.
4. On the Add TCP/IP Interface display, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Address</td>
<td>Specify the TCP/IP address you want to add. For example, enter 10.1.2.4.</td>
</tr>
<tr>
<td>Line Description</td>
<td>Specify the name of the line description for your LAN adapter. For example, enter TRNLINE.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the subnet mask that is appropriate for your interface. For example, enter 255.255.255.0.</td>
</tr>
</tbody>
</table>

5. Press Enter to add the new interface and return to the Work with TCP/IP Interfaces display.
6. To start an interface, type a 9 beside it and press Enter.

Updating the host table on IBM i:

Add an entry in the IBM i host table for your IBM Sametime server.
About this task

To add a host table entry for your Sametime server, follow these steps:

Procedure

1. From any IBM i command line, type the following command and press **Enter**:
   
   CFGTCP

2. Type 10 and press **Enter** to work with TCP/IP host table entries.

3. If one of the TCP/IP addresses that you selected is not listed in the Host Table, follow these steps to add a new entry:
   
   - Type a 1 in the **Opt** column next to the blank Internet Address and press **Enter** to add a Host Table Entry.
   - When the Add TCP/IP Host Table Entry display appears, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Address</td>
<td>Enter the TCP/IP address that you assigned to the Domino server. For example, enter 10.1.2.4.</td>
</tr>
<tr>
<td>Host name</td>
<td>Enter the fully qualified name of the Domino server as the host name. For example, enter stdom1.example.com.</td>
</tr>
</tbody>
</table>

   **Note**: Although you can add multiple host names for the same IP address, make sure you list the fully qualified name for your Domino server first, before any alternative short names.

   - Press **Enter** to create the Host Table Entry.

4. Follow these steps to update an existing Host Table Entry:

   **Note**: If the TCP/IP address you want to use is listed in the table, but the corresponding Domino server is not listed as one of the possible host names for that address, you must update the existing host table entry to include the additional host name.

   - Type a 2 in the **Opt** column next to the Internet Address and press **Enter** to change the Host Table Entry.
   - When the Change TCP/IP Host Table Entry display appears, you may need to **Page Down** to view the currently defined list of host names.
   - When you have displayed the last host name, enter a ‘+’ in the ‘+ for more values’ prompt and press **Enter**.
   - When the Specify More Values for Parameter HOSTNAME display appears, replace an existing host name or one of the *SAME entries with the fully qualified name of your Domino server (for example, stdom1.example.com).

   **Note**: The fully qualified name of your Domino server must be listed first in this table.

   - Press **Enter** to update the host name. Press **Enter** again to change the Host Table Entry.

   **Note**: You can remove a host name for an Internet Address by following the above steps to update the Host Table Entry and replacing the host name with *BLANK.
Updating the Domain Name Server for IBM i:

If you defined any additional host names, work with your TCP/IP administrator to ensure that the new host names are added to your Lotus Domain Name Server (DNS).

About this task

If you have configured TCP/IP to search the DNS before searching the host table, you may need to make additional changes in your configuration. Follow these steps to check your TCP/IP Configuration Properties:

Procedure

1. From any IBM i command line, type the following command and press Enter:
   CFGTCP
2. On the Configure TCP/IP display, type 12 and press Enter to change the TCP/IP domain information.
3. On the Change TCP/IP Domain (CHGTCPDMN) display, look for the "Host name search priority" setting.
   If the value is *REMOTE, either change this value to *LOCAL or verify with your network administrator that the fully qualified host name is the first value listed in the DNS for the IP address associated with your Sametime server. The fully qualified host name must be listed before any short names in order for your Sametime server to function correctly.
   If the value of this field is *LOCAL, you do not need to take any further action. You already ensured that the fully qualified host name was listed first in your local host table in an earlier step.
   **CAUTION:**
   **If you change the "Search order" you must stop and restart TCP/IP for the change to take effect.**
4. If your Sametime deployment will support IPv6 addressing, make sure that the IPv6 address is mapped to the server's host name. If you will support both IPv4 and IPv6 addressing, then each format should be mapped to the host name to ensure that connections of both types are enabled.
5. Press F3 to exit.

Verifying the system host name:

During the IBM Sametime Community Server startup, Sametime attempts to resolve the main system host name in addition to the Sametime server host name. The upgraded server will not start if Sametime cannot resolve the system host name to an IP address. Prior to Sametime 8.5, only the host name for the Sametime server was checked.

About this task

Verify that either the local IBM i host table (CFGTCP, option 10) or the DNS contain a fully qualified host name for the system and that the host name resolves to the correct IP address. If necessary, update the local IBM i host table or the DNS.

Updating the configuration of existing IBM i Domino servers:

Ensure your existing Lotus Domino servers are correctly bound to the specific fully qualified host names that you have assigned to them. This will prevent them from
conflicting with your Sametime Community Server. If necessary, you will modify the existing Lotus Domino server settings to enable partitioning and specify a unique fully qualified host name.

**About this task**

Even if you changed your server's fully qualified host name by modifying the server's notes.ini file, the change may not have occurred in the server document. This procedure updates both the server document and the notes.ini file.

**Procedure**

1. Using a profile with the authorities listed in Chapter 1, end the Domino server, if it is active, by typing the following command and pressing **Enter**:
   ```
   ENDDOMSVR DOM1
   ```
   where *DOM1* is the name of the Domino server.

   **Note:** Ending the Domino server may take a few minutes.

2. Change the Domino server settings by typing the following command and pressing **F4**:
   ```
   CHGDOMSVR DOM1
   ```
   where *DOM1* is the name of the Domino server.

3. In the **Advanced services** field, you should see *PARTITION* or *ALL*. If neither value is specified, then specify *PARTITION*.

4. In the **Internet Address** field, enter the fully qualified host name for this Domino server.

5. Press **Enter**.
   
   If the changes to the server settings were successful, the following message is displayed:
   ```
   Command CHGDOMSVR ended successfully.
   ```

6. Restart the Domino server by typing the following commands and pressing **Enter**:
   ```
   STRDOMSVR DOM1
   ```
   Where *DOM1* is the name of the Domino server.

   **Note:** Starting the Domino server may take a few minutes.

7. Using a Domino Administrator Client, edit the server settings in the Server Document so that the Domino HTTP server binds to the specific host name.
   - Select the **Configuration** tab.
   - In the left pane, click **Server** and select **All Server Documents**.
   - Open the server document for the Domino server and click the **Edit Server** button.
   - Select the **Internet Protocols** tab, and then select the **HTTP** tab.
   - In the **Host name(s)** field, verify the DNS name for the TCP/IP address that you specified in the Change Domino Server command.
   - In the **Bind to host name** field, select **Enabled**.
   - Select the **Ports** tab, then select the **Internet Ports** tab, then select the **Web** tab.
   - Verify in the HTTP settings that the TCP/IP port has a port number specified. The default port number is 80.
   - Click **Save and Close**.
8. Stop and restart the Domino server.
9. When the Domino server has restarted, access it through a Notes client or a
   web browser to make sure it is still accessible using TCP/IP.

Updating the HTTP server configuration on IBM i:

Your Sametime Community Server will use the Lotus Domino HTTP server. It is
possible that you may have already configured IBM HTTP Server for IBM i on
your system for other applications. If so, then you must verify that each instance of
the HTTP server is bound to a specific TCP/IP address. This will prevent it from
conflicting with your Sametime server.

About this task

To change the HTTP server settings using commands, follow these steps:

Procedure
1. If the HTTP server is currently running, type the following command on any
   IBM i command line and press Enter to end it:
   ENDTCPSVR SERVER(*HTTP)
2. Start the HTTP Administration server by typing the following command and
   pressing Enter:
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
3. Open the IBM HTTP server configurations page.
   - Start your web browser.
   - Enter the following URL:
     
     \texttt{http://mysystem:2001}

     where mysystem is the name of your system.
   - Click IBM Web Administration for IBM i.
   - Select the Manage tab.
   - Select the HTTP Servers tab.
4. Select a configuration from the menu at the top of the screen, and complete the
   following items for each configured instance of the HTTP server:
   - From the list on the left pane, select General Server Configuration.
   - In the right pane, find the IP address and port table in the section called
     Server IP address and ports to listen on.
   - If one of the rows in the table has an asterisk (*) in the IP Address column,
     then the server is listening on all IP addresses. Select that row. Replace the
     asterisk (*) with the IP address for this server and click Continue.
   - When finished updating the server IP address table, click Apply to save your
     changes.
5. When each instance of the HTTP server is configured to use a specific IP
   address, restart the HTTP servers by typing the following command and
   pressing Enter:
   STRTCPSVR SERVER(*HTTP)

Installing a Domino server:

Before you can install the Sametime Community Server, you must have already
installed an IBM Lotus Domino server.
Installing a Domino server in a new domain on IBM i:

Follow these steps to set up a Lotus Domino server in a new Lotus Domino domain.

**Procedure**

1. Launch the appropriate Domino wizard, depending on whether or not you have already installed Domino:
   - If you have not already installed Domino, launch the Domino InstallShield Wizard from a Windows workstation by running the `setup.exe` file located on the Domino product CD-ROM. Once you complete the installation, you are given the option to launch the Domino Server Setup Wizard to configure a Domino server.
   - If you have already installed Domino, launch the Domino Server Setup Wizard from a Windows workstation by running the `domwzd.exe` file located on the Domino product CD-ROM.

2. Follow the instructions on each wizard display to configure the new Domino server. Be sure to specify that you are configuring a Domino server in a new domain. If you need help with a particular setting, click **Help**.

3. Configure the Domino server with the following settings specific to a Sametime installation. Enter other values as needed.

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Enter the name of the new Domino server where you will add Sametime. For example, specify STDOM1.</td>
</tr>
<tr>
<td>Advanced server settings</td>
<td>Specify <strong>Yes</strong> for <strong>Enable server partitioning</strong> to allow multiple Domino servers to run on the same system.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the name of the Domino domain. For example, enter &quot;example.&quot;</td>
</tr>
<tr>
<td>Administrator's Name and Password</td>
<td>Specify the Domino administrator's name. This administrator will also be the Sametime server administrator. Specify a password for the Domino Administrator.</td>
</tr>
<tr>
<td>Internet Services</td>
<td>Select <strong>Web Browsers (HTTP services)</strong>. Sametime requires that you use the Domino HTTP server.</td>
</tr>
<tr>
<td></td>
<td>Deselect <strong>Directory Services (LDAP services)</strong>. Even if you plan to use an LDAP directory, you should not run it on the same server where you run Sametime.</td>
</tr>
<tr>
<td>Domino Network Settings</td>
<td>Click <strong>Customize</strong> to view the Advanced Network Settings.</td>
</tr>
</tbody>
</table>
Advanced Network Settings

Click the check box associated with the IP address for this server. Ensure that only one check box is selected.

You must edit the Host Name field and replace the IP address with the fully qualified Internet host name for this server. Type over the IP address displayed in the Host Name column and replace it with the fully qualified host name for the server. For example, STDOM1.example.COM. You must press Enter for the change to take effect.

Also, type the fully qualified host name in the field at the bottom of the display.

When finished, click OK and continue until Domino server setup is complete.

Related tasks

“Adding a Domino server to an existing Domino domain on IBM i”

You can install or add a Lotus Domino server into an existing Lotus Domino domain.

Adding a Domino server to an existing Domino domain on IBM i:

You can install or add a Lotus Domino server into an existing Lotus Domino domain.

Procedure

1. Register the additional server for your normal operating environment. You must specify the following settings during registration:
   - Store the server ID file that is created during registration somewhere on the system where you will configure the Sametime server. Record the path name; you will need to specify it when you configure the Sametime server.
   - Change the owner of the ID file to Qnotes by right-clicking the file in iSeries® Navigator and selecting Permissions.
   - Use the same network name as the first Lotus Domino server in the Lotus Domino domain.

2. Launch the appropriate Domino wizard, depending on whether or not you have already installed Domino:
   - If you have not already installed Domino, launch the Domino InstallShield Wizard from a Windows workstation by running the setup.exe file located on the Domino product CD-ROM. Once you complete the installation, you are given the option to launch the Domino Server Setup Wizard to configure a Domino server.
   - If you have already installed Domino, launch the Domino Server Setup Wizard from a Windows workstation by running the domwzd.exe file located on the Domino product CD-ROM.
3. Follow the instructions on each wizard display to complete the addition of the new Domino server. Be sure to specify that you are configuring an additional Domino server in an existing domain. If you need help with a particular setting, click Help.

4. Configure the Domino server with the following settings:

**Note**: This table only documents settings that directly apply to this Sametime installation. For settings that are not documented below, you can enter your own values.

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Name</td>
<td>Provide the registered name of the additional Domino server where you will add Sametime. For example, specify Sales1/example.</td>
</tr>
<tr>
<td>Advanced server settings</td>
<td>Specify Yes for Enable server partitioning to allow multiple Domino servers to run on the same system.</td>
</tr>
<tr>
<td>Internet Services</td>
<td>Select Web Browsers (HTTP services). Sametime requires that you use the Domino HTTP server. Deselect Directory Services (LDAP services). Even if you plan to use an LDAP directory, you should not run it on the same server where you run Sametime.</td>
</tr>
<tr>
<td>Domino Network Settings</td>
<td>Click Customize to view the Advanced Network Settings.</td>
</tr>
<tr>
<td>Advanced Network Settings</td>
<td>Click the check box associated with the IP address for this server. Ensure that only one check box is selected. You must edit the Host Name field and replace the IP address with the fully qualified Internet host name for this server. Type over the IP address displayed in the Host Name column and replace it with the fully qualified host name for the server. For example, stdom1.example.com. You must press Enter for the change to take effect. Also, type the fully qualified host name in the field at the bottom of the display. When finished, click OK and continue until Domino server setup is complete.</td>
</tr>
</tbody>
</table>
Related tasks
“Installing a Domino server in a new domain on IBM i” on page 671
Follow these steps to set up a Lotus Domino server in a new Lotus Domino domain.

Installing the Lotus Notes client and Lotus Domino administrative client on IBM i:

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 on IBM i:

Verify that your Lotus Domino server environment has the correct document settings and is accessible.
Verifying the Lotus Domino server document settings on IBM i:

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>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>Directory type</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>
</tbody>
</table>

<p>| Security tab                   |                                                                                        |
|--------------------------------|                                                                                        |
| Administrators                 | You complete this field during the Lotus Domino server installation. It contains the name of the Sametime administrator. If the name is incorrect, click the arrow to select a name from an address book. |
| Internet authentication        | The default value is Fewer name variations with higher security, which is better for tighter security. Select More name variations with lower security if you use Lotus Domino Directory authentication and want users to be able to use short names. |</p>
<table>
<thead>
<tr>
<th>Server document field</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access server</td>
<td>Leave this field blank. If you do include entries, you must add the following entry to the list of trusted directories:</td>
</tr>
<tr>
<td></td>
<td>Sametime Development/Lotus Notes 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 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 TCP/IP. 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 the Basics tab and the host name on the 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 port number changes after installation to 8088 automatically if you enable HTTP tunneling.</td>
</tr>
<tr>
<td>TCP/IP port status</td>
<td>This field must be enabled.</td>
</tr>
<tr>
<td>Name &amp; password</td>
<td>This field must be Yes.</td>
</tr>
<tr>
<td>Anonymous</td>
<td>This field must be Yes.</td>
</tr>
</tbody>
</table>

**Internet Protocols - HTTP tab**

<p>| Name &amp; password | This field must be Yes. |
| Anonymous       | This field must be Yes. |</p>
<table>
<thead>
<tr>
<th>Server document field</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<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, computername.domain_name.com or stdom1.example.com.</td>
</tr>
<tr>
<td>Bind to host name</td>
<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>
<tr>
<td>Allow HTTP clients to browse databases</td>
<td>This field must be set to Yes for portals.</td>
</tr>
<tr>
<td>Home URL</td>
<td>This field is set to stcenter.nsf during Sametime installation.</td>
</tr>
<tr>
<td>DSAPI filter file names</td>
<td>If this field is set to NDOLEXTN (Lotus Domino offline services), remove the value and leave this field blank.</td>
</tr>
<tr>
<td>Internet Protocols - Domino Web Engine tab</td>
<td></td>
</tr>
<tr>
<td>Session authentication</td>
<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 single-server.</td>
</tr>
<tr>
<td>Web SSO configuration</td>
<td>This field is set to LtpaToken during Sametime installation.</td>
</tr>
<tr>
<td>Java servlet support</td>
<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 581
An IBM Sametime deployment is made of up several component servers that can be started and stopped independently.

Installing a community server on IBM i
Follow these instructions to install a new Sametime Community Server on IBM i.

Preparing to install the community server from a downloaded image on IBM i:
Follow these steps to download the installation package for the Sametime Community Server for IBM i. If you are installing from physical media, skip this step.

Before you begin
You should have already installed Domino.

About this task
Follow these steps to download the installation package and create save files.

Procedure
1. Download the installation package for the Sametime Community Server if you have not already done so.
   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)
2. Sign on to the system with a user profile that has *ALLOBJ and *SECADM special authorities.
3. On any IBM i command line, run the following commands to create a library and the required empty save files for the Sametime software. The second save file, MYLIB/Q5724J23WC, is not needed for Sametime Entry.
   CRTLIB MYLIB
   CRTSAVF MYLIB/Q5724J23IM
   CRTSAVF MYLIB/Q5724J23WC
4. Open a Windows Command Prompt session on your workstation and change to the directory that contains the downloaded files. For example:
   cd c:\mydir
5. Start an FTP session with your system and transfer the downloaded files to the save files you created earlier. The second put command is not needed for Sametime Entry. Use the same user profile that you used in step 2.
The save files on your system now contain the Sametime Community Server software.

Related tasks
“Starting the Sametime System Console” on page 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Pre-accepting the Sametime software agreements on IBM i:

If you do not pre-accept the IBM Sametime software agreements, the installation process will restore the product to the system, but then stop and wait for you to accept the agreements before completing the installation. Skip this step if you are installing from a downloaded image.

Procedure
1. Insert the Sametime DVD into the optical drive of your system.
2. Enter the following command on an IBM i command line:
   ```
   GO LICPGM
   ```
The Work with Licensed Programs display appears.
3. From the Work with Licensed Programs (LICPGM) menu, select option 5 (Prepare for install) and press Enter. The Prepare for Install display appears.
4. Type 1 in the option field next to Work with software agreements. Press Enter. When the Work with Software Agreements display appears, you see all IBM licensed programs that require software agreement acceptance and whether the agreement has been accepted. Only licensed programs that are not yet installed appear on this display. The software agreements for Sametime will not appear in the list until you restore them from the DVD in a later step.
5. Press F22 (shift-F10) to restore the Software Agreements from the Sametime DVD.
   For the Device parameter, specify the name of your optical drive (For example, OPT01). Press Enter to restore the Sametime software agreements to the system.
6. If you are installing from physical media (not virtual optical media), the following message is displayed after the Software agreements are restored:
   ```
   Waiting for reply to message on message queue QSYSOPR
   ```
   You can sign on to another session to respond to the message or ask the system operator to respond.
   To view and respond to the message from another session:
   a. Enter the following command on an IBM i command line:
      ```
      WRKMSGQ QSYSOPR
      ```
   b. Select option 5 to display the messages in the QSYSOPR message queue.
   c. Locate the following message in the queue:
      ```
      Load the next volume in optical device OPT01. (X G)
      ```
   d. The Sametime software agreements have already been restored. If you want to restore more software agreements from another DVD, insert the next
7. The Work with software agreements display now shows the restored licenses for products that are not yet installed.
   • If you are using the DVD for the Entry version of Sametime, you will see an entry for Licensed Program 5724J23, option *BASE.
   • If you are using the DVD for Sametime Standard, you will see two entries for Licensed Program 5724J23: one entry for *BASE and another entry for Option 1.

8. For each entry for Licensed Program 5724J23, type 5 in the option field and press Enter to display the Software Agreement. Then press F14 (Accept) to accept the terms of the software agreement.

   Note: In some unusual situations, the following message may be issued when you attempt to display the Software Agreement:

   CPDB6D6 - Software agreement documents are missing. If this occurs, repeat step 5 to restore the Software Agreements again and continue with the remaining steps in this procedure.

Running the community server installation program on IBM i:

Run the installation program on the machine where you plan to install a Sametime Community Server.

Before you begin

You should have already installed Domino. If you intend to install from a downloaded image, you should have downloaded the community server installation package and created save files.

About this task

Use the IBM i command line to install the community server programs.

Procedure

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. From the IBM i command line, run the appropriate command for installing from a downloaded image or physical media.

Installing from a downloaded image

a. Use the RSTLICPGM command to install from the save files you created when you downloaded the installation package.
   This example uses the save files MYLIB/Q5724J23IM and MYLIB/Q5724J23WC.
   (For Sametime Entry, the second RSTLICPGM command is not needed.)
   RSTLICPGM LICPGM(5724J23) DEV(*SAVF) OPTION(*BASE) LNG(2924) SAVF(MYLIB/Q5724J23IM)
   RSTLICPGM LICPGM(5724J23) DEV(*SAVF) OPTION(1) SAVF(MYLIB/Q5724J23WC)

b. When you are prompted to accept the Sametime software agreement, you must accept it in order to continue.

Installing from physical media

Insert the Sametime disk in your system optical drive and run the RSTLICPGM command, specifying the correct name of the optical device. (For Sametime Entry, the second RSTLICPGM command is not needed.)
Verifying your IBM i library list:

While a single version of IBM Sametime supports multiple languages, the Sametime language feature for the Sametime licensed program is packaged using the English language feature code.

About this task

If the primary language of your system is not English, follow these steps to verify that QSYS2924 is in your library list:

Note: If the primary language of your system is English, you do not need to modify your library list.

Procedure

1. From an IBM i command line, type the following command and press Enter:
   WRKSYSVAL QSYSLIBL
2. On the Work with System Values display, type a 2 next to QSYSLIBL and press Enter.
3. On the Change System Value display, check whether QSYS2924 is included in the list. If it is listed, press F3 to exit. If it is not listed, proceed to step 4.
4. Type QSYS2924 next to Sequence Number 0 and press Enter.
5. Press F3 to exit.
6. If you changed the library list, sign off the system and sign back on to activate the new library list.

Adding the Sametime Community Server to an IBM i Domino Server:

To set up a Sametime Community Server running on IBM i, provide the necessary information, such as the directory type and ports.
About this task

Follow these steps to set up the Sametime Community Server.

Procedure

1. Sign on to the system with a user profile that has *ALLOBJ, *IOSYSCFG, and *JOBCTL special authorities.
2. Stop the Lotus Domino server.
3. On any IBM i command line, type the command ADDLSTDOM and press F4:
4. In the Domino server name field, type the name of the Domino server where you will add Sametime.
5. In the Directory type field, select which type of directory Sametime will use. You must select *LDAP if you want to use the Sametime System Console to administer this server.
   • If you chose *DOMINO, skip to the next step.
   • If you chose *LDAP, the following fields are displayed so you can provide the basic information that enables Sametime to connect to the LDAP server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the fully qualified host name of the LDAP server that Sametime will use. Do not specify the TCP/IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the IP port that Sametime will use. The default IP port for LDAP connections is 389.</td>
</tr>
<tr>
<td>Bind distinguished name (DN)</td>
<td>Enter the distinguished name of the LDAP directory entry that the Sametime server will use when binding to the LDAP directory. This is an optional parameter. If not specified, ensure the LDAP server is configured appropriately for anonymous access from a Sametime server.</td>
</tr>
<tr>
<td>Bind password</td>
<td>If you specified a Bind distinguished name (DN), enter the password associated with it.</td>
</tr>
<tr>
<td>Administrator name (DN)</td>
<td>Enter the distinguished name of an LDAP administrator who has authority to browse the LDAP directory. It is used when configuring policies. This parameter is optional and defaults to the same value as the Bind distinguished name.</td>
</tr>
</tbody>
</table>

6. In the HTTP Tunneling field, type either *YES or *NO and press Enter to display additional parameters.

   Note: This option enables Sametime clients that operate behind restrictive firewalls to connect to the Sametime server and use the presence, chat, screen-sharing, whiteboard, and broadcast features of Sametime.

7. Complete the following fields (you may need to press the Page Down key to view these fields):
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP server port</td>
<td>If you chose to allow HTTP tunneling, specify the port number on which the HTTP server will listen. The default is 8088.</td>
</tr>
<tr>
<td>Event server port</td>
<td>Enter the port on which the Event Server service for this Sametime server should listen.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you have more than one Sametime server installed on the same logical partition (LPAR) of your server, make sure the Event Server port is unique for each Sametime server.</td>
</tr>
<tr>
<td>Token server port</td>
<td>Enter the port on which the Authentication Server service for this Sametime server should listen.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you have more than one Sametime server installed on the same logical partition (LPAR) of your system, make sure the Token server port is unique for each Sametime server. Refer to the technote &quot;Verifying each Sametime for IBM i server on system uses unique ports&quot; for information on determining which Sametime ports are already in use. The technote is available at the following url <a href="http://www-1.ibm.com/support/docview.wss?rs=203">http://www-1.ibm.com/support/docview.wss?rs=203</a> &amp;uid=swg21212892.</td>
</tr>
</tbody>
</table>
Remote slide conversion

When files are attached to a meeting, Sametime Conversion Services is a feature that automatically provides a bitmap rendering so they can be shared in a meeting as slides.

Accept the default of *NONE if you will not host meetings on the Sametime Community Server.

If you do plan to host meetings on the Sametime Community Server, accept the default of *NONE if you prefer to run Conversion services as an integrated function of your Sametime server or if you plan to configure remote slide conversion at a later time. Note: Running integrated conversion services on IBM i requires that the following products be installed:

- Portable Application Solutions Environment (PASE), 5722SS1 or 5761SS1, option 33
- OS/400® - Additional Fonts, 5722SS1 or 5761SS1, option 43

If you are ready to provide connection information for a remote slide conversion server, specify the fully qualified host name or IP address of the Windows system where you will install Sametime Conversion Services.

8. Press F10 for additional parameters, then complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide conversion port</td>
<td>If you specified the name of a remote slide conversion server, specify the port on which the conversion server should listen for connections from the Sametime server.</td>
</tr>
<tr>
<td>Start Domino server</td>
<td>Specify whether or not you want to have this Sametime server start when the setup is complete.</td>
</tr>
</tbody>
</table>

9. Press Enter to run the command.

As Sametime is added to the Domino server, you will see a console screen that shows the progress of adding Sametime to a Domino server. When a message is displayed that the addition of Sametime is complete, press Enter.

10. If you did not choose to start the server during setup, start the Domino and Sametime Community Server now.
Results

The LDAP connection information is stored in a Directory Assistance database on the Sametime Community server. This database is normally created by ADDLSTDOM and named da.nsf. If a Directory Assistance database already exists on the server, then Sametime does not create it and the database may be named something else. The name of the Directory Assistance database can be found in the server document (Basics tab).

The LDAP information you provided in this task only allows Sametime to connect to the LDAP server. When you complete the LDAP configuration after installing the Sametime Community Server, you will enable Sametime to search the directory and authenticate web browser users.

What to do next

If you did not provide the correct LDAP information in this task, your Sametime server will be unable to connect to the LDAP server and Sametime will not start. Usually, the underlying Domino server will start with errors but you can still access the directory assistance database to make the necessary changes. Once you have corrected the LDAP connection information, restart the server.

If the Sametime startup failures cause a more serious problem and you are not able to access the Directory Assistance database, remove "staddin2" from the "Tasks" list in the Sametime server's notes.ini file, and restart the server. After making the necessary configuration changes, put "staddin2" back in the "Tasks" list and restart the Sametime server.

When you start the Sametime Community server it will automatically start an XVFB server (X Virtual Frame Buffer) that is used when converting files for display in meetings. If a Sametime Meeting Server is deployed on the same system as the Community Server, the Meeting and Community servers will share the XVFB server. If no meetings will be hosted on the system, you can prevent the Community Server from starting the XVFB server by editing the meetingserver.ini file in the server's data directory and changing the "DISPLAY=" value to "NONE. After saving the file, restart the Community Server.

Related tasks

“Starting Domino and a Sametime Community Server on IBM i” on page 928
Follow these instructions to start a Sametime Community Server on IBM i from an IBM i command line.

Completing the LDAP configuration on IBM i

After installing the Sametime Community Server on IBM i, use the Sametime Administration tool to provide the information that Sametime needs to search the LDAP directory and authenticate Sametime users against entries in the LDAP directory.

Before you begin

Start the Sametime Community Server.

Note: If you did not specify the correct LDAP connection information when you configured the Sametime server, the server will not start. See “Adding the Sametime Community Server to an IBM i Domino Server” on page 681 to correct this before proceeding.
About this task

Follow these steps to complete the LDAP directory configuration for Domino.

Procedure

1. Access the Sametime server by starting your web browser and entering the following URL:
   http://serverhostname.domain:port/stcenter.nsf
   Replace serverhostname.domain with your fully qualified server name and add the port number if you determined it is not the default port number 80. You must specify the server's fully qualified host name; if you do not, you will be able to access the Sametime Welcome Page, but you will not be able to log in.
   For example: http://st85comm1.example.com/stcenter.nsf
2. From the Sametime Welcome page, click **Administer the Server**.
3. At the login prompt, and specify the Domino server administrator ID and password and click **Enter**.
4. In the Sametime Administration Tool, click **LDAP Directory**.
5. Enter the settings to enable your Sametime server to access the LDAP directory.
   The settings should match the information you provided when you connected the Sametime System Console to the LDAP server.
6. Click **Save & Close**.
7. Restart the Sametime server to enable your settings.

What to do next

From a web browser, access the Sametime Welcome Page using the fully qualified host name of the Sametime server. Verify that you can log in with a User ID and password from the LDAP directory.

Related tasks

“Starting and stopping servers in a Sametime deployment” on page 581
An IBM Sametime deployment is made of up several component servers that can be started and stopped independently.

Related reference

“LDAP directory settings (IBM i)” on page 657
Find more details about LDAP settings for the guided activity, "Sametime prerequisite: Connecting to an LDAP server."

LDAP directory settings (IBM i):

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” on page 657
- “Base Distinguished Name and Filter for Searches” on page 659
- “Collect Person Settings” on page 660
- “Collect Group Settings” on page 662
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>
<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>
<tr>
<td>Anonymous access</td>
<td>Select this type of access only if you are certain all attributes are accessible when the Sametime server binds to the LDAP server.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Anonymous bind operations must be able to search on a unique ID attribute specific to the LDAP server in use. Use these attributes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lotus Domino LDAP: dominounid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IBM Directory Server: ibm-entryuuid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory: objectguid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Novell eDirectory: guid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sun ONE: nsuniqueid</td>
<td></td>
</tr>
<tr>
<td>Deployment Name for this LDAP connection</td>
<td>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.</td>
<td>Sample deployment name: ST_LDAP</td>
</tr>
<tr>
<td>Host name</td>
<td>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.</td>
<td>Sample host name: ldap1.example.com</td>
</tr>
<tr>
<td>Port of the LDAP server</td>
<td>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.</td>
<td>Default 389</td>
</tr>
</tbody>
</table>
Table 82. 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 83. 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 ldapserver 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><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 84. 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>
</tbody>
</table>
### Table 84. Collect Person Settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>Allows the user to authenticate with more than one attribute of the user's entry. Use any of these properties: <code>mail</code>, <code>cn</code>, or <code>uid</code>. The properties must be separated by a semicolon (<code>;</code>). <strong>Important:</strong> For the Meeting Server to work, the first field of the Authentication attribute must be set to <code>mail</code> and it must be listed first.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sample authentication attributes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mail;cn</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mail;cn;uid</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consider an LDAP person entry containing the following attributes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• mail: <a href="mailto:jlock@example.com">jlock@example.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• cn: James Lock</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the authentication attribute is mail, the user authenticates with <a href="mailto:jlock@example.com">jlock@example.com</a>. If the authentication attribute is cn, the user authenticates with James Lock.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 <code>sAMAccountName</code>, the attribute <code>sAMAccountName</code> is used in the filter. Similarly, if &quot;Display Name&quot; 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Search Attributes</strong></td>
<td>Specifies the fields used for searching the directory for users. The fields must be separated by a semicolon (<code>;</code>).</td>
<td>Sample search attributes: <code>mail;cn;uid</code></td>
</tr>
<tr>
<td><strong>Object Class</strong></td>
<td>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.</td>
<td>The value is set automatically to a default value based on the type of LDAP directory detected.</td>
</tr>
<tr>
<td><strong>Person attributes</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 84. 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 <strong>Distinguished Name</strong> 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. 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>
<td></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. If you have installed multiple Sametime servers, each user's person entry in an LDAP directory must contain a field in which a user's home server is specified. You can either: • Add a new field to the LDAP directory to store the name of each user's home server. This field must be in the person entry of every Sametime user in the LDAP directory. • Use a field that exists in the person entries of each Sametime user, such as the email address.</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 85. 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     |                                                                             | Sample display name: cn                                                                 |
| 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. | Sample display name: cn                                                                 |
| Distiguisher         |                                                                             | Sample display name: cn                                                                 |
| Group membership     | 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. | Sample display name: cn                                                                 |
| Attribute            |                                                                             | Sample display name: cn                                                                 |
| membership attribute |                                                                             | Sample display name: cn                                                                 |

Related tasks

“Sametime prerequisite: Connecting to an LDAP server” on page 144
This activity takes you through the steps for identifying users and groups in an LDAP directory that need access to IBM Sametime.

Registering a Community Server on IBM i with the System Console
After installing a Sametime Community Server on IBM i, register it with the Sametime System Console, so you can manage all of the Sametime servers from a central location.

Before you begin
Make sure the following servers are ready for the registration task:
The 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. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's `sametime_server_data_directory`/console directory.
   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 86. 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.
   The only required value in this file is

   **DepName**: Provide a descriptive name for your deployment; it must be a unique deployment name on the Sametime System Console.
4. Run the registerSTServerNode.sh registration 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 register the server: registerSTServerNode.sh
   d. As the registration utility runs, you will be prompted to enter the following
      information:

      | Location of notes.ini file | Type the full path to the directory containing the notes.ini file (for example, /stserver/data), and press Enter. |
      | Lotus Domino administrator user name | This is the account that you created for managing the 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. |

   e. When the registration script completes, press F3 to exit QSH.
      The utility registers the server and generates a log file called
      ConsolUtility.log, storing it in the consoles/logs directory. If the
      registration is successful, a console.pid will also be generated.

5. 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

**Enabling IPv6 support on a Sametime Community Server on IBM i**

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 on IBM i:

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 IBM i:

Before an IBM Sametime server can support IPv6 addressing on IBM i, you must configure IPv6 support for the Lotus Domino server on which it is hosted.

About this task

In Lotus Domino, only IPv4 addressing is enabled by default. Configuring Lotus Domino to support IPv6 involves several steps, including adding configuration settings to the notes.ini file for the Lotus Domino server. The steps for enabling only IPv6 support are different from the steps for enabling support for both IPv4 and IPv6; follow the instructions in the appropriate topic:

Configuring Lotus Domino to support both IPv4 and IPv6 addressing on IBM i:

Before an IBM Sametime Community Server can support both IPv4 and IPv6 addressing on IBM i, you must configure support for both addressing protocols on the Lotus Domino server where the Community Server 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 additionally support IPv6 addressing involves several steps, including adding configuration settings to the notes.ini file for the Lotus Domino server.

Procedure

1. Enable support for both IPv4 and IPv6 addresses in Lotus Domino by adding the following settings to the notes.ini file:
   tcp_enableipv6=1
   DONT_USE_REMEMBERED_ADDRESSES=1
2. If you want to be able to use a Lotus Notes client to access the server with an IPv6 address, add the IPv6 information to the Domino server configuration by running the CHGDOMSVR command as follows:
   a. On any IBM i command line, type CHGDOMSVR and press F4 to display the command prompt.
   b. Specify the Lotus Domino server name and press Enter to display additional parameters. Then page down to display the TCP/IP port options prompt.
   c. Type a plus sign (+) in the entry field that follows the prompt (as shown below) and press Enter.

   Log client session events . . . . *SAME
   TCP/IP port options: +
   Communications port . . . . . . *SAME

   This displays the current TCP/IP port options.
   d. Page down to display a second section, where you can enter information for the additional TCP/IP port. Specify the following settings:

<table>
<thead>
<tr>
<th>Communications port:</th>
<th>TCPIPV6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet address:</td>
<td>Specify the explicit IPv6 address (not the host name).</td>
</tr>
<tr>
<td>Enable port:</td>
<td>*YES</td>
</tr>
</tbody>
</table>

   For the remaining parameters, specify the options of your choice, and then press Enter.
   e. Now press Enter to run the command.
   f. Verify that the port options were updated in the notes.ini file to look like this:

   Ports=TCPIP,TCPIPV6
   TCPIP=TCP,0,15,0,,12288
   TCPIPV6=TCP,0,15,0,,12288
   TCPIP_TcpIPaddress=0,Domino_server’s_explicit_IPv4_address
   TCPIPV6_TcpIPaddress=0,Domino_server’s_explicit_IPv6_address

3. Verify that the server host table and the Domain Name Server use the server’s IPv6 address. Both the IPv4 and IPv6 address should map to the same host name.

   You should have set these values when setting up your IBM i server before installing Lotus Domino; for information, see the section Preparing the TCP/IP environment on IBM i.

   The contents of the Domain Name Server should be 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.

4. Restart the Lotus Domino server so your changes can take effect.

5. Determine which IP address must be added to the HTTP hostname field in the server document:

   The choice of IP address depends on how the Domain Name Server resolves the host name. To determine which IP address to add to the server document, attempt to access the Sametime Community Server from a web browser using an IPv4 client:

   http://Community_Server_host_name

   - If you can access the server with the IPv4 client, update the Community Server’s “Server” document in Lotus Domino by adding the IPv6 address (see next step).
• If you cannot access the server with the IPv4 client, then update the Community Server’s "Server" document in Lotus Domino by adding the IPv4 address (see next step).

6. Update the **HTTP hostname** field in the Community Server’s "Server" document:
   b. In the Domino Administrator, navigate to the **Server** pane and double-click your Community Server’s name to open the corresponding "Server" document.
   c. In the “Server” document, navigate to the **Internet Protocols > HTTP** tab. The fully qualified host name of the Community Server should already appear in the **HTTP hostname** field.
   d. Update the **HTTP hostname** field by pressing Enter (used as a delimiter) and then adding the appropriate IP address as determined in the previous step.
      • If you were able to access the server with the IPv4 client, add the IPv6 address now.
      • If you were not able to access the server with the IPv4 client, add the IPv4 address now.

   **Attention:** Do not add both the IPv6 and the IPv4 addresses.
   e. Save and close the "Server" document.

7. Restart the HTTP service on the Lotus Domino server by running the following command in the console:
   ```
tell http restart
   ```

8. Verify that you can access the Community Server using either an IPv4 or an IPv6 client with the following URL:
   ```
   http://Community_Server_host_name
   ```

**Configuring Lotus Domino to support only IPv6 addressing on IBM i:**

Before an IBM Sametime Community Server can support IPv6 addressing on IBM i, 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 addressing involves several steps, including adding configuration settings to the notes.ini file for the Lotus Domino server.

For information on supporting IPv6 with Lotus Domino, see "IPv6 and Lotus Domino" in the Lotus Domino Administration information center.
Procedure

1. Enable support for IPv6 addresses in Lotus Domino by adding the following settings to the `notes.ini` file:
   - `tcp_enableipv6=1`
   - `DONT_USE_REMEMBERED_ADDRESSES=1`

2. Update the Domino TCP/IP port settings in the `notes.ini` file so they only specify the IPv6 address, like this:
   - `Ports=TCPIPV6`
   - `TCPIPV6=TCP,0,15,0,,12288`
   - `TCPIPV6_TcpIPaddress=0,Domino_server's_explicit_IPv6_address`

3. Update the `stcommsrvrtk.jar` file in the Lotus Domino installation directory:
   To support IPv6–only addressing for a Sametime Community Server running on IBM i, you must replace the `stcommsrvrtk.jar` file with a newer version. Run the following command, where "8xx" is the version of Lotus Domino that you are using for your Community Server:
   ```
   CPY OBJ('/QIBM/ProdData/LOTUS/sametime/stcommsrvrtk.jar') TODIR('/QIBM/ProdData/LOTUS/domino8xx') REPLACE(+YES) OWNER(+KEEP)
   ```
   For example, if your Community Server is running on a Domino 8.0.2 server, run this command:
   ```
   CPY OBJ('/QIBM/ProdData/LOTUS/sametime/stcommsrvrtk.jar') TODIR('/QIBM/ProdData/LOTUS/domino802') REPLACE(+YES) OWNER(+KEEP)
   ```

4. Verify that the server host table and the Domain Name Server use the server’s IPv6 address, which is mapped to the host name.
   You should have set these values when setting up your IBM i server before installing Lotus Domino; for information, see the section Preparing the TCP/IP environment on IBM i.

5. Restart the Lotus Domino server so your changes can take effect.

6. Determine whether you need to add the IPv6 address to the **HTTP hostname** field in the Community Server’s "Server" document in Lotus Domino:
   This depends on how the Domain Name Server resolves the host name. To determine whether you need to add the IPv6 address to the "Server" document, attempt to access the Community Server from a web browser using an IPv6 client:
   ```
   http://Community_Server's_host_name
   ```
   - If you do need to add the IPv6 address, continue with step 7; otherwise, skip to step 8.

7. To add the IPv6 address to the **HTTP hostname** field in the server document, complete the following substeps:
   b. In the Domino Administrator, navigate to the Server pane and double-click your Community Server’s name to open the corresponding "Server" document.
   c. In the "Server" document, click **Internet Protocols > HTTP**.
      The fully qualified host name of the Community Server should already appear in the **HTTP hostname** field.
   d. Update the **HTTP hostname** field by pressing **Enter** (used as a delimiter) and then adding the IPv6 address to the field.
   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:
8. Verify that you can access the Community Server from a web browser using an IPv6 client:

http://Community_Server’s_host_name

Configuring the Sametime Community Server to support IPv6 addressing on IBM i:

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 87. Accepted values for STLINKS_HOST

<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:

  \[
  VPMX_DISABLE_CONFIGUPDATE=1
  VPMX_HOSTNAME=::,0.0.0.0
  VPMX_PORT=1533
  VPHMX_HOSTNAME=::,0.0.0.0
  VPHMX_PORT=8082
  \]

  Where:
  - VPMX_DISABLE_CONFIGUPDATE=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 88. 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>
</tbody>
</table>
Table 88. Accepted values for VPMX_HOSTNAME (continued)

<table>
<thead>
<tr>
<th>Type of address</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<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 89. 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.

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.

Installing and setting up a Windows-based stand-alone Community Services multiplexer for use with Sametime on IBM i

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 98
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 on Windows:

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 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 from Sametime on IBM i:

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 93
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 582
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 from Sametime on IBM i:
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 used by Sametime on IBM i:
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 used by Sametime on IBM i:

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.

   VPMX_ASSUME_COMMUNITY_ISFUNC=1

7. Save the sametime.ini file.

Enabling IPv6 on a multiplexer used by Sametime on IBM i:

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
   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 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).
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 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 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>

Table 90. Accepted values for VPMX_HOSTNAME

Table 91. Accepted values for VPHMX_HOSTNAME
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.

(Optional) Load-balancing client connections to multiplexers used by Sametime on IBM i:

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 193
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 195
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 i)**

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 88
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 (IBM i):

Create a Domino server cluster, then register Community Servers in the cluster.

Replicating the Domino Directory across all servers in the cluster (IBM i):

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 (IBM i):

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.
When the administrator client starts, make sure the Sametime server is the current server.

Click the **Configuration** tab.

In the **Tasks** pane, expand **Server** and click **All Server Documents**.

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.

Click **Add to Cluster**.

In the **Cluster Name** dialog box, click **Create New Cluster**, and then click OK.

Type the name of the new cluster and then click **OK**.

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><strong>Action</strong></th>
<th><strong>What you should see</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Domino Administrator, expand <strong>Clusters</strong> 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 <strong>Configuration</strong> tab, expand <strong>Cluster</strong>, and then click <strong>Clusters</strong>.</td>
<td>1. The name of the cluster followed by the names of the cluster servers displayed in the <strong>Results</strong> pane.</td>
</tr>
<tr>
<td>2. In the <strong>Results</strong> pane, open the Server documents of the servers you added to the cluster.</td>
<td>2. The name of the cluster in the <strong>Cluster name</strong> field on the <strong>Basics</strong> tab.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the <strong>Server</strong> pane, and then click the <strong>Server - Status</strong> tab.</td>
<td>CLDBDIR (the Cluster Database Directory Manager) and CLREPL (the Cluster Replicator) in the <strong>Task</strong> list.</td>
</tr>
<tr>
<td>From the Domino Administrator, click a cluster server in the <strong>Server</strong> pane, and then click the <strong>Files</strong> 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 (IBM i):**

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.

Copying a cluster document to all Sametime Community servers (IBM i):

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 (IBM i):

After configuring a cluster of IBM Sametime servers on IBM i, 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, 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. 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.
3. Complete the following steps for each server in the cluster to verify each server document’s Net Address field:
   a. From a Lotus Notes client, open the Server document for the Sametime Community Server you are working on.
   b. Click the Ports tab.
   c. Click the Notes Network Ports tab and check the Net Address field:
      This field should contain the fully qualified host name of the current Sametime Community Server. If the field contains an IP address change it now.
   d. Click Save if you made a change, and then click Close to close the Server document.
   e. If you changed the Server document, restart the server.
   f. Remember to repeat this task for every server in the cluster.
4. Now run the registerSTCluster.sh registration utility from one of the servers in the cluster:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: QSH
   b. Navigate to the server's sametime_server_data_directory/console directory; for example: cd /stserver/data/console.
   c. Run the shell script:
      registerSTCluster.sh
   d. As the registration utility runs, you will be prompted to enter the following information:

| Cluster name                  | Type the name you created when you configured the cluster, and press Enter. |
|                              |                                                                         |
| Location of notes.ini file    | Type the full path to the Sametime Community Server data directory containing notes.ini file (for example, /stserver/data), and press Enter. |
**Lotus Domino administrator user name**

This is the account that you created for managing the 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.

- When the registration script completes, press F3 to exit QSH.

  The utility registers the cluster, generating a log file called ConsoleUtility.log and storing it in the consoles/logs directory.

5. Restart the Sametime Community Server where you ran the registration utility.

*Creating a community ID for all nodes in a cluster (IBM i):*

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:
   ```ini
   ST_COMMUNITY_ID=community_name
   ```
   For example, the following value names the community sametime.example.com:
   ```ini
   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 (IBM i):*

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 stand-alone multiplexers (IBM i):**

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 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 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 (IBM i):

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 csclusters.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.

The diagram depicts the flow of client connections to the rotating DNS, which then directs them to the multiplexers. The multiplexers route the connections to the Sametime servers in the cluster. The Sametime servers are part of a Domino server cluster, and there is an LDAP directory server as well.

**Rotating DNS Limitations with cached DNS resolve requests (IBM i):**

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 (IBM i):

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 on IBM i
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 for IBM**
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 on IBM i:**

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>
</table>
| Port 80                                 | 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. |
| Alternate HTTP port (8088)              | 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.  
**Note:** 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. |
| Port 389                                | 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.                                                                 |
| Port 443                                | The Domino HTTP server listens for HTTPS connections on this port by default.                                                                                                                                 |
| Port 1352                               | The Domino server on which Sametime is installed listens for connections from Notes clients and Domino servers on this port.                                                                                                               |
| Port 9092                               | 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.                                                           |
### Default Port

<table>
<thead>
<tr>
<th>Port 9094</th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 206 for a discussion on resolving access to this port.</td>
<td></td>
</tr>
</tbody>
</table>

### 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.  
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. |
| 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. |
<table>
<thead>
<tr>
<th>Default Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 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 8082.</td>
</tr>
</tbody>
</table>

Changing the HTTP port of a Domino HTTP server on IBM i:

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.)
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 on IBM i:**

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 IBM i 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 on IBM i:*

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 connections for Sametime on IBM i**

Configure the IBM Sametime Community Server to work with LDAP and Domino directories.

**Specifying a user's login ID for Sametime on IBM i:**

Specify an LDAP attribute that is appropriate for logging in to IBM Sametime.

**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. 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 **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 for Sametime on IBM i:

If your Sametime servers connect to an Active Directory (LDAP) server, you must assign the "DistinguishedName" directory attribute to be the internal ID for Sametime users. Doing so guarantees that Active Directory returns the DistinguishedName attribute in the same case-sensitive and space-sensitive format. Allowing Sametime to use that consistent attribute for the internal userID prevents awareness problems caused by ambiguous internal userIDs.

About this task

If you do not assign the "DistinguishedName" directory 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.

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.

Mapping the user ID to a unique directory attribute for Sametime on IBM i:

If you map the Sametime user ID to a unique LDAP directory attribute, 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, does not trigger a user ID change when a name changes.
About this task

Sametime provides the 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. RESOLVE mode migrates the \texttt{VpUserInfo.nsf} database, from the old user ID to the new user ID.

With this release, IBM Sametime uses the UUID LDAP attribute by default, which ensures ID uniqueness. The UUID for the LDAP directory type can be chosen for the Sametime user ID. Its value will never change.

- Lotus Domino LDAP: dominounid
- IBM Tivoli Directory Server: ibm-entryuuid
- Microsoft Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

If you are upgrading from a previous release, you can map the Sametime user ID to an LDAP directory attribute that is unlikely to change.

Preparing user IDs for RESOLVE mode for Sametime on IBM i:

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

You change the Sametime LDAP configuration to map the user ID to a directory attribute in the person entry that is not bound to change. This change eliminates the need for running the Name Change tool. The Sametime Community server stores contact and privacy lists in the \texttt{VpUserInfo.nsf} file. Name Change RESOLVE mode migrates that database, from the old user ID to the new user ID

Note: The old name will still appear in the contact list for users that have previously added them.

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 \texttt{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. In case you prefer to use an existing attribute instead of modifying the schema, choose an attribute that is not bound 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: dominounid
- Novell Directory Server (NDS): guid
- SunOne: nsuniqueid
- Active Directory: 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
lookup 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 on IBM i:

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 is 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 on IBM i:

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 for Sametime on IBM i:**

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, "Mapping the user ID to a unique directory attribute."

- Create a CSV file with the RESOLVE mode indicated.
- Create a name change task.
- 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.

**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 each and every user ID in the database against the directory, and replaces...
the old user ID with the directory user ID. 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.

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 212.

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."


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" on page 212
   - "Running the name change utility in RESOLVE mode on UNIX" on page 217
   - "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 IBM i:*

Follow these steps to run the name conversion utility in RESOLVE mode on IBM i.

**Procedure**

1. Stop the IBM Sametime Community Server, but leave the Domino server running by running TELL STADDIN2 QUIT from the Domino console.

2. Go to the OS/400 command line 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,StCommunity,SOFT
   #SERVERAPP StPolling,StCommunity,SOFT
   ```

3. Restart the Sametime Community Server by running LOAD STADDIN2 from the Domino console. 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.

4. Go to the OS/400 command line, and enter the following command: "QSH" This opens up a command line where the Name Change task is run.
5. Type the following commands:
   
   ```
   cd <data directory>
   stnamechange <data directory>
   ```

6. Use the Sametime Administration Tool to change the Sametime Community Server LDAP configuration. See “Change your Sametime Community Server LDAP configuration” on page 213.

7. Stop the IBM Sametime Community Server, but leave the Domino server running by running TELL STADDIN2 QUIT from the Domino console.

8. Go to the OS/400 command line and edit the `data-directory/STCommLaunch.dep` file and remove the number sign # from the following line.
   ```
   SERVERAPP StMux,StCommunity,SOFT
   SERVERAPP StPolling,StCommunity,SOFT
   ```

Creating custom Java classes for searching the LDAP for Sametime on IBM i:

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 for Sametime on IBM i:

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;
        }
    }
    return escapedName.toString();
}
```
default:
    escapedName.append(name.charAt(i));
    i++;
}
}
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 for Sametime on IBM i:

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 on IBM i:*
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 on IBM i:**

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:

   ```ini
   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 LDAP settings for Sametime on IBM i:

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 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 214
The resolve and the authentication filters need to be customized Java filters.

Preparing the Sametime Community server on IBM i for users
Before deploying clients, set up the login and licensing requirements that suit your environment.

Assigning users to a home Sametime Community Server on IBM i:
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 on IBM i:

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 on IBM i:**

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 for Sametime on IBM i:

You can manage the manner and order of client logins to IBM Sametime.

Related concepts
“Supporting older Sametime clients during migration” on page 1409
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 for Sametime on IBM i:

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.

   ```
   [Config]
   VPS_ALLOWED_LOGIN_TYPES=130B,130A
   ```

   **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.
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 for Sametime on IBM i:**

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:
   ```ini
   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.
   ```ini
   VPS_EXCLUDED_LOGIN_TYPES=clienttype1, clienttype2
   ```
   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.
   ```ini
   VPS_EXCLUDED_LOGIN_TYPES=1002, 1304
   ```
5. Save the sametime.ini file.

**Configuring the preferred login list for Sametime on IBM i:**

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,1308,1306,1304,1435,1434,1433,1432,
   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 on IBM i:

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 127

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.

Disabling or enabling meetings on an IBM i Sametime Standard server:

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.
About this task

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.

Follow these steps to use the CHGLSTDOM command to disable meetings on a particular server.

Procedure

1. On any IBM i command line, type the following and press F4:
   
   CHGLSTDOM

2. On the Change Sametime on Domino display, set Web Conferencing to *NO and press Enter.

What to do next

If you decide to enable Web Conferencing on the server later, run the CHGLSTDOM command again, specifying *YES for Web Conferencing.

Related concepts

“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 127

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.

Related tasks

“Running the community server installation program on IBM i” on page 680

Run the installation program on the machine where you plan to install a Sametime Community Server.

Creating meeting user groups in a mixed-license environment on IBM i:

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 229
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 on IBM i:

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.
Installing a Sametime Proxy Server on IBM i

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, 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.

Related concepts

“Configuring a Sametime Proxy Server” on page 1650
Configure connection settings to enable the IBM Sametime Proxy Server to communicate with other servers in the deployment.

Preparing the Sametime Proxy Server installation file on IBM i

Follow these steps to customize the response.properties file to prepare for installing the Sametime Proxy Server on IBM i.

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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
2. Extract the installation files to the directory where you stored the installation package.
a. From an IBM i command line, run the following command to start the QShell Interpreter:

QSH

b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:

cd /MySametimePackages

c. Run the following shell command, specifying the name of the .zip file:

jar -x name_of_installation_package

d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:

/MySametimePackages/SametimeProxyServer/IBMi/stii_stp/licenses

For DVD:

/qopt/volume_id/IBMi/stii_stp/licenses

4. Navigate to the program image directory; for example:

/MySametimePackages/SametimeProxyServer/IBMi/stii_stp

For DVD:

/qopt/volume_id/IBMi/stii_stp

5. Make a copy of the stp.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
   - Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Meeting Server. This is necessary for live names to work correctly in meeting rooms.

**Example**

"Default Sametime Proxy Server installation file on IBM i"

**Default Sametime Proxy Server installation file on IBM i:**

The response.properties file contains settings used to install or upgrade a Sametime Proxy Server on IBM i.
The default content for the response.properties file for installing the Sametime Proxy Server follows:

```
# Sametime 8.5.2 Proxy Server Installation Properties file for IBM i
#
# Preparing to Install
#
# This file is used for either installing a new Sametime 8.5.2 Proxy Server or
# upgrading a Sametime Proxy Server to Sametime 8.5.2.
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime Proxy Server on IBM i and
# running the installation program.
#
# The Information Center is available online from the Lotus Sametime documentation
# library:
#
#   http://www.ibm.com/developerworks/lotus/documentation/sametime
#
# License Acceptance
#
# By changing the silentInstallLicenseAcceptance property in this response file
# to "true", you agree that you have reviewed and agree to the terms of the
# IBM International Program License Agreement accompanying this program, which
# is located at CD_ROOT\IBM\stii_stp\licenses.
#
# If you do not agree to these terms, do not change the value or otherwise
# download, install, copy, access, or use the program and promptly return the
# program and proof of entitlement to the party from whom you acquired it to
# obtain a refund of the amount you paid.
#
# Valid values for silentInstallLicenseAcceptance:
#   true - Accept the license terms continue with product installation.
#   false - Decline the license terms and do not install the product.
#
# silentInstallLicenseAcceptance=false
#
# Installation Type
#
# Set this value to the type of installation you wish to perform.
# The setting determines the WAS nodes that are created during installation.
#
# Valid values for install.type:
#   Cell - (default) Cell installation, recommended for new deployments.
#     Creates both a deployment manager node and a primary application
#     server node with the Sametime Proxy Server installed. The primary
#     node is federated into the deployment manager's cell.
#     If the cell installation already exists, both the deployment manager
#     node and the primary application server node are upgraded. Secondary
#     nodes must be upgraded separately.
#   PN - Primary Node installation.
#     Creates a primary application server node with the Sametime Proxy
#     Server installed or upgrades an existing primary application server
#     node to Sametime 8.5.2.
#     For new installations, the primary node must be federated into the
#     Deployment Manager's cell when registering the node with the
#     Sametime System Console.
#   SN - Secondary Node installation.
#     Creates a secondary application server node with the Sametime Proxy
#     Server installed or upgrades an existing secondary application server
#     node to Sametime 8.5.2.
```

Chapter 3. Installing 749
For new installations, the node is federated into the Deployment Manager's cell specified by the Secondary Node Properties (later in this file). After installation, this node may be clustered with the primary node in the cell. When upgrading a secondary node, the node's federation and clustering status is not changed.

install.type=Cell

# Websphere Settings
# These values are used when configuring the Websphere Application Server nodes.
# stwas.was.hostname - (required) For new installs, specify the fully qualified hostname that your WAS server will use.
# For upgrades, specify the fully qualified hostname of the existing WAS server.
# stwas.was.admin.id - (required) For new installs, specify the user ID that you will use to log into the Deployment Manager's Integrated Solutions Console once security is enabled. This name must not exist as a user in any LDAP directory that you plan to connect to the server. For upgrades, specify the user ID that you use to log into the Deployment Manager's Integrated Solutions Console.
# stwas.was.admin.password - (required) The password associated with the user ID specified for 'stwas.was.admin.id'
# stwas.was.hostname=
# stwas.was.admin.id=
# stwas.was.admin.password=

# Secondary Node Settings
# These settings are used only for Secondary Node installations (SN). For new installations, the settings specify the cell that the secondary node should be federated into. For upgrades, the settings specify the cell that the existing secondary node is already federated into. The Deployment Manager for the cell must be started before running a secondary node install or upgrade.
# These values are ignored if not installing or upgrading a secondary node.
# stwas.sn.dm.hostname - (required for 'SN' install) The fully qualified hostname of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade). The Deployment Manager must be running and listening on this hostname or the install will fail.
# stwas.sn.dm.soap.port - (required for 'SN' install) The soap port of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade). The Deployment Manager must be running and listening for SOAP connections on this port or the install will fail.
# stwas.sn.dm.hostname=
# stwas.sn.dm.soap.port=

# STATIC Websphere Settings
# These settings are used by the installer to control how Websphere is configured during installation. The values have been set specifically for installing the
### DO NOT CHANGE ###
stwas.was.installlocation=/QIBM/ProdData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.profilelocation=/QIBM/UserData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.dpfile.default=STPDMgrProfile
stwas.was.serverprofile.default=STPAppProfile
stwas.was.snsprofile.default=STPSNAppProfile
stwas.was.appserver=STProxyServer
### DO NOT CHANGE ###

# Sametime Community Server Information

# These settings are used for new installs to specify the Sametime Community Server that the Proxy Server will connect to. The settings in this section are not used for upgrade installations.

# stp.sametime.community.server.hostname - (required) The fully qualified host name of the Sametime Community Server

# stp.sametime.community.server.port - (required) The server-to-server connection port of the Sametime Community Server

stp.sametime.community.server.hostname=
stp.sametime.community.server.port=1516

# End of File

### Installing a Sametime Proxy Server (IBM i) ###

Run the install script to set up the Sametime Proxy Server on IBM i.

**Before you begin**

If you intend to install from a downloaded image, you should have downloaded the proxy server installation package. For all installations, you should have completed the preparation steps.

**About this task**

Follow these steps to install the Sametime Proxy Server and WebSphere Application Server.

**Procedure**

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH

4. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:

   /MySametimePackages/SametimeProxyServer/IBMi/stii_stp
   For DVD:

   cd /qopt/volume_ID/IBMi/stii_stp

5. Start the installation with the following shell command:
install_stp.sh
-Dinstall.response.file=path_and_name_of_customized_response.properties_file

6. When the installation completes, press F3 to exit QSH.

7. If the Sametime Proxy server is installed on a system with multiple active IP addresses, follow these steps. 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.
      1) Find the stproxyconfig.xml file in the Proxy Server's deployment manager profile configuration in this location:
          /qibm/UserData/WebSphere/AppServer/v7/SametimeWAS/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 logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STPROXY_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STPROXY_20091215_0307.log
What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

If you have installed both the Sametime Meeting Server and the Sametime Proxy Server on the same system, you must update the table of Host Aliases associated with the Sametime Proxy Server’s `default_host` virtual host so that it does not use the same host name and IP address as the Sametime Meeting Server. Follow the steps in Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine.

Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 581
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.
“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Registering a Sametime Proxy Server on IBM i with the Sametime System Console
After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

Before you begin
Before you register the server, verify that you have completed the following tasks.

Sametime Community Server
• The community server must be configured to use an LDAP directory.
• The community server must be started.
• The Sametime System Console must be started.
• The LDAP server must be started.
• The LDAP server must be connected to the Sametime System Console.

Sametime Proxy Server
• The Sametime System Console must be started.
• The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.
• When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

Sametime Meeting Server
• The Sametime System Console must be started.
• The LDAP server must be started.
• The LDAP server must be connected to the Sametime System Console.
The Meeting Server database (STMS) must be connected to the Sametime System Console.

When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

**About this task**

Working from the Sametime server that you want to connect with the console, follow these steps to update properties files and run the registration utility to register the server with the console.

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

- **console.properties**
- **productConfig.properties**

**Procedure**

1. On the Sametime server you plan to register, navigate to the console directory.
   - **Community Server**
     The console directory is a subdirectory of the Sametime Community server data directory.
   - **Proxy Server**
     `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`
     The date and time indicate when the Proxy Server was installed.
   - **Meeting Server**
     `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`
     The date and time indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with 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 92. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
</tbody>
</table>
Table 92. `console.properties` settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 “true.”</td>
</tr>
</tbody>
</table>

4. Now update the `productConfig.properties` file with the values needed for the server you are registering. Then save the file.

   Required values not listed below are filled in automatically.

   - **Sametime Community Server**
     
     - **DepName**: Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.

   - **Sametime Proxy Server**
     
     - **WASPassword**: Specify the password associated with the WASUserID.
     
     If you are registering a primary node, you must specify additional values for the cell where the node will be added:
     
     - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
     
     - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

   - **Sametime Meeting Server**
     
     - **DBAppPassword**: Specify the password associated with the database ID.
     
     - **WASPassword**: Specify the password associated with the WASUserID.
     
     - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.
     
     If you are registering a primary node, you must specify additional values for the cell where the node will be added:
     
     - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
     
     - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

5. If you are registering a Sametime Community Server, start the server.

   Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```
   QSH
   ```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   - **Sametime Community Server**
     
     ```
     registerSTServerNode.sh
     ```

     When prompted, specify the following information:
     
     - Full path to the Sametime Community server data directory where the notes.ini file is located.
     
     - The Community Server Administrator ID and password.

   - **Sametime Proxy Server**
     
     ```
     registerProduct.sh
     ```
If registering a primary node, run the following command:
`registerProduct.sh -federateNode`

- **Sametime Meeting Server**
  
registrerProduct.sh
If registering a primary node, run the following command:
`registerProduct.sh -federateNode`

9. When the registration script completes, press F3 to exit QSH.

**Verifying a Sametime Proxy Server installation on IBM i**

Open the Sametime Web client to verify that the installation was successful.

**About this task**

Follow these steps to verify the installation.

**Procedure**

1. Using a browser, log in to the Sametime Proxy Server application with the following command:
   
   `http://serverhostname.domain:port/stwebclient/index.jsp`
   
   Replace `serverhostname.domain` with your server name and add the port number.
   
   **Tip:** To verify the HTTP port number being used by the 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:
   
   `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs/AboutThisProfile.txt`
   
   For example:
   
   `http://stproxy1.example.com:9081/stwebclient/index.jsp`

2. Log in to the Sametime Client and verify that you can create or view contacts.

**Related tasks**

"Logging in to the console" on page 584

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 a Sametime Proxy Server on IBM i 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 Multiplexers, 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.

**Clustering Sametime Proxy Servers (IBM i)**

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 88
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.

**Related tasks**

“Registering a Sametime Proxy Server on IBM i with the Sametime System Console” on page 753
After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

**Setting clocks on the Sametime Proxy Servers to be clustered (IBM i):**

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 (IBM i):

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 582

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

Guided activity: Clustering Sametime Proxy Servers (IBM i):

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 Manger’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 (IBM i):**

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 (IBM i):*

   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 an IBM i 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:
      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 93. 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>Cluster: st-cluster.example.com</td>
<td>Deployment Manager (Sametime System Console)</td>
<td>192.0.2.3</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 an IBM i 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 an IBM i 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 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 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 for an IBM i 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.
   - **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:
   - Open a command window on the load balancer server.
   - Start the load balancer's Dispatcher process by clicking Start > Control Panel > Administrative Tools > Services. right-click IBM Dispatcher (ULB), and then click Start.
   - 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.
   - 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.

Installing a Sametime Meeting Server on IBM i

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, 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.

Related tasks
“Configuring a Sametime Meeting Server” on page 1675
This section describes how to configure a Sametime Meeting Server.

Preparing the meeting server installation file on IBM i

Follow these steps to customize the response.properties file to prepare for installing the Sametime Meeting Server on IBM i.

Before you begin

You should have completed the preparation steps in “Preparing to install Sametime on IBM i.”
About this task

Skip the first two steps if you are installing from physical media.

Procedure
1. Download the installation package if you have not already done so.
   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
2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:
      cd /MySametimePackages
   c. Run the following shell command, specifying the name of the .zip file:
      ajar -x name_of_installation_package
   d. Press F3 to exit QSH.
3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms/licenses
   For DVD:
   /qopt/volume_ID/IBMi/stii_stms/licenses
4. Navigate to the program image directory, for example:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   For DVD:
   /qopt/volume_ID/IBMi/stii_stms
5. Make a copy of the stms.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.
6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   • For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
For the database.db.user.id and database.db.user.password settings in the properties file, specify the user profile and password you created to be the owner of the Meeting Server database schemas.

Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Sametime Meeting Server. This is necessary for live names to work correctly in meeting rooms.

Example

“Default meeting server installation file for IBM i”

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Default meeting server installation file for IBM i:

The response.properties file contains settings used to install or upgrade a Sametime Meeting Server on IBM i.

The default content for the response.properties file for installing the Sametime Meeting Server follows:

```
# Sametime 8.5.2 Meeting Server Installation Properties file for IBM i
#
# Preparing to Install
#
# This file is used for either installing a new Sametime 8.5.2 Meeting Server or
# upgrading a Sametime Meeting Server to Sametime 8.5.2.
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime Meeting Server on IBM i and
# running the installation program.
#
# The Information Center is available online from the Lotus Sametime documentation
# library:
#
#   http://www.ibm.com/developerworks/lotus/documentation/sametime
#
# License Acceptance
#
# By changing the silentInstallLicenseAcceptance property in this response file
# to "true", you agree that you have reviewed and agree to the terms of the
# IBM International Program License Agreement accompanying this program, which
# is located at CD_ROOT\IBM\stii_stms\licenses.
#
# If you do not agree to these terms, do not change the value or otherwise
# download, install, copy, access, or use the program and promptly return the
# program and proof of entitlement to the party from whom you acquired it to
# obtain a refund of the amount you paid.
#
# Valid values for silentInstallLicenseAcceptance:
```
true - Accept the license terms continue with product installation.
false - Decline the license terms and do not install the product.
silentInstallLicenseAcceptance=false

Installation Type

Set this value to the type of installation you wish to perform.
The setting determines the WAS nodes that are created or upgraded during installation.
Valid values for install.type:
Cell - (default) Cell installation, recommended for new deployments.
    Creates both a deployment manager node and a primary application server node with the Sametime Meeting Server installed. The primary node is federated into the deployment manager's cell.
    If the cell installation already exists, both the deployment manager node and the primary application server node are upgraded. Secondary nodes must be upgraded separately.
PN - Primary Node installation.
    Creates a primary application server node with the Sametime Meeting Server installed or upgrades an existing primary application server node to Sametime 8.5.2.
    For new installations, the primary node must be federated into the Deployment Manager's cell when registering the node with the Sametime System Console.
SN - Secondary Node installation.
    Creates a secondary application server node with the Sametime Meeting Server installed or upgrades an existing secondary application server node to Sametime 8.5.2.
    For new installations, the node is federated into the Deployment Manager's cell specified by the Secondary Node Properties (later in this file). After installation, this node may be clustered with the primary node in the cell.
    When upgrading a secondary node, the node's federation and clustering status is not changed.
install.type=Cell

Websphere Settings

These values are used when configuring the Websphere Application Server nodes.

stwas.was.hostname - (required) For new installs, specify the fully qualified hostname that your WAS server will use.
    For upgrades, specify the fully qualified hostname of the existing WAS server.

stwas.was.admin.id - (required) For new installs, specify the user ID that you will use to log into the Deployment Manager's Integrated Solutions Console once security is enabled. This name must not exist as a user in any LDAP directory that you plan to connect to the server.
    For upgrades, specify the user ID that you use to log into the Deployment Manager's Integrated Solutions Console.

stwas.was.admin.password - (required) The password associated with the user ID specified for 'stwas.was.admin.id'

stwas.was.hostname=
stwas.was.admin.id=
stwas.was.admin.password=

Chapter 3. Installing
# Secondary Node Settings

# These settings are used only for Secondary Node installations (SN).
# For new installations, the settings specify the cell that the secondary node
# should be federated into.
# For upgrades, the settings specify the cell that the existing secondary node is
# already federated into.
# The Deployment Manager for the cell must be started before running a secondary
# node install or upgrade.
# These values are ignored if not installing or upgrading a secondary node.
#
# stwas.sn.dm.hostname - (required for 'SN' install) The fully qualified hostname
# of the Deployment Manager for the cell that the secondary node will be
# federated into (new install) or is already federated into (upgrade).
# The Deployment Manager must be running and listening on this hostname
# or the install will fail.
#
# stwas.sn.dm.soap.port - (required for 'SN' install) The soap port of the
# Deployment Manager for the cell that the secondary node will be
# federated into (new install) or is already federated into (upgrade).
# The Deployment Manager must be running and listening for SOAP connections
# on this port or the install will fail.

stwas.sn.dm.hostname=
stwas.sn.dm.soap.port=

# STATIC Websphere Settings

# These settings are used by the installer to control how Websphere is configured
# during installation. The values have been set specifically for installing the
# Sametime Meeting Server.
# DO NOT CHANGE this settings unless instructed to do so by IBM Support.
#
# *** DO NOT CHANGE ***

stwas.was.installlocation=/QIBM/ProdData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.profilelocation=/QIBM/UserData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.dmprofile.default=STMDMgrProfile
stwas.was.serverprofile.default=STMAppProfile
stwas.was.nsserverprofile.default=STMSNAppProfile
stwas.was.appserver=STMeetingServer

# *** DO NOT CHANGE ***

# Database Settings

# These settings define the database that will be used for the Sametime Meeting
# Server.
# For new installations, they control how the database resources are configured
# in the Websphere Application Server.
# For upgrades, they allow the installer to connect to the database resources.
#
# database.db.hostname - (required) The fully qualified hostname of the system
# where the database is running.
#
# database.db.user.id - (required) The user ID that will be used when making a
# connection to the database.
#
# database.db.user.password - (required) The password for the user ID specified
# by database.db.user.id.

database.db.hostname=
database.db.user.id=
database.db.user.password=
# STATIC Database Settings

# These settings are used by the installer to control how database connections are configured during installation. The values have been set specifically for installing the Sametime Meeting Server.
# DO NOT CHANGE these settings unless instructed to do so by IBM Support.

### DO NOT CHANGE ###
database.db.type=db2_iseries
database.db.name=STMS
database.db.port=50000
### DO NOT CHANGE ###

# LDAP Settings

# These values are used for new installs to define the LDAP server that the Sametime Meeting Server will connect to.
# The settings in this section are not used for upgrade installations.

# ldap.hostname - (required) The fully qualified hostname of the LDAP server.
# ldap.port - (required) The port used to connect to the LDAP server.
# ldap.displayname - (required) Attribute for the displayname in Websphere Identity Manager. The default value is "cn".
# ldap.loginfield - (required) Indicates the attribute name used for login. The default value is "mail".
# ldap.basedn - The starting point for LDAP searches of the directory service.
# ldap.binddn - Specifies the Bind distinguished name (DN) that the meeting server will use to authenticate with the LDAP server. If not specified, the meeting server will use anonymous access.
# ldap.binddn.password - (required if ldap.binddn is set) Specifies the password that the meeting server will use to authenticate with the LDAP server.
# ldap.skip.ldap.config - If set to "true", the LDAP will not be configured during installation and you will need to complete the configuration manually. Only change this setting if you need LDAP to connect using SSL.

ldap.hostname=
ldap.port=389
ldap.displayname=cn
ldap.loginfield=mail
ldap.basedn=
ldap.binddn=
ldap.binddn.password=
ldap.skip.ldap.config=false

#

End of File

Creating the Meeting Server database schemas and tables on IBM i
Run the script to create the database schemas for the IBM Sametime Meeting Server on IBM i.
Before you begin

You should have prepared the Meeting Server installation file as described in "Preparing the Meeting Server installation file on IBM i."

About this task

On the IBM i system that will install the Sametime Meeting Server, follow these steps to create the database schema and tables:

Procedure

1. Log in with a user profile that has *ALLOBJ and *SECADM special authorities. These authorities are required to create the database schemas. The database schemas will be created on the system specified in your copy of the stms.default.response.properties file and owned by the user profile specified in the file.
2. From an IBM i command line, run the following command to start the QShell Interpreter:
   QSH
3. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example
   /MySametimePackages/SametimeMeetingServer/IBM/i/stii_stms
   For DVD:
   /qopt/volume_ID/IBM/i/stii_stms
4. The POLICY schema is shared by the Meeting Server and the System Console. If the POLICY schema already exists, the Meeting Server database setup script will only create the MTG schema.
   setupDB_stms.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file
5. When the script completes, press f3 to exit QSH.

Results

If the database schema creation was not successful, look at the script log for more information about what occurred during the attempt. Fix the problem, then try running the script again. The script log is stored in the following location:

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

stms_dbsetup_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

stms_dbsetup_20091215_0307.log

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Installing a meeting server on IBM i

Run the database schema and install scripts to set up the Sametime Meeting Server on IBM i.
Before you begin

If you intend to install from a downloaded image, you should have downloaded the meeting server installation package. For all installations, you should have completed the preparation steps. The database schemas required for the Meeting Server (MTG and POLICY) should already exist.

About this task

Follow these steps to install the Sametime Meeting Server and WebSphere Application Server.

Procedure

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   QSH
4. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   For DVD:
   cd /qopt/volume_ID/IBMi/stii_stms
5. Start the Meeting Server installation with the following shell command:
   install_stms.sh -Dinstall.response.file=path_and_name_of_customized_response.properties_file
6. When the script completes, press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STMEETINGS_yyyymmd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STMEETINGS_20091215_0307.log

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

If you have installed both the Sametime Meeting Server and the Sametime Proxy Server on the same system, you must update the table of Host Aliases associated
with the Sametime Proxy Server's `default_host` virtual host so that it does not use
the same host name and IP address as the Sametime Meeting Server. Follow the
steps in Deploying Sametime Proxy Server and Sametime Meeting Server on the
same machine.

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

**Connecting Sametime Meeting Server on IBM i 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 `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 582
When started, the Sametime System Console runs as a task in the WebSphere
Application Server administrative console.

**Sametime prerequisite: Connecting Sametime Meeting Server on IBM i 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.
   - 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.
   - 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.
   - 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.
   - In the **Database name** field, enter the name of the database you want to connect to.
   - 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.
   - In the **Application password** field, enter the password for the DB2 administrative user ID.
   - (Meeting Server or Gateway databases) If you are connecting to a database on an IBM i server, click **Hosted on IBM i**.
   - Click **Finish**.
Registering a Sametime Meeting Server on IBM i with the Sametime System Console

After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

Before you begin

Before you register the server, verify that you have completed the following tasks.

Sametime Community Server
- The community server must be configured to use an LDAP directory.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.
- The LDAP server must be connected to the Sametime System Console.

Sametime Proxy Server
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.
- When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

Sametime Meeting Server
- The Sametime System Console must be started.
- The LDAP server must be started.
- The LDAP server must be connected to the Sametime System Console.
- The Meeting Server database (STMS) must be connected to the Sametime System Console.
- When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

About this task

Working from the Sametime server that you want to connect with the console, follow these steps to update properties files and run the registration utility to register the server with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure
1. On the Sametime server you plan to register, navigate to the console directory.
   - Community Server
The console directory is a subdirectory of the Sametime Community server data directory.

- **Proxy Server**
  
  `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`

  The *date* and *time* indicate when the Proxy Server was installed.

- **Meeting Server**
  
  `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`

  The *date* and *time* indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with 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 94. `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. The value for SSCSSLEnabled is &quot;false.&quot; To determine the correct HTTP port, open the <code>AboutThisProfile.txt</code> 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. On IBM i, look for the <code>AboutThisProfile.txt</code> file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</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. Now update the `productConfig.properties` file with the values needed for the server you are registering. Then save the file.

   Required values not listed below are filled in automatically.

   - **Sametime Community Server**
     
     - **DepName**: Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.

   - **Sametime Proxy Server**
     
     - **WASPassword**: Specify the password associated with the WASUserID.

     If you are registering a primary node, you must specify additional values for the cell where the node will be added:

     - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
- **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

* Sametime Meeting Server
  - **DBAppPassword**: Specify the password associated with the database ID.
  - **WASPassword**: Specify the password associated with the WASUserID.
  - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.

If you are registering a primary node, you must specify additional values for the cell where the node will be added:
  - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
  - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

5. If you are registering a Sametime Community Server, start the server. Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```
   QSH
   ```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:
   - **Sametime Community Server**
     ```
     registerSTServerNode.sh
     ```
     When prompted, specify the following information:
     - Full path to the Sametime Community server data directory where the `notes.ini` file is located.
     - The Community Server Administrator ID and password.
   - **Sametime Proxy Server**
     ```
     registerProduct.sh
     ```
     If registering a primary node, run the following command:
     ```
     registerProduct.sh -federateNode
     ```
   - **Sametime Meeting Server**
     ```
     registerProduct.sh
     ```
     If registering a primary node, run the following command:
     ```
     registerProduct.sh -federateNode
     ```

9. When the registration script completes, press F3 to exit QSH.

**Verifying a Sametime Meeting Server installation on IBM i**

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.

Clustering Sametime Meeting Servers (IBM i)
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**

“Clustering Sametime servers for high enterprise availability” on page 88  
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.

**Related tasks**

“Registering a Sametime Meeting Server on IBM i with the Sametime System Console” on page 782  
After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

**Setting clocks on the Meeting Servers to be clustered (IBM i):**

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 Meeting Servers (IBM i):

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 582

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

Guided activity: Clustering Meeting Servers (IBM i):

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 Manger’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 Meeting Server cluster (IBM i):
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 Meeting Server cluster (IBM i):*

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 Meeting Server cluster (IBM i):**

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 Meeting Server cluster (IBM i):**

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 Meeting Server cluster (IBM i):**

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.
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 a Meeting Server cluster (IBM i):**

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 Meeting Server cluster (IBM i):**

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 (IBM i):

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 582
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 (IBM i):

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.

*Removing the Sametime product from the new node in a Meeting Server cluster (IBM i):*

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 in 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 a Meeting Server cluster (IBM i):*

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 > Proxy Servers.
   b. In the "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 in a Meeting Server cluster (IBM i):*

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 "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.
6. Synchronize all nodes in the cluster:
   b. Select all of the nodes in the cluster.
   c. Click Full Resynchronize.

Creating object cache instances for the WebSphere proxy server in a Meeting Server cluster (IBM i):

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 in a Meeting Server cluster (IBM i):

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.
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 for an IBM i Meeting Server cluster:
Install and configure IBM Load Balancer to distribute workload among a cluster of
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:
      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):</td>
</tr>
<tr>
<td>loadbal.example.com</td>
<td>(Cluster address)</td>
<td>192.0.2.15</td>
</tr>
<tr>
<td>Cluster:</td>
<td></td>
<td>Cluster: 192.0.2.0</td>
</tr>
<tr>
<td>st-cluster.example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fully qualified host name</td>
<td>Server's role in deployment</td>
<td>Server's IP address</td>
</tr>
<tr>
<td>--------------------------</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 for an IBM i 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 for an IBM i Meeting 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 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 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 for an IBM i 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:
   
   ```
   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 \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:

\begin{verbatim}
stms-cluster.example.com
\end{verbatim}

f. Add the cluster port:

\begin{verbatim}
dscontrol port add cluster's\_fully\_qualified\_host\_name@port
\end{verbatim}

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:

\begin{verbatim}
stms-cluster.example.com@80
\end{verbatim}

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

\begin{verbatim}
dscontrol server add cluster_host@port@primary_node

dcontrol server add cluster_host@port@secondary_node
\end{verbatim}

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:

\begin{verbatim}
stms-cluster.example.com@80@meetsvr1.example.com
\end{verbatim}

- \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:

\begin{verbatim}
stms-cluster.example.com@80@meetsvr2.example.com
\end{verbatim}

h. Add the cluster to the executor:

\begin{verbatim}
dscontrol executor add cluster's\_fully\_qualified\_host\_name
\end{verbatim}

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:

\begin{verbatim}
stms-cluster.example.com
\end{verbatim}

i. Start the manager:

\begin{verbatim}
dscontrol manager start
\end{verbatim}

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

\begin{verbatim}
dscontrol advisor start http 80
\end{verbatim}

k. Now you can stop the service:

\begin{verbatim}
dsserver stop
\end{verbatim}

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, loadbal1.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**.

### Preparing the Sametime Meeting server on IBM i for users

Before deploying clients, set up the preferences and login requirements that suit your environment.

**Preconfiguring a Sametime Meeting Server using managed preferences on IBM i:**

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 on IBM i:**

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
      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 1618
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 1581
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 on IBM i:

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,
   "stmsNNNNNNNNNNNNN", 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 1618
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 1581
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 a Sametime Gateway server on IBM i

Plan a deployment and install IBM DB2 and then one or more Sametime Gateway servers.

What to do next

After installation, you can perform other required and optional configuration tasks for Sametime Gateway.
• Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Configure LDAP for Sametime Gateway (IBM i)
• Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Connect servers to Sametime Gateway (IBM i)
• Set up SSL
• Other optional configuration steps

Related tasks

“Configuring a Sametime Gateway” on page 1679
Configure one or more IBM Sametime Gateway servers.

Creating the Gateway database schemas and tables on IBM i

Before you install Sametime Gateway, you must create the DB2 database, including tables and bufferpools, needed by Sametime Gateway. Sametime Gateway stores community settings and custom properties in the database.

About this task

For a multi-server installation, you should perform the steps once on the IBM i server where you want to host the data for Sametime Gateway. Afterwards, when you install Sametime Gateway, you use the host name of that IBM i server when specifying the server name on the database information panel of the wizard.

On the IBM i system that will host your database, proceed as follows:

Procedure

1. Create a user profile on the system that will be the owner of the schema created for the Sametime Gateway data. The profile that you create can have a user class of *USER, and will not require special authorities.
2. Log in as the profile that will be the owner of the schema.
3. From the installation media, copy the Sametime Gateway installation image to a temporary directory \TMP\SametimeGateway and unzip the contents.

4. Locate a copy of \TMP\SametimeGateway\database\db2_iseries\createDbi50S and copy it to a temp directory in the IFS of the database server.

5. On the IBM i system, start a QSHELL session. From an IBM i command line, type the command:
   
   QSH

6. Change to the temp directory where you copied the file createDbi50S and type the following command:
   
   createDbi50S <schema name>

   Where <schema name> is the name of the schema you would like Sametime Gateway to use. The name must meet the requirements for a library name in IBM i, and must not already be used. For example, STGW.

**What to do next**

You can now proceed with the Sametime Gateway installation.

**Installing Sametime Gateway on IBM i**

Install an IBM Sametime Gateway server. This section provides procedures for installing a single server and installing a cluster of servers. When installing a cluster, you install a Deployment Manager server, SIP and XMPP proxy servers, a primary server, and at least one additional server on its own machine. You can install the primary server and Deployment Manager on the same machine, or each on its own machine. For better performance, install the SIP and XMPP proxy servers on their own machine; however, they can share a machine with other components of the cluster if necessary.

**Before you begin**

Before installing Sametime Gateway, verify that the fully qualified domain name of the external endpoint is externally resolvable by the domain name server, and is not set in the "hosts" file. When you install a single Gateway server, the external endpoint is the computer hosting the Gateway server. When you install a cluster, the external endpoint is the computer hosting the SIP and XMPP proxy servers.

**About this task**

Unlike other Sametime components, the Sametime Gateway does not install with a deployment plan created on the Sametime System Console. Instead, you enter required information as you proceed through the installation program. Once the installation is complete, you will register the Gateway with the Sametime System Console; from then on, you will administer the Gateway server from the System Console, just like all the other Sametime components.

**What to do next**

After installation, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
• Set up SSL
• Other optional configuration steps

**Installing a stand-alone Sametime Gateway server on IBM i:**

Choose to install a single Sametime Gateway server on Windows, AIX, Linux, Solaris, or IBM i.

**Installing a single server on IBM i:**

To install Sametime Gateway on IBM i, you must first install WebSphere Application Server. You can install more than one instance of Sametime Gateway on a single IBM i system.

**Installing WebSphere Application Server on IBM i:**

Install WebSphere Application Server before you install Sametime Gateway. After you install WebSphere Application Server, you can install more than one instance of Sametime Gateway on a single IBM i system.

**Before you begin**

If WebSphere Application Server Network Deployment has been installed by another Sametime product from the current release, you may use that WebSphere Application Server installation for Sametime Gateway. You need *ALLOBJ and *SECADM authorities to successfully complete the WebSphere Application Server Network Deployment installation.

**About this task**

Information on downloading packages for Sametime is located at the following Web address:

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

**Procedure**

1. Create the temporary file folder /TMP/WASCD on a PC that can connect to the IBM i system.
2. Copy the file part_number.zip to the temporary folder /TMP/WASCD
3. Open a command window and navigate to the folder /TMP/WASCD.
4. Extract all files to the temporary directory /TMP/WASCD. When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.
5. Copy the ifpackage folder to the IFS of the IBM i system.
6. In the folder you copied to the IFS of the IBM i system, edit the file ifpackage/WAS/responsefile.nd.txt
7. Accept the license to install. Read the comments in the file regarding License Acceptance and then set the value of silentInstallLicenseAcceptance to true. For example:

   -OPT silentInstallLicenseAcceptance="true"

8. Change the following options in the file:

   -OPT profileType="none"
   -OPT installLocation="/QIBM/ProdData/WebSphere/AppServer/V7/SametimeWAS"
   -OPT defaultProfileLocation="/QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS"
9. Save the file. The rest of the install options in the file are correct for a default installation.

10. To run the install, start a QSHELL session.

11. Navigate to the ifpackage/WAS directory.

12. Run the following command:

   ```bash
   install -options responsefile.nd.txt
   ```

13. When the installation is successful, you will see a message such as this:

   ```
   ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS.
   ```

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

*Installing WebSphere iFixes for a stand-alone Sametime Gateway server on IBM i:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.

   The iFixes are included in the following package: IBM WebSphere V7.0.0.3
   iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
   Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Installing a single Sametime Gateway server on IBM i:*

Complete these steps to install a single Sametime Gateway server on IBM i. If you need to create a cluster of Sametime Gateway servers later, follow the procedure for installing a cluster of servers.

**Before you begin**

Before you begin, WebSphere Application Server must be installed. You need
*ALLOBJ and *SECADM authorities to successfully complete the Sametime Gateway installation.

Information on downloading packages for Sametime is located at the following Web address:
About this task

IBM i allows multiple instances of Sametime Gateway to be installed on a single IBM i system. If a Sametime Gateway server is running while you install a new Sametime Gateway server, the running server must be restarted before you can use the Integrated Solutions Console to administer Sametime Gateway.

Procedure

1. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as c:\TMP.
2. Extract the contents of part_number.exe to the temporary directory c:\TMP.
3. Navigate to the folder: c:\TMP\SametimeGateway.
4. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

   **Important:** If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.

   • To run the installer in wizard mode, type the following command:
     
     ```
     installi5OS.bat
     ```

   • To run the installer in console mode, perform these steps:
     
     a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
     b. Start a QSHELL session.
     c. Navigate to the /TMP/SametimeGateway directory and type the following command:
        
        ```
        install.sh -console
        ```

        **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

        ```
        install.sh -console -V BypassWasInfoCheck=true
        ```

        Because your input will not be verified during installation, you should take extra care when typing values.

5. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.
6. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.
7. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.
8. Select **Standalone server**, and then click **Next**.
9. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, /QIBM/proddata/websphere/AppServer/v7/nd

   This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.
10. See node, cell, and host name profile information provided by the installer. If the supplied information is okay, click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, exampleNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td>Profile name</td>
<td>Name of the WebSphere Application Server profile that will be created and be installed with the Sametime Gateway. For example: STGW_Profile</td>
</tr>
<tr>
<td>Starting port</td>
<td>IBM i supports running multiple profiles and instances of WebSphere Application Server at the same time; to avoid port conflicts the profile created will not use the default ports. Select a port range of 50 consecutive unused ports on your system, and enter the first port number as your starting port. For example: 10000.</td>
</tr>
</tbody>
</table>

11. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: `;*!"'<>|+&`\^%

12. Click **Next** to continue with the installation. The **DB2 Database Properties** dialog is displayed.

13. Click **Next** to enter properties required by DB2:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

14. Click **Next** to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LDAP now</td>
<td>Select if you want to set up a connection between Sametime Gateway and LDAP that does not need an SSL connection. You will need to know the host name and port of the LDAP server.</td>
</tr>
<tr>
<td>Configure LDAP after the installation</td>
<td>Select this option if you need to set up an SSL connection with LDAP, or if you do not know the host name and port number used by LDAP. If you are installing Sametime Gateway outside the firewall and the LDAP directory is located inside the firewall, choose this option.</td>
</tr>
</tbody>
</table>

If you selected **Configure LDAP now**, complete the next four steps. Otherwise, proceed to Step 19.

15. Select an LDAP host name from list of **Registered host names and ports in your domain**, or select **Other** and enter a host name or IP address in the **Host name** field. The default port number is 389. Click **Next**.

16. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous access</td>
<td>Select this option if you don’t need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.</td>
</tr>
<tr>
<td>Authenticated access</td>
<td>Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.</td>
</tr>
</tbody>
</table>

17. Enter the **Bind distinguished name (DN)** and **Bind password**. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:
ADDONPANEL

- Bind distinguished name:
  uid=ldapadmin,cn=users,l=shipley,st=kansas,c=us,ou=sales,o=medical,DC=EXAMPLE,DC=COM
- Bind password: C@pital1

18. Click Next. Choose a base distinguished name from the list of **Suggested base distinguished names in your LDAP** or enter a base DN in the **Base distinguished name** field. The base distinguished name indicates the starting point for LDAP searches of the directory service. For example, for the bind distinguished name given as an example in the previous step, you can specify the base DN as: **DC=EXAMPLE,DC=COM**. For authorization purposes, this field is case sensitive. This panel is not shown if you are connecting to Domino LDAP.

19. Click Next to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click Back to make changes.

20. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

21. Read the summary and click Finish. To view the installation log, open the log file at `stgw_server_root\logs\installlog.txt`

**Adding a stand-alone Sametime Gateway server (IBM i) 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.

### Starting a stand-alone Sametime Gateway server on IBM i:

This section explains how to start a standalone Sametime Gateway server. Skip these steps if you are setting up a cluster.

#### About this task

Single server configurations must have the Sametime Gateway server running to access the Integrated Solutions Console, while a Sametime Gateway cluster must have the Deployment Manager running to access the Integrated Solutions Console. Do not start Sametime Gateway at this time if you are creating a cluster of Sametime Gateway servers.

#### Procedure

1. Log in to the server machine as a user with administrative privileges.
2. Navigate to the Sametime Gateway profile directory that contains binaries:
   `stgw_profile_root\bin`
3. Type the following command to start Sametime Gateway. Note that **RTCGWServer** is case-sensitive.
   **AIX, Linux, and Solaris**
   
   `./startServer.sh RTCGWServer`

   **Windows**
   
   `startServer.bat RTCGWServer`

   **IBM i**
   
   `startServer RTCGWServer`

### Connecting a stand-alone Sametime gateway server (IBM i) to DB2:

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 582

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

Sametime prerequisite: Connecting a stand-alone Sametime Gateway server (IBM i) to DB2:

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**.

**Registering a new Gateway server on IBM i with the System Console:**

After installing an IBM Sametime Gateway server on IBM i, register it with the Sametime System Console, which allows you to manage all Sametime servers from a central location.

**Before you begin**

Before you register the server, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.
About this task

Working from the server that you want to connect with the console, follow these steps to update properties files and run the registration utility.

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

- console.properties
- productConfig.properties

Procedure

1. Working on the Sametime Gateway server, navigate to the /qibm/userdata/STGateway/ProfileName/console directory.
   The ProfileName is the one you specified when you installed the Gateway.
2. Make backup copies (using different names) of the console.properties and productConfig.properties files.
3. Update the console.properties file with the following values, and then save and close the file.

   Table 96. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>

4. Update the productConfig.properties file with the following values, and then save and close the file.
   Only the required values in this file are listed here:

   Table 97. productConfig.properties settings

   | InstallType | Specify "Cell" as the installation type since this is a non-clustered server. |
Table 97. \textit{productConfig.properties} settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{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>\texttt{NodeIP}</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>\texttt{WASAdminPassword}</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>\texttt{LDAPBindPassword}</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>\texttt{DB2AdminPassword}</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>\texttt{CommunityServerHost}</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>\texttt{CommunityServerPort}</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>\texttt{LDAPHost}</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>\texttt{LDAPPort}</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>\texttt{LDAPBindDN}</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>\texttt{LDAPBindPwd}</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>\texttt{LDAPBaseDN}</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>\texttt{isFederated}</td>
<td>Set the value to \texttt{true} for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

5. Run the registration utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: \texttt{QSH}
   b. Run the \texttt{cd} shell command, specifying the fully qualified path to the console directory you used in Step 1.
   c. Run the shell script to register the server: \texttt{registerProduct.sh}
   d. When the registration script completes, press \texttt{F3} to exit QSH.

   The utility registers the cluster, as well as each node, generating a log file called \texttt{ConsoleUtility.log} and storing it in the \texttt{consoles/logs} directory. If the registration is successful, a \texttt{console.pid} will also be generated.

6. Start Sametime Gateway server, if it is not already running.

   \textit{Optional network configuration for a stand-alone Sametime Gateway server on IBM i:}

After you complete your IBM Sametime Gateway installation, you can optionally modify some network configuration settings.

\textit{Configuring network interface cards to simulate a NAT for a Sametime Gateway server on IBM i:}

This optional procedure describes how to you can simulate a Network Address Translator (NAT) to provide additional security by using two Network Interface Cards (NICs), one for an internal IP address facing the Sametime community server, and the other for an external IP address facing the Internet. This procedure

826 IBM Sametime: Installation, Migration, and Configuration Guide
applies to standalone Sametime Gateway deployments only. If you use this configuration, you must update the default host using the Integrated Solutions Console.

**Before you begin**

The procedure applies to single server installations only. If you have a cluster of Sametime Gateway servers, and you want to set up two Network Interface Cards, install the NICs on the proxy server node in the cluster. The proxy server node is smart enough to handle incoming and outgoing addresses on two different IP addresses without additional configuration.

**About this task**

Perform these steps to configure multiple NIC support in a single server installation. When Sametime Gateway has two IP addresses, one external facing and one internal facing, sometimes the Sametime Gateway sends subscribe requests such that the external community is instructed to respond back to the internal IP address. To ensure that Sametime Gateway sends the external IP address instead of the internal IP, perform the following configuration steps:

**Procedure**
1. Log into Integrated Solutions Console.
2. Click Servers > Application servers.
3. Click RTGWServer.
4. Under Communications, click Ports.
5. Click SIP_DEFAULTHOST.
6. In the Host field, type the external IP address; for example: 192.0.2.10
7. Click SIP_DEFAULTHOST_SECURE.
8. In the Host field, type the external IP address. For example: 192.0.2.10
9. Click Apply, then Save.
10. Restart the Sametime Gateway server.

**Installing Sametime Gateway servers in a cluster on IBM i:**

Complete these steps to install a cluster of Sametime Gateway servers in a network deployment. A cluster is a group of application servers that are managed together and participate in workload management. A network deployment is a group of nodes administered by the same cell, and controlled by a Deployment Manager.
About this task

Sametime Gateway supports cluster members on multiple nodes across many nodes in a cell, with nodes either coexisting on the same hardware, or running on dedicated systems. A network deployment is made up of a Deployment Manager, which manages the cell, SIP and XMPP proxy servers, a primary node, a primary server (primary cluster member), and, if needed, one or more secondary cluster members. You expand the cluster by adding additional cluster members either on existing nodes, or by adding a new secondary node and then adding the member to the new node.

Note the following restrictions:
• All of the cluster components (deployment manager, nodes, proxies) must be deployed in the same LAN.
• Deploying components over a WAN is not supported.
• Placing a firewall between two components is not supported (even if the firewall is configured to allow the relevant traffic).
• When fronting the WebSphere Application Server SIP Proxies with a load balancer, the load balancer must be able to communicate with the proxies in Layer 2, using MAC forwarding. IP forwarding (Layer 3) is not supported.

Before you begin, upgrade existing Sametime Gateway servers to the current release before you install new servers.

Except in the case of IBM i, the Sametime Gateway install wizard deploys both WebSphere Application Server and the Sametime Gateway server application in one installation.

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.

Related concepts
“Clustering Sametime servers for high enterprise availability” on page 88

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.

About network deployments:

A network deployment is a distributed WebSphere environment. Unlike a stand-alone environment that contains only one application server node, a network deployment contains many application server nodes that can distribute the workload of Sametime Gateway applications across several physical systems. The purpose of a network deployment is to provide a topology that is scalable and has load balancing and failover capabilities.

Typically, a network deployment contains one node per physical computer. This is not a requirement. Nodes are logical groupings of application servers, so you can
have more than one node installed on a physical system. For performance reasons, most installations have only one cluster member per node, since each cluster member creates its own JVM footprint.

In a network deployment, all nodes are federated into the deployment manager's cell. The deployment manager serves to manage the deployment. A Deployment Manager is nothing more than a node that is responsible for administering a cell. In Sametime Gateway, the only things configured on the Deployment Manager node are a few minor cell level attributes, and the Sametime Gateway administrative portlet plugin extensions. Sametime Gateway application files all run on the cluster member application servers.

The primary node is basically the same thing as a standalone node installation, minus a few cell level configurations that will be trumped by the Deployment Manager's configuration. The primary node contains all the applications and WebSphere Application Server components that are required to run Sametime Gateway. When you install a primary node, you create a server instance called RTCGWServer. This server instance is cloned for use with all secondary nodes across the cluster. There can only be one primary Sametime Gateway node installed in any network deployment, because applications can only be added to the cell from one node. In the Sametime Gateway network deployment, the primary node also configures the database server.

The secondary nodes are WebSphere Application Server placeholders that can run additional cluster members (servers created as clones of the primary server). When you install a secondary node for Sametime Gateway, the installation creates a node and default server instance, as well as some node level WebSphere Application Server attributes such as data sources, WebSphere variables, and shared library definitions. A network deployment of Sametime Gateway can contain as many secondary nodes as your environment needs.

**Installing the Sametime Gateway deployment manager on IBM i:**

Install the Deployment Manager on its own machine, or on the same machine as the primary node. Installing the Deployment Manager on the same machine as the primary node provides the efficiency of multiple Java Virtual Machines and takes advantage of a fast CPU. If you are installing the Deployment Manager on the same machine with an existing primary node from a previous release, upgrade the primary node to the present release before installing the Deployment Manager.

**Installing the Deployment Manager on IBM i:**

Install the Deployment Manager on IBM i by first installing WebSphere Application Server on IBM i. After WebSphere Application Server is installed, you can install multiple instances of Sametime Gateway on the same machine.

**Installing WebSphere Application Server for the Sametime Gateway deployment manager on IBM i:**

Install WebSphere Application Server before you install Sametime Gateway. After you install WebSphere Application Server, you can install more than one instance of Sametime Gateway on a single IBM i system.
Before you begin

If WebSphere Application Server V6.1 Network Deployment has been installed for use by a previous version of Sametime Gateway, use the procedure for updating your installation of WebSphere Application Server V6.1 rather than the steps for a new installation. You need *ALLOBJ and *SECADM authorities to successfully complete the WebSphere Application Server Network Deployment installation.

About this task

Information on downloading packages for Sametime is located at the following Web address:

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

Note: Complete details on requirements for WebSphere Application Server Network Deployment are available from: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

Procedure

1. Create the temporary file folder /TMP/WASCD on a PC that can connect to the IBM i system.
2. Copy the file part_number.zip to the /TMP/WASCD folder.
3. Open a command window and navigate to the folder /TMP/WASCD.
4. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.
5. Copy the ifpackage folder to the IFS of the IBM i system.
6. In the folder you copied to the IFS of the IBM i system, edit the file ifpackage/WAS/responsefile.nd.txt
7. Accept the licence to install. Read the comments in the file regarding Licence Acceptance and then set the value of silentInstallLicenseAcceptance to true.
   For example:
   -OPT silentInstallLicenseAcceptance="true"
8. Save the file. The rest of the install options in the file are correct for a default installation.
9. To run the install, start a QSHELL session.
10. Navigate to the ifpackage/WAS directory.
11. Run the following command:
    ```
    install -options responsefile.nd.txt
    ```
12. When the installation is successful, you will see a message such as this:
    ```
    ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS.
    install ni.ismp.actions ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS
    ```

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

Installing WebSphere iFixes for the Sametime Gateway deployment manager on IBM i:
Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Installing the Deployment Manager for Sametime Gateway on IBM i:*

Complete these steps to install the Deployment Manager server on IBM i. Install the Deployment Manager on the same machine as the primary server, or on its own machine.

**Before you begin**

Before you begin, create the database schema for Sametime Gateway and then install the primary node.

Information on downloading packages for Sametime is located at the following Web address:

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

**About this task**

Note that there are special naming rules for each node and cell that are part of a cluster. When installing each node, the node name and the cell name must be unique across all machines. *No two nodes can have the same cell name.* Later, when you federate each node into the cluster, the cell name is automatically changed to the Deployment Manager's cell name.

**Procedure**

1. From the installation media, copy the Sametime Gateway installation image (`part_number.exe`) to a temporary directory such as `/TMP`.
2. Extract the contents of `part_number.exe` to the temporary directory `/TMP`.
4. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

   **Important:** If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.
   - To run the installer in wizard mode, type the following command:
installI5OS.bat

- To run the installer in console mode, perform these steps:
  a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
  b. Start a QSHELL session.
  c. Navigate to the /TMP/SametimeGateway directory and type the following command:
     `install.sh -console`

**Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:
`install.sh -console -V BypassWasInfoCheck=true`

Because your input will not be verified during installation, you should take extra care when typing values.

5. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.
6. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.
7. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.
8. Select **Deployment Manager** as the type of installation.
9. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, `/QIBM/proddata/websphere/AppServer/v7/nd`. This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.
10. Click **Next** to continue with the installation. The WebSphere Application Server Configuration dialog is displayed.
11. Type the node name, cell name, host name, profile name, and starting port value for the WebSphere Application Server as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td>Logical name for the node. For example, exampleNode.</td>
</tr>
<tr>
<td><strong>Cell</strong></td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCell.</td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td><strong>Profile name</strong></td>
<td>Name of the WebSphere Application Server profile that will be created and be installed with the Sametime Gateway. For example: STGW_Profile</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Starting port | IBM i supports running multiple profiles and instances of WebSphere Application Server at the same time; to avoid port conflicts the profile created will not use the default ports. Select a port range of 50 consecutive unused ports on your system, and enter the first port number as your starting port. For example: 10000.

12. Click **Next** and create a user ID and password for logging into the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: `;*!?"<>|+&'`\[\]^.

13. Click **Next** to continue with the installation. The **DB2 Database Properties** dialog is displayed.

14. Type the required information for DB2 for IBM i as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

15. Click **Next** to connect to an LDAP server at this time. The LDAP server must be the same LDAP used by Sametime.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure LDAP now</strong></td>
<td>Select if you want to set up a connection between Sametime Gateway and LDAP that does not need an SSL connection. You will need to know the host name and port of the LDAP server.</td>
</tr>
<tr>
<td><strong>Configure LDAP after the installation</strong></td>
<td>Select this option if you need to set up an SSL connection with LDAP, or if you do not know the host name and port number used by LDAP. If you are installing Sametime Gateway outside the firewall and the LDAP directory is located inside the firewall, choose this option.</td>
</tr>
</tbody>
</table>

If you selected **Configure LDAP now**, complete the next four steps. Otherwise, proceed to Step 20.
16. Select an LDAP host name from list of Registered host names and ports in your domain, or select Other and enter a host name or IP address in the Host name field. The default port number is 389. Click Next.

17. If anonymous access is successful to the LDAP host name, you may have the option of continuing with anonymous access or changing the access to authenticated access. If anonymous access is not permitted, you will not have this option because you must supply a bind distinguished name and password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous access</td>
<td>Select this option if you don’t need authenticated access to the LDAP server. Sametime Gateway only requires anonymous access to an LDAP server.</td>
</tr>
<tr>
<td>Authenticated access</td>
<td>Select this option if your LDAP server requires authenticated access. You must provide an authentication identity, including a bind distinguished name and password from the LDAP administrator.</td>
</tr>
</tbody>
</table>

18. Enter the Bind distinguished name (DN) and Bind password. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. For example:
   - Bind distinguished name:
     
     uid=ldapadmin,cn=users,l=shipley,st=kansas,c=us,ou=sales,o=medical,DC=example,DC=COM
   - Bind password:
     
     C@pital1

19. Click Next. Choose a base distinguished name from the list of Suggested base distinguished names in your LDAP or enter a base DN in the Base distinguished name field. The base distinguished name indicates the starting point for LDAP searches of the directory service. For example, for the bind distinguished name given as an example in the previous step, you can specify the base DN as: DC=EXAMPLE,DC=COM. For authorization purposes, this field is case sensitive. This panel is not shown if you are connecting to Domino LDAP.

20. Click Next to see the Sametime Gateway installation summary. You can review the installation summary settings and, if necessary, click Back to make changes.

21. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

22. Read the summary and click Finish to complete the installation. To view the installation log, click View log file or open the log file at stgw_server_root\logs\installlog.txt

23. To test the Deployment Manager installation and ensure that LDAP settings are correct, log into the Deployment Manager node as a user with administrative privileges.

24. Navigate to the stgw_profile_root/bin directory.

25. Start the Deployment Manager with the following command:

    ./startManager dmgr

26. Log in into the Integrated Solutions Console using the administrative user ID and password that you created.
27. Test the LDAP connectivity. Click Users and Groups > Manage users.
28. Verify that you can search and retrieve users in your LDAP directory.
29. Leave the Deployment Manager node running as you install other nodes in the cluster.

Adding the Sametime Gateway deployment manager (IBM i) 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 Sametime Gateway primary node on IBM i:
Install a primary node for a cluster. You can install the primary node and the Deployment Manager on the same machine. Installing the primary node on the same machine as the Deployment Manager provides the efficiency of multiple Java Virtual Machines and takes advantage of a fast CPU. If you are installing the primary node on the same machine with an existing Deployment Manager from a previous release, upgrade the Deployment Manager to the present release before installing the primary node.

*Installing the primary server on IBM i:*

To install the primary server on IBM i, you must install WebSphere Application Server first. After WebSphere Application Server is installed, you can install multiple instances of Sametime Gateway on the same machine.

’*Installing a WebSphere Application Server primary node on IBM i:*

Install WebSphere Application Server before you install Sametime Gateway. After you install WebSphere Application Server, you can install more than one instance of Sametime Gateway on a single IBM i system.

**Before you begin**

If WebSphere Application Server V6.1 Network Deployment has been installed for use by a previous version of Sametime Gateway, use the procedure for updating your installation of WebSphere Application Server V6.1 rather than the steps for a new installation. You need *ALLOBJ and *SECADM authorities to successfully complete the WebSphere Application Server Network Deployment installation.

**About this task**

Information on downloading packages for Sametime is located at the following Web address:

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

**Note:** Complete details on requirements for WebSphere Application Server Network Deployment are available from: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

**Procedure**

1. Create the temporary file folder `/TMP/WASCD` on a PC that can connect to the IBM i system.
2. Copy the file `part_number.zip` to the temporary folder `/TMP/WASCD`
3. Open a command window and navigate to the folder `/TMP/WASCD`
4. Extract all files to the temporary directory `/TMP/WASCD`. When you are done extracting the files, you should have a `/TMP/WASCD/ifpackage` folder with WAS and JDK folders inside the ifpackage folder.
5. Copy the ifpackage folder to the IFS of the IBM i system.
6. In the folder you copied to the IFS of the IBM i system, edit the file `ifpackage/WAS/responsefile.nd.txt`
7. Accept the licence to install. Read the comments in the file regarding Licence Acceptance and then set the value of `silentInstallLicenseAcceptance` to true. For example:
   ```
   -OPT silentInstallLicenseAcceptance="true"
   ```
8. Save the file. The rest of the install options in the file are correct for a default installation.
9. To run the install, start a QSHELL session.
10. Navigate to the ifpackage/WAS directory.
11. Run the following command:
    ```
    install -options responsefile.nd.txt
    ```
12. When the installation is successful, you will see a message such as this:
    ```
    ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS.
    install.ni.ismp.actions.ISMPLogSuccessMessageAction,
    msg1, INSTCONFSUCCESS
    ```

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

*Installing WebSphere iFixes for the Sametime Gateway primary node on IBM i:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

*About this task*

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

*Procedure*

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Installing the primary node for Sametime Gateway on IBM i:*

Complete these steps to install the primary Sametime Gateway node in a cluster on IBM i.

*Before you begin*

Before you begin, install WebSphere Application Server. You need *ALLOBJ and *SECDATA authorities to successfully complete the Sametime Gateway installation.

Information on downloading packages for Sametime is located at the following Web address:

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

IBM i allows multiple instances of Sametime Gateway to be installed on a single IBM i system. If a Sametime Gateway server is running while you install a new Sametime Gateway server, the running server must be restarted before you can use the Integrated Solutions Console to administer Sametime Gateway.

Note that there are special naming rules for each node and cell that are part of a cluster. When installing each node, the node name and the cell name must be unique across all machines. No two nodes can have the same cell name. Later, when you federate each node into the cluster, the cell name is automatically changed to the Deployment Manager's cell name.

Procedure

1. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as c:\TMP\SametimeGateway.
2. Extract the contents of part_number.exe to the temporary directory c:\TMP\SametimeGateway.
3. Navigate to the folder: c:\TMP\SametimeGateway.
4. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

   **Important:** If you are installing on an IPv6-enabled server, you must use the second option below to install using the console.

   • To run the installer in wizard mode, type the following command:
     installi5OS.bat
   • To run the installer in console mode, perform these steps:
     a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
     b. Start a QSHELL session.
     c. Navigate to the /TMP/SametimeGateway directory and type the following command:
        install.sh -console

     **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
        install.sh -console -V BypassWasInfoCheck=true

     Because your input will not be verified during installation, you should take extra care when typing values.
5. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.
6. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.
7. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.
8. **Primary Node** is selected as the installation type by default; however, sometimes the default selection is not captured. To ensure you really install a Primary Node:
a. Select any other installation type.
b. Then select **Primary Node** as the installation type.

9. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, /QIBM/proddata/websphere/AppServer/v7/nd

   This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.

10. Click **Next** to continue with the installation. The WebSphere Application Server Configuration dialog is displayed.

11. Type the node name, cell name, host name, profile name, and starting port value for the WebSphere Application Server as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, acmeNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, acmeCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.acme.com</td>
</tr>
<tr>
<td>Profile name</td>
<td>Name of the WebSphere Application Server profile that will be created and be installed with the Sametime Gateway. For example: STGW_Profile</td>
</tr>
<tr>
<td>Starting port</td>
<td>IBM i supports running multiple profiles and instances of WebSphere Application Server at the same time; to avoid port conflicts the profile created will not use the default ports. Select a port range of 50 consecutive unused ports on your system, and enter the first port number as your starting port. For example: 10000.</td>
</tr>
</tbody>
</table>

12. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same administrative user ID and password that you created when installing the Deployment Manager. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters: `;*!"<>|+$'[]\^`  

13. Click **Next** to continue with the installation. The **DB2 Database Properties** dialog is displayed.

14. Type the required information for DB2 for IBM i as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.acme.com</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

15. Click **Next** to continue with the installation. The Sametime Gateway summary dialog is displayed.

16. You can review the installation summary settings and if necessary click **Back** to make changes.

17. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating the successful installation of Sametime Gateway and WebSphere Application Server.

18. Read the summary and click **Finish** to complete the installation. To view the installation log, click **View log file** or open the log file at `stgw_server_root\logs\installlog.txt`

**Adding the Sametime Gateway primary node (IBM i) 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.

   **Federating the Sametime Gateway primary node into the cell on IBM i:**

   After you create the primary node you must add the primary node to the Deployment Manager's cell.

   **Federating the primary node into the cell on IBM i:**

   Add the primary node to the Deployment Manager's cell on IBM i. Adding the primary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console. You will not be able log into the primary node's Integrated Solutions Console after this step.

**Before you begin**

Expected state: the Deployment Manager is running.

**Procedure**

1. Make sure that the system clocks on the Deployment Manager and the primary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the primary node to make sure the host name is resolvable.

3. Log in to the IBM i system where the Deployment Manager node is installed as a user with administrative privileges.

4. On the IBM i command line, run the STRQSH (Start Qshell) command.

5. Navigate to the `stgw_profile_root\bin` directory for the Deployment Manager profile.

6. Run the following command to obtain the `SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number as you will need it to add nodes to the cluster:
   ```
   dspwasinst
   ```

7. Log in to the IBM i system, where the primary node is installed, with administrative privileges.
8. On the IBM i command line, run the STRQSH (Start Qshell) command.
9. Navigate to the `stgw_profile_root/bin` directory for the primary node profile.
10. Run the following command to add the primary node to the Deployment Manager's cell:
    
    ```
    addNode DM_server_host_name DM_SOAP_port -includeapps
    -username WAS_Admin_username_on_DM -password WAS_Admin_password_on_DM
    ```
    
    Where:
    - `DM_server_host_name` is the resolvable host name of the Deployment Manager.
    - `DM_SOAP_port` is the port that the Deployment Manager's SOAP port is listening on.
    - `WAS_Admin_username_on_DM` is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
    - `WAS_Admin_password_on_DM` is the password associated with that WebSphere Application Server administrator account on the Deployment Manager.
    
    For example:
    ```
    addNode gateway_dm.acme.com 8880 -includeapps -username wasadmin -password waspassword
    ```

11. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

    ```
    Node MyserverNodePrimary has been successfully federated.
    ```

12. To verify that the primary node has joined the Deployment Manager's cell, log into the Integrated Solutions Console (http://localhost:9060/ibm/console) using your administrative user ID and password and click **Servers > Application servers**. Make sure you can see the primary node's information.

    If you already logged in, you must log out and then log in again before you can see changes.

**What happens when you federate the primary node into the cell on IBM i?**

When you federate the primary node into the Deployment Manager's cell, the primary node's original configuration is backed up. This means that you can remove the primary node from the Deployment Manager at a later time, and you can restore the profile configuration to the state it was in before federation.

The primary node's scope changes to include the Deployment Manager's cell.

Before federation, the scope of the RTCGWServer was:
```
<cell>:<PrimaryCell>/node:<PrimaryNode>/server:RTCGWServer
```

After federation, the scope of the server is the following:
```
<cell>:<Deployment Manager Cell>/node:<PrimaryNode>/server:RTCGWServer
```

When you federate, the Integrated Solutions Console of the primary node is disabled because you will be using the Integrated Solutions Console from the Deployment Manager. The primary node inherits all the cell level configuration data from the Deployment Manager. Any information you can see through the Deployment Manager's Integrated Solutions Console is now stored in XML on the primary node, so it is accessible from any application. The applications that were installed to RTCGWServer are now included on the RTCGWServer in the Deployment Manager's cell. If you attempt to federate another node that contains these same applications, they are excluded.
Because the LDAP configuration and your credentials as the WebSphere Application Server administrative user in the Deployment Manager are defined at the cell level, this data overwrites the security settings of the primary node. The Deployment Manager's settings apply to the primary node. If you remove the primary node from the cell, the primary node's original security configuration are restored.

When you federate the primary server into the cell, a single server of Sametime Gateway can be managed by a Deployment Manager. You can actually run a real environment and configure your Sametime communities just as you would in a standalone server environment. What is lacking is failover and load balancing capabilities. In order to add those features, you need to add a secondary node and create a cluster in the later steps.

*Installing additional nodes in a Sametime Gateway cluster on IBM i:*

Depending upon your capacity requirements, install secondary nodes as needed.

*Installing an additional server on IBM i:*

Install an additional server on IBM i by first installing WebSphere Application Server on IBM i. After WebSphere Application Server is installed, you can install multiple instances of Sametime Gateway on the same machine.

*Installing a WebSphere Application Server additional node on IBM i:*

Install WebSphere Application Server before you install Sametime Gateway. After you install WebSphere Application Server, you can install more than one instance of Sametime Gateway on a single IBM i system.

**Before you begin**

If WebSphere Application Server V6.1 Network Deployment has been installed for use by a previous version of Sametime Gateway, use the procedure for updating your installation of WebSphere Application Server V6.1 rather than the steps for a new installation. You need *ALLOBJ* and *SECADM* authorities to successfully complete the WebSphere Application Server Network Deployment installation.

**About this task**

Information on downloading packages for Sametime is located at the following Web address:

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

**Note:** Complete details on requirements for WebSphere Application Server Network Deployment are available from: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

**Procedure**

1. Create the temporary file folder `/TMP/WASCD` on a PC that can connect to the IBM i system.
2. Copy the file `part_number.zip` to the `/TMP/WASCD` folder.
3. Open a command window and navigate to the folder `/TMP/WASCD`. 
4. Extract all files to the temporary directory /TMP/WASCD. When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.

5. Copy the ifpackage folder to the IFS of the IBM i system.

6. In the folder you copied to the IFS of the IBM i system, edit the file ifpackage/WAS/responsefile.nd.txt

7. Accept the licence to install. Read the comments in the file regarding Licence Acceptance and then set the value of silentInstallLicenseAcceptance to true. For example:
   -OPT silentInstallLicenseAcceptance="true"

8. Save the file. The rest of the install options in the file are correct for a default installation.

9. To run the install, start a QSHELL session.

10. Navigate to the ifpackage/WAS directory.

11. Run the following command:
    ```shell
    install -options responsefile.nd.txt
    ```

12. When the installation is successful, you will see a message such as this:
    
    ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS.
    install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

*Installing WebSphere iFixes for an additional node in a Sametime Gateway cluster on IBM i:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

*Installing an additional server for Sametime Gateway on IBM i:*
Install an additional server or secondary server on IBM i that will be part of a cluster of Sametime Gateway servers.

Before you begin

Before you begin, install WebSphere Application Server on the machine. You need *ALLOBJ and *SECADM authorities to successfully complete the Sametime Gateway installation.

Information on downloading packages for Sametime is located at the following Web address:

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

About this task

IBM i allows multiple instances of Sametime Gateway to be installed on a single IBM i system. If a Sametime Gateway server is running while you install a new Sametime Gateway server, the running server must be restarted before you can use the Integrated Solutions Console to administer Sametime Gateway.

Note that there are special naming rules for each node and cell that are part of a cluster. When installing each node, the node name and the cell name must be unique across all machines. No two nodes can have the same cell name. Later, when you federate each node into the cluster, the cell name is automatically changed to the Deployment Manager's cell name.

Procedure

1. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as /TMP/SametimeGateway.
2. Extract the contents of part_number.exe to the temporary directory /TMP/SametimeGateway.
4. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

Important: If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.

- To run the installer in wizard mode, type the following command:
  installi5OS.bat
- To run the installer in console mode, perform these steps:
  a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
  b. Start a QSHELL session.
  c. Navigate to the /TMP/SametimeGateway directory and type the following command:
     install.sh -console
Attention: If one or more of the domain addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

`install.sh -console -V BypassWasInfoCheck=true`

Because your input will not be verified during installation, you should take extra care when typing values.

5. Select the language to be used for the installation and click OK. The Sametime Gateway Welcome screen is displayed.

6. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.

7. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click Next to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.

8. Select Secondary node as the type of installation.

9. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, `/QIBM/proddata/websphere/AppServer/v7/nd`

This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.

10. Click Next to continue with the installation. The WebSphere Application Server Configuration dialog is displayed.

11. Type the node name, cell name, host name, profile name, and starting port value for the WebSphere Application Server as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Logical name for the node. For example, acmeNode.</td>
</tr>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, acmeCell.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.acme.com</td>
</tr>
<tr>
<td>Profile name</td>
<td>Name of the WebSphere Application Server profile that will be created and be installed with the Sametime Gateway. For example: STGW_Profile</td>
</tr>
<tr>
<td>Starting port</td>
<td>IBM supports running multiple profiles and instances of WebSphere Application Server at the same time; to avoid port conflicts the profile created will not use the default ports. Select a port range of 50 consecutive unused ports on your system, and enter the first port number as your starting port. For example: 10000.</td>
</tr>
</tbody>
</table>

12. Create a user ID and password to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same
administrative user ID and password that you created when installing the Deployment Manager and primary node. The user ID must not exist in the LDAP directory. Passwords must not contain accented characters or any of the following characters:

`;/?"<>|+&'`

13. Click Next to continue with the installation. The DB2 Database Properties dialog is displayed.

14. Type the required information for DB2 for IBM i as follows:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.acme.com</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
</tbody>
</table>

15. Click Next to continue with the installation. The Sametime Gateway summary dialog is displayed.

16. You can review the installation summary settings and if necessary click Back to make changes.

17. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating the successful installation of Sametime Gateway and WebSphere Application Server.

18. Read the summary and click Finish to complete the installation. To view the installation log, open the log file at `stgw_server_root\logs\installlog.txt`

Adding the Sametime Gateway additional node (IBM i) 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.

**Federating secondary nodes into the cell on IBM i:**

Add secondary nodes to the Deployment Manager's cell to create a network deployment of Sametime Gateway servers.

**About this task**

In this release, a Sametime Gateway cluster can support only two nodes: one Primary Node and one Secondary Node.

**Federating a secondary node on IBM i into the cell:**

Add the secondary node to the Deployment Manager's cell on IBM i. Adding the secondary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

**Before you begin**

Expected state: the Deployment Manager is running.
Procedure

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.

3. Log in to the IBM i system where the Deployment Manager node is installed with administrative privileges.

4. On the IBM i command line, run the STRQSH (Start Qshell) command.

5. Navigate to the $gw_profile_root/bin directory for the Deployment Manager profile.

6. Run the following command to obtain the SOAP_CONNECTOR_ADDRESS port number. Make a note of the port number as you will need it to add nodes to the cluster:

   dspwasinst

7. Log into the secondary node.

8. On the IBM i command line, run the STRQSH (Start Qshell) command.

9. Navigate to the $gw_profile_root/bin directory for the secondary node profile.

10. Run the following command to add the secondary node to the Deployment Manager's cell. Note the omission of the -includeapps qualifier.

    addNode DM_server_host_name DM_SOAP_port -username WAS_Admin_user_name_on_DM -password WAS_Admin_password_on_DM

    where:
    • $DM_server_host_name is the resolvable host name of the Deployment Manager.
    • $DM_SOAP_port is the port that the Deployment Manager's SOAP port is listening on.
    • $WAS_Admin_user_name_on_DM is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
    • $WAS_Admin_password_on_DM is the password associated with the WebSphere Application Server administrator account.

    For example:

    addNode gateway_dm.example.com 8880 -username wasadmin -password waspassword

11. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

    Node Machine22NodeSecondary has been successfully federated.

12. For each additional IBM i secondary node, repeat the preceding steps.

13. Navigate to the $gw_profile_root/bin directory for the Deployment Manager profile.

14. Restart the Deployment Manager by typing the following commands. Wait for the first command to finish before starting the Deployment Manager:

    ./stopServer.sh dmgr -username username -password password
    ./startServer.sh dmgr
What to do next

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers” on page 505.

Creating a cluster and proxy servers on IBM i:

Create a Sametime Gateway cluster, install proxy servers, and then configure the proxy servers to use the cluster. Set up node replication only if you need high availability and failover, and then start the cluster.

About this task

Starting a cluster involves starting the Deployment Manager, starting the node agents on all the nodes, and then starting the servers, including the proxy servers, on each node.

Creating the Sametime Gateway cluster on IBM i:

Create a new cluster of Sametime Gateway servers by running the Cluster Configuration Wizard. If you are upgrading an existing Sametime Gateway cluster, you can skip this step because there is no need to create a new cluster.

Before you begin

Expected state: the Deployment Manager is running and nodes are stopped.

About this task

The instructions that follow describe steps for setting up a horizontal cluster, the most common cluster configuration. The primary node already has the primary server installed, so no additional server is needed on that computer. To add servers to the horizontal cluster, create one cluster member for each secondary node (computer).

Procedure

1. On the Deployment Manager, open a command window, navigate to the `stgw_server_root\config` directory, and run the following command:
   - AIX, Linux, and Solaris
     ./configwizard.sh
   - Windows
     configwizard.bat
   - IBM i
     configwizard.sh

   **Note:** To run this program in console mode (instead of using the graphical interface), add the `-console` argument to the command line; for example:
     configwizard.bat -console

2. View the Welcome page and click **Next**.
3. For each secondary node, do the following:
   a. Select a secondary node from the **Node** drop down list and type a unique name in the **Server Name** field.
b. Click Add Member.

4. When you have finished adding the secondary nodes, click Next.

5. Type the Schema user ID and Schema password for the database. These credentials have appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID for the database.

6. Read the summary and click Configure. When finished, you can view the configuration log at You can review the configuration wizard log at stgw_server_root\logs\configwizard.log.

7. Restart the Deployment Manager with the following commands:
   AIX, Linux, and Solaris
   
   ./stopManager.sh -username wasadmin_username -password wasadmin_password
   ./startManager.sh
   
   Windows
   
   stopManager.bat -username wasadmin_username -password wasadmin_password
   
   startManager.bat
   
   IBM i
   
   stopmanager -username wasadmin_username -password wasadmin_password
   
   startManager

8. Complete the following steps on every node in the cluster, including the primary node:
   a. Log in to the node's operating system.
   b. Navigate to the stgw_profile_root\bin directory.
   c. Start the node agent on the node with the following command:
      AIX, Linux, and Solaris
      
      ./startNode.sh
      
      Windows
      
      startNode.bat
      
      IBM i
      
      startNode

   **Note:** During installations, the Node agent on primary and secondary servers may be loaded, and issuing a startnode command may result in the error: "Conflict detected on port 8878. Likely causes: a) An instance of the server nodeagent is already running b) some other process is using port 8878." If this occurs you can confirm the nodeagent status by running the command serverstatus nodeagent from the stgw_profile_root\bin directory. When prompted, supply the Sametime Gateway administrator credentials. Verify that the nodeagent is running (the status will read, "The Node Agent "nodeagent" is STARTED). If the agent is running, continue to the next step.

9. When all the node agents are started, verify that the cluster configured properly by performing the following steps:
   a. Log into the Integrated Solutions Console using your administrative user ID and password on the Deployment Manager machine.
   b. Click Servers > Clusters, and verify that SametimeGatewayCluster appears in the table.
Creating a vertical Gateway cluster by adding servers to existing nodes on IBM i:

In an IBM Sametime deployment, create a vertical cluster of Sametime Gateway servers by installing additional servers onto existing nodes.

About this task

Add cluster members to an existing node to create a vertical cluster.

Procedure

1. On the cluster's Deployment Manager, log in to the IBM WebSphere Application Server's Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Clusters > WebSphere application server clusters > SametimeGatewayCluster > Cluster members.
3. Add a new cluster member as follows:
   a. In the list of cluster members, click the New button.
   b. Type a name for the new cluster member; for example: Node1RTCGWServer2.
   c. Select the node where you want to install this new cluster member.
      
      Tip: To see which servers the nodes are hosted on, use another tab to navigate to: System Administration > Nodes.
   d. Leave the remaining settings alone so that they use their default values.
   e. Click Add Member.
   f. Click Next.
   g. At the "Step 3: Summary" screen, click Finish.
4. Click Save.
5. Complete the following tuning procedures for each newly created server:
   This is necessary because the newly created server might be missing some tuning values used by existing servers in the cluster.
   • Setting thread pool values
   • Setting the JVM garbage collection policy
   • Setting log files size and rotation
6. Repeat steps 1 through 5 for each additional server that you want to add to an existing node.

Connecting a Sametime Gateway cluster on IBM i 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 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 582

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

**Sametime prerequisite: Connecting a Sametime Gateway cluster on IBM i 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**.

*Creating Common Event Infrastructure data source for IBM i:*

The Common Event Infrastructure data source must be manually created on IBM i after running the configuration wizard to create a Sametime Gateway cluster. These steps apply to clustered deployments only.

**Before you begin**

Expected state: the Deployment Manager is running and nodes are stopped.

**Procedure**

1. Log into the Integrated Solutions Console (http://localhost:9060/ibm/console) and select **Resources** > **JDBC** > **Data sources**.
2. Set the scope to **Cluster=SametimeGatewayCluster**
3. Click **New**.
4. Type the data source name: `CommonEventInfrastructure_Bus`
5. Type the JNDI name: `jdbc/com.ibm.ws.sib/SametimeGatewayCluster-CEI.DM_cell_name.BUS`
Where DM_cell_name is the cell name of the Deployment Manager which is input in the installation of the Deployment Manager.

6. Select the existing Event_DB2iSeries_JDBC_Provider and click Next.

7. Type the server name. This is the hostname of the IBM i system where your database schema is located.

8. For the Component-managed auth alias, select:

   \[ DM\_cell\_name/SametimeGatewayCluster/EventAuthDataAliasDB2iSeries \]

   and then click Next.

9. Deselect CMP

10. Click Next.

11. Click Finish.

12. Click the data source you just created, CommonEventInfrastructure_Bus, to see its properties.


14. Select the property named libraries.

15. Set the Value to the name of the schema you are using for the Sametime Gateway cluster.

16. Select OK.

17. Save your changes to the configuration.

18. Select Resources > JDBC > JDBCProviders.

19. Select the Event_DB2iSeries_JDBC_Provider.

20. Change the Class path to:

   /QIBM/ProdData/OS400/jt400/lib/jt400Native.jar

21. Click OK and then Save to save your changes to the configuration.

**Installing SIP and XMPP proxy servers for a Sametime Gateway cluster on IBM i:**

SIP and XMPP proxy servers act as the initial point of entry for messages that flow into and out of the enterprise. Both types of proxies are capable of securing the transport, using secure sockets layer (SSL), and the content, using various authentication and authorization schemes.

**Before you begin**

Expected state: DB2, LDAP, and Sametime Gateway servers are installed.

**About this task**

A SIP proxy server facilitates automatic load balancing, affinity matching, and failover for a cluster of Sametime Gateway servers. The enterprise's public SIP fully qualified domain name leads to the SIP proxy host, either directly, or through an IP sprayer that load balances incoming traffic to multiple proxies.

You must set up a Sametime Gateway cluster with at least one node before creating and federating SIP proxy servers. While you can install these proxy servers on an IBM Sametime Gateway node, it is recommended that you install them on a separate machine to isolate the proxy processing from the Sametime Gateway cluster. After you set up a Lotus Sametime Gateway cluster and a SIP proxy server, you can add external communities to Sametime Gateway. All of this information is set in the Sametime Gateway Web administration console (also available through the Sametime System Console after the Gateway is registered).
For network security, IBM recommends that you install the XMPP and SIP proxy server node and the Sametime Gateway cluster in the network DMZ. Installing the SIP proxy in the DMZ by itself is not a supported configuration because it places a firewall device between that server and the Sametime Gateway cluster. All of these components should be able to communicate freely which each other without traversing through a firewall device.

**Installing a SIP and XMPP proxy server on IBM i:**

The SIP and XMPP proxy servers are the first point of contact, after the firewall, for messages that flow into and out your enterprise. To set up a Sametime Gateway deployment, install a SIP and XMPP proxy server on its own node.

**Before you begin**

Before you begin, WebSphere Application Server must be installed. You need *ALLOBJ and *SECDATA authorities to successfully complete the WebSphere Application Server Network Deployment installation.

Information on downloading packages for Sametime is located at the following Web address:

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

**Procedure**

1. From the installation media, copy the Sametime Gateway installation image (C17KCML.exe) to a temporary directory such as /TMP.
2. Extract the contents of part_number.exe to the temporary directory /TMP.
4. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.
   - To run the installer in wizard mode, type the following command:
     ```bash
     installi5OS.bat
     ```
   - To run the installer in console mode, perform these steps:
     a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
     b. Start a QSHELL session.
     c. Navigate to the /TMP/SametimeGateway directory and type the following command:
        ```bash
        install.sh -console
        ```
5. Select the language to be used for the installation and click OK. The Sametime Gateway Welcome screen is displayed.
6. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.
7. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.
8. Select **SIP and XMPP proxy servers** as the type of installation.
9. Click **Next** to continue with the installation. The WebSphere Application Server Configuration dialog is displayed.
10. Type the node name, cell name, host name, profile name, and starting port value for the WebSphere Application Server as follows:
<table>
<thead>
<tr>
<th>Node</th>
<th>Logical name for the node. For example, exampleNodePrimary.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell</td>
<td>Name for the cell. Every WebSphere Application Server is created on a node inside a cell. A cell is a collection of nodes for administration and workload management. For example, exampleCellPrimary.</td>
</tr>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td></td>
<td>Note: If the server where you are installing has multiple NICs/IPs/DNS names, or for more information about considerations in choosing a host name, read the section 'Host name considerations' in the WebSphere Application Server information center topic, Creating an application server profile.</td>
</tr>
<tr>
<td>Profile name</td>
<td>Name of the WebSphere Application Server profile that will be created and be installed with the Sametime Gateway. For example: STGW_Proxy_Profile</td>
</tr>
<tr>
<td>Starting Port</td>
<td>IBM i supports running multiple profiles and instances of WebSphere Application Server at the same time; to avoid port conflicts the profile created will not use the default ports. Select a port range of 50 consecutive unused ports on your system, and enter the first port number as your starting port. For example: 10000.</td>
</tr>
</tbody>
</table>

11. Type the administrative user ID and password used to log in to the Integrated Solutions Console, the administrative interface for managing Sametime Gateway. Use the same user ID and password that you created when you installed the Deployment Manager. The user ID must not exist in the LDAP directory. Click Next.

12. Click Next to see the installation summary. You can review the installation summary settings and, if necessary, click Back to make changes.

13. Click Install to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 to 20 minutes to complete. When the installation is complete, the wizard displays a message indicating a successful installation.

14. Read the summary and click Finish to complete the installation. To view the installation log, click View log file or open the log file at stgw_server_root/logs/installlog.txt

**What to do next**

**Note:** If you start the SIPProxyServer instance now and log into the Integrated Solutions Console, you cannot view the SIPProxyServer instance. After you federate the node in the next procedure, you then see the SIPProxyServer instance.

*Installing WebSphere iFixes for a Sametime Gateway cluster’s proxy server:*
Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   - The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

---

**Guidelines for using multiple SIP or XMPP proxy servers for a Sametime Gateway cluster on IBM i:**

In enterprise deployments with high traffic from the public Internet, install multiple SIP or XMPP proxy servers with a Sametime Gateway cluster. Then front these proxy servers with an IP sprayer to ensure load balancing and high availability. Configure the IP sprayer to balance connections coming in from the Internet between the proxy servers.

**About multiple XMPP proxy servers**

This release does not support multiple XMPP proxy server configurations. Although the installer will install an XMPP proxy server instance with every SIP proxy server installation, configure only one XMPP proxy server in the cell and in the IP sprayer.

Follow these guidelines for setting up multiple proxy servers to work with an IP sprayer with Sametime Gateway.

**Installing the proxy server nodes**

1. Install each SIP or XMPP proxy server's node on its own host.
2. Federate and configure the additional proxy servers as additional nodes.

**Setting up traffic forwarding via the IP sprayer**

The IP sprayer is typically a hardware-based load balancer. Ask your network administrator for help setting it up and configuring it.

When communicating with public external communities (such as AOL), the Sametime Gateway SIP/XMPP Proxy servers inspect the IP source address of incoming IP packets, and compare these IP addresses to a list of well known IP addresses associated with the external public communities. To ensure a connection can be complete, the original source IP address must be retained as it passes through the IP sprayer (passthrough mode). The IP sprayer should not replace the IP address of the incoming IP packets with its own (IP sprayer) IP address.
The TCP/IP connection between the proxy servers and an external Internet server may remain open for very long periods of time. Be sure that there are no TCIP/IP inactivity timeout intervals set up for TCP-aware devices that the connection is tunneled through.

**Monitoring proxy server availability**

Ask your network administrator to set up the IP sprayer to check the availability of each proxy server every two seconds, by making sure that the following TCP/IP ports are available.

- **SIP proxy servers**: Ports 5060/5061
- **XMPP proxy servers**: Port 5269

If the proxy server is unavailable, the IP sprayer should suspend spraying new TCP connections until the proxy server becomes available again.

**Federating the proxy server node into the cell on IBM i:**

After you install the SIP and XMPP proxy server node, you must federate the node into the Deployment Manager’s cell so that the proxy server becomes part of the cluster.

**Before you begin**

Expected state: The Deployment Manager is running.

**About this task**

To federate or add the proxy server node into the cell, you run the `addnode` command on the proxy server node and specify the hostname of the Deployment Manager.

**Procedure**

1. Log into the proxy server node’s operating system.
2. **IBM i only**: On the command line, run the STRQSH (Start Qshell) command.
3. Synchronize the system clocks on the Deployment Manager and the proxy node so that they are within five minutes of one another and are set for the same time zone.
   
   Federation fails if the clocks are not synchronized within five minutes of each other.
4. On the proxy server node, open a command window and navigate to the `stgw_profile_root\bin` directory.
5. **IBM i only**: Run the following command to obtain the `SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number as you will need it to add nodes to the cluster:

   ```bash
dspwasinst
   ```

6. Run the following command to add the proxy server node to the Deployment Manager’s cell:

   **AIX, Linux, and Solaris:**
   ```bash
   ./addNode.sh DM_server_host_name DM_port_number -includeapps
   ```

   **Windows**
   ```bash
   addNode.bat DM_hostname DM_port_number -includeapps
   ```

   **IBM i:**
addNode DM_server_host_name DM_SOAP_port -username WAS_Admin_user_name_on_DM -password WAS_Admin_password_on_DM

where:

- **DM_server_host_name** is the resolvable host name of the Deployment Manager.
- **DM_SOAP_port** is the port that the Deployment Manager's SOAP port is listening on.
- **WAS_Admin_user_name_on_DM** is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
- **WAS_Admin_password_on_DM** is the password associated with the WebSphere Application Server administrator account.

For example:

```
addNode gateway_dm.example.com 8879 -includeapps -username wasadmin -password waspassword
```

7. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

```
Node MyProxyNode has been successfully federated.
```

8. Verify that the proxy servers are installed correctly:

   a. Log into the Integrated Solutions Console.
      If you already logged in, you must log out and then log in again before you can see changes.
   b. Click **Servers > Server Types > WebSphere proxy servers**. You should see the SIP proxy server.
   c. Click **Servers > Server Types > WebSphere application servers**. You should see the XMPP proxy server.

*Configuring a SIP proxy server on IBM i:*

Configure the Session Initiation Protocol (SIP) proxy server for a cluster of IBM Sametime Gateway servers. There is no need to configure external domains in the SIP proxy server; this is done through the Sametime Gateway configuration.

*Before you begin*

Set up a cluster with at least one secondary node and install the SIP and XMPP proxy servers on the same physical hardware as a Deployment Manager, primary node, or secondary node, or install the proxy servers on separate hardware. The SIP and XMPP installation creates a new profile for the SIP and XMPP proxy servers.

*About this task*

After you finish setting up a SIP proxy server, you'll have a port number. You provide the port number in combination with the domain name of the node on which the SIP proxy server runs to external servers to connect to your Sametime Gateway.

*Assigning the SIP proxy to work with the Sametime Gateway cluster on IBM i:*

Assign the SIP proxy server to function with the IBM Sametime Gateway cluster.
Procedure

1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers**.
2. In the "WebSphere proxy servers" page, click the **SIPProxyServer** link corresponding to the proxy server you want to update.
3. Click **SIP Proxy server settings > SIP Proxy settings**.
4. From the drop down list, select the Sametime Gateway cluster name.
5. Click **OK**, then click **Save**.

**Configuring the SIP Proxy server to listen on ports 5060 and 5061 on IBM i:**

Configure the IBM Sametime Gateway cluster's SIP Proxy server to listen on ports 5060 and 5061.

**Before you begin**

Configure a cluster of Sametime Gateway servers.

**About this task**

Public instant messaging providers require you to accept connections on ports 5060 and 5061, so you will need to confirm that the SIP Proxy server’s host name is resolvable and is listening on these ports. If the cluster’s SIP Proxy server is installed on a node that is already hosting Sametime Gateway, and the SIP Proxy server is not already listening on ports 5060 and 5061, reconfigure the port settings as follows:

**Procedure**

1. Determine which ports the SIP Proxy server is currently listening on:
   a. On the cluster's Deployment Manager, log in to the Integrated Solutions Console as the WebSphere administrator.
   b. Click **Servers > WebSphere proxy servers > SIPProxyServer > Ports**.
   c. Check the listening ports for the following names:
      - **PROXY_SIP_ADDRESS**
      - **PROXY_SIPS_ADDRESS**
      
      If **PROXY_SIP_ADDRESS** listens on port 5060 and **PROXY_SIPS_ADDRESS** listens on port 5061, you can skip the rest of this task. Otherwise, proceed to the next step to change the port settings.

2. Determine whether any servers share the IP address and host name with the SIP Proxy server.
   If another server shares the IP address and host name, change the default host port settings for that server to avoid a conflict with the SIP Proxy server.
   a. Still on the Deployment Manager, click **Server > Server Types > WebSphere application servers**.
   b. Check whether any servers use the same IP address and host name as the SIP Proxy server.
   c. If a server does share the IP address and host name, check its port settings for the following names:
      - **SIP_DEFAULTHOST**
      - **SIP_DEFAULTHOST_SECURE**
d. If SIP_DEFAULTHOST is not set to 5060 and SIP_DEFAULTHOST_SECURE is not set to 5061, skip to step 3.

e. If ports 5060 and 5061 are already in use, change those settings now by setting:
   • SIP_DEFAULTHOST to port 5080
   • SIP_DEFAULTHOST_SECURE to port 5081

f. Save your changes to the master configuration by clicking **Save** when prompted.

3. Now reset the SIP ports on the SIP Proxy server to use ports 5060 and 5061:
   a. On the Deployment Manager, click **Servers > WebSphere proxy servers > SIPProxyServer > Ports**.
   b. Change the port settings for the following names:
      • PROXY_SIP_ADDRESS to port 5060
      • PROXY_SIPS_ADDRESS to port 5061
   c. Save your changes 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. Select the **Synchronize nodes** option before clicking the **Save** button.

---

### Configuring the correct network address for the SIP Proxy on IBM i:

If the SIP proxy server has multiple network addresses, use these instructions to configure the one that the Sametime Gateway uses to contact the SIP Proxy. If the SIP proxy server has one network address, you can skip this task.

**Before you begin**

Follow these steps to determine which address to configure:

Start the SIP Proxy server. Then from the Sametime Gateway server, issue `telnet` commands to each of the network addresses the SIP Proxy uses. Use `telnet` commands to attempt to connect to the SIP Proxy machine. For example, with network addresses of 127.0.0.1 and 127.0.0.2, run the following commands:

```
telnet 127.0.0.1

telnet 127.0.0.2
```

Make a note of the address that you connected with successfully.

**About this task**

Follow these steps to configure the network address.

**Procedure**

1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers**.
2. In the "WebSphere proxy servers" page, click the **SIPProxyServer** link corresponding to the proxy server you want to update.
3. Click **SIP Proxy server settings > SIP Proxy settings**.
4. For the network address that the SIP Proxy server listens on, supply the host name or IP address for the following three fields:
   - UDP interface
   - TCP interface
   - TLS interface (UDP port should be left as an asterisk (*))
5. Click OK, then click Save.

Creating a virtual host for the SIP proxy on IBM i:

Create virtual host definitions for ports 5060 and 5061.

Procedure
1. To identify the SIP proxy port number in the proxy server table, click the name of the SIP proxy server that you created.
2. Under Proxy Settings, select SIP proxy server settings > SIP Proxy server transports.
3. Make a note of the port number defined for SIP_PROXY_CHAIN and SIPS_PROXY_CHAIN. The port number in combination with the domain name of the node on which the SIP proxy server runs is needed for configuring external servers to connect to your Lotus Sametime Gateway server.
4. Now move to the Environment section if the Integrated Solutions Console.
5. Click Virtual Hosts > default_host > Host Aliases > New.
6. Verify the virtual host definitions for 5060/5061. If the virtual host is not defined, define the new alias as follows:
   a. Add * to the Host Name field.
   b. Add 5060 or 5061 to the Port field.
   c. Click OK.
   d. Click Save.
   The additional Virtual Host entry is needed if the default ports are not added during installation. Port 5060, however, only covers non-TLS installs. For secure setups, the following entry may also need to be added: *:5061

Creating custom properties for the SIP proxy server on IBM i:

Define custom properties for the SIP proxy server.

About this task

Define custom properties that will instruct the SIP proxy server to do the following:
   - Return the "503 Service Unavailable" message when the server is down, rather than the default error "404 Page not found" message.
   - Accept messages that do not contain a forwarding header.

Procedure
1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers > your_new_SIP_proxy.
2. Click SIP Proxy server settings > SIP Proxy settings > Custom properties.
3. Create a custom property to set up the "503 Service Unavailable" message text:
   a. Click New.
   b. Enter the following information:
4. Create the custom property to define the error code to be displayed with the new message:
   a. Click **New**.
   b. Enter the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>lsnLookupFailureResponseCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>503</td>
</tr>
</tbody>
</table>

   c. Click **OK**.

5. Create another customer property to accept messages without a forwarding header:
   a. Click **New**.
   b. Enter the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>maxForwardsHeaderRequired</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>False</td>
</tr>
</tbody>
</table>

   c. Click **OK**.

6. Click **Save** to save all of the new custom properties.

**Tuning the SIP proxy on IBM i:**

This section describes the steps for tuning a SIP proxy.

**About this task**

Tune the JVM garbage collection policy for the SIP proxy server as follows:

**Procedure**

1. In the Integrated Solutions Console, click **Servers > Server Types > WebSphere proxy servers > SIPProxyServer**.
2. Perform the following instructions for each of the sip proxies in the list:
   a. Select a proxy server by clicking it in the list.
   b. Under **Server Infrastructure**, click **Java and Process management > Process Definition**.
   c. Under **Additional Properties**, click **Java Virtual Machine**.
   d. In the **Initial Heap Size** field, enter 600.
   e. In the **Maximum Heap Size** field, enter 600.
   f. In the **Generic JVM arguments** field, enter the following value as one continuous line:

   ```shell
   -Xmx60m -Xgc:policy:gencon -Xgc:noAdaptiveTenure,tenureAge=8,
   stdGlobalCompactToSatisfyAllocate -Xtgc:parallel
   ```
   g. Click **OK**, and click **Save** to save changes to the master configuration.
Configure a cluster of IBM Sametime Gateway servers to operate in a NAT (Network Address Translation) environment. The NAT environment configuration requires that the SIP Proxy’s external Fully Qualified DNS Name (FQDN), as known to external communities, be the same as its internal FQDN.

Before you begin

Traversing a NAT environment is a known issue in the SIP domain. There are several ways to solve this issue, while some of them have been formed as IETF standard (RPORT, STUN and ICE), others have been formed as proprietary solutions. So what is the problem? Some of the SIP communication parameters contain the Fully Qualified DNS Name (FQDN) or the IP address, and the port, but a SIP device deployed in a NAT environment does not know how it will be seen from the internet because the NAT device translates the IP address. The SIP message will contain IP address and port – which are not accessible from the internet. There are several paradigms to solve this issue:

- SIP Friendly NAT device – NAT devices that can analyze a SIP message and then replace the IP address and ports listed inside of it. This solution does not support encrypted SIP communication such as TLS.
- IETF Standard – a method using a standardized protocol such as RPORT, STUN, or ICE.

Currently, the IBM WebSphere SIP infrastructure does not provide a solution to this problem because it does not support any of the IETF standards. Therefore, any SIP application deployed on WebSphere has to develop its own solution. The solution provided here assumes that you have the following elements in your deployment:

- A clustered environment, with one ore more clustered servers.
- A SIP proxy server federated to the cluster.
- All cluster members (including the SIP proxy server) are deployed within the same subnet.
- A static NAT is defined in the NAT or firewall; the public IP address should be mapped to the SIP proxy server’s internal IP address.

About this task

The following diagram illustrates the NAT environment that this solution was designed for:
Limitations:
- Only static NAT is supported
- A single SIP proxy deployment was tested; a multiple-SIP proxy deployment was never tested but can be applied with the same setting.
- Single-server deployment is not supported, but a clustered deployment which contains only one server is supported.

Procedure
1. Map a fully qualified domain name to the public IP address serving the Sametime Gateway.
   This FQDN will be used when registering the Gateway for provisioning with AOL, as well as in the SRV record used for communicating with Google.
2. Install the SSL certificate.
   The CN name for the certificate should be the one defined as FQDN mapped to the public IP in step 1. For example, the diagram above uses the FQDN gw.ibm.com. For information on requesting the certificate, see Creating a certificate request.
3. Define a custom property to map the cluster FQDN for traversing the NAT:
   Define a custom property to enable communications in a NAT (Network Address Translation) environment. Traversing NAT is known issue for the SIP domain; defining the "FQDN" custom property for Sametime Gateway is a workaround for this issue. Before beginning, make sure the following requirements have been satisfied:
   - A static NAT should be defined in the NAT or Firewall (only static NATs are supported).
   - The public IP address should be mapped to the SIP proxy internal IP address.
   - A fully qualified domain name must be mapped to the public IP address serving the Sametime Gateway.
   This FQDN will be used when registering the Sametime Gateway for provisioning with AOL, as well as the SRV record used for communicating with Google.
a. Log in to the Integrated Services Console as a Sametime Gateway administrator.

b. Click System administration > Cell > Custom Properties.

c. Click New and enter information for the new custom property:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type com.ibm.sametime.gateway.fqdn as the name of the new property.</td>
</tr>
<tr>
<td>Value</td>
<td>Type your fully qualified domain name.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the new property.</td>
</tr>
</tbody>
</table>

d. Click Apply, and then click OK.

e. Perform a full synchronize with the nodes:

   1) In the Deployment Manager's Integrated Solutions Console, click System administration > Nodes.

   2) Click Full Resynchronize.

f. Restart all Sametime Gateway nodes.

For example, If you set the custom property to gw.ibm.com (and the port is set to 5070), the INVITE SDP would look like this:

```
v=0
o=- 0 0 IN IP4 gw.ibm.com
s=session
a=IN IP4 gw.ibm.com
a=t=0 0
m=message 5070 sip null
```

4. Enable the SIP Proxy IP Sprayer as follows:

a. In the Integrated Solutions Console, click Servers > Server Types > WebSphere proxy servers.

b. In the list of proxy servers, click the link for your SIP proxy server to open its Configuration page.

c. Click SIP Proxy server settings > SIP Proxy settings > Custom properties.

d. Define the TLS IP Sprayer by clicking New, adding the following settings, and then clicking OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tls.IPSprayer.host</td>
<td>The SIP Proxy server's external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>tls.IPSprayer.port</td>
<td>The port used by the IP sprayer for TLS encrypted communications; for example: 5061</td>
</tr>
</tbody>
</table>

e. Optionally define a TCP IP Sprayer by clicking New, adding the following settings, and then clicking OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp.IPSprayer.host</td>
<td>The SIP Proxy server's external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>tcp.IPSprayer.port</td>
<td>The port used by the IP sprayer for TCP communications; for example: 5060</td>
</tr>
</tbody>
</table>

f. Optionally define a UDP IP Sprayer by clicking New, adding the following settings, and then clicking OK:
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp.IPSprayer.host</td>
<td>The SIP Proxy server's external fully qualified host name; for example: stgw.example.com.</td>
</tr>
<tr>
<td>udp.IPSprayer.port</td>
<td>The port used by the IP sprayer for UDP communications; for example: 5060</td>
</tr>
</tbody>
</table>

- g. Click **Save**.
- h. Restart the SIP proxy server.
- i. Restart the cluster.

*Configuring the XMPP proxy server on IBM i:*

Configure the XMPP proxy server to allow Google Talk, and other XMPP-based instant messaging systems to flow to and from the Sametime Gateway.

*Before you begin*

Expected state: the SIP and XMPP proxy server node is installed and federated into the cell. A Sametime cluster has been installed. The Deployment Manager is started.

*Procedure*

1. On the Deployment Manager node, log into the Integrated Solutions Console.
2. Click **Servers > Application Servers** and select the **XMPPProxyServer** from the list.
3. Click **Ports**.
4. Click **New** to add a port.
5. Select **User-defined Port**.
6. Type **XMPP_INTERNAL_PORT** in the **Specify port name** field.
7. In the **Host name** field, type the IP address of the machine on which XMPPProxyServer is installed.
8. In the **Port** field, type 5271.

A note about ports:

- **XMPP_INTERNAL_PORT** is used for listening to traffic from the proxy server.
  - If the XMPPProxy and XMPPServer are installed on the same physical computer, they will attempt to listen to the same default value of XMPP_INTERNAL_PORT which is 5271. As a result, the proxy will listen to the incoming connections from the server, and the server will listen to the proxy. In order to break this endless loop, set XMPP_INTERNAL_PORT to another value for the proxy (for example, 5272).
- **XMPP_SERVER_ADDRESS** port is used on the proxy server itself to listen to traffic from an external community.
  - The XMPP_SERVER_ADDRESS port (5269) is unrelated to the “port 5269” value that appeared on the XMPP community page when you created the community. That community page port refers to the port that the external community is listening on, and is used when Sametime Gateway performs a DNS-SRV record lookup.

If you need to change a default port, click **Application Servers > Server Name** and, under the ‘Communications’ section, click **Ports**.
9. Click **OK** and **Save**.

10. In the Integrated Solutions Console, click **System administration > Cell**.

11. Under Additional properties, click **Custom Properties**, and click **New**.

12. Create **Name** and **Value** pairs for the Sametime Gateway cluster, XMPP proxy node name, and XMPP proxy server name. Type the names and values as they are spelled out in the table below. For **XMPP proxy node name**, substitute the name of the node on which the XMPP proxy resides.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STGW_CLUSTER_NAME</strong></td>
<td>SametimeGatewayCluster</td>
</tr>
<tr>
<td><strong>XMPP_PROXY_NODENAME</strong></td>
<td>XMPP proxy node name</td>
</tr>
<tr>
<td><strong>XMPP_PROXY_SERVERNAME</strong></td>
<td>XMPPProxyServer</td>
</tr>
</tbody>
</table>

13. Click **Apply** and **Save** after you type each pair. When you are done, you will have a table that looks something like this:

![Cell Properties](image)

**What to do next**

Next, you must configure a class loader and a shared library for the XMPP proxy server.

**Setting up node replication and failover for the cluster on IBM i:**

This optional procedure sets up node replication to provide high availability and fail-over support for the cluster. If one member of the cluster goes down, other nodes can continue to process the SIP request. Use this procedure only if you require high availability and fail-over support.

**Before you begin**

Before you begin, you must install IBM Sametime Gateway on each node, add the nodes to a cluster, and then start the cluster and the SIP proxy server.
Enabling high availability uses additional memory which reduces your server’s session capacity. For more information about enabling high availability, see the IBM Sametime Gateway sizing guide in the Sametime wiki:

http://www-10.lotus.com/ldd/stwiki.nsf/dx/IBM_Lotus_Sametime_Gateway_8.5.08.5.1_sizing_guidelines

About this task

Sametime Gateway offers a comprehensive high availability (HA) solution. High availability means an environment that doesn’t have a single point of failure, and therefore prevents the users from losing presence awareness in the event of a Gateway server instance failure.

Replication domains

A SIP cluster with replication and failover can consist of many server instances. Each replication domain contains a set of two servers. Therefore, the number of replication domains needed is half the number of server instances. You need to create a new replication domain for each pair of Sametime Gateway instances (deployment manager and proxy server do not count). For example: if you have eight Sametime Gateway instance, you will be creating four replication domains. In case one server instance fails, the remaining server instance begins servicing the replicated SIP sessions of the failed instance. Therefore, IBM recommends that you pair server instances that are NOT likely to fail at the same time. For example, you should not pair server instances if both are running on the same physical host.

Procedure

1. Validate that the environment is ready:
   a. Click Servers > clusters and verify that the Sametime Gateway cluster is started and the status is green.
   b. Click Servers > Proxy Servers and verify that the SIP proxy is started and the status is green.
   c. Click SIP proxy > SIP Proxy Server Settings > SIP proxy settings and verify that the cluster in the drop down box is the same Sametime Gateway cluster defined in the previous step.

2. Create your new replication domains:
   a. Click Environment > Replication Domains, and then click New. Note: Disregard the GatewayCache. This is the DynaCache used to propagate the configuration across the cluster, and is not used for SIP session replication.
   b. Type a name for the new replication domain. For example: SIPRD1.
   c. Under Number of Replicas, select Entire Domain so that the SIP session is replicated to both Gateway instances, and click OK.
   d. Repeat the above process for each replication domain you wish to create.

3. Assign replication domains to server instances:
   a. Click Servers > Application Servers, and then select a member of the cluster.
   b. Under Container Settings, click Session management.
   c. Under Additional Properties, click Distributed environment settings.
   d. Under Distributed sessions, click Memory-to-memory replication. The distributed session option will become enabled once configured.
e. Under Replication domain, select one of the replication domains that you created in previous steps. Remember, each replication domain must be assigned to exactly two server instances.

f. In the Replication mode field, select Both client and server, then click OK, and Save. Memory to memory replication is now enabled for this member of the cluster.

g. Repeat the previous step for each member of the cluster.

Starting a Sametime Gateway cluster on IBM i:

When starting a cluster for the first time, you must start the Deployment Manager, node agents, and then all Sametime Gateway servers in the cluster.

Before you begin

Before begin these steps, you must install Sametime Gateway on each node, federate the nodes into the cell, run the Cluster Configuration Wizard, and then set up SIP and XMPP proxy servers for your cluster.

About this task

In the steps that follow, you start the Deployment Manager in a command window so that you can log in to the Integrated Solutions Console and complete the remaining steps. After the Deployment Manager is started, you can view the Integrated Solutions Console pages. However, you cannot view the Sametime Gateway administration pages until you start at least one node agent and the Sametime Gateway server on that node.

Procedure

1. Log in to the Deployment Manager node as a user with administrative privileges.

2. Open a command window (QShell session on IBM i) and navigate to the stgw_profile_root\bin directory.

3. If not already started, start the Deployment Manager with the following command.

   AIX, Linux, and Solaris
   ./startManager.sh

   Windows
   startManager.bat

   IBM i
   startManager

4. Log in to one of the Sametime Gateway nodes.

5. Open a command window (QShell session on IBM i) and navigate to the stgw_profile_root\bin directory.

6. Start the node agent with the following command.

   AIX, Linux, and Solaris
   ./startNode.sh

   Windows
   startNode.bat

   IBM i
   startNode
7. Log in to the other nodes, except the Deployment Manager node, and repeat the previous steps to start the node agent on each node.

Stopping and starting a Sametime Gateway cluster’s deployment manager on IBM i:

This topic describes how to stop and start the Deployment Manager.

Procedure
1. Log in to the Deployment Manager node as a user with administrative privileges.
2. Open a command window (QShell session on IBM i) and navigate to the stgw_profile_root\bin directory.
3. Stop the Deployment Manager. Use the administrative user ID and password that you created when you installed the Deployment Manager. Note that you do not have to provide the username and password qualifiers in the command; you can wait to be prompted and then enter your credentials. Type the following commands:
   - **AIX, Linux, and Solaris**
     ```sh
     ./stopManager.sh -username username -password password
     ./startManager.sh
     ```
   - **Windows**
     ```bat
     stopManager.bat -username username -password password
     startManager.bat
     ```
   - **IBM i**
     ```sh
     stopManager -username username -password password
     startManager
     ```

Stopping and starting a Sametime Gateway cluster’s node agents on IBM i:

This topic describes how to stop and start the node agents. Typically, you stop and start node a node agent by logging onto a node and running the stop node or start node command. If they are stopped, you must start the node agents from nodes themselves.

Procedure
1. Log in to one of the Sametime Gateway nodes.
2. Open a command window (QShell session on IBM i) and navigate to the stgw_profile_root\bin directory.
3. Stop the node agent with the following command:
   - **AIX, Linux, and Solaris**
     ```sh
     ./stopNode.sh
     ```
   - **Windows**
     ```bat
     stopNode.bat
     ```
   - **IBM i**
     ```sh
     stopNode
     ```
4. Start the node agent with the following command.
   - **AIX, Linux, and Solaris**
     ```sh
     ./startNode.sh
     ```
   - **Windows**
     ```bat
     startNode.bat
     ```
   - **IBM i**
5. Log in to the other nodes, except the Deployment Manager node, and repeat the previous steps to stop and start the node agent on each node.

What to do next

You can also use the Deployment Manager Integrated Solutions Console to stop node agents:
1. Make sure the Deployment Manager is running and log into the Integrated Solutions Console on the Deployment Manager node.
2. Click **System Administration > Node agents**.
3. Select all node agents, and then click **Stop**.

**Stopping and starting a Sametime Gateway cluster on IBM i:**

Complete these steps to stop and start a cluster of Sametime Gateway servers from the Integrated Solutions Console.

**Before you begin**

Expected state: the Deployment Manager, node agents, and all servers in the cluster are started.

**About this task**

You must restart the cluster when you add, delete, or change a community.

**Procedure**
1. Log into the Integrated Solutions Console on the Deployment Manager server as a user with administrative privileges.
2. Click **Servers > Clusters**.
3. Select the Sametime Gateway cluster, and click **Stop**, and wait for the cluster to stop.
4. Click **Servers > Clusters**.
5. Select the Sametime Gateway cluster, and click **Start**.
6. Click **Servers > Proxy servers**.
7. Select the SIP proxy server and click **Start** if it is not already started.
8. Click **Servers > Application servers**.
9. Select the XMPP proxy server and click **Start** if it is not already started.

**Stopping and starting servers in a Sametime Gateway cluster on IBM i:**

This topic describes how to stop or start individual servers or nodes in a cluster.

**Procedure**
1. Log into the Integrated Solutions Console on the Deployment Manager server as a user with administrative privileges.
2. Click **Servers > Application Servers**.
3. If you want to stop a server, select the application server's check box and click **Stop**.
4. If you want to start a server, select the application server's check box and click **Start**.
Stopping and starting a stand-alone Sametime Gateway server on IBM i:

Complete these steps to stop and start a single Sametime Gateway server in a single server environment.

Procedure
1. Log in to the server machine as a user with administrative privileges.
2. Open a command window and navigate to the Sametime Gateway profile directory that contains binaries: stgw_profile_root/bin
3. Type the following command to stop the Sametime Gateway server. Note that RTCGWServer is case-sensitive, and that on all the stopserver commands, you are prompted to enter your administrative user ID and password that you created.
   - Windows:
     stopserver.bat RTCGWServer
   - Linux, AIX, or Solaris:
     ./stopserver.sh RTCGWServer
   - IBM i:
     stopServer RTCGWServer
4. Type the following command to start Sametime Gateway.
   - Windows:
     startserver.bat RTCGWServer
   - Linux, AIX, or Solaris:
     ./startserver.sh RTCGWServer
   - IBM i:
     startServer RTCGWServer

Starting the SIP and XMPP proxy servers in a Sametime Gateway cluster on IBM i:

The XMPP and SIP proxy server node is different from other Sametime Gateway node installation types in that it contains more than one server. Based on the type of traffic you expect to have in your environment (SIP or XMPP), you can start or stop the appropriate proxy server instance on the node. This removes the need to define a proxy server for each type of protocol. If you require the XMPP proxy functionality only, then start the XMPPProxyServer only. If you need SIP proxy functionality only, then start the SIPPProxyServer only. If you need both, start both.

About this task

Table 98. Instant Messaging Systems and Proxy Servers

<table>
<thead>
<tr>
<th>Instant Messaging System</th>
<th>Proxy Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime</td>
<td>SIP</td>
</tr>
<tr>
<td>AOL Instant Messenger</td>
<td>SIP</td>
</tr>
<tr>
<td>Office Communications Server</td>
<td>SIP</td>
</tr>
<tr>
<td>Google Talk</td>
<td>XMPP</td>
</tr>
<tr>
<td>Jabber</td>
<td>XMPP</td>
</tr>
</tbody>
</table>

Before you start the SIP and XMPP proxy servers, you must add nodes to the cluster, create the cluster, set up a SIP and XMPP proxy server, and then start the cluster.
Procedure
1. On the Deployment Manager node, log in to the Integrated Solutions Console.
2. Choose Servers > Clusters.
3. Verify that the cluster status is Started (shown with a green arrow).
4. Click Servers > Proxy servers.
5. Select the SIP proxy server and click Start.
6. Choose Servers > Applications servers.
7. Select the XMPP proxy server and click Start.

Registering a new Gateway cluster on IBM i with the System Console:

After installing the IBM Sametime Gateway cluster on IBM i, register it with the Sametime System Console, which allows you to manage all Sametime servers from a central location.

Before you begin

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the cluster’s Deployment Manager, follow these steps to update properties files and run the registration utility to register the cluster with the console.

Note: Run this utility only on the Deployment Manager; do not register individual nodes because they will be registered automatically during the cluster registration.

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

- console.properties
- productConfig.properties

Procedure
1. On the Deployment Manager, navigate to the stgw_server_root/console directory.

   Note: If a cluster’s Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager’s profile.

2. Make backup copies (using different names) of the console.properties and productConfig.properties files.
3. Update the Deployment Manager’s console.properties file:
   a. Open the file for editing.
b. Update the file with the following values:

**Table 99. console.properties settings for the Deployment Manager**

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</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.

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. |
| 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." |

(c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

4. Update the Deployment Manager's productConfig.properties file:
   a. Open the file for editing.
b. Update the file with the following values:
   Only the required values in this file are listed here:

**Table 100. productConfig.properties settings for the Deployment Manager**

<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>WASPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBindAnonymous</td>
<td>Change to &quot;true&quot; only if you are allowing anonymous access to the LDAP server.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

5. Update the Primary Node’s productConfig.properties file on the Deployment Manager server:
   a. Navigate to the `app_server_root/profiles/DMProfile/config/cells/DMCell/nodes/PNnode` directory.
   b. Open the file for editing.
   c. In the `DepName` setting, provide a descriptive name for Primary Node deployment; it must be a unique deployment name on the Sametime System Console.
   d. Set the value of `isFederated` to true for a primary or secondary node. The registration utility cannot run without this value.
   e. Verify that the remaining settings are appropriate for the Primary Node.
   f. Save and close the file.

6. Update the Secondary Node’s productConfig.properties file on the Deployment Manager server:
   a. Navigate to the `app_server_root/profiles/DMProfile/config/cells/DMCell/nodes/SNnode` directory.
   b. Open the file for editing.
   c. In the `DepName` setting, provide a descriptive name for the Secondary Node deployment; it must be a unique deployment name on the Sametime System Console.
   d. Set the value of `isFederated` to true for a primary or secondary node. The registration utility cannot run without this value.
   e. Verify that the remaining settings are appropriate for the Secondary Node.
   f. Save and close the file.

7. Run the registration utility:
   b. From an IBM i command line, run the following command to start the QShell Interpreter: `QSH`.
   c. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.
   d. Run the shell script to register the server: `registerProduct.sh`.
   e. When the utility prompts for the cluster’s name, type the name and press `Enter`.
   f. When the registration script completes, press F3 to exit QSH.

The utility registers the cluster, as well as each node, generating a log file called `ConsoleUtility.log` and storing it in the `consoles/logs` directory. If the registration is successful, a `console.pid` will also be generated.

8. Start the Sametime Gateway cluster, if it is not already running.

Installing Sametime Gateway in silent mode on IBM i:
IBM Sametime Gateway can be installed silently using a response file. You can either generate your own response file by installing using the install wizard, or by editing the default response file that is provided.

Performing a silent installation on IBM i:

IBM Sametime Gateway can be installed silently using a response file. You can either generate your own response file by installing using the install wizard, or by editing the default response file that is provided.

Before you begin

You must install WebSphere Application Server separately before performing a silent installation. The silent installation program must be run in QSH mode.

Information on downloading packages for Sametime is located at the following Web address:

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

About this task

A response file is a text file that contains all the options that would normally be specified in the installation dialogs. Silent installation is useful in situations where automation is desired.

To perform a silent installation, you have to create a new response file or edit the existing response file that is included with the product. On the root of the Sametime Gateway installation CD is a fully-documented response file: installresponse.txt. Copy this file to the machine and edit it with values appropriate for your environment, or complete the following steps to create a response file based on a real installation.

Procedure

1. From the installation media, copy and unzip the following Sametime Gateway installation image to a temporary directory /TMP on the machine where you will be installing Sametime Gateway:
   
   C17KOML.exe

   This step creates a folder: /TMP/SametimeGateway.

2. Copy the folder /TMP/SametimeGateway to the IFS of the IBM i system.

3. Start a QSHELL session.

4. Navigate to the /TMP/SametimeGateway folder.

5. Record a response file by typing the following command. This will perform an installation and generate a response file:

   install.sh -options-record response_file

   where response_file is an absolute path to the response file to be generated.

   install.sh -options-record /TMP/SametimeGateway/gatewayOptions.txt

6. If another Sametime Gateway installation exists on the system, you must allow for the existence of more than one Sametime Gateway server by completing the sub steps that follow:

   a. Using a text editor, open the response file.

   b. Search for the line starting with "-V Coexist=".
c. If the line exists set the value to be `-V Coexist="true"`. If the line does not exist, add `-V Coexist="true"` to the bottom of the file.

d. Save and close the response file.

7. Once a response file is created, either by modifying the `installresponse.txt` file included with the installer, or by generating your own response file, open a command window.

8. Type the following command to use the response file that you created:
   
   ```bash
   install.sh -options response_file -silent
   ```

Results

Upon completion of the installation, control will return to the command window. Validation or installation errors are logged to the installation log file.

Note: Generating response files using the `-options-record` option puts clear text passwords in the response file.

Adding a Sametime Gateway server on IBM i 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.

### Configuring LDAP for Sametime Gateway on IBM i

Configure Sametime Gateway to use the LDAP directory used by the local Sametime environment. If you did not connect to LDAP when you installed Sametime Gateway, or you did connect to LDAP but now want to create a secure connection, use these procedures. Sametime Gateway must look up names and groups in the LDAP directory to grant users and groups access to external communities.

### About this task

Use Sametime Gateway with virtually any LDAP directory that is supported by Sametime and the WebSphere Application Server environment. Sametime Gateway deployment does not require changes to existing directory structures. It's recommended that you configure the same LDAP directory that is used by the Sametime community server. You can use a separate LDAP directory, but information between the two LDAP directories must be replicated and identical.

**Note:** The use of an LDAP directory is not required for Sametime Gateway, but it lets you implement an access control list (ACL) that controls which users and groups can access, and be accessed from, external communities. If you do not want to configure the use of an LDAP directory at this time, you can skip the procedure. If you later decide to start using an LDAP directory for Sametime Gateway, you can configure the interaction at that time.

Be sure to read the first topic below before setting up your LDAP directory:

### LDAP and access to external and internal users with Sametime Gateway on IBM i

Sametime Gateway works with the LDAP user registry used by your local Sametime community so that you can assign local users permission to access members in external and clearinghouse communities. For local users to chat with and share presence with a member of an external community, two events must happen: you must assign the local user to the external community and the external community administrator must assign the external community member access to your Sametime community.

You can use Sametime Gateway with virtually any LDAP directory that is supported by Sametime or the WebSphere Application Server environment. Sametime Gateway deployment does not require changes to existing directory structures. When you configure WebSphere Application Server to use an LDAP user registry, you are identifying to Sametime Gateway the LDAP directory that houses members of the local Sametime community. As an administrator, you look up names and groups in the LDAP directory and assign them capabilities when accessing an external community.
Using LDAP, you can assign users and group to capabilities such as instant messaging or presence or both when assigning users and groups access to an external community. Sametime Gateway displays group names, user names (short names), and user e-mail addresses. Groups do not have e-mail addresses.

**Access to internal and external communities**

When you assign a local user from your LDAP directory access to an external community, you provide, at the local level, permission for that local user to exchange instant messages with potentially all members of an external community. You cannot give the user permission to subscribe to *some* members of the external community because you cannot control who in the external community has access to the local user. If the administrator in an external community assigns all members in the external directory access to your local community, your local Sametime user can subscribe to all members of the external community and all external community members can subscribe to your user.

As an administrator, you cannot set access for external users because there is no way for you to configure access in external directories. External users can only have instant messaging and presence with the members of your local community for whom you have assigned access. The only people who can be subscribed to by external users are the users and groups who have been granted access by you.

For example, if local user John has not been granted access to external community, and external user Mary subscribes to John's presence, Mary will never receive a response because local user John does not have the rights to send a response. Any subscription requests from an external user is blocked by the Sametime Gateway because the local user is not granted access to subscribe to the external community.

**Configuring LDAP for a single server on IBM i:**

IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use a Lightweight Directory Access Protocol (LDAP) user registry that contains members of the local Sametime community. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

**Before you begin**

Expected state: Administrative security is enabled. The Deployment Manager is running.

**Procedure**

1. If not already started, start Sametime Gateway:
   a. Open a QShell session.
   b. Navigate to the Sametime Gateway profile directory that contains binaries: `stgw_profile_root\bin`
   c. Type the following command. Note that `RTCGWServer` is case-sensitive.
      ```
      startServer RTCGWServer
      ```
2. Ensure that the enterprise LDAP server is running.
3. Complete the following sub steps to connect to LDAP over SSL, otherwise skip this step. 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.

a. From the Integrated Solutions Console, select Security > SSL Certificates and key management, then select Key stores and certificates.

b. Click NodeDefaultTrustStore.

c. Click Signer certificates.

d. Click Add.

e. In the Alias field, type a description for the certificate, whether it's self-signed or a public CA.

f. In the File name field, type the path to the certificate file.

g. Click Apply and then Save.


5. Make sure the Enable administrative security and Enable application security options are selected.

6. In the Available realm definitions, select Federated repositories.

7. Click Set as current.

8. Click Configure.

9. Click Add base entry to the Realm.

10. On the next screen, click Add Repository...

11. Type a logical name for the repository in the Repository Identifier field. The identifier can be any value, as long as it's unique within the cell.

12. Select the type of LDAP server to use from the Type list. If you have an IBM Lotus Domino Version 7.0 server, select IBM Lotus Domino Version 6.5 as your LDAP type.

13. Enter the fully qualified host name of the LDAP server in the Primary host name field. You can enter either the IP address or domain name system (DNS) name.

14. Enter the LDAP server port number in the Port field. The host name and the port number represent the realm for this LDAP server in the WebSphere Application Server cell. The default value is 389.

15. Optionally, enter the bind DN name in the Bind distinguished name field. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. Leave this field blank to connect to the LDAP server anonymously.

16. Optionally enter the password corresponding to the bind DN in the Bind password field. Leave this field blank to connect to the LDAP server anonymously.

17. Specify the Login properties when setting up the repository. The cn, uid, and mail are common login property values. If your LDAP server uses a login property other than uid, you must change the value to match your user prefix.

18. Click Apply, and then click Save.

19. In the Distinguished name of a base entry that uniquely identifies this set of entries in the realm field, type the base DN of your choice such as "o=myLDAPRealm" or "o=defaultWIMLDAPBasedRealm". This DN is for internal Websphere Application Server use only and is used to identify a set of entries when returning search results.

20. In the Distinguished name of a base entry in this repository field, type the DN of the base entry within the directory to begin searches. Leave this field blank to start LDAP searches at the root of your LDAP repository, or if you...
have a Domino LDAP, which always begins searches at the root of the directory. An example of a DN for the base entry in a repository:

dc=IBM,dc=COM

21. Click **Apply**, and then click **Save**.

22. Use a text editor and open `wimconfig.xml`. The directory path that follows is all on one line but represented here on two lines for printing:

```plaintext
app_server_root\profiles\RTCW_Profile
\config\cells\<cell_name>\wim\config\wimconfig.xml
```

The `<cell_name>` is the name of your cell.

23. Search for the following text:

```xml
<config:attributeConfiguration>
```

24. Below this line of text, add the following line if it does not exist:

```xml
<config:externalIdAttributes name="dominounid"/>
```

25. The correct value for your directory from the following list:

- Domino LDAP: dominounid
- IDS: ibm-entryuuid
- Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

For example, if you have a Domino LDAP, your text may look like this. Note that your text may be different.

```xml
<config:attributeConfiguration>
  <config:externalIdAttributes name="dominounid"/>
  <config:attributes name="userPassword" propertyName="password"/>
  <config:entityTypes>Group</config:entityTypes>
  <config:attributes>
    <config:attributes name="cn" propertyName="cn"/>
    <config:entityTypes>Group</config:entityTypes>
  </config:attributes>
  <config:propertiesNotSupported name="businessAddress"/>
</config:attributeConfiguration>
```

25. Now find the `<config:repositories>` element and add the following line to the `<config:attributeConfiguration>` element block:

```xml
<config:externalIdAttributes name="<unique_attribute>" syntax="<attribute_syntax>"/>
```

where `<unique_attribute>` is the unique LDAP attribute that you want to use and `<attribute_syntax>` identifies the syntax. Include the syntax attribute only if the syntax is something other than a type of string.

For example, to use a string called `dominounid`, edit the `wimconfig.xml` file to include the following element:

```xml
<config:externalIdAttributes name="dominounid"/>
```

If the attribute was not a string, you would identify its syntax as well. For example:

```xml
<config:externalIdAttributes name="GUID" syntax="octetString"/>
```

The following are some examples of commonly used unique attributes for different some flavors of LDAP:

- Domino LDAP: dominounid
- IDS: ibm-entryuuid
- Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid
26. Save the file. Note: the **dominounid** attribute was introduced in Lotus Domino 6.5.4 and 7.0. In some cases this attribute may not appear in the schema database or on the Server Configuration document (LDAP tab). This can occur when the administration server for the Domino domain is version 6.5.3 or lower. The Administration server controls the creation of the Schema database, as well as which attributes are available for anonymous queries through the Configuration document. To resolve the issue, the Administration server should be upgraded to Domino version 6.5.4 or above. In addition, while a particular Domino LDAP may not require to bind, binding is necessary to retrieve the **dominounid** attribute. Any bind user would be acceptable, read only is fine.

27. Stop and then restart the Sametime Gateway server:
   a. Navigate to the directory that contains binaries: `stgw_profile_root\bin`
   b. Type the following commands, depending on your operating system, to stop and then start Sametime Gateway. You must use the user name and password that you provided when you enabled administrative security to stop the server. Wait for the `stopserver` command to finish before executing the `startserver` command. Note that RTCGWServer is case-sensitive.
      
      ```
      stopServer RTCGWServer -username username -password password
      startServer RTCGWServer
      ```

28. log into the Integrated Solutions Console.

29. Select **Users and Groups > Manage Users.**

30. Click **Search** to verify that you can search your LDAP directory. If your LDAP functionality is enabled, you should see a list of users on the screen.

31. Click a user name and make sure you can see the user's content. You can verify group names as well.

32. Copy the script: `stgw_server_root/config/adminscripts/rtcgw_vmm.jacl` to `stgw_profile_root/bin`.

33. Open a separate command window and navigate to `stgw_profile_root/bin`.

34. Run the following command:
   ```
   wsadmin -username username -password password -f rtcgw_vmm.jacl
   ```
   Where `username` is the administrative user ID that you use to log into the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. For example:
   ```
   wsadmin -username wasadmin -password gateway4u -f rtcgw_vmm.jacl
   ```

35. Stop and then restart the Sametime Gateway server:
   a. Navigate to the directory that contains binaries: `stgw_profile_root\bin`
   b. Type the following commands, depending on your operating system, to stop and then start Sametime Gateway. You must use the user name and password that you provided when you enabled administrative security to stop the server. Wait for the `stopserver` command to finish before executing the `startserver` command. Note that RTCGWServer is case-sensitive.
      
      **AIX, Linux, and Solaris**
      ```
      ./stopServer.sh RTCGWServer -username username -password password
      ./startServer.sh RTCGWServer
      ```
      **Windows**
      ```
      stopServer.bat RTCGWServer -username username -password password
      startServer.bat RTCGWServer
      ```
      **IBM i**
stopServer RTCGWServer -username username -password password
startServer RTCGWServer

36. The remaining optional steps apply to an LDAP server that is not a Domino LDAP directory. By default, Sametime uses mail as the attribute in an LDAP record to search for users. If your LDAP directory uses a different attribute, you can change Sametime to use that attribute instead. For example, if you want to change Sametime to instead use the attribute displayName, complete the following steps:
   a. Use a Lotus Notes client on the Sametime server to open the Sametime Configuration database (stconfig.nsf).
   b. Click File > Database > Open and select the Local server.
   c. Select the Sametime Configuration database (stconfig.nsf).
   d. Click Open.
   e. In the right pane of the Configuration database, locate the LDAP server entry in the Form Name column of the Configuration.
   f. Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the Last Modified Date column. The date represents the last time the LDAP server document was modified.
   g. To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
   h. When the LDAP Server document opens, double-click the document to put it in edit mode.
   i. Search and replace mail with displayName.

Search filter for resolving person names:

\((objectclass=organizationalPerson)\(uid=%s*\)(givenname=%s*)(sn=%s*)(mail=%s*)\)

Search filter to use when resolving a user name to a distinguished name:

\((objectclass=organizationalPerson)\(uid=%s\)(givenname=%s)(sn=%s)(mail=%s)\)

"Attribute of the person entry that defines the person's e-mail address" mail

j. Save your changes and then restart the Domino server.

k. On the Sametime Gateway server that is connected to LDAP, use a text editor and open the following file:

stgw_profile_root\config\cells\<cell_name>\wim\config\wimconfig.xml

l. Add the following line under the other configuration attributes:
   <config:attributes name="displayName" propertyName="mail"/>
   For example:
   <config:attributes name="userPassword" propertyName="password"/>
   - <config:attributes name="cn" propertyName="displayName">
   <config:entityTypes>Group</config:entityTypes>
   </config:attributes>
   - <config:attributes name="cn" propertyName="cn">
   <config:entityTypes>Group</config:entityTypes>
   </config:attributes>
   <config:propertiesNotSupported name="businessAddress"/>

m. Save the file.

n. Stop and restart the Sametime Gateway server.

Configuring LDAP for a cluster on IBM I:
The IBM Sametime Gateway requires that IBM WebSphere Application Server be configured to use the Lightweight Directory Access Protocol (LDAP) user registry that contains members of the local Sametime community. These steps include information for setting up a connection to LDAP using a self-signed certificate. Complete the following steps if you did not create a connection to LDAP at installation, or you completed a connection to LDAP but want to secure that connection over SSL.

Before you begin

Expected state: the Deployment Manager and node agents are started. The servers are stopped. Administrative security is enabled.

Procedure

1. Log in to the Deployment Manager node as a user with administrative privileges. Make sure you have an enterprise LDAP server that contains members of the local Sametime community and the LDAP server is running.
2. Complete the following sub steps to connect to LDAP over SSL, otherwise skip this step. If your LDAP server is using a public CA, 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.
   a. From the Integrated Solutions Console, select Security > SSL Certificates and key management, then select Key stores and certificates.
   b. Click CellDefaultTrustStore.
   c. Click Signer certificates.
   d. Click Add.
   e. In the Alias field, type a description for the certificate, whether it's self-signed or a public CA.
   f. In the File name field, type the path to the certificate file. For example, c:\certname.cer.
   g. Click Apply and then Save.
4. Make sure the Enable administrative security and Enable application security options are selected.
5. In the Available realm definitions, select Federated repositories.
6. Click Set as current.
7. Click Configure.
8. Click Add base entry to the Realm...
9. On the next screen, click Add Repository...
10. Type a logical name for the repository in the Repository Identifier field. The identifier can be any value, as long as it is unique within the cell.
11. Select the type of LDAP server to use from the Type list. If you have a IBM Lotus Domino Version 7.0 server, select IBM Lotus Domino Version 6.5 as your LDAP type.
12. Enter the fully qualified host name of the LDAP server in the Primary Host field. You can enter either the IP address or domain name system (DNS) name.
13. Enter the LDAP server port number in the Port field. The host name and the port number represent the realm for this LDAP server in the WebSphere Application Server cell. The default value is 389.
14. Optionally, enter the bind DN name in the **Bind distinguished name** field. The bind distinguished name can be any user with read permission for the directory server. The bind DN need not be the LDAP administrator. Leave this field blank to connect to the LDAP server anonymously.

15. Optionally, enter the password corresponding to the bind DN in the **Bind password** field. Leave this field blank to connect to the LDAP server anonymously.

16. Specify the **Login properties** when setting up the repository. The *cn*, *uid*, and *mail* are common login property values. If your LDAP server uses a login property other than *uid*, you must change the value to match your user prefix.

17. Click **Apply**, and then click **Save**.

18. In the **Distinguished name of a base entry that uniquely identifies this set of entries in the realm** field, type the base DN of your choice such as "o=myLDAPRealm" or "o=defaultWIMLDAPBasedRealm". This DN is for internal Websphere Application Server use only and is used to identify a set of entries when returning search results.

19. In the **Distinguished name of a base entry in this repository** field, type the DN of the base entry within the directory to begin searches. Leave this field blank to start LDAP searches at the root of your LDAP repository, or if you have a Domino LDAP, which always begins searches at the root of the directory. An example of a DN for the base entry in a repository:

   dc=IBM,dc=COM

20. Click **Apply**, and then click **Save**.


22. On the Deployment Manager, use a text editor and open wimconfig.xml. The directory path that follows is all on one line but represented here on two lines for printing:

   app_server_root/profiles/RTCGW_Profile/config/cells/cell_name/wim/config/wimconfig.xml

   The **cell_name** is the name of your cell.

23. Find the **configLdapRepository** section:

   </config:repositories><config:repositories xsi:type="config:LdapRepositoryType">

24. Within that section, find the **config:attributeConfiguration** element block.

25. Add a line for **config:externalIdAttributes** if one does not already exist, using one of the following formats.

   • Add this line if the ID attribute has a default syntax type of string.

     <config:externalIdAttributes name="unique_attribute"/>

     where **unique_attribute** is the unique LDAP attribute that you want to use. The following example adds a string called **dominounid**:

     <config:externalIdAttributes name="dominounid"/>

   • Add this line if the ID attribute has a syntax type other than string.

     <config:externalIdAttributes name="unique_attribute" syntax="attribute_syntax"/>

     where **unique_attribute** is the unique LDAP attribute that you want to use and **attribute_syntax** identifies the syntax. You must include the syntax attribute only if the syntax is a type other than string.

     The following example adds an octetString attribute called **GUID**, which is the Novell eDirectory attribute:

     <config:externalIdAttributes name="GUID" syntax="octetString"/>
The following are some examples of commonly used unique attributes for different flavors of LDAP:

- Domino LDAP: dominounid
- IDS: ibm-entryuuid
- Active Directory: objectguid
- Novell eDirectory: guid
- Sun ONE: nsuniqueid

26. Save the file.

27. Navigate to the \texttt{rtcgw\_profile\_root/bin} directory.

28. 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 created when you enabled administrative security. Type the following commands:

\texttt{./stopServer.sh dmgr -username \_username -password \_password
startServer.sh dmgr}

29. Synchronize your changes to all nodes in the cluster. Click \textbf{System Administration > Nodes}.

30. Select all nodes in the cluster, then click \textbf{Full Resynchronize}.

31. Restart the node agents.
   a. Log into the Integrated Solutions Console on the Deployment Manager node.
   b. Click \textbf{System Administration > Node agents}.
   c. Select all node agents, and then click \textbf{Restart}.

32. Choose \textbf{Servers > Clusters}.

33. Select the Sametime Gateway cluster and click \textbf{Start}. Verify that the cluster status is started. (shown with a green arrow).

34. Select \textbf{Users and Groups > Manage Users}.

35. Click \textbf{Search} to verify that you can search your LDAP directory. If your LDAP functionality is enabled, you should see a list of users on the screen.

36. Click a user name and make sure you can see the user's content. You can verify group names as well.

37. Copy the following script:

\texttt{from:
stgw\_server\_root/config/adminscripts/rtcgw\_vmm.jacl
to the Deployment Manager node:
app\_server\_root/bin}

38. Open a QShell session and navigate to \texttt{app\_server\_root/bin}.

39. Run the following command:

\texttt{wsadmin -username \_username -password \_password -f rtcgw\_vmm.jacl}

Where \texttt{username} is the administrative user ID that you use to log into the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. For example:

\texttt{wsadmin -username wasadmin -password gateway4u -f rtcgw\_vmm.jacl}

This script will place the default file repository of the WebSphere Application Server at the bottom of listed \texttt{config\_repositories} tags of wimconfig.xml, so it is searched after the newly created repository.

40. In the DB2 window on the Deployment Manager node, 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. Type the following commands:

\`
stopManager -username username -password password
startManager
``

41. Restart the node agents.
   a. Log into the Integrated Solutions Console on the Deployment Manager node.
   b. Click **System Administration > Node agents**.
   c. Select all node agents, and then click **Restart**.

42. Choose **Servers > Clusters**

43. Select the Sametime Gateway cluster and click **Start**. Verify that the cluster status is started. (shown with a green arrow).

44. The remaining optional steps apply to an LDAP server that is not a native internal Domino directory. Complete these steps to change the default attribute of the person entry that defines the person's e-mail address in `app_server_root/profiles/RTCGW_Profile/config/cells/cell_name/wim/config/wimconfig.xml`. The default attribute is `mail`. If you want to change the default attribute to `displayName`, complete the following steps:
   a. Use a Lotus Notes client on the Sametime server to open the Sametime Configuration database (stconfig.nsf).
   b. Click **File > Database > Open** and select the Local server.
   c. Select the Sametime Configuration database (stconfig.nsf).
   d. Click **Open**.
   e. In the right pane of the Configuration database, locate the LDAP server entry in the **Form Name** column of the Configuration.
   f. Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the **Last Modified Date** column. The date represents the last time the LDAP server document was modified.
   g. To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
   h. When the LDAP Server document opens, double-click the document to put it in edit mode.
   i. Search and replace `mail` with `displayName`.
      
      Search filter for resolving person names:
      `(&(objectclass=organizationalPerson) (|(uid=%s*)(givenname=%s*)(sn=%s*)(mail=%s*)))`
      
      Search filter to use when resolving a user name to a distinguished name:
      `(&objectclass=organizationalPerson) (|(uid=%s)(givenname=%s)(sn=%s)(mail=%s))`
      
      "Attribute of the person entry that defines the person's e-mail address" mail
   j. Save your changes and then restart the Domino server.
   k. On the Sametime Gateway server that is connected to LDAP, use a text editor and open the following file:
      `app_server_root/profiles/RTCGW_Profile/config/cells/cell_name/wim/config/wimconfig.xml`
   l. Add the following line under the other configuration attributes:
      `<config:attributes name="displayName" propertyName="mail"/>` For example:
      ```xml
      <config:attributeConfiguration>
        <config:externalIdAttributes name="dominounid"/>
        <config:attributes name="userPassword" propertyName="password"/>
        <config:attributes name="cn" propertyName="displayName">
        <config:attributes name="displayName" propertyName="mail"/>
      </config:entityTypes>Group</config:entityTypes>
      ```
m. Save the file. Note: the dominounid attribute was introduced in Lotus Domino 6.5.4 and 7.0. In some cases this attribute may not appear in the schema database or on the Server Configuration document (LDAP tab). This can occur when the administration server for the Domino domain is version 6.5.3 or lower. The Administration server controls the creation of the Schema database, as well as which attributes are available for anonymous queries through the Configuration document. To resolve the issue, the Administration server should be upgraded to Domino version 6.5.4 or above. In addition, while a particular Domino LDAP may not require to bind, binding is necessary to retrieve the dominounid attribute. Any bind user would be acceptable, read only is fine.

n. Stop and restart the Deployment Manager, the node agents and Sametime Gateway servers.

Results

You are now ready to set up SSL on a cluster.

Connecting servers to Sametime Gateway on IBM i

To complete IBM Sametime Gateway setup, you connect servers to the Sametime Gateway by performing some configuration steps on the local Sametime server, adding the local community to the Sametime Gateway, registering your Sametime Gateway server with AOL so that Sametime Gateway can connect to the AOL clearinghouse, and then, after you complete your registration, adding the AOL clearinghouse community to the Sametime Gateway. Finally, you want to note the port numbers so you can provide these ports to external communities.

Opening ports in the firewalls (IBM i):

Open specific ports in the internal and external firewalls to allow messages to flow to and from the Sametime Gateway server in the DMZ to the local Sametime community, and to permit access to LDAP and DB2. In addition, verify that the external firewall allows inbound and outbound connections to and from specific IP addresses. Make sure any kind of SIP fixup or SIP inspection is disabled in your firewall settings.

About this task

A Sametime Gateway server or cluster is normally deployed in the DMZ, which is the zone between the internal and external firewalls. Work with your network firewall administrator to open ports in the internal firewall to allow Sametime Gateway to connect to the local Sametime community servers, LDAP, and DB2. You also need to open ports in the external firewall to allow Sametime Gateway to connect with external communities.
You can deploy a Network Address Translator (NAT) between local Sametime community servers and a Sametime Gateway. However, deploying a NAT device between Sametime Gateway and the Internet is not supported when trying to connect Sametime Gateway to AOL or TLS-encrypted SIP-based external communities. While there are SIP-aware NAT devices, they are not sufficient because AOL communities require secure SIP (SSL/TLS) communication, and a NAT device would not be able to decrypt and translate the packets for proper operation. NAT has no affect on the XMPP protocol, so exchanges using Google Talk over XMPP are always permitted to pass through a NAT-enabled firewall that is between Sametime Gateway and the Internet.

Procedure
1. Open the following ports in the internal firewall:
   - Port 1516 on the internal firewall to each Sametime community server in the local Sametime community, the Sametime Gateway will be the one creating the TCP connection to the destination IP at destination port 1516.
   - Port 389 on the internal firewall to the LDAP directory, or port 636 if LDAP access is over SSL.
   - Port 50000 on the internal firewall to a DB2 server.
2. Open the following ports on the external firewall as needed:
   - Port 5269 on the external firewall to Google Talk and non-secured XMPP.
   - Port 5270 on the external firewall to secured XMPP.
   - Port 5061 on the external firewall to external Sametime or AOL communities using a secure TLS/SSL connection.
   - Port 5060 on the external firewall to an external Sametime community (only if using a non-TLS/SSL connection).
   - Port 53 on the external firewall to external DNS servers to resolve the fully qualified domain name of external community servers.
3. Verify that the external firewall allows inbound and outbound connections to and from the following IP addresses:
AOL:
64.12.162.248, 205.188.153.55

For Google Talk, update your firewall rules to allow inbound and outbound traffic on the list of IP ranges supported by Google Talk.

**Note:** The list of supported IP ranges for connecting Google Talk changes periodically. For the current list of IP ranges, see List of supported Google Talk IP ranges for use with Sametime Gateway.

In the command window, type:
nslookup talky.l.google.com
Then type:
nslookup talkz.l.google.com
For example:

```
C:\>nslookup talky.l.google.com
Name: talky.l.google.com
Addresses: 74.125.47.125, 74.125.65.125, 74.125.155.125, 209.85.137.125
209.85.163.125, 209.85.229.125, 216.239.51.125, 64.233.169.125, 72.14.203.125
72.14.247.125
```

```
C:\>nslookup talkz.l.google.com
Non-authoritative answer:
Name: talkz.l.google.com
```

The talky.l.google.com addresses are for connections that are incoming from the enterprise to Google. The talkz.l.google.com addresses are for connections that are incoming from Google to the enterprise.

4. Make sure that the Sametime Gateway server can resolve a reverse lookup on each of the Google IP addresses.

You can verify this by substituting each IP address into the following command:
```
\nslookup
> 209.85.163.125
Server: UnKnown
Address: 129.42.250.40
```

Name: el-in-f125.google.com
Address: 209.85.163.125

**Connecting the local Sametime Community Server to Sametime Gateway (IBM i):**

Complete these steps to prepare and then add your local Community Server to Sametime Gateway.

*Adding Sametime Gateway (IBM i) 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 completely 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.

**Specifying the mail attribute for LDAP person records used by Sametime Gateway (IBM i):**

If your Sametime servers are configured to use an LDAP server that is not a native internal Domino directory, you must specify the attribute in an LDAP record that contains the user's email address. This setting is required because SIP entities are identified by their email addresses.

**Procedure**

1. From the Sametime server home page, click the *Administer the Server* link to open the Sametime Administration Tool.
2. Choose *LDAP Directory - Basics*.
3. In the *Basics settings for server* drop-down list, select the LDAP server.
4. In the *Attribute of a person entry that defines the person's email address* setting, type the attribute that your LDAP directory uses to hold the user’s email address. Default attribute names include the following:
• Type `mail` (default) if your LDAP directory is a Domino Directory, IBM Directory Server, or Sun ONE Java System Directory Server.

• Type `userPrincipalName` (default) if you are using Microsoft Active Directory.

5. Click **Update**.


7. In the search filter for resolving person names, update the search filter to contain the attribute specified in step 4 above. For example, if the LDAP directory uses the mail attribute, then update the search filter to include the mail attribute. For example:
   \(((&(objectclass=organizationalPerson)\((cn=%s*)(givenname=%s*)(sn=%s*)(mail=%s*))))\)

8. Click **Update** and restart the server for the change to take effect.

---

**Allowing local Sametime clients to add external users connected through Sametime Gateway (IBM i):**

Complete these steps to allow your Sametime clients to add external users to Contact Lists.

**About this task**

Follow these steps to change policies to allow users to add external contacts.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. In the Instant Messaging tab, select the policy you want to change and click **Edit**.
5. In the Chat section select "Allow user to add external users using Sametime gateway communities."
6. Click **OK**.

**Results**

After you complete these steps, users will see an **External Contact** check box on the **Add New Contact** dialog. To add an external contact, users type the external user’s email address (name@domain), select **External Contact**, and then click **Add**.

---

**Disabling the Sametime SIP Gateway (IBM i) on the local Sametime server:**

To use Sametime Gateway with a local Sametime server version 6.5.1 or 7.0, you must disable the Sametime SIP Gateway application.

**Procedure**

1. **Windows:** Disable the Sametime SIP Gateway application by completing the following steps:
   a. Click **Start** > **Programs** > **Administrative tools** > **Services**.
   b. Right click on **ST SIP Gateway** and click **Stop**.
   c. Right click on **ST SIP Gateway** and click **Properties**.
   d. In the **Startup type** drop-down list, select **Disabled**.
   e. Click **OK**.
f. Restart the Sametime server.

2. **AIX, Solaris, IBM i:** Disable the Sametime SIP Gateway application by completing the following steps:
   a. Open a command window. On IBM i, run the STRQSH (Start Qshell) command.
   b. Navigate to \\lotus\\domino.
   c. Use a text editor and open the StCommLaunch.dep file.
   d. Delete the following line from the file:
      ```
      AIX and Solaris:
      SERVERAPP ST SIP Gateway,ST Community,SOFT
      ```
      ```
      IBM i:
      SERVERAPP StGateway,StCommunity,SOFT
      ```
   e. Save the file.
   f. Restart the Sametime server.

*Adding a local Community Server to Sametime Gateway (IBM i):*

Connect a local Sametime Community Server or Sametime community cluster to Sametime Gateway to enable Sametime users to have instant messaging with external users.

**Before you begin**

Before you can add a local Sametime server to Sametime Gateway, make sure you've completed the preceding steps:

- Opened port 1516 on the internal firewall to the local Sametime community server. If the Sametime community is clustered, you opened port 1516 to each of the Sametime community servers, allowing both inbound and outbound traffic between Sametime Gateway and each community server.
- Configured the Sametime server to trust the IP addresses of Sametime Gateway servers.
- Disabled the legacy Sametime SIP Gateway on the Sametime community server.
- Allowed local Sametime clients to add external users to Contact Lists.

**Important:** You can only connect one gateway to a community; otherwise the awareness and chat features may not work properly. Likewise, you can connect only one local Sametime community to Sametime Gateway. You must add the local community to Sametime Gateway before you add external communities.

**About this task**

**Expected state:**

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway servers are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities.**
2. In the table that lists communities, click **New.**
3. In the **Name** field, type a logical name for the local community such as Sametime Users.

4. In the **Community Type** field, select **Local**.

5. In the **Domains** field, type the domain names in which users are found in the local community.

**Notes:**
- Wildcards are not supported in this field, you must type each complete domain name.
- Each domain name must access the same user directory. For example: acme.com, us.acme.com, fr.acme.com, and uk.acme.com must all be linked by a common user directory to be in the community. Obtain this information from the system administrator of the local Sametime community.
- If you plan to connect to Google Talk or other XMPP communities, all the domains listed must have an existing SRV record. See the instructions in Connecting to Google talk community. If even a single listed domain does not have an SRV record, the Google community cannot connect.

6. In the **Translation Protocol** field, select **VP**.

7. Provide the **Host name** that Gateway connects to when it reads the overall configuration of the Community Servers. Depending on the size of your deployment, Sametime Gateway connects to either a single Sametime Community Server or a virtual IP address if you have one configured one for routing to multiple Community Servers.

Type the appropriate host name.

- **One Sametime Community Server**
  - Enter the server's host name.

- **Multiple Community Servers (in a distributed or clustered environment)**
  - Enter the host name of a Virtual IP (VIP) configured to route to an available Community Server at all times. This is a bootstrapping phase, in which the Gateway connects to the Community Server the VIP is currently pointing to so it can read the cluster configuration information. This information contains the list of Community Server host names. The Gateway then closes the connection to the VIP and begins connecting to each of the Community Servers directly instead.

  **Note:** Do not enter the host name of a MUX or IP sprayer that Sametime clients connect to.

8. Set the **Port** to 1516. The **transport protocol** is automatically set to TCP (Transmission Control Protocol).

9. Click **OK**.

10. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.

**Connecting to instant messaging communities (IBM i):**

Add instant messaging communities such as the AOL clearinghouse, AOL Instant Messenger, Google Talk, XMPP, and Office Communications Server to Sametime Gateway.
About this task

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.

Note: Sametime client users must use the Sametime client version 7.5 or later when exchanging instant messages and presence information with public instant messaging providers such as AOL Instant Messenger, Office Communications Server, and Google Talk. Pre-7.5 clients are not licensed to connect with public instant messaging providers. The Sametime server will check and disable the Add external user checkbox if a client of a lower version is used. It is the responsibility of the Sametime Gateway administrator to comply with the licensing agreement.

Registering your Sametime Gateway (IBM i) with AOL:

The IBM Sametime Provisioning Application enables you to set up interoperability with certain public instant messaging services such as AOL. The application prompts you for relevant information, validates your organization’s entitlement to use IBM Sametime Gateway, provides the information to the instant messaging service, and notifies you when you have been added by the service.

Before you begin

Attention: The Sametime Gateway host name's public DNS registration is required before creating the provisioning request; otherwise public external provider might fail during the provisioning request.

The procedure for registering your Sametime Gateway depends on how you acquired Sametime Standard or Sametime Advanced:

Registering Sametime Gateway (IBM i) with AOL directly:

If you acquired licenses for IBM Sametime Standard or Sametime Advanced using the IBM Passport Advantage website, then register your IBM Sametime Gateway directly using the Sametime Provisioning Application.

Before you begin

Before you begin, collect the following information:

- The primary contact for your site. The primary contact is the person who is entering into the Passport Advantage or Passport Advantage Express contractual relationship with IBM on behalf of your company. IBM communicates directly with this person on issues such as Agreement modification and so forth. This person may be a procurement or purchasing professional.
- Your Passport Advantage site number.
- Your Sametime Gateway name. This can be any name that you assign to Sametime Gateway.
- Your Sametime Gateway host name.
• Your Sametime Gateway port number.
• Your Sametime Gateway SSL certificate common name.
• Your Sametime Gateway SSL certificate issuer (VeriSign, Comodo, Thawte, and so on).
• An email address for you to be notified when provisioned.
• The Sametime community domains that you want to expose to the instant messaging service.

Procedure
2. Type your IBM ID and password:
   • If you do not have an IBM ID and password, click the register link. You receive your web identity when you complete the registration.
   • If your web identity is not affiliated with a Passport Online Advantage site, you will be redirected to a self-nomination site where you should use the information you collected before starting this procedure. Unless you know you are the primary contact for your site, please select No when prompted "I believe I am the Primary Contact for this Site." Once you have completed the self-nomination form, the Primary Contact for your site must process the form. When you receive a self-nomination approval by email, go to http://www.ibm.com/software/lotus/sametime/federation and start the provisioning process.

   Once your web identity is verified, the system checks whether you are a Sametime customer that is entitled to deploy the Sametime Gateway.
3. If you are entitled to deploy Sametime Gateway, enter the information needed by the instant messaging service.
4. Submit the provisioning form. After the instant messaging service receives your information and adds your site, you will receive an email notification from IBM that you have been provisioned. This can take up to seven business days.
5. Before accessing a public instant messaging service through the Sametime Gateway, you are required to agree to the terms of service or end-user license agreement for such public instant messaging services and IBM is not a party to any such agreement.

Registering Sametime Gateway (IBM i) with AOL using email:

If you did not acquire licenses for IBM Sametime Standard or Sametime Advanced through IBM Passport Advantage, then register your IBM Sametime Gateway by emailing the required information to the provided address. For example, if you are an IBM Business Partner or have purchased IBM Sametime Standard for Cisco Unified Communications from Cisco or an authorized Cisco reseller, you must use this procedure.

Before you begin

Send the information below to the following email address:
sametime@us.ibm.com:

Registration Code:
• Registration code
This is available on the Sametime for Cisco Unified Communications software DVD. If you are an IBM Business Partner, you can get this code from your Business Partner representative.

**Technical information:**
- Gateway host name (the fully qualified domain name of your gateway; for example: stgateway.company.com)
- The port on which you want to accept incoming TLS/SIP requests (port 5061 is used by default)
- Gateway certificate common name
- Gateway certificate issuer
- SIP realm to be used (for example: company.com)
- Do you wish to be provisioned for AOL AIM?
- Do you wish to participate in the AOL Clearing House?

**Contact information:**
- Company Name
- ID or Order # (If IBM Business Partner, use Partnerworld ID #; otherwise, use Order #)
- Contact first/last name
- Contact email address
- Contact telephone number
- Contact instant messaging address (optional)

*Connecting Sametime Gateway (IBM i) to an AOL community:*

Set up a connection by choosing either the AOL instant messenger community or the AOL clearinghouse community, but not both. The AOL clearinghouse is a superset of the AOL instant messenger community.

**Before you begin**

You must set up SSL prior to connecting to an AOL community.

**About this task**

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.

*Connecting Sametime Gateway (IBM i) to the AOL clearinghouse community:*

Use this procedure to add the AOL clearinghouse community to IBM Sametime Gateway. The AOL clearinghouse connects your Sametime users to a wide community that includes AOL, ICQ, iChat, and other users from AOL Enterprise Federation Partner communities, including external Sametime communities.
Connect to the AOL clearinghouse community or the AOL community, but not both, as the former is a superset of the latter.

**Before you begin**

You must set up SSL prior to connecting to an AOL clearinghouse community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
nsllookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

**Note:** IBM recommends that you do not configure both the AOL clearinghouse and the AOL 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.

Before you add the AOL clearinghouse community, you must establish the local community, and use the provisioning application to register your Sametime with AOL Public Instant Messaging Services.

**About this task**

**Expected state:**

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a logical name for the new clearinghouse community.
4. In the **Community Type** field, select **Clearinghouse**.
5. Select a **Translation Protocol**. Choose **SIP for AOL** for AOL Clearinghouse community connections.
6. In the **Host Name** field, type the following:
   ```
   sip.oscar.aol.com
   ```
7. In the **Port** field, type the port number. The default port is 5061.
8. Because AOL clearinghouse requires a secure connection, the **Transport protocol** is set to **TLS**, so there is nothing to do.
9. Click **OK** to save the new community.
10. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign users access to the AOL clearinghouse community.
11. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.
12. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.

   a. Click **Custom Properties** to include additional IP addresses for AOL Instant Messenger servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from AOL. The **Custom properties** link is available only after the community is saved.

   b. In the **Route properties** field, set the maximum sessions for **instant messaging** or **presence** for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway.

   c. Select the check box to disable the route to the community.

   d. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.

**What to do next**


**Connecting Sametime Gateway (IBM i) to the AOL Instant Messenger community:**

Use this procedure to add the AOL Instant Messenger community to IBM Sametime Gateway so that your users can exchange instant messages and presence with AOL Instant Messenger users. Add the AOL community only if you have not added the AOL clearinghouse community because the AOL clearinghouse is a superset of the AOL community.

**Before you begin**

You must set up SSL prior to connecting to an AOL clearinghouse community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
nslslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

**Note:** IBM recommends that you do not configure both the AOL clearinghouse and the AOL 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.

You must establish the local community first before adding an external community.

**About this task**

Expected state:

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.
Procedure
1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. In the table that lists communities, click New.
3. In the Name field, type a logical name for the new community such as AOL IM.
4. Under Community Type, select External.
5. In the Domains field, type: aol.net, corp.aol.com, aol.com
6. In the Translation Protocol list, select SIP for AOL.
7. In the Host Name field, type sip.oscar.aol.com.
8. In the Port field, type a port number. The default port is 5061.
9. In the Transport protocol field, TLS (Transport Layer Security) is already selected.
10. Click AOL IM from the list to edit the connection properties.
11. Click OK to save the new community.
12. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click Assign local users to this community to assign local users access to the external community.
13. Click Assign local users to this community to assign local users access to the external community. This link is inoperable until you first save the new external community.
14. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.
15. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.
   a. Click Custom Properties to include additional TCP/IP addresses for AOL Instant Messenger servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from AOL. When setting up the community for the first time, the Custom properties links are available only after the community is saved.
   b. In the Route properties field, set the maximum sessions for instant messaging or presence for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If Route properties are not visible, you must connect to a local community first.
   c. Select the check box to disable the route to the community.
   d. Click the Translation Protocol link to set custom properties for the translation protocol. The Custom properties links are available only after the community is saved.

What to do next


Connecting Sametime Gateway (IBM i) to a Google Talk community:

IBM Sametime Gateway users can exchange instant messages with the Google Talk community over the Extensible Messaging and Presence Protocol, or XMPP. To communicate with the Google Talk community, you must first set up a DNS service (SRV) record and publish it to DNS so that Google Talk users and local
Sametime users can discover each other and establish a connection. This topic instructs you to create a DNS SRV record first, and then add Google Talk as an external community.

**Before you begin**

**Note:** IBM cannot guarantee the availability of the instant messaging federation with GoogleTalk. Sametime Gateway is fully dependent on GoogleTalk’s service availability.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```
slookup talkz.1.google.com
nslookup 64.12.162.248
nslookup -type=SRV -class=all _xmpp-server._tcp.google.com
```

Make sure all domains you specified in the internal community are not registered with “Google Apps.” To determine whether a domain is registered with Google Apps, see the IBM Technote Unable to establish awareness with Google Talk users through the Sametime Gateway.

Your firewall rules should be set up as described in the “GoogleTalk” section of the topic, “Opening ports in the firewalls” on page 551.

**About this task**

Work with your network administrator to set up a DNS SRV record for each domain defined in your internal community using the following format:

```
_xmpp-server._tcp.domain name. IN SRV priority weight port target.
```

For example:

```
```

<table>
<thead>
<tr>
<th>SRV record format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain name</td>
<td>Wild cards are not allowed. Note that the domain name must end with a period. The domain name must match the domain name that you used when you added the local Sametime server to the Sametime Gateway.</td>
</tr>
<tr>
<td>priority</td>
<td>Priority determines the proxy query order when used in an Sametime Gateway cluster. With multiple SRV records, lower values are queried first.</td>
</tr>
<tr>
<td>weight</td>
<td>Weight determines proportionally how often a proxy is queried when you have multiple SRV records of similar priority in a cluster. Higher values are queried more often. So, a weight of 20 would be queried twice as often as one of 10. A weight of 30 would be queried three times as often as one of 10.</td>
</tr>
<tr>
<td>port</td>
<td>The port on which this service is found. Use port 5269.</td>
</tr>
<tr>
<td>target</td>
<td>Fully qualified host name of the machine running the Sametime Gateway. Note that the target must end with a period. For example: sttest.lotus.com.</td>
</tr>
</tbody>
</table>

Expected state: the Sametime Gateway single server or cluster is started
Procedure

1. Create an individual DNS SRV record (_xmpp-server._tcp) for each domain name that you will support.
   For example, you might support two local domain names, called lotus.com and ibm.com. For each of the domain names you want to support, you must create an individual DNS SRV record. The records will be identical except for the domain name field's value.

2. Verify that the DNS SRV record that you added to DNS is correct by using the nslookup command:
   a. Open a command window and run nslookup.
   b. Type set type=SRV.
   c. Type set class=IN.
   d. Search the _xmpp-server.tcp record using the supported domains added in the previous step.
   Using the example above, you enter _xmpp-server._tcp.lotus.com and repeat the searching for _xmpp-server._tcp.ibm.com. Using lotus.com, the full command and returned value appears as follows:
      nslookup>set type=SRV
      >set class=IN
      >_xmpp-server._tcp.lotus.com.

      Make sure the correct hostname of the Sametime Gateway server and IP address are returned. The following is an example only:
      Server: sbydns01.srv.ibm.com
      Address: 9.0.4.1

      Non-authoritative answer:
      _xmpp-server._tcp.lotus.com SRV service location
      priority  = 5
      weight    = 0
      port      = 5269
      srv hostname = sttest.lotus.com
      lotus.com nameserver = wtf-ns1.lotus.com
      lotus.com nameserver = wtf-ns2.lotus.com
      lotus.com nameserver = ns0.lotus.com
      sttest.lotus.com internet address = 129.42.249.45
      >

3. In the Integrated Solutions Console, click Sametime Gateway > Communities.
4. In the table that lists communities, click New.
5. In the Name field, type Google Talk.
6. Under Community Type, select External.
7. In the Domains field, type:
   gmail.com
8. Select XMPP as the Translation Protocol.
9. Ignore the host name. XMPP uses the Fully qualified domain name of the host as specified in the target field of the DNS SRV record instead.
10. In the Port field, type 5269.
11. In the Transport protocol field, select TCP. TCP is the only transport protocol for Google Talk.
12. Click OK to save the new community.
13. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click Assign local users to this community to assign local users access to the external community. By default all users can access the external community.

14. The following sub steps are optional:
   a. In the Route properties field, set the maximum sessions for instant messaging or presence for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If Route properties are not visible, you must connect to a local community first.
   b. Select the check box if you ever need to disable the route to the community.
   c. Click the Translation Protocol link to set custom properties for the translation protocol. The Custom properties links are available only after the community is saved.

15. Restart the Sametime Gateway server.

What to do next

Google's IP addresses associated with talky.l.google.com and talkz.l.google.com change occasionally. Google typically adds new IP addresses to DNS at least a week before the Google Talk service starts using them, but occasionally the IP address changes can be seen immediately, potentially causing service disruptions. There are various products that monitor DNS addresses for changes. See these search results for DNS monitoring tools available. Work with your network administrator to actively monitor DNS and update the firewall rules to accommodate new IP addresses.


Connecting Sametime Gateway (IBM i) to an Office Communications Server community:

Connect to a Office Communications Server community so that your users can exchange instant messages with Microsoft Communicator users.

Before you begin

You must establish the local community first before adding an Office Communications Server community. Please also note that setting SSL is a prerequisite for connecting to an Office Communications Server community.

Remember that the IBM Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

nslookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
nslookup [OCS Edge Server]

Expected state:
• Single server: the Sametime Gateway server is started.
• Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.
Procedure

1. In the Integrated Solutions Console, click **Sametime > Gateway Communities**
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a logical name for the new community.
4. Under Community Type, select **External**.
5. In the **Domains** field, type the domain names of the Office Communications Server community. For example: `ocs.example.com`.
6. Select **SIP for OCS** as the translation protocol.
7. In the **Host Name** field, type the host name or the IP address of the OCS Edge Server.
8. In the **Port** field, type a port number. The default port is 5061.
9. In the **Transport Protocol** field, TLS (Transport Layer Security) is already selected.
10. Click **OK** to save the new community.
11. Create a new custom property.
   - Single server:
     - Click **Servers > WebSphere application servers > RTCGWServer**. Under Server Infrastructure, expand **Administration** and select **Custom properties**.
     - Click **New**.
   - Clustered server:
     - Click **System administration > Cell**. Under Additional properties, select **Custom properties**. Click **New**.
12. In the **Name** field type `com.ibm.sametime.gateway.fqdn`.
13. In the **Value** field, type the fully qualified domain name of the Sametime gateway (or the SIP Proxy server in a clustered environment). For example: `stgw.example.com`.
14. Click **OK** to save the new custom property.
15. Click **New** again.
16. In the **Name** field type `com.ibm.sametime.gateway.port`
17. In the **Value** field type the gateway's port. For example: 5061.
18. Click **OK** to save this new custom property.
19. On the Communities panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users and capabilities** to assign users access to the external community.
20. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.
21. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community:
   - Click **Custom Properties** to include additional host names for OCS edge servers. Sametime Gateway uses these IP addresses to determine which SIP requests originate from Office Communications Server. When setting up the community for the first time, the Custom properties links are available only after the community is saved.

*Connecting Sametime Gateway (IBM i) to an XMPP community:*

IBM Sametime Gateway users can exchange instant messages with an XMPP community over the Extensible Messaging and Presence Protocol, or XMPP. To communicate with an XMPP community, you must first set up a DNS service (SRV) record and publish it to DNS so that users and local Sametime users can
discover each other and establish a connection. This topic instructs you to create a DNS SRV record first, and then add XMPP domains as an external community.

**Before you begin**

You must set up SSL and establish the local community first before adding the XMPP community.

Remember that the Sametime Gateway servers must have access to a DNS server that can resolve public DNS records (A records, SRV records, and PTR records). For example the following commands should be able to resolve successfully:

```plaintext
nsllookup sip.oscar.aol.com
nslookup 64.12.162.248
nslookup -type=all -class=all _xmpp-server._tcp.google.com
```

**About this task**

**Expected state:**
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. Create an individual DNS SRV record (_xmpp-server._tcp) for each domain name that you will support.
   For example, you might support two local domain names, called lotus.com and ibm.com. For each of the domain names you want to support, you must create an individual DNS SRV record. The records will be identical except for the domain name field's value.

2. Verify that the DNS SRV record that you added to DNS is correct by using the `nslookup` command:
   a. Open a command window and run `nslookup`.
   b. Type `set type=SRV`.
   c. Type `set class=IN`.
   d. Search the `_xmpp-server._tcp` record using the supported domains added in the previous step.

   Using the example above, you enter `_xmpp-server._tcp.lotus.com` and repeat the searching for `_xmpp-server._tcp.ibm.com`. Using `lotus.com`, the full command and returned value appears as follows:

   ```plaintext
   nslookup>set type=SRV
   >set class=IN
   >_xmpp-server._tcp.lotus.com.
   
   Non-authoritative answer:
   _xmpp-server._tcp.lotus.com SRV service location
   priority   = 5
   weight     = 0
   port       = 5269
   svr hostname = sttest.lotus.com
   ```
3. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.

4. In the table that lists communities, click **New**.

5. In the **Name** field, type a logical name for the new community.

6. Under **Community Type**, select **External**.

7. In the **Domains** field, type the domains provided by the XMPP community.
   
   **Attention:** Wildcards are not supported in this field, you must type each complete domain name.

8. Select **XMPP** as the translation protocol.

   When you select XMPP as your protocol, the **Host Name** field defaults to "Localhost" as its value while Sametime Gateway resolves the domain value that you entered in step 5; once the domain is resolved, an appropriate value is entered automatically into the **Host Name** field.

9. In the **Port** field, the default port is 5269.

10. In the **Transport protocol** field, select **TCP** (Transmission Control Protocol) or **TLS** (Transport Layer Security).

11. Click **OK** to save the new community.

12. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign local users access to the external community.

13. Restart the Sametime Gateway server. If you have a cluster of servers, restart the cluster.

14. The following steps are optional, but be sure to restart the Sametime Gateway servers if you make any changes to the community.

   a. Click **Custom Properties** to include additional host names for XMPP servers. Sametime Gateway uses these IP addresses to determine which XMPP requests originate from this community. Note that the **Custom properties** link is available only after the community is saved.

   b. In the **Route properties** field, set the maximum sessions for **instant messaging** or **presence** for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If **Route properties** are not visible, you must connect to a local community first.

   c. Select the check box to disable the route to the community.

   d. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.

**What to do next**


*Managing external watching from commercial IM providers:*
The Sametime server allows an external watcher, or user who has someone on his
or her contact list that is unaware of being watched, to conduct this activity;
however, this capability can be disabled.

Configuring user consent

Instant messaging users from commercial IM providers such as Google can watch
the status of internal Sametime users unless the server is configured to manage this
functionality. This functionality can be managed through the 'user consent' feature.
When the server is configured to require permission from the Sametime user, the
Sametime user sees a pop-up window on his screen, asking for permission for the
external user to watch the Sametime user's status. The Sametime user can give
consent, or not.

To require the external IM watcher to gain permission of the 'watched' person,
follow these steps:
1. Open the sametime.ini file.
2. In the [Config] section, add:
   
   `AWARENESS_EXTERNAL_NEED_PERMISSION=1`
3. Shut down and restart the Sametime server to effect the change.

By default, the configuration flag is set to 0.

When the server is configured to require permission from the Sametime user, the
Sametime user sees a popup window requesting permission for the external user
to watch the Sametime user's status. The Sametime user can approve or decline.

Connecting to external Sametime communities using Sametime Gateway (IBM
i):

Connect to external Sametime communities by working, if necessary, with an
administrator from an external community to prepare the external Sametime server
and by then adding the external Sametime community to your list of communities.

Preparing external Sametime servers for Sametime Gateway (IBM i) communications:

This topic presents general information on steps needed to configure Sametime
servers versions 6.5.1 or 7.0 that exist in external communities. Work with the
external community's administrator to prepare the legacy Sametime server for
Sametime Gateway communications. For example, if your local Sametime server is
a member of widgets.com, and you want to connect to an external Sametime 6.5.1
server at acme.com, you may want to know the steps required to set up the
external Sametime server to have instant messaging and presence with your
Sametime Gateway.

Procedure
1. If the external community's Sametime server is version 6.5.1, or 7.0, the external
   community must enable the Sametime SIP Gateway on the server. See the
   chapter "Enabling the SIP Gateway" in the Sametime Server Administration
   Guide.
2. The latest patches and Cumulative Fix Packs must be installed on the external
   community's Sametime server. Go to Sametime Product Support to download
   the latest support files for the external Sametime server.

Adding external Sametime communities to Sametime Gateway (IBM i):

Chapter 3. Installing  909
Add an external Sametime community to IBM Sametime Gateway. You connect to a Sametime community by specifying domains in the external community, selecting a translation protocol, and setting the host name, port, and transport protocol for the external community.

Before you begin

You must add the local Sametime community first before adding an external community. In addition, if you are not connecting to a Sametime 7.5 or later server using its own Sametime Gateway, be sure that the external Sametime 6.5.1 or 7.0 server has the Sametime SIP Gateway enabled. Finally, confirm that the external Sametime server and Sametime Gateway have the latest fixes installed.

About this task

Expected state:

- Single server: the local Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and a Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the table that lists communities, click **New**.
3. In the **Name** field, type a name for the new community.
4. Under **Community Type**, select **External**.
5. In the **Domains** field, type the Fully qualified domain names in which users are found in the external community. Each domain name must access the same user directory. For example: acme.com, us.acme.com, fr.acme.com, and uk.acme.com must all be linked by a common user directory to be in the community. Obtain this information from the system administrator in the external community.
6. Select a **Translation Protocol**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use <strong>SIP for Sametime Gateway</strong> for connections to Sametime Gateway versions 7.5 or later communities.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>Use <strong>SIP for legacy Sametime Gateway</strong> for Sametime versions 7.0 or 6.5.1 communities.</td>
</tr>
</tbody>
</table>
7. In the **Host Name** field, type the name of the external real-time communication server such as ExampleServer1.com, for example.

   **Note**: If the host name is an IPv6-format network address, set an explicit address here; do not use an abbreviated address (no brackets, no leading zeroes). For example, all of these IPv6-format network addresses are equivalent, but only the first form is accepted:
   - \12::6:7:8 [acceptable]
   - 1:2::6:7:8 [do not use this abbreviated format]
   - 01:2:0:0:006:0007:8 [do not use leading zeroes]
8. In the **Port** field, type the port number (the default port number is 5061).
The port you use is dependent on the **Transport protocol** you select in the next step:

- TLS uses port 5061
- TCP uses port 5060

9. In the **Transport protocol** field, select **TLS** (Transport Layer Security) or **TCP** ( Transmission Control Program or TCP/IP).

   If you select TLS as the protocol, you must set up SSL with a certificate signed by a Certificate Authority and exchange trusted certificates with the external community.

10. Click **OK** to save the new community. Note that you can't assign users to the community until you save the community.

11. On the **Communities** panel, select the name of the community that you created, scroll to the bottom, and click **Assign local users to this community** to assign local users access to the external community.

12. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

13. The following steps are optional:
   
   a. In the **Route properties** field, set the maximum sessions for **instant messaging** or **presence** for this community. The session numbers set for this community cannot exceed the global maximum sessions set for Sametime Gateway. If **Route properties** are not visible, you must connect to a local community first.
   
   b. Select the check box to disable the route to the community.
   
   c. Click the **Translation Protocol** link to set custom properties for the translation protocol. The **Custom properties** links are available only after the community is saved.
   
   d. Click **Custom Properties** to set additional properties for the community. The **Custom properties** links are available only after the community is saved.

---

**Using Sametime Gateway (IBM i) to prevent communication with external communities:**

You can prevent external users from communicating with a particular IBM Sametime community by creating an exclusion list. The Sametime Gateway server will deny external communication requests for users hosted on all servers and clusters specified on the list.

**Before you begin**

This feature requires you to define a Home Server (cluster) for all users within the targeted community, so that the Sametime Gateway server can determine whether the user belongs to a community on the exclusion list. For information on defining a user’s Home Server, see Forcing users to connect to a home server.

**About this task**

An exclusion list is a list of clusters (for a stand-alone Sametime server, the cluster name is the server name) deployed within a local Sametime community; you define the list as a Sametime Gateway custom property. Use the exclusion list to prohibit external users from communicating with users in a community hosted on one of the specified clusters. Subscribe (awareness) and chat (instant messaging) requests from all external users to the local users hosted on the clusters listed on
the exclusion list, will be rejected by the Sametime Gateway server. You enable this feature with the custom property called "Sametime community exclusion list".

For example, suppose the Example Corporation has two distributed Sametime clusters, called eu.acme.com (Europe) and usa.acme.com (USA). In addition, Sametime Gateway is installed on gw.acme.com.

On the Sametime Gateway server (gw.acme.com), there is an exclusion list containing "eu.acme.com" – this prevents the Sametime Gateway server from connecting to any servers in the eu.acme.com cluster. When an external user (outside of Example Corporation; for example, on AOL) adds a user hosted on eu.acme.com to her contact list, the subscribe request is routed to the Sametime Gateway server, which denies the request because it cannot access users in that cluster. In this example, the usa.acme.com cluster does not appear on the exclusion list, so the external user can access people in that cluster.

Follow these steps to define an exclusion list. For details see Adding custom properties.

Procedure
1. Log in to the Integrated Services Console as a Sametime Gateway administrator.
2. Click Sametime Gateway > Communities.
3. Select the local community for which you want to define an exclusion list.
4. In the Name field, type: Sametime community exclusion list as the name of the new property.
5. In the Value field, type the list of excluded servers and clusters.
   Type the server names and cluster names as a list using any of these characters to separate names:
   • comma ,
   • semicolon ;
   • space
   Cluster names must appear as defined in the Cluster Document; for more information, see "Creating a cluster document in the Configuration database". Standalone server names must appear as defined in the sametime.ini file's VPS_NAME property (for example, CN=st1/O=acme).
6. Click OK.
7. Restart the Sametime Gateway server so your changes can take effect. If the server was previously connected to Sametime servers that are now excluded, restart those servers as well.

Providing a port number to external communities that communicate with Sametime Gateway (IBM i):

The procedures describe how to obtain and update the port number that the SIP container uses to communicate with external communities. You want to provide the port number to external communities so they can use the same port. You may also need to change the TLS port number that Sametime Gateway uses.

Providing a port number to external communities for stand-alone Sametime Gateway (IBM i) deployments:
These steps describe how to obtain and update the port number that the SIP container uses to communicate with external communities. You want to provide the port number to external communities so they can use the same port. You may also need to change the TLS port number that the Sametime Gateway uses.

Before you begin

This procedure assumes that you have installed the Sametime Gateway.

About this task

A standalone Sametime Gateway server uses a SIP container port that is, by default, 5061 for Transport Layer Security (TLS). Therefore, if an external community wants to connect to Sametime Gateway, the external community must define port 5061. Check the `SIP_DEFAULTHOST_SECURE` parameter to verify the TLS port for the SIP container service.

Expected state: the Sametime Gateway server is started.

Procedure

1. To obtain the port number used by a single Sametime Gateway server, in the Integrated Solutions Console:
   a. Click **Servers** > **Application servers** > `server_name`, where `server_name` is the name of the Sametime Gateway server.
   b. Under Communication, click **Ports**.
   c. Look for the port number in `SIP_DEFAULTHOST_SECURE` and make a note of this number.

2. Check that the port number is added to the **Default Virtual Host**. The port is added default but you may need to update the default virtual host if you make changes to the ports:
   a. Click **Environment** > **Virtual Hosts** > `default_host` > **Host Aliases**.
   b. Click **New** and type a new port number if the port does not exist.
   c. Click **OK**, and then **Save**, and **Save** again.

What to do next

Now you can provide a port number to external communities.

Providing port numbers to external communities for clustered Sametime Gateway (IBM i) deployments:

These steps describe how to obtain and update port numbers that the SIP and XMPP proxy servers uses to communicate with external communities. You want to provide the port numbers to external communities so they can use the same port. You may also need to change the TLS/SSL port number Sametime Gateway uses.

Before you begin

This procedure assumes that you have installed Sametime Gateway, have created a cluster, and have installed and configured a SIP and XMPP proxy server.
About this task

By default, the SIP proxy uses port 5061 over TLS/SSL, and the XMPP proxy server uses port 5269 for SSL and non-SSL connections.

Expected state: the Deployment Manager is started.

Procedure
1. To obtain the port numbers used by the Sametime Gateway cluster:
   a. In the Integrated Solutions Console, click Servers > Proxy servers > SIPProxyServer.
   b. Under Communication, click Ports.
   c. Look for the port number in PROXY_SIPS_ADDRESS and make a note of this number.
2. Click Application Servers > Server Name and, under the Communications section, click Ports to view the port number for XMPP_SERVER_ADDRESS. Make a note of this number.
3. Check that the ports are added to the Default Virtual Host. The port is added by default but you may need to update the default virtual host if you make changes to the port:
   a. Click Environment > Virtual Hosts > default_host > Host Aliases.
   b. Click New and type a new port number if the port does not exist.
   c. Click OK, and then Save, and Save again.

What to do next

The port number in combination with the DNS name of the node on which the SIP and XMPP proxy servers run is needed for configuring external instant messaging communities to connect to your Sametime Gateway.

Adding external contacts to the Sametime Connect client Contacts list:

After you install and configure Sametime Gateway, and add an external community or clearinghouse community, your users can add external contacts to their Sametime Contact List. Give these instructions to your Sametime users so they will know how to add external contacts to their Contact List.

Procedure
1. In the Sametime Connect client, click File > Add > Contact.
2. Select the Add external user by email address check box.
3. Type the external contact’s email address.
4. Select an existing group, or type a new group name, in the Add to group field.
5. Click Add

Installing the WebSphere Application Server Update Installer on IBM i

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. Extract the packages and run the Update Installer install program from the workstation that you download the update package to. The Update Installer will be remotely installed to your IBM i system.

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, 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.
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. Install onto IBM i remotely from a Windows machine. Navigate to the directory where you extracted the Update Installer and run the install program.
   install.exe
7. The installation wizard initializes and displays the Welcome screen. 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. The Installation summary panel appears. Review the summary. Click Next to begin the installation or click Back to make changes to previous panels.
11. The Installation results panel is displayed. Verify the success of the installer program by examining the completion panel.

Installing WebSphere Application Server updates on IBM i

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, 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.
2. Extract the updates to a local directory such as stwas Fixes.
3. 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:
   updateInstall_Home/maintenance

   By default updateInstall_Home is the root directory of the Update Installer, /QIBM/ProdData/WebSphere/UpdateInstaller/V7/UPDI.
4. Ensure that you stop all running processes as described in “Command reference for starting and stopping servers” on page 588.
5. Open the document called updateInstall_Home/os400_readme_updateinstaller.html.
   Follow the instructions in "Installing multiple maintenance packs with silent install" to install the update package.
6. 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/install/updatelog.txt.
7. Start the servers as described in “Command reference for starting and stopping servers” on page 588.

Results

To verify which updates have been installed, run the versionInfo command from the was_install_root/bin directory.

./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 IBM i” on page 914
Use the WebSphere Application Server Update Installer to add required software updates.

Starting and stopping servers in a Sametime deployment on IBM i
An IBM Sametime deployment is made up of several component servers that can be started and stopped independently.

Starting and stopping servers running on WebSphere Application Server on IBM i
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 on IBM i:
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 on IBM i:
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
./stopManager.sh -username admin_user -password admin_password

**Windows**
startManager.bat stopManager.bat -username admin_user -password admin_password

**IBM i**
startManager dmgr
stopManager -username admin_user -password admin_password

**Related tasks**
“Starting and stopping WebSphere Application Servers on Windows” on page 587
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 588
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 running on IBM i:**

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
ci
startServer STConsoleServer
Related tasks
“Logging in to the console” on page 584
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 582
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

Related reference
“Command reference for starting and stopping servers” on page 588
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 on IBM i:
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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Logging in to the Sametime system console on IBM i:
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.
   http://serverhostname.domain:port/ibm/console
   For example:
   http://sametime.example.com:8700/ibm/console
   https://sametime.example.com:8701/ibm/console
   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

Chapter 3. Installing 919
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

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. 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 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.

**What to do next**

“Connecting to an LDAP server” on page 143

**Related tasks**

“Starting the Sametime System Console” on page 582

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

*Logging in to the console for a cell profile on IBM i:*

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`.

**Related concepts**

- "Ports used by Sametime servers" on page 68
  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.

**Command reference for starting and stopping servers on IBM i:**

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>
<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 102. 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 103. 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 -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
<tr>
<td>Meeting Server</td>
<td>./stopServer.sh STMeetingServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopServer.sh STMeetingHttpProxy -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>./stopServer.sh STProxyServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
<tr>
<td>Media Manager</td>
<td>./stopServer.sh STMediaServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
</tbody>
</table>
Table 103. Stop server commands for AIX, Linux, or Solaris (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Sametime Gateway | ./stopserver.sh RTCGWServer -username username -password password  
|                | ./stopNode.sh -username username -password password |
| Sametime Advanced | ./stopServer.sh STAdvancedServer -username username -password password  
|                | ./stopNode.sh -username username -password password |

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 104. Start server commands for Windows

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Sametime System Console | startNode.bat                                     
|                       | startServer.bat STConsoleServer                    |
| Meeting Server        | startNode.bat                                      
|                       | startServer.bat STMeetingHttpProxy                
|                       | startServer.bat STMeetingServer                    |
| Proxy Server          | startNode.bat                                      
|                       | startServer.bat STProxyServer                      |
| Media Manager         | startNode.bat                                      
|                       | startServer.bat STMediaServer                      |
| Sametime Gateway      | startNode.bat                                      
|                       | startServer.bat RTCGWServer                        |
| Sametime Advanced     | startNode.bat                                      
|                       | startServer.bat STAdvancedServer                  |

Note: Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.
Table 105. 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 106. 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>
</tbody>
</table>
### Table 106. Start server commands for IBM i (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<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 107. 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>
<tr>
<td>Meeting Server</td>
<td>stopServer STMMeetingServer -username username-password password</td>
</tr>
<tr>
<td></td>
<td>stopServer STMMeetingHttpProxy -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 581
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 582
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.
“Starting and stopping WebSphere Application Servers on Windows” on page 587
Use the Start Programs menu in Microsoft Windows to start or stop any Sametime servers running on WebSphere Application Server.

Starting and stopping servers running on Lotus Domino on IBM i
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.

Starting and stopping a Sametime server on IBM i while Domino is running:

IBM Sametime on IBM i 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. On any IBM i, command line, enter the Work with Domino Console command and press F4:
   WRKDOMCSL
2. Enter the server name and press Enter.
3. In the Domino server console, choose one of the following actions:
   • To start the Sametime service on a Domino server that is already running, type this command:
     load STADDINZ
   • To stop the Sametime services without stopping the Domino server, type this command:
     tell STADDINZ Quit
4. Periodically press F5 to refresh your screen and look for a message to confirm that Sametime has started or stopped.

Starting and stopping Domino and a Sametime Community Server on IBM i:

Learn how to start and stop a Sametime Community Server running on IBM i.
Starting Domino and a Sametime Community Server on IBM i:

Follow these instructions to start a Sametime Community Server on IBM i from an IBM i command line.

About this task

Follow these steps to start both Domino and a Sametime Community Server.

Procedure

1. From any IBM i command line, run the following command:
   WRKDOMSVR
2. On the Work with Domino Servers display, start the server by typing 1 in the Opt column next to the Domino server where you added Sametime and press Enter.
3. Press Enter to confirm your server selection.
4. Periodically press F5 to refresh your screen and wait for the Domino server status to be *STARTED.
   To confirm that all Sametime components have started, type 5 in the Opt column next to the server and press Enter to display the Domino console. On the Display Domino Console display, look for the message “Sametime: Server startup successful” which indicates that all Sametime components have started. You may need to press F5 periodically to refresh the screen until this message is displayed.

   Tip: You can also use IBM i Navigator to start the Sametime server by selecting Network > Servers > Domino. Right-click on the Domino server where you added Sametime and select Start.

Stopping Domino and a Sametime Community Server on IBM i:

Follow these instructions to stop a Sametime server on IBM i from an IBM i command line.

About this task

Follow these steps to stop both Domino and a Sametime Community Server from an IBM i command line.

Procedure

1. From any IBM i command line, run the following command:
   WRKDOMSVR
2. On the Work with Domino Servers display, stop the server by typing 6 in the Opt column next to the Domino server where you added Sametime and press Enter.
3. Press Enter to confirm your server selection.
4. Periodically press F5 to refresh your screen and wait for the Domino server status to be *ENDED.

   Tip: You can also use IBM i Navigator to stop the Sametime server by selecting Network > Servers > Domino. Right-click on the Domino server where you added Sametime and select Stop.
Uninstalling on IBM i

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.

Uninstalling a non-clustered server on IBM i

Uninstall a non-clustered server running any IBM Lotus Sametime component running on IBM i.

About this task

The procedure for uninstalling Sametime vary according to the component you are uninstalling:

Uninstalling a Sametime Community Server on IBM i:

When you uninstall an IBM Sametime Community Server on IBM i, you unregister the server from the Sametime System Console, and then remove it from the IBM Lotus Domino server where it is hosted.

About this task

Complete these tasks to uninstall a Lotus Sametime Community Server on IBM i:

Unregistering a Community Server on IBM i:

To remove an IBM Sametime Community Server running on IBM i from the list of the Sametime System Console's managed servers, run the unregister utility on the server. You should only unregister the server on IBM i if you plan to uninstall the server or if you are performing some other activity that requires removing it 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

A Sametime Community Server reverts back to using legacy policies if you remove it from the console.

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's `sametime_server_data_directory/console` directory.
b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Verify the following values in the console.properties file that were specified when the server was initially registered. All of the values, including the encrypted System Console password should already be in the properties file.

<table>
<thead>
<tr>
<th>Table 108. console.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
</tr>
<tr>
<td>SSCHTTPPort</td>
</tr>
<tr>
<td>SSCUserName</td>
</tr>
<tr>
<td>SSCPassword</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
</tr>
<tr>
<td>SSCHTTPSPort</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. The only required value in this file is **DepName:** When you are unregistering, 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.

4. Start the Sametime Community Server.

5. Run the unregisterProductNode.sh unregistration 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 server: unregisterProductNode.sh
   d. As the unregistration 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.

e. When the registration script completes, press F3 to exit QSH.

The utility unregisters the server and generates a log file called ConsoleUtility.log, storing it in the consoles/logs directory. If the unregistration is successful, the console.pid is removed.

Related reference

“Command reference for starting and stopping servers” on page 588
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.

Removing the Sametime Community Server from an IBM i Domino Server:

You can remove Sametime files from a Lotus Domino server without deleting the Sametime Community Server software from your system. Use the RMVLSTDOM command to reverse the changes made when you ran the ADDLSTDOM command after installing the Sametime Community Server.

About this task

When you remove Sametime Community Server from a Domino server, all files related to Sametime that were added to the Domino server data directory or were created while running Sametime components are removed. Updates that were made to the Domino Directory, including person documents, server documents and changes to the ACL are not removed. To remove Sametime from a Domino server, follow these steps:

Procedure
1. End the Domino server where you plan to remove Sametime.
2. On any IBM i command line, type the following command and press F4:
   RMVLSTDOM
3. Enter the name of the Domino server where you want to remove Sametime and press Enter.
4. When prompted, type a "g" to complete the Remove Sametime from a Domino server command.
   A message will appear indicating that Sametime has been removed.
5. Using the Domino Administrator Application, modify the Domino server document by changing the Is this a Sametime server? field to No.
6. Delete any Sametime Connection documents between this Sametime server and other Sametime servers.
7. Optional: If the Sametime Community Server used an LDAP directory, an LDAP document for that server exists in the Directory Assistance database. You may want to remove this and any other unnecessary documents from the Directory Assistance database.

Results

The server is once again a Domino server.
If you want to delete the Sametime Community Server software from the system, remove Sametime from your servers and then run the DTLICPGM (Delete Licensed Program) command.

- For Sametime Standard, delete 5724J23 option 1 and then delete 5724J23 *BASE.
- For Sametime Entry, delete 5724J23 *BASE.

**Uninstalling a WebSphere-based Sametime server on IBM i:**

Uninstalling an IBM Sametime Meeting Server, Lotus Sametime Proxy Server, or Sametime System Console uses a different procedure from Sametime Gateway.

**About this task**

Follow these steps to uninstall a Sametime Meeting Server, Sametime Proxy Server, or Sametime System Console:

**Unregistering a Sametime Proxy Server or Meeting Server on IBM i:**

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 should only unregister a server on IBM i after uninstalling or if you are performing some other activity that requires removal of the product from the console.

**About this task**

This procedure applies to the following Sametime servers:

- Sametime Proxy Server
- Sametime Meeting Server

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. Navigate to the server's InstallLocation/console directory.
      - Proxy Server
        /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        The date and time indicate when the Proxy Server was installed.
      - Meeting Server
        /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
        The date and time indicate when the Meeting Server was installed.
   
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Verify the following values in the console.properties file that were specified when the server was initially registered. You will need to add the Sametime System Console password. After you make the changes, save and close the file.
Table 109. `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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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. <strong>Note:</strong> If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to &quot;false.&quot; Otherwise the registration will fail.</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 110. 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>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 111. 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>
<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>
<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>
4. If you are unregistering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.

5. Run the unregisterWASProduct.sh unregistration utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      ```bash
      QSH
      ```
   b. Navigate to the server's console directory.
      - **Proxy Server**
        ```bash
        /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        ```
      - **Meeting Server**
        ```bash
        /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
        ```
      The date and time indicate when the Proxy Server was installed.
      c. Run the shell script to unregister the server: `unregisterWASProduct.sh`
      d. When the registration script completes, press **F3** to exit QSH.

      The utility unregisters the server and generates a log file called `ConsoleUtility.log`, storing it in the `console/logs` directory. If the unregistration is successful, the `console.pid` will be removed.

      **Related reference**
      “Command reference for starting and stopping servers” on page 588
      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 Sametime Gateway on IBM i:**

      Before you uninstall an IBM Sametime Gateway server on IBM i, 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. Navigate to the server's `InstallLocation/console` directory.
            ```bash
            /QIBM/UserData/STGateway/ProfileName directory where ProfileName is the one you specified when you installed the Gateway.
            ```
         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 112. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
</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 113. 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 server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Now unregister the server:
   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. /QIBM/UserData/STGateway/ProfileName directory where ProfileName is the one you specified when you installed the Gateway.
   c. Run the shell script to unregister the server: unregisterWASProduct.sh -uninstall
   d. When the registration script completes, press F3 to exit QSH.

The utility unregisters the server and generates the ConsoleUtility.log file, storing it in the console/logs. If the unregistration is successful, the utility deletes the console.pid file from the console directory.

### Uninstalling IBM i Sametime servers running on WebSphere Application Server:

Uninstall IBM Sametime System Console, Sametime Meeting Server, or Sametime Proxy Server on a server running IBM i. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.
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

Procedure

1. For the type of server you plan to uninstall, shut down the servers listed below:
   - **Sametime System Console**
     Shut down the System Console Deployment Manager, the System Console application server, and the associated node agent.
   - **Proxy Server**
     Shut down the Proxy Deployment Manager, the Sametime Proxy application server, and the associated node agent.
   - **Meeting Server**
     Shut down the Meeting Deployment Manager, the Sametime Meeting application server, and the associated node agent.

2. From an IBM i command line, run the following command to start the QShell Interpreter:
   ```bash
   QSH
   ```

3. Run the `cd` shell command, specifying the fully qualified path to the uninstall directory for the server.
   - **Sametime System Console**
     ```bash
     cd /QIBM/UserData/Lotus/stii/STCONSOLE/STCONSOLE_date_time/uninstall
     ```
     where date and time indicate when the system console was installed.
   - **Proxy Server**
     ```bash
     cd /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/uninstall
     ```
     where date and time indicate when the proxy server was installed.
   - **Meeting Server**
     ```bash
     cd /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/uninstall
     ```
     where date and time indicate when the meeting server was installed.

4. Run the following shell command:
   ```bash
   uninstall.sh
   ```
   When the script completes, a summary of the results is displayed.

5. Press F3 to exit QSH.

6. Remove the Sametime application from the server by following 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.
   - On the Deployment Manager computer, start the Sametime server on the Deployment Manager if it is not already started.
   - 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.

**Results**

If the uninstall was not successful, look at the log for more information. Fix the problem, then try uninstalling again. The uninstall logs are stored in the following location: `QIBM/UserData/Lotus/stii/logs` and the log name contains the date and time in this form: `uninstall_ServerType_yyyymmdd_hhmm.log`. For example, this log for uninstalling a meeting server was created at 3:07 A.M. on December 15, 2009: `uninstall_STMEETINGS_20091215_0307.log`.

During uninstallation, the server is unregistered from the Sametime System Console, both the Sametime and the WebSphere Application Server applications are removed from the server. 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 or Meeting Server
- Updating the Sametime System Console when server unregistration fails

**What to do next**

When you have successfully uninstalled a server, there are other items associated with Sametime that you may want to remove from the system.

- **WebSphere Application Server installation**

  The WebSphere Application Server installation directory is typically shared by all of the Sametime servers running on WebSphere Application Server. Do not remove the WebSphere Application Server installation if there are any other Sametime servers on the system that are still using it. The sample commands below use the default installation directory.

  **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.

  To uninstall WebSphere Application Server, run the following QSH command:
  ```bash
  /qibm/proddata/websphere/appserver/v7/sametimewas/uninstall/uninstall -silent
  ```

  To remove the WebSphere Application Server data from the system, run the following QSH commands:
  ```bash
  rm -R /qibm/proddata/websphere/appserver/v7/sametimewas
  rm -R /qibm/userdata/websphere/appserver/v7/sametimewas
  ```

- **Sametime installation information**

  Remove installation information associated with the server you uninstalled in one of these ways:
If you still have other Sametime servers on the system, you can remove the installation information associated with the server that you uninstalled. Run the following QSH command, specifying the appropriate date and time:

- **Sametime System Console**
  
  ```bash
  rm -R /qibm/userdata/lotus/stii/STConsole/STConsole_date_time
  ```

- **Sametime Proxy Server**
  
  ```bash
  rm -R /qibm/userdata/lotus/stii/STProxy/STProxy_date_time
  ```

- **Sametime Meeting Server**
  
  ```bash
  rm -R /qibm/userdata/lotus/stii/STMeetings/STMEETINGS_date_time
  ```

If there are no other Sametime servers installed on the system, you can remove all Sametime installation information, by running the following QSH command.

```bash
rm -R /qibm/userdata/lotus/stii
```

**Sametime databases**

If you are certain that no other Sametime servers are still using the databases used by the Meeting Server (MTG and POLICY) or the Sametime System Console (SSC and POLICY), you can delete them. Remember that the POLICY database is shared between the Meeting Server and the Sametime System Console.

**Uninstalling Sametime Gateway on IBM i:**

Uninstall IBM Sametime Gateway on a server running IBM i.

**About this task**

On IBM i, you may choose to uninstall WebSphere Application Server after uninstalling Sametime Gateway, as described below.

**Procedure**

1. Shut down any servers that are running, including the Deployment Manager and node agents if you are uninstalling a cluster.
2. Start a QShell session.
3. Navigate to the following folder: `stgw_server_root/_uninst`
4. Type `uninstalli5OS.sh`
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. Click **Uninstall** to begin the procedure. The progress is displayed on the screen.
8. When the uninstall is complete, read the summary information and click **Finish** to exit the wizard.
9. If you are uninstalling a cluster of servers, repeat the preceding steps on each node, running the uninstall utility as you would on a single server deployment.
10. Uninstall WebSphere Application Server.

Complete details on uninstalling WebSphere Application Server are available from the WebSphere Application Server information center.
What to do next

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
- Updating the Sametime System Console when server unregistration fails

**Uninstalling one clustered server on IBM i**
Use the instructions in this section to uninstall one clustered Sametime server on IBM i.

**About this task**

Follow the procedure for the clustered Sametime server you want to uninstall:

**Related tasks**

- "Uninstalling all Sametime servers in a cluster on IBM i" on page 952

Use the instructions in this section to remove and uninstall a cluster of Sametime server on IBM i.

**Uninstalling one clustered Sametime Community Server on IBM i:**

You can uninstall one clustered IBM Sametime Community Server running on IBM i.

**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 servers on IBM i" on page 952

To remove a cluster of Sametime Community servers on IBM i, remove the nodes and the cluster first, then uninstall the individual servers.

**Removing a Sametime Community Server from a cluster on IBM i:**

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. Navigate to the Community Server’s `sametime_server_data_directory/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. |

---

Chapter 3. Installing   939
### Table 114. `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; To determine the correct HTTP port, open the <code>AboutThisProfile.txt</code> 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. On IBM i, look for the <code>AboutThisProfile.txt</code> file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code></td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

3. Run the `updateSTCluster` registration 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: `updateSTCluster.sh -remove`.
   d. When the utility prompts for the cluster's name, type the name and press `Enter`.
   e. When the utility finishes, press `F3` to exit QSH.

   The utility removes the Sametime Community Server from the cluster and generates the `ConsoleUtility.log` file in the `console/logs` directory.

### Unregistering a clustered Community Server on IBM i:

To remove an IBM Sametime Community Server running on IBM i from the list of the Sametime System Console's managed servers, run the unregister utility on the server. You should only unregister the server on IBM i if you plan to uninstall the server or if you are performing some other activity that requires removing it 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`

A Sametime Community Server reverts back to using legacy policies if you remove it from the console.
Procedure
1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's `sametime_server_data_directory/console` directory.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.
2. Verify the following values in the console.properties file that were specified when the server was initially registered. All of the values, including the encrypted System Console password should already be in the properties file.

   Table 115. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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. <strong>Note:</strong> If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to &quot;false.&quot; Otherwise the registration will fail.</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.
   The only required value in this file is
   **DepName:** When you are unregistering, 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.
4. Start the Sametime Community Server.
5. Run the unregisterProductNode.sh unregistration 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 server: `unregisterProductNode.sh`
d. As the unregistration 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.

e. When the registration script completes, press F3 to exit QSH.
   The utility unregisters the server and generates a log file called 
   ConsoleUtility.log, storing it in the consoles/logs directory. If the 
   unregistration is successful, the console.pid is removed

Related reference
“Command reference for starting and stopping servers” on page 588
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.

Removing a clustered Sametime Community Server from an IBM i Domino server:

You can remove Sametime files from a Lotus Domino server without deleting the 
Sametime Community Server software from your system. Use the RMVLSTDOM 
command to reverse the changes made when you ran the ADDLSTDOM command 
after installing the Sametime Community Server.

About this task

When you remove Sametime Community Server from a Domino server, all files 
related to Sametime that were added to the Domino server data directory or were 
created while running Sametime components are removed. Updates that were 
made to the Domino Directory, including person documents, server documents and 
changes to the ACL are not removed. To remove Sametime from a Domino server, 
follow these steps:

Procedure
1. End the Domino server where you plan to remove Sametime.
2. On any IBM i command line, type the following command and press F4:
   
   RMVLSTDOM

3. Enter the name of the Domino server where you want to remove Sametime and 
   press Enter.
4. When prompted, type a "g" to complete the Remove Sametime from a Domino 
   server command.
   
   A message will appear indicating that Sametime has been removed.
5. Using the Domino Administrator Application, modify the Domino server 
   document by changing the Is this a Sametime server? field to No.
6. Delete any Sametime Connection documents between this Sametime server and 
   other Sametime servers.
7. Optional: If the Sametime Community Server used an LDAP directory, an 
   LDAP document for that server exists in the Directory Assistance database. You 
   may want to remove this and any other unnecessary documents from the 
   Directory Assistance database.

Results

The server is once again a Domino server.
If you want to delete the Sametime Community Server software from the system, remove Sametime from your servers and then run the DLTLCPGM (Delete Licensed Program) command.

- For Sametime Standard, delete 5724J23 option 1 and then delete 5724J23 *BASE.
- For Sametime Entry, delete 5724J23 *BASE.

**Uninstalling one clustered WebSphere-based server on IBM i:**

Uninstall a clustered IBM Sametime Proxy Server or Sametime Meeting Server running on IBM i.

**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 IBM i” on page 957

To remove a cluster of Sametime servers running on WebSphere Application Server on IBM i, remove the nodes and the cluster first, then uninstall the individual servers.

**Removing a node from the Deployment Manager on IBM i:**

Afer uninstalling an IBM Sametime server that was clustered with an IBM WebSphere Application Server network deployment, remove the node from the Deployment Manager.

**About this task**

If you are uninstalling a cluster, run the utility on every node in the cluster.

**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 the 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 IBM i:**

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:
- Proxy Server
- Meeting Server
- Gateway

Procedure
1. Update the console.properties file on the Deployment Manager:
   a. On the Deployment Manager server, navigate to the following directory:
      - **Proxy Server**: /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        where the date and time indicate when the Proxy Server was installed.
      - **Meeting Server**: /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
        where the date and time indicate when the Meeting Server was installed.
      - **Gateway**: /qibm/userdata/STGateway/ProfileName
        where ProfileName is the profile for the Deployment Manager.
      **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:
      - **SSCHostName**: Type the fully qualified host name of the Lotus 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 SSCSSEnabled 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. Now run the `updateWASCluster.sh -remove` utility to remove the node from the cluster:
a. From an IBM i command line, run the following command to start the QShell Interpreter:
   `QSH`

b. Run the `cd shell` command, specifying the fully qualified path to the console directory you used in Step 2.

c. Run the following shell command: `updateWASCluster.sh -remove`
   **Attention:** You must specify the `-remove` parameter. Otherwise, you will unregister the entire cluster rather than remove the one node.

d. When prompted by the utility, enter the name of the cluster from which you are removing the node, and press Enter.
   The 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.

e. Press F3 to exit QSH

Unregistering a Sametime Meeting Server or Sametime Proxy Server on IBM i:

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 should only unregister a server on IBM i after uninstalling or if you are performing some other activity that requires removal of the product from the console.

**About this task**

This procedure applies to the following Sametime servers:
- Sametime Proxy Server
- Sametime Meeting Server

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. Navigate to the server's `InstallLocation/console` directory.
      - **Proxy Server**
         `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`
         The `date` and `time` indicate when the Proxy Server was installed.
      - **Meeting Server**
         `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`
         The `date` and `time` indicate when the Meeting Server was installed.
   b. Make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

2. Verify the following values in the `console.properties` file that were specified when the server was initially registered. You will need to add the Sametime System Console password. After you make the changes, save and close the file.
Table 116. 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 “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 &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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 “true” to connect to the Sametime System Console using a secure connection. <em>Note:</em> If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to “false.” Otherwise the registration will fail.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to “true.”</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 117. 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>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 118. 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>
<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>
<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>
4. If you are unregistering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.

5. Run the unregisterWASProduct.sh unregistration 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.
      • **Proxy Server**
        /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        The *date* and *time* indicate when the Proxy Server was installed.
      • **Meeting Server**
        /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
        The *date* and *time* indicate when the Meeting Server was installed.
   c. Run the shell script to unregister the server: unregisterWASProduct.sh
   d. When the registration script completes, press F3 to exit QSH.

   The utility unregisters the server and generates a log file called ConsoleUtility.log, storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.

**Related reference**

“Command reference for starting and stopping servers” on page 588
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 clustered Sametime Gateway server on IBM i:**

Before you uninstall an IBM Sametime Gateway server on IBM i, 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. Navigate to the server's InstallLocation/console directory.
      /QIBM/UserData/STGateway/ProfileName directory where *ProfileName* is the one you specified when you installed the Gateway.
   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 119. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
</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 120. 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 server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Now unregister the server:
   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. /QIBM/UserData/STGateway/ProfileName directory where ProfileName is the one you specified when you installed the Gateway.
   c. Run the shell script to unregister the server: unregisterWASProduct.sh -uninstall
   d. When the registration script completes, press F3 to exit QSH.

Uninstalling Sametime servers running on WebSphere Application Server on IBM i:

Uninstall IBM Sametime System Console, Sametime Meeting Server, or Sametime Proxy Server on a server running IBM i. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.
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

Procedure
1. For the type of server you plan to uninstall, shut down the servers listed below:
   - **Sametime System Console**
     Shut down the System Console Deployment Manager, the System Console application server, and the associated node agent.
   - **Proxy Server**
     Shut down the Proxy Deployment Manager, the Sametime Proxy application server, and the associated node agent.
   - **Meeting Server**
     Shut down the Meeting Deployment Manager, the Sametime Meeting application server, and the associated node agent.
2. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH

3. Run the cd shell command, specifying the fully qualified path to the uninstall directory for the server.
   - **Sametime System Console**
     cd /QIBM/UserData/Lotus/stii/STCONSOLE/STCONSOLE_date_time/uninstall
     where date and time indicate when the system console was installed.
   - **Proxy Server**
     cd /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/uninstall
     where date and time indicate when the proxy server was installed.
   - **Meeting Server**
     cd /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/uninstall
     where date and time indicate when the meeting server was installed.
4. Run the following shell command:
   ```
   uninstall.sh
   ```
   When the script completes, a summary of the results is displayed.
5. Press F3 to exit QSH.
6. Remove the Sametime application from the server by following 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.

Results

If the uninstall was not successful, look at the log for more information. Fix the problem, then try uninstalling again. The uninstall logs are stored in the following location: QIBM/UserData/Lotus/stii/logs and the log name contains the date and time in this form: uninstall_ServerType_yyyymmdd_hhmm.log. For example, this log for uninstalling a meeting server was created at 3:07 A.M. on December 15, 2009: uninstall_STMEETINGS_20091215_0307.log.

During uninstallation, the server is unregistered from the Sametime System Console, both the Sametime and the WebSphere Application Server applications are removed from the server. 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 or Meeting Server
- Updating the Sametime System Console when server unregistration fails

What to do next

When you have successfully uninstalled a server, there are other items associated with Sametime that you may want to remove from the system.

- **WebSphere Application Server installation**
  
The WebSphere Application Server installation directory is typically shared by all of the Sametime servers running on WebSphere Application Server. Do not remove the WebSphere Application Server installation if there are any other Sametime servers on the system that are still using it. The sample commands below use the default installation directory.

  **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.

To uninstall WebSphere Application Server, run the following QSH command:

```
/qibm/proddata/websphere/appserver/v7/sametimewas/uninstall/uninstall -silent
```

To remove the WebSphere Application Server data from the system, run the following QSH commands:

```
rm -R /qibm/proddata/websphere/appserver/v7/sametimewas
rm -R /qibm/userdata/websphere/appserver/v7/sametimewas
```

- **Sametime installation information**
  
Remove installation information associated with the server you uninstalled in one of these ways:
If you still have other Sametime servers on the system, you can remove the installation information associated with the server that you uninstalled. Run the following QSH command, specifying the appropriate date and time:

- **Sametime System Console**
  
  `rm -R /qibm/userdata/lotus/stii/STConsole/STConsole_date_time`

- **Sametime Proxy Server**
  
  `rm -R /qibm/userdata/lotus/stii/STProxy/STProxy_date_time`

- **Sametime Meeting Server**
  
  `rm -R /qibm/userdata/lotus/stii/STMeetings/STMEETINGS_date_time`

If there are no other Sametime servers installed on the system, you can remove all Sametime installation information, by running the following QSH command.

`rm -R /qibm/userdata/lotus/stii`

**Sametime databases**

If you are certain that no other Sametime servers are still using the databases used by the Meeting Server (MTG and POLICY) or the Sametime System Console (SSC and POLICY), you can delete them. Remember that the POLICY database is shared between the Meeting Server and the Sametime System Console.

**Uninstalling a Sametime Gateway server on IBM i:**

Uninstall IBM Sametime Gateway on a server running running IBM i.

**About this task**

On IBM i, you may choose to uninstall WebSphere Application Server after uninstalling Sametime Gateway, as described below.

**Procedure**

1. Shut down any servers that are running, including the Deployment Manager and node agents if you are uninstalling a cluster.
2. Start a QShell session.
3. Navigate to the following folder: `stgw_server_root/_uninst`
4. Type `uninstall50S.sh`
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. Click **Uninstall** to begin the procedure. The progress is displayed on the screen.
8. When the uninstall is complete, read the summary information and click **Finish** to exit the wizard.
9. If you are uninstalling a cluster of servers, repeat the preceding steps on each node, running the uninstall utility as you would on a single server deployment.
10. Uninstall WebSphere Application Server.

  Complete details on uninstalling WebSphere Application Server are available from the WebSphere Application Server information center.
What to do next

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
- Updating the Sametime System Console when server unregistration fails

Uninstalling all Sametime servers in a cluster on IBM i

Use the instructions in this section to remove and uninstall a cluster of Sametime server on IBM i.

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 servers on IBM i:

To remove a cluster of Sametime Community servers on IBM i, 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 IBM i:

If you will uninstall an entire cluster of IBM Sametime Community Servers, you must unregister the cluster from the Lotus Sametime System Console before you uninstall Sametime on the individual servers.

Before you begin

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 sametime_server_data_directory/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 12.1. console.properties settings
Table 121. 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 SSCSSEnabled 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.
|             | On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt |

3. Run the removeClusterRegistration registration 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: removeClusterRegistration.sh.
   d. When the utility prompts for the cluster's name, type the name and press Enter.
   e. When the utility finishes, press F3 to exit QSH.

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.

Removing a Sametime Community Server from an IBM i 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. Navigate to the Community Server's sametime_server_data_directory/console directory.
2. Update the following values in the console.properties file before saving and closing the file:

Table 122. console.properties settings

| SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
Table 122. `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; 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. On IBM i, look for the AboutThisProfile.txt file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

3. Run the `updateSTCluster` registration 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: `updateSTCluster.sh -remove`.
   d. When the utility prompts for the cluster's name, type the name and press `Enter`.
   e. When the utility finishes, press `F3` to exit QSH.

The utility removes the Sametime Community Server from the cluster and generates the `ConsoleUtility.log` file in the `console/logs` directory.

Unregistering a clustered IBM i Community Server:

To remove an IBM Sametime Community Server running on IBM i from the list of the Sametime System Console's managed servers, run the unregister utility on the server. You should only unregister the server on IBM i if you plan to uninstall the server or if you are performing some other activity that requires removing it 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`

A Sametime Community Server reverts back to using legacy policies if you remove it from the console.
Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's `sametime_server_data_directory/console` directory.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Verify the following values in the console.properties file that were specified when the server was initially registered. All of the values, including the encrypted System Console password should already be in the properties file.

   Table 123. 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." |
   |             | 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. |
   |             | 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. |
   | SSCSSLEnabled | Change this value to "true" to connect to the Sametime System Console using a secure connection. |
   |             | **Note:** If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to "false." Otherwise the registration will fail. |
   | 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.
   The only required value in this file is
   **DepName:** When you are unregistering, 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.

4. Start the Sametime Community Server.

5. Run the unregisterProductNode.sh unregistration 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 server: unregisterProductNode.sh
d. As the unregistration 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.

e. When the registration script completes, press F3 to exit QSH.

The utility unregisters the server and generates a log file called ConsoleUtility.log, storing it in the consoles/logs directory. If the unregistration is successful, the console.pid is removed.

Related reference
“Command reference for starting and stopping servers” on page 588
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.

Removing the clustered Sametime Community Server from an IBM i Domino server:

You can remove Sametime files from a Lotus Domino server without deleting the Sametime Community Server software from your system. Use the RMVLSTDOM command to reverse the changes made when you ran the ADDLSTDOM command after installing the Sametime Community Server.

About this task

When you remove Sametime Community Server from a Domino server, all files related to Sametime that were added to the Domino server data directory or were created while running Sametime components are removed. Updates that were made to the Domino Directory, including person documents, server documents and changes to the ACL are not removed. To remove Sametime from a Domino server, follow these steps:

Procedure
1. End the Domino server where you plan to remove Sametime.
2. On any IBM i command line, type the following command and press F4:
   
   RMVLSTDOM

3. Enter the name of the Domino server where you want to remove Sametime and press Enter.
4. When prompted, type a "g" to complete the Remove Sametime from a Domino server command.
   
   A message will appear indicating that Sametime has been removed.
5. Using the Domino Administrator Application, modify the Domino server document by changing the Is this a Sametime server? field to No.
6. Delete any Sametime Connection documents between this Sametime server and other Sametime servers.
7. Optional: If the Sametime Community Server used an LDAP directory, an LDAP document for that server exists in the Directory Assistance database. You may want to remove this and any other unnecessary documents from the Directory Assistance database.

Results

The server is once again a Domino server.
If you want to delete the Sametime Community Server software from the system, remove Sametime from your servers and then run the DTLICPGM (Delete Licensed Program) command.

- For Sametime Standard, delete 5724J23 option 1 and then delete 5724J23 *BASE.
- For Sametime Entry, delete 5724J23 *BASE.

Removing a cluster of WebSphere-based Sametime servers on IBM i:

To remove a cluster of Sametime servers running on WebSphere Application Server on IBM i, 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 the deployment manager on IBM i:

After uninstalling an IBM Sametime server that was clustered with an IBM WebSphere Application Server network deployment, remove the node from the Deployment Manager.

About this task

If you are uninstalling a cluster, run the utility on every node in the cluster.

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 the 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 an IBM i 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:
- Proxy Server
- Meeting Server
- Gateway

Procedure
1. Update the console.properties file on the Deployment Manager:
   a. On the Deployment Manager server, navigate to the following directory:
      - Proxy Server: /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        where the date and time indicate when the Proxy Server was installed.
      - Meeting Server: /QIBM/UserData/Lotus/stii/STMetings/STMEETINGS_date_time/console
        where the date and time indicate when the Meeting Server was installed.
      - Gateway: /qibm/userdata/STGateway/ProfileName
        where ProfileName is the profile for the Deployment Manager.
        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:
      - SSCHostName: Type the fully qualified host name of the Lotus 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. Now run the updateWASCluster.sh -remove utility to remove the node from the cluster:
a. From an IBM i command line, run the following command to start the QShell Interpreter: QSH

b. Run the `cd shell` command, specifying the fully qualified path to the console directory you used in Step 2.

c. Run the following shell command: `updateWASCluster.sh -remove`
   
   **Attention:** You must specify the `-remove` parameter. Otherwise, you will unregister the entire cluster rather than remove the one node.

d. When prompted by the utility, enter the name of the cluster from which you are removing the node, and press Enter.
   
   The 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.

e. Press F3 to exit QSH

*Unregistering a cluster of WebSphere-based servers on IBM i:*

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.

These instructions apply to the following Sametime servers:

- Proxy Server
- Meeting Server
- Gateway

**Procedure**

1. On the Deployment Manager, update the `console.properties` file.
   a. Navigate to the following directory:
      
      - **Proxy Server**: `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`
      where the date and time indicate when the Proxy Server was installed.
      - **Meeting Server**: `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`
      where the date and time indicate when the Meeting Server was installed.
      - **Gateway**: `/qibm/userdata/STGateway/ProfileName`
      where `ProfileName` is the profile for the Deployment Manager.

      **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:
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.

1. Save and close the file.
2. Now run the `removeWASClusterRegistration.sh` utility to unregister the cluster:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: `QSH`
   b. Run the `cd shell` command, specifying the fully qualified path to the console directory you used in Step 2.
   c. Run the following shell command: `removeWASClusterRegistration.sh`
   d. When prompted by the utility, enter the name of the cluster from which you are removing the node, and press Enter.
      The utility deletes the cluster and generates a log file called `ConsoleUtility.log`, which it stores in the `console/log` directory.
   e. Press F3 to exit QSH

### Unregistering a Sametime Proxy Server or Sametime Meeting Server on IBM i:

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 should only unregister a server on IBM i after uninstalling or if you are performing some other activity that requires removal of the product from the console.

### About this task

This procedure applies to the following Sametime servers:

- Sametime Proxy Server
- Sametime Meeting Server

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. Navigate to the server's InstallLocation/console directory.
      - **Proxy Server**
        /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
        The date and time indicate when the Proxy Server was installed.
      - **Meeting Server**
        /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
        The date and time indicate when the Meeting Server was installed.
   b. Make backup copies (using different names) of the console.properties and productConfig.properties files.

2. Verify the following values in the console.properties file that were specified when the server was initially registered. You will need to add the Sametime System Console password. After you make the changes, save and close the file.

   **Table 124. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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></td>
<td><strong>Note:</strong> If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to &quot;false.&quot; Otherwise the registration will fail.</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 125. Sametime Proxy Server**
   | WASPassword     | Specify the password associated with the WASUserID. |

Chapter 3. Installing 961
Table 125. Sametime Proxy 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 126. 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>
<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>

4. If you are unregistering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.
5. Run the unregisterWASProduct.sh unregistration 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.
      • Proxy Server
         /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
         The date and time indicate when the Proxy Server was installed.
      • Meeting Server
         /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
         The date and time indicate when the Meeting Server was installed.
   c. Run the shell script to unregister the server: unregisterWASProduct.sh
   d. When the registration script completes, press F3 to exit QSH.

The utility unregisters the server and generates a log file called ConsoleUtility.log, storing it in the console/logs directory. If the unregistration is successful, the console.pid will be removed.

Related reference
“Command reference for starting and stopping servers” on page 588
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 Sametime Gateway (IBM i):

Before you uninstall an IBM Sametime Gateway server on IBM i, 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. Navigate to the server's `InstallLocation/console` directory.
      `/QIBM/UserData/STGateway/ProfileName` directory where `ProfileName` is the one you specified when you installed the Gateway.
   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 127. `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 <code>SSCSSLEnabled</code> is &quot;false.&quot;</td>
</tr>
<tr>
<td></td>
<td>To determine the correct HTTP port, open the <code>AboutThisProfile.txt</code> 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 <code>STSCAppProfile</code>.</td>
</tr>
<tr>
<td></td>
<td>On IBM i, look for the <code>AboutThisProfile.txt</code> file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</td>
</tr>
<tr>
<td>SSCPASSWORD</td>
<td>Enter the WebSphere Application Server password associated with the <code>SSCUserName</code>.</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 128. `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 server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Now unregister the server:
   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. `/QIBM/UserData/STGateway/
ProfileName` directory where `ProfileName` is the one you specified when you
installed the Gateway.

c. Run the shell script to unregister the server: `unregisterWASProduct.sh
-uninstall`

d. When the registration script completes, press **F3** to exit QSH.
The utility unregisters the server and generates the `ConsoleUtility.log` file,
storing it in the `console/logs`. If the unregistration is successful, the utility
deletes the `console.pid` file from the console directory.

**Editing the multibroker.xml file before removing a cluster on IBM i:**

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 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"?>
<xml:XML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com/websphere/appserver/schemas/5.0/multibroker.xmi">
  <multibroker:DataReplicationDomain xmi:id="DataReplicationDomain_1285354058851" name="stCellDRS"/>
  <defaultDataReplicationSettings xmi:id="DataReplication_1285354058851"
    requestTimeout="5" encryptionType="NONE" numberOfReplicas="-1" />
  <partition xmi:id="DRSPartition_1285354058851" partitionOnEntry="false"/>
  <serialization xmi:id="DRSSerialization_1285354058851" entrySerializationKind="BYTES"
    propertySerializationKind="BYTES" />
  <pooling xmi:id="DRSConnectionPool_1285354058851" poolConnections="false" />
</defaultDataReplicationSettings>
</multibroker:DataReplicationDomain>
```

**Removing a cluster from WebSphere Application Server on IBM i:**

Remove the IBM 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 IBM i Sametime servers hosted on WebSphere Application Server:

Uninstall IBM Sametime System Console, Sametime Meeting Server, or Sametime Proxy Server on a server running IBM i. These servers all run on IBM WebSphere Application Server, similar to Sametime Gateway, but require a different process for uninstallation.

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

Procedure
1. For the type of server you plan to uninstall, shut down the servers listed below:
   • Sametime System Console
     Shut down the System Console Deployment Manager, the System Console application server, and the associated node agent.
   • Proxy Server
     Shut down the Proxy Deployment Manager, the Sametime Proxy application server, and the associated node agent.
   • Meeting Server
     Shut down the Meeting Deployment Manager, the Sametime Meeting application server, and the associated node agent.
2. From an IBM i command line, run the following command to start the QShell Interpreter:
   QSH
3. Run the cd shell command, specifying the fully qualified path to the uninstall directory for the server.
   • Sametime System Console
     cd /QIBM/UserData/Lotus/stii/STCONSOLE/STCONSOLE_date_time/uninstall
     where date and time indicate when the system console was installed.
   • Proxy Server
     cd /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/uninstall
where date and time indicate when the proxy server was installed.

- **Meeting Server**
  
  ```bash
cd /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/uninstall
  
  cd /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/uninstall
  
  where date and time indicate when the meeting server was installed.
```

4. Run the following shell command:

```bash
uninstall.sh
```

When the script completes, a summary of the results is displayed.

5. Press **F3** to exit QSH.

6. Remove the Sametime application from the server by following 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.

**Results**

If the uninstall was not successful, look at the log for more information. Fix the problem, then try uninstalling again. The uninstall logs are stored in the following location: `QIBM/UserData/Lotus/stii/logs` and the log name contains the date and time in this form: `uninstall_ServerType_yyyymmdd_hhmm.log`. For example, this log for uninstalling a meeting server was created at 3:07 A.M. on December 15, 2009: `uninstall_STMEETINGS_20091215_0307.log`.

During uninstallation, the server is unregistered from the Sametime System Console, both the Sametime and the WebSphere Application Server applications are removed from the server. 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 or Meeting Server
- Updating the Sametime System Console when server unregistration fails

**What to do next**

When you have successfully uninstalled a server, there are other items associated with Sametime that you may want to remove from the system.

- **WebSphere Application Server installation**
  
  The WebSphere Application Server installation directory is typically shared by all of the Sametime servers running on WebSphere Application Server. Do not remove the WebSphere Application Server installation if there are any other
Sametime servers on the system that are still using it. The sample commands below use the default installation directory.

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.

To uninstall WebSphere Application Server, run the following QSH command:
/qibm/proddata/websphere/appserver/v7/sametimewas/uninstall/uninstall -silent

To remove the WebSphere Application Server data from the system, run the following QSH commands:
rm -R /qibm/proddata/websphere/appserver/v7/sametimewas
rm -R /qibm/userdata/websphere/appserver/v7/sametimewas

• Sametime installation information

Remove installation information associated with the server you uninstalled in one of these ways:

If you still have other Sametime servers on the system, you can remove the installation information associated with the server that you uninstalled. Run the following QSH command, specifying the appropriate date and time:

– Sametime System Console
  rm -R /qibm/userdata/lotus/stii/STConsole/STConsole_date_time

– Sametime Proxy Server
  rm -R /qibm/userdata/lotus/stii/STProxy/STProxy_date_time

– Sametime Meeting Server
  rm -R /qibm/userdata/lotus/stii/STMeetings/STMEETINGS_date_time

If there are no other Sametime servers installed on the system, you can remove all Sametime installation information, by running the following QSH command.
rm -R /qibm/userdata/lotus/stii

• Sametime databases

If you are certain that no other Sametime servers are still using the databases used by the Meeting Server (MTG and POLICY) or the Sametime System Console (SSC and POLICY), you can delete them. Remember that the POLICY database is shared between the Meeting Server and the Sametime System Console.

Uninstalling a Sametime Gateway node on IBM i:

Uninstall IBM Sametime Gateway on a server running running IBM i.

About this task

On IBM i, you may choose to uninstall WebSphere Application Server after uninstalling Sametime Gateway, as described below.

Procedure

1. Shut down any servers that are running, including the Deployment Manager and node agents if you are uninstalling a cluster.
2. Start a QShell session.
3. Navigate to the following folder: stgw_server_root/_uninst
4. Type uninstalli5OS.sh
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. Click Uninstall to begin the procedure. The progress is displayed on the screen.
8. When the uninstall is complete, read the summary information and click Finish to exit the wizard.
9. If you are uninstalling a cluster of servers, repeat the preceding steps on each node, running the uninstall utility as you would on a single server deployment.
10. Uninstall WebSphere Application Server.
    Complete details on uninstalling WebSphere Application Server are available from the WebSphere Application Server information center.

What to do next

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
- Updating the Sametime System Console when server unregistration fails

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 1024.

**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.
Related tasks

“Preparing servers running on WebSphere Application Server for single sign-on” on page 1485
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.

“Adding a Sametime Proxy Server to the Sametime Community Server’s trusted IP addresses” on page 241
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.

“Deploying Sametime Meeting Server and Sametime Proxy Server on the same computer” on page 451
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.

“Adding the Sametime Media Manager to the Sametime Community Server’s trusted IP addresses” on page 267
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.

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:


### 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 969
- 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 971
- 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.xxyz.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\Local\Low\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 1417

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//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 sametime-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 1581

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 982

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 988

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 985

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 980
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 982
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 988
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 985
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:

```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
```
Below are Sample resourcebundle messages.properties

Add a new contact by entering a name below.

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 1581
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 994
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 992
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
   -->
   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 977

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>
<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><code>com.ibm.collaboration.realtime.oi.standalone.feature</code></td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Office</td>
<td><code>com.ibm.collaboration.realtime.oi.smarttags.feature</code></td>
</tr>
<tr>
<td>Microsoft Outlook calendar availability</td>
<td><code>com.ibm.collaboration.realtime.exchange.feature</code></td>
</tr>
<tr>
<td>Sametime Connect integrator for Microsoft Outlook</td>
<td><code>com.ibm.collaboration.realtime.oi.toolbar.feature</code></td>
</tr>
<tr>
<td>Sametime meeting integrator for Microsoft Outlook</td>
<td><code>com.ibm.collaboration.realtime.oi.webConfTab.feature</code></td>
</tr>
<tr>
<td>Sametime Connect integrator for SharePoint</td>
<td><code>com.ibm.collaboration.realtime.oi.sharepoint.feature</code></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><code>com.ibm.collaboration.realtime.notes.connector.standalone.feature</code></td>
</tr>
<tr>
<td>Sametime availability status updates based on person's Lotus Notes calendar entries</td>
<td><code>com.ibm.collaboration.realtime.notes.connector.feature</code></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 installaddon.xml file for the Lotus Notes embedded client:

You can customize the installaddon.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 installaddon.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\installaddon.xml

   Windows
   $Save_files_in_folder_directory\deploy\installaddon.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.

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: <!--
End a comment with this marker: -->

<!-- This is a sample comment; it can run across multiple lines in the file -->
<!-- The marker can be on the same line as other text, or on its own line. -->

For example, you may want to enable one or more Microsoft Office Integration features for clients running on Windows:

Table 130. 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 131. 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>com.ibm.collaboration.realtime.oi.embedded.feature</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>
<tr>
<td>Optional feature</td>
<td>Feature ID</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Outlook calendar availability</td>
<td>com.ibm.collaboration.realtime.exchange.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for</td>
<td>com.ibm.collaboration.realtime.oi.toolbar.feature</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td></td>
</tr>
<tr>
<td>Sametime meeting integrator for</td>
<td>com.ibm.collaboration.realtime.oi.webConfTab.feature</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td></td>
</tr>
<tr>
<td>Sametime Connect integrator for</td>
<td>com.ibm.collaboration.realtime.oi.sharepoint.feature</td>
</tr>
<tr>
<td>SharePoint</td>
<td></td>
</tr>
<tr>
<td>Notes calendar integration</td>
<td>com.ibm.collaboration.realtime.notes.connector.feature</td>
</tr>
<tr>
<td>Sametime availability status</td>
<td></td>
</tr>
<tr>
<td>updates based on person’s Lotus Notes calendar entries</td>
<td></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" size="4302" action="install" shared="true" mergeaction="add" url="jar:${installer.root}/sametime.embedded.update.site.20091027-2140.zip!/"/>
```
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:

```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!/"/>
<!-- 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/install.mac/
     sametime.internal.macosx_build.tar
   - IBM i server
     /STserver/domino/html/sametime/network-install/install.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:
   <!-- 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/insta11.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/insta11.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><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>
</tbody>
</table>
Table 132. 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.oil.toolbar.feature</td>
</tr>
<tr>
<td>Sametime meeting integrator for Microsoft Outlook</td>
<td>com.ibm.collaboration.realtime.oil.webConfTab.feature</td>
</tr>
<tr>
<td>Sametime Connect integrator for SharePoint</td>
<td>com.ibm.collaboration.realtime.oil.sharepoint.feature</td>
</tr>
<tr>
<td>Notes calendar integration</td>
<td>com.ibm.collaboration.realtime.notes.connector.feature</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="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oil.sharepoint.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="3833"
    size="3833" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oil.smarttags.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="5685"
    size="5685" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oil.standalone.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="7"
    size="7" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oil.toolbar.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="4302"
    size="4302" action="install" shared="true" mergeaction="add"
    url="${installer.root}"/>
<feature id="com.ibm.collaboration.realtime.oil.webConfTab.feature"
    version="8.5.0.20091027-2140" match="compatible" download-size="315"
    size="315" action="install" shared="true" mergeaction="add"
    url="${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.

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_i5OS.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 1028
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 134. 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 <em>community-config.xml</em> file. If you use a custom <em>plugin_customization.ini</em> 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 <em>plugin_customization.ini</em> 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 980
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 1028
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 1028
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 1029
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 1028
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:

   \texttt{rm -rf /tmp/deploy /tmp/sametime-connect-*.rpm /tmp/install.sh}

2. Install the compat runtime library by running the following command:

   \textbf{RHEL 5.x}
   \begin{verbatim}
   rpm -ivh compat-libstdc++-33-3.2.3-61.i386.rpm
   \end{verbatim}

   \textbf{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
   \texttt{stserver.example.com}, you open \url{http://stserver.example.com/stcenter.nsf}.

4. Click \textbf{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 \textbf{Install Now} to begin the download and installation process.
   Once all files have been downloaded, the actual client installer will start and
   runs automatically.

   \textbf{Tip:} If there are problems running the network client installer applet, or if you
   want to install at a later time, you can select \textbf{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.

\textbf{Related tasks}

- “Uninstalling the Sametime Connect client on Linux” on page 1028
- Uninstall or revert to an earlier version of the IBM Sametime Connect client on
  Linux.

\textbf{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.

\textbf{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:

      \texttt{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
   \texttt{stserver.example.com}, you open \url{http://stserver.example.com/stcenter.nsf}.

3. Click \textbf{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 \textbf{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 1029
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: https://www-304.ibm.com/support/docview.wss?rs=477&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: 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
```

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 1029

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.

```
rm -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 1029
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 1030
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 1030 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:

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:
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 977
- 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 1024
  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:

   ```xml
   <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>
   </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.

   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

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 977
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.onfocusin=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):
      ```
      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 `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;
      }
      ```

10. Save and close the `Init.js` file.
    Next you will make similar changes to the `OWS.js` file.

11. Replace the `EnsureIMNCtrl` function in the `OWS.js` file as follows:
    a. Open the `OWS.js` file for editing.
    b. Open the `EnsureIMNCtrl.js` file that you copied to the server back in step 1.
    c. Copy the `EnsureIMNCtrl` function from this file (leave the file open for now).
    d. Back in the `OWS.js` file, search for its own version of the `EnsureIMNCtrl` function, delete that, and paste the newer version in its place.
    e. Close the `EnsureIMNCtrl.js` file.

12. 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 `OWS.js`, 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):
       ```javascript
       if (typeof(IMNDictionaryObj[id])=='undefined')
       ```
    c. Change the assignment from `IMNDictionaryObj[id]=1` to `IMNDictionaryObj[id]=0` so the "if" statement looks like this:
       ```javascript
       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=IMNShowOOUUIKyb;
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):
if (fFirst)
{
  var objRet=IMNGetOOUILocation(obj);
  objSpan=objRet.objSpan;
  if (objSpan)
  {
    objSpan.onmouseover=IMNShowOOUIMouse;
    objSpan.onfocusin=IMNShowOOUUIKyb;
    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:
      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 1019
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 977
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.

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 1013
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 1017
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

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 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:
   ```bash
   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 Ubuntu.
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 lotus folder, stored in the User 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

From a DOS command prompt, 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 4. 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

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.

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:

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 a prerequisite to installing this release of IBM Sametime. Upgrade DB2 on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing a newer version over an existing version if you do not already have the prerequisite version.
Before you begin

Back up the database using the DB2 Control Center or the db2 backup
database_name command.

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 supported for
this release.

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:
   &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
   ```

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.

   **AIX, Linux, and Solaris**
   
   Log in as the db2admin user and run the DB2 upgrade command.
   
   ```
   su db2admin
   db2 upgrade database database_name
   ```

   **Windows**
   
   Run the DB2 upgrade command.
   
   ```
   db2 upgrade database database_name
   ```

**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 DB2 from a Sametime 8.5.1 installation on AIX, Linux, Solaris, and Windows:**
IBM DB2 9.7 is a prerequisite to installing this release of IBM Sametime. Upgrade DB2 on IBM AIX, Linux, Sun Solaris, or Microsoft Windows by installing a newer version over an existing version if you do not already have the prerequisite version.

Before you begin

Back up the database using the DB2 Control Center or the `db2 backup database_name` command.

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 supported for this release.

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:
      ```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
      ```
   4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
      - **Linux** 
        ```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
      ```
      ```bash
      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, and 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.
   AIX, Linux, and Solaris
   Log in as the db2admin user and run the DB2 upgrade command.
   su db2admin
   db2 upgrade database database_name
   Windows
   Run the DB2 upgrade command.
   db2 upgrade database database_name

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.
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, seeBacking 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.
   - 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: 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
   ```

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
   ```
   ./update_85_SCDb.sh STSC dbadmin
   ```
   Windows
   ```
   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:
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.

**Upgrading a Sametime 8.5 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 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:
   &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
   ```

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 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 terminal 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
```

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:**

/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 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.

**Upgrading a Sametime 8.5 or 8.5.1 Community Server on AIX, Linux, Solaris, or 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:
      ```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
      ```

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**
   ```bash
   ./setupaix.bin
   ```

   **Linux**
   ```bash
   ./setuplinux.bin
   ```

   **Solaris**
   ```bash
   ./setupsolaris.bin
   ```

   **Windows**
   ```bash
   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:
     
     ```ini
     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:
     
     ```ini
     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`

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**
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 Sametime 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:
     ```
     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: 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
      ```

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**
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.

Upgrading a stand-alone 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 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 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/conversion/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:


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 8.5 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 1417

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
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 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/STSCOMgrProfile/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
```

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 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 -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 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:

```
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:

- **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 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/instalableApps/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 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:
   &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
   ```

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 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`
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:
&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
```

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 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:**
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:
&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
   ```

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:

   ```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. 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
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 -o ro /dev/cd0 /cdrom
   ```

   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:
   - 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 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/STSCOMgrProfile/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:
         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:

```
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 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:

   \texttt{install\_root/SametimeMeetingServerOffering/SametimeServer/STMeeting/meeting/installableApps/meeting.server.ear}

b. Copy the file to the following location on the Sametime System Console:

   \texttt{WAS\_install\_root/AppServer/profiles/STSCDMgrProfile/config/temp/}

\textbf{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.

\textbf{AIX, Linux, or Solaris}

\texttt{/var/ibm/InstallationManager/logs}

\textbf{SSC connection log:}

\texttt{/tmp/SSCLogs/ConsoleUtility0.log}

\textbf{Windows 2008}

\texttt{%ALLUSERSPROFILE%\IBM\Installation Manager\logs}

\textbf{Windows 2003}

\texttt{%ALLUSERSPROFILE%\Application Data\IBM\Installation Manager\logs}

\textbf{SSC connection log:}

\begin{verbatim}
Documents and Settings\username\Local Settings\Temp\SSCLogs\ConsoleUtility0.log
\end{verbatim}

\begin{verbatim}
Starting servers in the upgraded Sametime Meeting Server cluster on AIX, Linux, Solaris, or Windows:
\end{verbatim}

In an IBM Sametime deployment, start the servers in the upgraded cluster of Sametime Meeting Servers.

\textbf{Before you begin}

Upgrade all nodes in the cluster before you start the cluster.

\textbf{Procedure}

1. On the server hosting the Deployment Manager, open a command window and start the cluster’s Deployment Manager:

   \textbf{AIX, Linux, Solaris}: ./startManager.sh dmgr

   \textbf{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:
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. **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:
   - **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.

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/ProxyApp1-8.5.2.ear
        install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarApp1-8.5.2.ear

   b. Copy the files to the following location on the Sametime System Console:
      WAS_install_root/AppServer/profiles/STSCOMgrProfile/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:
         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
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:
   - **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.

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
```

**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 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.
   - In the Deployment Manager's Integrated Solutions Console, click **System
     Administration > Nodes**.
   - 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: 
        ```bash
        ./stopServer.sh Conference_Manager_name -username WAS_admin_username -password WAS_admin_password
        ```
      - Windows:
        ```cmd
        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:
        ```bash
        ./stopServer.sh WAS_proxy_server_name
        ```
      - Windows:
        ```cmd
        stopServer.bat WAS_proxy_server_name
        ```
   c. Stop the node agent:
      - Linux:
        ```bash
        ./stopNode.sh -username WAS_admin_username -password WAS_admin_password
        ```
      - Windows:
        ```cmd
        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: 
     ```bash
     ./stopManager.sh dmgr -username WAS_admin_username -password WAS_admin_password
     ```
   - Windows: 
     ```cmd
     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:
         &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`
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:
   - **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.

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 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:
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. 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:

- 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.

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.

9. 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/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:
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`

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 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: 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`

   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:
      • **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.

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/ProxyApp1-8.5.2.ear
        install_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/installableApps/RegistrarApp1-8.5.2.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 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:
            &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
```

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:
   - **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.

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 \textbf{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 \textbf{I accept the terms in the license agreements} option and click \textbf{Next}.

13. Validate the WebSphere Application Server administrator ID and password, and then click \textbf{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 \textbf{Validate}.

16. After the \textbf{Validate} button changes to \textbf{Validated}, click \textbf{Next}.

17. Click \textbf{Update}.

18. Click \textbf{Finish} when the installation process is complete.

19. Click \textbf{Exit} to close the Installation Manager.

20. If this is the Primary Node for a cluster and the Sametime System Console does \textit{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:
     \texttt{install\_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/}
     \texttt{installableApps/ConferenceFocus.ear}
   - SIP Proxy and Registrar cluster's Primary Node contains two EAR files to copy:
     \texttt{install\_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/}
     \texttt{installableApps/ProxyAppl-8.5.2.ear}
     \texttt{install\_root/SametimeMediaServerOffering/SametimeServer/SMServer/media/}
     \texttt{installableApps/RegistrarAppl-8.5.2.ear}

b. Copy the files to the following location on the Sametime System Console:
   \texttt{WAS\_install\_root/AppServer/profiles/STSCDMgrProfile/config/temp/}

\textbf{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 \texttt{logs} directory and the \texttt{ant} and \texttt{native} subdirectories.

You can use the \texttt{collectLogs} utility to gather the logs; \texttt{collectLogs} is located at the root of the installation media.

\textbf{Linux}

\texttt{/var/ibm/InstallationManager/logs}

\textbf{SSC connection log:}

\texttt{/tmp/SSCLogs/ConsoleUtility0.log}

\textbf{Windows 2008}

\texttt{%ALLUSERSPROFILE}\%IBM\Installation Manager\logs
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.

ODistributing 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 Sametime 8.5 or 8.5.1 Gateway on AIX, Linux, Solaris, or Windows**

Follow the instructions for your operating system to upgrade one or more Sametime Gateway servers running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

**What to do next**

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps
Upgrading a single Sametime 8.5 or 8.5.1 Gateway server on AIX, Linux, Solaris, or Windows:

Upgrade a single, non-clustered IBM Sametime 8.5 Gateway server running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

Upgrading a single, non-clustered Sametime Gateway server requires upgrading the server software, applying IBM WebSphere Application Server iFixes, and registering the upgraded server with the Sametime System Console.

What to do next

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.
• Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Configure LDAP for Sametime Gateway (IBM i)
• Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Connect servers to Sametime Gateway (IBM i)
• Set up SSL
• Other optional configuration steps

Installing WebSphere iFixes before upgrading Sametime Gateway server:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Upgrading the Sametime 8.5 or 8.5.1 Gateway application on AIX, Linux, Solaris, or Windows:

Upgrade the IBM Sametime 8.5 Gateway server application on a computer running IBM AIX, Linux, Sun Solaris, or Microsoft Windows.
About this task

Upgrade cluster components in the following order:
1. 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.

The instructions for upgrading the Gateway application vary according to the server's operating system:

*Upgrading a Sametime 8.5 or 8.5.1 Gateway server on AIX, Linux, or Solaris:*

Upgrade an IBM Sametime 8.5 Gateway server running on IBM AIX, Linux, or Sun Solaris.

**Before you begin**

Before you can upgrade a Sametime Gateway server, the Sametime System Console must be upgraded and running.

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

**About this task**

If you have more than one node deployed on the same computer, repeat this upgrade process for each of the nodes. Each node has its own STgateway* directory entry under the WebSphere installation root directory; each requires an upgrade.

**Procedure**

1. Log in as root on the server to be upgraded.
   **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.

2. If the Sametime Gateway server is running, stop it now: `./stopServer.sh Gateway_server_name -username WAS_admin_username -password WAS_admin_password`

3. If the WebSphere Application Server is running, stop it now: `./stopServer.sh server1 -username WAS_admin_username -password WAS_admin_password`

4. 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.

5. Download the installation package for the Sametime Gateway server.
   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
```


7. From the installation media, copy the WebSphere Application Server installation image for your operating system to `/TMP/WASCD`.

8. Open a command window and navigate to the directory `/TMP/WASCD`.

9. Run the following command to extract the files:

```
gunzip -c part_number.tar.gz | tar -xvf -
```

When you are done extracting the files, you should have the following folder:

`/TMP/WASCD/ifpackage`

Verify that you have WAS and JDK folders inside the `ifpackage` folder.

10. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the temporary directory `/TMP`.

11. Navigate to the `/TMP` directory and extract the following file:

```
unzip part_number.tar
```

This creates the folder `/TMP/SametimeGateway`

12. Navigate to the `/TMP/SametimeGateway` directory and type the following command:

```
install.sh -console
```
Attention: If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:

```
install.sh -console -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

13. Select the language for the installation wizard and click OK.
14. At the Welcome screen, click Next.
15. Read the Software License Agreement and click the appropriate radio button option to accept the terms; then click Next.
16. Select Upgrade a server.
17. On the same screen, review the location of the Sametime Gateway node to upgrade. If the location is correct, click Next.

Note: If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for *.pid file, delete the file, and continue from this step.

18. Important: If you are upgrading the server that contains the Deployment Manager and the Primary Node for a cluster, upgrade the Deployment Manager first to ensure proper functionality.
19. Deployment Manager upgrade only: On the "Cluster configuration" screen, verify that the correct cluster name appears, and then click Next.

Tip: To obtain the cluster name from the Integrated Solutions Console, click Servers > Clusters. The default cluster name is "SametimeGatewayCluster".
20. Verify the DB2 properties; these should not change for an upgrade.

Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

21. Review the installation summary settings and, if necessary, click **Back** to make changes.

22. Click **Install** to begin the installation process (new files are installed during an upgrade). A progress bar is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete.

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`

Upgrading a Sametime 8.5 or 8.5.1 Gateway server on Windows:

Upgrade an IBM Sametime 8.5 Gateway server running on Microsoft Windows.

**Before you begin**

Before you can upgrade a Sametime Gateway server, the Sametime System Console must be upgraded and running.

**About this task**

If you have more than one node deployed on the same computer, repeat this upgrade process for each of the nodes. Each node has its own `STgateway*` directory entry under the WebSphere installation root directory; each requires an upgrade.

**Procedure**

1. Log in as the Windows administrator on the server to be upgraded.

2. If the Sametime Gateway server is running, stop it now: `stopServer.bat Gateway_server_name` -username WAS_admin_username -password WAS_admin_password

3. If the WebSphere Application Server is running, stop it now: `stopServer.bat server1` -username WAS_admin_username -password WAS_admin_password

4. 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.
5. Download the installation package for the Sametime Gateway server.
   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
      ```
   6. Create the temporary file folder \TMP\WASCD.
   7. From the installation media, copy the WebSphere Application Server installation image WAS_part_number.exe to the folder \TMP\WASCD.
   8. Open a command window and navigate to the folder \TMP\WASCD.
   9. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK folders inside the ifpackage folder.
   10. From the installation media, copy the Sametime Gateway installation image part_number.exe to the \TMP folder.
   11. Extract the files in part_number.exe. This step creates the folder \TMP\SametimeGateway.
   12. Navigate to the \TMP\SametimeGateway folder containing the extracted files.
   13. Open a command window and type the following command:
       - For wizard mode: install.bat
       - For console mode: install.bat -console
Attention: If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

```
install.bat -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

14. Select the language for the installation wizard and click **OK**.

The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

15. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed.

16. Select **Upgrade a server**, and then click **Next**.

17. On the same panel, review the location of the Sametime Gateway to upgrade. If the location is correct, click **Next**.

The Sametime Gateway location is the folder that contains Gateway-specific files, not the profile for each Sametime Gateway component. For instance, the Gateway files for the Deployment Manager are usually in the `\WebSphere\STgateway` folder and Gateway files for the Primary Node are usually in the `\WebSphere\STgatewayPrimary` folder.

**Note:** If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for `*.pid` file, delete the file, and continue from this step.

18. **Important:** If you are upgrading the server that contains the Deployment Manager and the Primary Node for a cluster, upgrade the Deployment Manager first to ensure proper functionality.

19. Deployment Manager upgrade only: On the "Cluster configuration" screen, verify that the correct cluster name appears.

**Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is "SametimeGatewayCluster".

20. Verify the DB2 properties; these should not change for an upgrade.

Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

21. Review the installation summary settings and, if necessary, click **Back** to make changes.

22. Click **Install** to begin the installation process (new files are installed during an upgrade).
   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click **Finish**. To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`

Registering an upgraded Sametime Gateway server with the System Console:

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

**Before you begin**

Before you register the server, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.
About this task

Working from the server that you want to connect to the console, follow these steps to update properties files and run the registration utility.

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 the topic in a new browser tab or window so you can keep it open for reference:

- console.properties
- productConfig.properties

Procedure

1. On the Sametime Gateway server, navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.
2. In the console directory, make backup copies (using different names) of the console.properties and productConfig.properties files.
3. Update the console.properties file with the following values, and then save and close the file.

   **Table 136. 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 “false.”</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 path is: 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>SCCPassword</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 137. productConfig.properties settings**

   | InstallType | Specify "Cell" as the installation type since this is a non-clustered server. |
Table 137. productConfig.properties settings (continued)

<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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node.</td>
</tr>
</tbody>
</table>

5. Set the application server path in the registration utility:
   a. Navigate to the `stgw_server_root/IBM/WebSphere/STgateway/console` directory and open a command window.
   b. Open the registration utility file for editing.
      - **AIX, Linux, Solaris**
        registerProduct.sh
      - **Windows**
        registerProduct.bat
   c. Locate the following statement:
      ```
      SET PATH=../../WebSphere/AppServer/java/bin
      ```
   d. Change it to reflect IBM WebSphere Application Server version 7:
      ```
      SET PATH=../../WebSphere/AppServer7/java/bin
      ```
   e. Save and close the file.

6. Run the registration utility.
   - **AIX, Linux, Solaris**
     - Already registered
       registerProduct.sh -upgrade
     - First-time registration
       registerProduct.sh
   - **Windows**
     - Already registered
registerProduct.bat -upgrade

- First-time registration
  registerProduct.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 will also be generated.

7. Start the Sametime Gateway server, if it is not already running.

Upgrading a cluster of Sametime 8.5 or 8.5.1 Gateway servers on AIX, Linux, Solaris, or Windows:

Upgrade a cluster of IBM Sametime 8.5 Gateway 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 Gateway 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, start the cluster, register the upgraded cluster with the Sametime System Console, and then run the clustering guided activity to update configuration information.

Upgrade the Deployment Manager first, followed by the Primary Node and then the Secondary Nodes, making sure to upgrade all nodes in the cluster. If the cluster includes a SIP proxy server or an XMPP server, you will apply WebSphere Application Server fixes to update those servers for use with this release of Sametime Gateway.

What to do next

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

Preparing the Sametime 8.5 or 8.5.1 Gateway cluster for an upgrade on AIX, Linux, Solaris, or Windows:

Before upgrading servers in a cluster of IBM Sametime Gateway 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: Leave the WebSphere Application Server itself running.
a. Stop the Sametime Gateway server:
   AIX, Linux, Solaris: ./stopServer.sh Gateway_server_name -username WAS_admin_username -password WAS_admin_password
   Windows: stopServer.bat Gateway_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. Stop the WebSphere Application Server:
   AIX, Linux, Solaris: ./stopServer.sh server1 -username WAS_admin_username -password WAS_admin_password
   Windows: stopServer.bat server1 -username WAS_admin_username -password WAS_admin_password
e. 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

3. Still on the Deployment Manager computer, stop the WebSphere Application Server:
   AIX, Linux, Solaris: ./stopServer.sh server1 -username WAS_admin_username -password WAS_admin_password
   Windows: stopServer.bat server1 -username WAS_admin_username -password WAS_admin_password

Upgrading a clustered Sametime 8.5 or 8.5.1 Gateway server on AIX, Linux, Solaris, or Windows:

Upgrade a clustered IBM Sametime 8.5 Gateway server running on IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

Upgrading a clustered Sametime Gateway server requires upgrading the server software and applying IBM WebSphere Application Server iFixes. You do not need to register the upgraded server with the Sametime System console because the entire cluster will be registered at once.

Installing WebSphere iFixes before upgrading the Sametime Gateway node:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.
About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Upgrading the Sametime 8.5 or 8.5.1 Gateway node on AIX, Linux, Solaris, or Windows:

Upgrade the IBM Sametime 8.5 Gateway server application on a computer running IBM AIX, Linux, Sun Solaris, or Microsoft Windows.

About this task

Upgrade cluster components in the following order:
1. 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.

The instructions for upgrading the Gateway application vary according to the server’s operating system:

Upgrading a Sametime 8.5 or 8.5.1 Gateway node on AIX, Linux, or Solaris:

Upgrade an IBM Sametime 8.5 Gateway server running on IBM AIX, Linux, or Sun Solaris.

Before you begin

Before you can upgrade a Sametime Gateway server, the Sametime System Console must be upgraded and running.

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

About this task

If you have more than one node deployed on the same computer, repeat this upgrade process for each of the nodes. Each node has its own STgateway* directory entry under the WebSphere installation root directory; each requires an upgrade.
Procedure

1. Log in as root on the server to be upgraded.
   
   **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.

2. If the Sametime Gateway server is running, stop it now: 
   ```bash
   ./stopServer.sh Gateway_server_name -username WAS_admin_username -password WAS_admin_password
   ```

3. If the WebSphere Application Server is running, stop it now: 
   ```bash
   ./stopServer.sh server1 -username WAS_admin_username -password WAS_admin_password
   ```

4. 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.

5. Download the installation package for the Sametime Gateway server.
   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:
         ```url
         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
      ```


7. From the installation media, copy the WebSphere Application Server installation image for your operating system to `/TMP/WASCD`.

8. Open a command window and navigate to the directory `/TMP/WASCD`.

9. Run the following command to extract the files:
   ```bash
   gunzip -c part_number.tar.gz | tar -xvf -
   ```
When you are done extracting the files, you should have the following folder:

/TMP/WASCD/ifpackage

Verify that you have WAS and JDK folders inside the ifpackage folder.

10. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the temporary directory `/TMP`.

11. Navigate to the `/TMP` directory and extract the following file:

   `unzip part_number.tar`

   This creates the folder `/TMP/SametimeGateway`

12. Navigate to the `/TMP/SametimeGateway` directory and type the following command:

   `install.sh -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:

   `install.sh -console -V BypassWasInfoCheck=true`

   Because your input will not be verified during installation, you should take extra care when typing values.

13. Select the language for the installation wizard and click **OK**.

14. At the Welcome screen, click **Next**.

15. Read the Software License Agreement and click the appropriate radio button option to accept the terms; then click **Next**.

16. Select **Upgrade a server**.

17. On the same screen, review the location of the Sametime Gateway node to upgrade. If the location is correct, click **Next**.

   **Note:** If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for *.pid file, delete the file, and continue from this step.

18. **Important:** If you are upgrading the server that contains the Deployment Manager and the Primary Node for a cluster, upgrade the Deployment Manager first to ensure proper functionality.

19. Deployment Manager upgrade only: On the “Cluster configuration” screen, verify that the correct cluster name appears, and then click **Next**.

   **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is “SametimeGatewayCluster”.

20. Verify the DB2 properties; these should not change for an upgrade.

   Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database</td>
</tr>
<tr>
<td></td>
<td>name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

21. Review the installation summary settings and, if necessary, click Back to make changes.

22. Click Install to begin the installation process (new files are installed during an upgrade). A progress bar is displayed and the activity is logged to the Sametime Gateway log file. This installation takes about 10 minutes to complete.

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click Finish. To view the installation log, click View log file or open the log file at stgw_server_root/logs/installlog.txt

**Upgrading a Sametime 8.5 or 8.5.1 Gateway node on Windows:**

Upgrade an IBM Sametime 8.5 Gateway server running on Microsoft Windows.

**Before you begin**

Before you can upgrade a Sametime Gateway server, the Sametime System Console must be upgraded and running.

**About this task**

If you have more than one node deployed on the same computer, repeat this upgrade process for each of the nodes. Each node has its own STgateway* directory entry under the WebSphere installation root directory; each requires an upgrade.
Procedure

1. Log in as the Windows administrator on the server to be upgraded.

2. If the Sametime Gateway server is running, stop it now: stopServer.bat
   Gateway_server_name -username WAS_admin_username -password WAS_admin_password

3. If the WebSphere Application Server is running, stop it now: stopServer.bat
   server1 -username WAS_admin_username -password WAS_admin_password

4. 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.

5. Download the installation package for the Sametime Gateway server.
   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

6. Create the temporary file folder \TMP\WASCD.

7. From the installation media, copy the WebSphere Application Server installation image WAS_part_number.exe to the folder \TMP\WASCD.

8. Open a command window and navigate to the folder \TMP\WASCD.

9. Extract all files to the temporary directory \TMP\WASCD. When you are done extracting the files, you should have a \TMP\WASCD\ifpackage folder with WAS and JDK folders inside the ifpackage folder.

10. From the installation media, copy the Sametime Gateway installation image part_number.exe to the \TMP folder.
11. Extract the files in `part_number.exe`. This step creates the folder \TMP\SametimeGateway.

12. Navigate to the \TMP\SametimeGateway folder containing the extracted files.

13. Open a command window and type the following command:
   - For wizard mode: `install.bat`
   - For console mode: `install.bat -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:

   `install.bat -V BypassWasInfoCheck=true`

   Because your input will not be verified during installation, you should take extra care when typing values.

14. Select the language for the installation wizard and click **OK**.

   The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

15. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click **Next** to proceed.

16. Select **Upgrade a server**, and then click **Next**.

17. On the same panel, review the location of the Sametime Gateway to upgrade. If the location is correct, click **Next**.

   The Sametime Gateway location is the folder that contains Gateway-specific files, not the profile for each Sametime Gateway component. For instance, the Gateway files for the Deployment Manager are usually in the \WebSphere\STgateway folder and Gateway files for the Primary Node are usually in the \WebSphere\STgatewayPrimary folder.

   **Note:** If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for *.pid file, delete the file, and continue from this step.

18. **Important:** If you are upgrading the server that contains the Deployment Manager and the Primary Node for a cluster, upgrade the Deployment Manager first to ensure proper functionality.

19. Deployment Manager upgrade only: On the “Cluster configuration” screen, verify that the correct cluster name appears.

   **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is “SametimeGatewayCluster”.

20. Verify the DB2 properties; these should not change for an upgrade.

    Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

21. Review the installation summary settings and, if necessary, click Back to make changes.

22. Click Install to begin the installation process (new files are installed during an upgrade).

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click Finish. To view the installation log, click View log file or open the log file at stgw_server_root/logs/installlog.txt

Re-installing the Gateway administration portlet on the upgraded deployment manager:

During the Deployment Manager upgrade process, the IBM Sametime Gateway administration portlet is removed and must be manually re-installed. This task is needed only if your configuration includes a Deployment Manager, a SIP proxy server, and an XMPP proxy server installed on the same computer; otherwise, skip this task.

Before you begin

Upgrade the Deployment Manager, the Primary node, the Secondary node, the SIP proxy server, and the XMPP server.
About this task

During the Deployment Manager upgrade process, the Sametime Gateway administration portlet is removed. Complete these steps on the Deployment Manager to re-install the portlet:

Procedure

1. Log in to the Deployment Manager's Integrated Solutions Console as the IBM WebSphere administrator.
2. Open the wsadmin console:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile/bin`.
      where `app_server_root` is the root directory for the creation of WebSphere Application Server profile directories.
   b. Run the `wsadmin` file to open the console:
      - Windows: `wsadmin.bat -conntype NONE`
      - AIX, Linux, Solaris: `./wsadmin.sh -conntype NONE`
3. In the wsadmin console, execute the following commands:
   $AdminApp update isclite modulefile {-operation delete -contenturi RTCAdminPortlet.war}
   $AdminConfig save
   quit
4. Delete the following file/directory: `was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war`
5. Now copy a file to replace the one you just deleted:
   Copy this file from the installation image:
   `../../setup/installableApps/RTCAdminPortlet.war`
   and paste it in:
   `was_install_root/systemApps/isclite.ear/`
6. Open the wsadmin console again:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile/bin`.
   b. Run the `wsadmin` file to open the console:
      - Windows: `wsadmin.bat -conntype NONE`
      - AIX, Linux, Solaris: `./wsadmin.sh -conntype NONE`
7. In the wsadmin console, execute the following commands.
   Note: Type the command as one continuous line.
   $AdminApp update isclite modulefile { -operation add -contents "was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war" -contenturi RTCAdminPortlet.war -usedefaultbindings -server dmgr -preCompileJSPs -contextroot /ibm/RTCGW -MapWebModToVH {{.* .* admin_host}}}
Completing the Sametime Gateway server cluster upgrade on AIX, Linux, Solaris, or Windows:

Complete the upgrade of a cluster of IBM Sametime Gateway servers by starting the cluster and then running a guided activity to update the cluster’s configuration settings.

Before you begin

Upgrade Sametime Gateway on the Deployment Manager and all nodes in the cluster before beginning this task.

Procedure

1. Apply WebSphere Application Server fixes to the cluster’s SIP proxy server as described in Installing WebSphere iFixes for Sametime Gateway.

2. Apply the same set of WebSphere Application Server fixes to the cluster’s XMPP proxy server using the same process as in the previous step (see Installing WebSphere iFixes for Sametime Gateway).

3. On the Deployment Manager computer, start the cluster’s Deployment Manager:
   - AIX, Linux, Solaris: ./startManager.sh dmgr
   - Windows: startManager.bat dmgr

4. 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 Gateway_server_name
      - Windows: startServer.bat Gateway_server_name
   - e. Repeat for every node in the cluster.

Registering an upgraded Sametime Gateway cluster with the System Console:

After upgrading an IBM Sametime Gateway cluster 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

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
The LDAP server must be connected to the System Console and must be started.
The Gateway database must be connected to the System Console and must be started.
The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the cluster's Deployment Manager, Primary Node, and Secondary Nodes, follow these steps to update console.properties and productConfig.properties files. Then run the registration utility on the nodes and the Deployment Manager to register them with the console.

During this task you will edit the following files: click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure

1. On the Deployment Manager, navigate to the $tgw_server_root/IBM/WebSphere/STgateway/console directory.

   **Note**: If a cluster's Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager's profile.

2. Make backup copies (using different names) of the console.properties and productConfig.properties files.
3. Update the Deployment Manager's console.properties file:
   a. Open the file for editing.
   b. Update the file with the following values:

<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 path is: 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>
Table 138. console.properties settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCSSEnabled</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 SSCSSEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

4. Update the Deployment Manager's productConfig.properties file:
   a. Open the file for editing.
   b. Update the file with the following required values.

Table 139. productConfig.properties settings for the Deployment Manager

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;DM&quot; because you are working in the Deployment Manager's profile right now.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

5. On the Primary Node machine, navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
6. Edit the Primary Node's console.properties file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.
Table 140. *console.properties* settings for the Primary Node

<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 SSCSSEnabled 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 path is: 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>SSCSSEnabled</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 SSCSSEnabled is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

7. Edit the Primary Node's *productConfig.properties* file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 141. *productConfig.properties* settings for the Primary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify 'PN' because you are now working in the Primary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 141. `productConfig.properties` settings for the Primary Node (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to <code>true</code> for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>


9. Edit the Secondary Node's `console.properties` file with the following required values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.

Table 142. `console.properties` settings for the Secondary Node

<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 path is: <code>C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</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>

10. Edit the Secondary Node's `productConfig.properties` file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 143. `productConfig.properties` settings for the Secondary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;SN&quot; because you are now working in the Secondary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
</tbody>
</table>
Table 143. productConfig.properties settings for the Secondary Node (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

11. Run the registration utility on the Primary Node.
   a. Log on to the Primary Node machine.
   b. Navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
   c. (AIX, Linux, and Solaris) Edit the registerProduct.sh file to change the
      SET PATH= statement to reflect IBM WebSphere Application Server version 7.
      SET PATH=../../WebSphere/AppServer7/java/bin
      Then save the file.
   d. At a command prompt, run the registration utility.
      AIX, Linux, Solaris
      • Already registered
        registerProduct.sh -upgrade
      • First-time registration
        registerProduct.sh
      Windows
      • Already registered
        registerProduct.bat -upgrade
      • First-time registration
        registerProduct.bat

12. Run the registration utility on the Secondary Node.
   a. Log on to the Secondary Node machine.
   b. Navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
c.  **(AIX, Linux, and Solaris)** Edit the `registerProduct.sh` file to change the
SET PATH= statement to reflect IBM WebSphere Application Server
version 7.

```
SET PATH=../../WebSphere/AppServer7/java/bin
```

Then save the file.

d. At a command prompt, run the registration utility.

**AIX, Linux, Solaris**

- **Already registered**
  
  `registerProduct.sh -upgrade`

- **First-time registration**
  
  `registerProduct.sh`

**Windows**

- **Already registered**
  
  `registerProduct.bat -upgrade`

- **First-time registration**
  
  `registerProduct.bat`

13. Run the registration utility on the Deployment Manager.

  a. Log on to the Deployment Manager machine.

  b. Navigate to the `stgw_server_root/IBM/WebSphere/STgateway/console`
directory.

  c. Run the registration utility.

    **AIX, Linux, Solaris**

    - **Already registered**
      
      `registerProduct.sh -upgradeCluster`

    - **First-time registration**
      
      `registerProduct.sh`

    **Windows**

    - **Already registered**
      
      `registerProduct.bat -upgradeCluster`

    - **First-time registration**
      
      `registerProduct.bat`

  d. When prompted for the cluster's name, type the name you assigned the
     cluster when you created it, and press **Enter**.

14. Start the Sametime Gateway cluster, if it is not already running.

---

**Upgrading Sametime 8.5 or 8.5.1 on IBM i**

Upgrade an IBM Sametime deployment running on IBM i.

**Before you begin**

To help track your progress, print this page and use it as a checklist.

**About this task**

Upgrade the Sametime System Console first, before upgrading the other servers in
a Sametime deployment. 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:

**Upgrading the Sametime 8.5 or 8.5.1 System Console on IBM i**
Upgrade the IBM Sametime System Console running on IBM i by installing the update over the existing product.

**About this task**
Be sure to update the database used by the Sametime System Console before attempting to upgrade the console itself:

**Preparing the console installation file for upgrading on IBM i:**
Follow these steps to customize the `response.properties` file to prepare for installing the Sametime System Console on IBM i.

**Before you begin**
You should have completed the preparation steps in “Preparing to install Sametime on IBM i.”

**About this task**
Skip the first two steps if you are installing from physical media.

**Procedure**
1. Download the installation package if you have not already done so.
   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`
2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      `QSH`
   b. Run the cd shell command, specifying the fully qualified path to the installation package directory; for example:
      `cd /MySametimePackages`
   c. Run the following shell command, specifying the name of the `.zip` file:
      `ajar -x name_of_installation_package`
   d. Press F3 to exit QSH.
3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image; for example:
4. Navigate to the program image directory; for example:

   /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc

   For DVD:
   /qopt/volume_ID/IBMi/stii_ssc

5. Make a copy of the ssc.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
   - For the database.db.user.id and database.db.user.password settings in the properties file, specify the user profile and password you created to be the owner of the Sametime System Console database schemas.
   - Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

**Example**

"Default console installation file for IBM i" on page 645

**Related tasks**

"Preparing to install Sametime on IBM i" on page 642
Follow these steps to prepare IBM i for Sametime server installations.

**Using the default console installation file for upgrading on IBM i:**

The response.properties file contains settings used to install or upgrade a Sametime System Console on IBM i.

The default content for the response.properties file for installing the Sametime System Console follows:

```
# Sametime 8.5.2 System Console Server Installation Properties file for IBM i
#
# Preparing to Install
#
# This file is used for either installing a new Sametime 8.5.2 System Console or
# upgrading a Sametime System Console to Sametime 8.5.2.
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime System Console on IBM i and
# running the installation program.
# The Information Center is available online from the Lotus Sametime documentation
# library:
#
#   http://www.ibm.com/developerworks/lotus/documentation/sametime
```
# License Acceptance
# By changing the silentInstallLicenseAcceptance property in this response file
# to "true", you agree that you have reviewed and agree to the terms of the
# IBM International Program License Agreement accompanying this program, which
# is located at CD_ROOT\IBM\stii_ssc\licenses.
#
# If you do not agree to these terms, do not change the value or otherwise
# download, install, copy, access, or use the program and promptly return the
# program and proof of entitlement to the party from whom you acquired it to
# obtain a refund of the amount you paid.
#
# Valid values for silentInstallLicenseAcceptance:
#   true - Accept the license terms continue with product installation.
#   false - Decline the license terms and do not install the product.
#
silentInstallLicenseAcceptance=false

# Installation Type
# Set this value to the type of installation you wish to perform.
# The setting determines the WAS nodes that are created during installation.
#
# Valid values for install.type:
#   Cell - (default) Cell installation, recommended for new deployments.
#   Creates both a deployment manager node and a primary application
#   server node with the Sametime System Console installed. The primary
#   node is federated into the deployment manager's cell.
#   If the cell installation already exists, both the deployment manager
#   node and the primary application server node are upgraded.
#
# install.type=Cell

# Websphere Settings
# These values are used when configuring the Websphere Application Server nodes.
#
# stwas.was.hostname - (required) For new installs, specify the fully qualified
# hostname that your WAS server will use.
# For upgrades, specify the fully qualified hostname of the existing
# WAS server.
#
# stwas.was.admin.id - (required) For new installs, specify the user ID that
# you will use to log into the Deployment Manager's Integrated
# Solutions Console once security is enabled. This name must not exist
# as a user in any LDAP directory that you plan to connect to the
# server.
# For upgrades, specify the user ID that you use to log into the
# Deployment Manager's Integrated Solutions Console.
#
# stwas.was.admin.password - (required) The password associated with the user ID
# specified for 'stwas.was.admin.id'
#
# stwas.was.hostname=
stwas.was.admin.id=
stwas.was.admin.password=

# STATIC Websphere Settings
# These settings are used by the installer to control how Websphere is configured
# during installation. The values have been set specifically for installing the
# Sametime System Console Server.
Upgrading the Sametime 8.5 or 8.5.1 System Console (IBM i):

Upgrade an IBM Sametime System Console running on IBM i 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.
About this task

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.

Procedure

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   `QSH`

4. Run the following shell command, specifying the fully qualified path to the installation kit directory; for example:
   
   `/MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc`

   For installing from DVD:
   
   `cd /qopt/volume_ID/IBMi/stii_ssc`

5. Start the Sametime System Console installation with the following shell command:
   
   `install_ssc.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file`

   When the script completes, a summary of the results is displayed. Make a note of the URL for connecting to the Integrated Solutions Console. The "Admin port" displayed is the port you must use when logging in to the system console.

6. Press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location:

`/QIBM/UserData/Lotus/stii/logs`

The log name contains the date and time in this form:

`install_STCONSOLE_yyyymmdd_hhmm.log`

For example, this log was created at 3:07 A.M. on December 15, 2009:

`install_STCONSOLE_20091215_0307.log`

Upgrading a Sametime 8.5 or 8.5.1 Community Server on IBM i

Upgrade one or more IBM Sametime Community Servers running on IBM i.

Upgrading a single Sametime 8.5 or 8.5.1 Community Server on IBM i:
Upgrade a single, non-clustered IBM Sametime Community Server running on IBM i.

**Related tasks**

“Disabling or enabling meetings on an IBM i Sametime Standard server” on page 744

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

**Verifying the system host name on IBM i:**

During the IBM Sametime Community Server startup, Sametime attempts to resolve the main system host name in addition to the Sametime server host name. The upgraded server will not start if Sametime cannot resolve the system host name to an IP address. Prior to Sametime 8.5, only the host name for the Sametime server was checked.

**About this task**

Verify that either the local IBM i host table (CFGTCP, option 10) or the DNS contain a fully qualified host name for the system and that the host name resolves to the correct IP address. If necessary, update the local IBM i host table or the DNS.

**Checking supported releases of Lotus Domino and Sametime on IBM i:**

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 on IBM i:**

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 144. 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>
</tbody>
</table>
Table 144. Sametime server data to back up (continued)

<table>
<thead>
<tr>
<th>Data to back up</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<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 STprevious_versionBU. 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>
<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>

Pre-accepting the Sametime software agreements for an upgrade on IBM i:

If you do not pre-accept the IBM Sametime software agreements, the installation process will restore the product to the system, but then stop and wait for you to accept the agreements before completing the installation. Skip this step if you are installing from a downloaded image.

Procedure
1. Insert the Sametime DVD into the optical drive of your system.
2. Enter the following command on an IBM i command line:
   ```
   GO LICPGM
   ```
   The Work with Licensed Programs display appears.
3. From the Work with Licensed Programs (LICPGM) menu, select option 5 (Prepare for install) and press Enter. The Prepare for Install display appears.
4. Type 1 in the option field next to Work with software agreements. Press Enter.
   When the Work with Software Agreements display appears, you see all IBM licensed programs that require software agreement acceptance and whether the agreement has been accepted. Only licensed programs that are not yet installed appear on this display. The software agreements for Sametime will not appear in the list until you restore them from the DVD in a later step.
5. Press F22 (shift-F10) to restore the Software Agreements from the Sametime DVD.
   For the Device parameter, specify the name of your optical drive (For example, OPT01). Press Enter to restore the Sametime software agreements to the system.
6. If you are installing from physical media (not virtual optical media), the following message is displayed after the Software agreements are restored:
   Waiting for reply to message on message queue QSYSOPR.
You can sign on to another session to respond to the message or ask the system operator to respond.

To view and respond to the message from another session:

a. Enter the following command on an IBM i command line:
   WRKMSGQ QSYSOPR

b. Select option 5 to display the messages in the QSYSOPR message queue.

c. Locate the following message in the queue:
   Load the next volume in optical device OPT01. (X G)

d. The Sametime software agreements have already been restored. If you want to restore more software agreements from another DVD, insert the next DVD and respond with G. When the software agreements have been restored, the message is issued again. When you are done, respond to the message with X.

7. The Work with software agreements display now shows the restored licenses for products that are not yet installed.
   • If you are using the DVD for the Entry version of Sametime, you will see an entry for Licensed Program 5724J23, option *BASE.
   • If you are using the DVD for Sametime Standard, you will see two entries for Licensed Program 5724J23: one entry for *BASE and another entry for Option 1.

8. For each entry for Licensed Program 5724J23, type 5 in the option field and press Enter to display the Software Agreement. Then press F14 (Accept) to accept the terms of the software agreement.

   Note: In some unusual situations, the following message may be issued when you attempt to display the Software Agreement:

   CPDB6D6 - Software agreement documents are missing. If this occurs, repeat step 5 to restore the Software Agreements again and continue with the remaining steps in this procedure.

Running the upgrade on the 8.5 or 8.5.1 Community Server on IBM i:

Upgrade an IBM Sametime 8.5 Community Server running on IBM i by installing the new release over the existing product.

Before you begin

Before you can upgrade a Sametime Community Server, the Sametime System Console must be upgraded and running.

About this task

Use the IBM i command line to install the community server programs.

Procedure

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.

2. From the IBM i command line, run the appropriate command for installing from a downloaded image or physical media.

   Installing from a downloaded image
a. Use the RSTLCPGM command to install from the save files you created when you downloaded the installation package.

This example uses the save files MYLIB/Q5724J23IM and MYLIB/Q5724J23WC.
(For Sametime Entry, the second RSTLCPGM command is not needed.)

RSTLCPGM LICPGM(5724J23) DEV(*SAVF) OPTION(*BASE) LNG(2924) SAVF(MYLIB/Q5724J23IM)
RSTLCPGM LICPGM(5724J23) DEV(*SAVF) OPTION(1) SAVF(MYLIB/Q5724J23WC)

b. When you are prompted to accept the Sametime software agreement, you must accept it in order to continue.

Installing from physical media

Insert the Sametime disk in your system optical drive and run the RSTLCPGM command, specifying the correct name of the optical device. (For Sametime Entry, the second RSTLCPGM command is not needed.)

RSTLCPGM LICPGM(5724J23) DEV(OPT01) OPTION(*BASE) LNG(2924)
RSTLCPGM LICPGM(5724J23) DEV(OPT01) OPTION(1)

The system loads the Sametime programs to the appropriate libraries and /QIBM directories. You will see status messages as the system installs the software.

Updating registration of an IBM i Sametime server with the Sametime System Console:

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

Before you begin

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server’s registration information, verify that you have completed the following tasks.

**Sametime Community Server**
- The community server must already be registered with the Sametime System Console.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.

**Sametime Proxy Server**
- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

**Sametime Meeting Server**
- The meeting server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The LDAP server must be started.
About this task

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server's registration information with the console.

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

- console.properties
- productConfig.properties

Procedure

1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.
   - Community Server
     The console directory is a subdirectory of the Sametime Community server data directory.
   - Proxy Server
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.
   - Meeting Server
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.

3. Verify the following values in the console.properties file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.

Table 145. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
</tbody>
</table>
### Table 145. `console.properties` settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. Now update the `productConfig.properties` file with the values needed for the server you are updating. Then save and close the file.

   Required values not listed below are filled in automatically.

   - **Sametime Community Server**
     - The information from the original registration should already be in the file. If the **DepName** is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

   - **Sametime Proxy Server**
     - **WASPassword**: Specify the password associated with the WASUserID.

   - **Sametime Meeting Server**
     - **DBAppPassword**: Specify the password associated with the database ID.
     - **WASPassword**: Specify the password associated with the WASUserID.
     - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server.

   Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   QSH

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   - **Sametime Community Server**
     - `registerSTServerNode.sh -upgrade`

   - **Other servers**
     - `registerProduct.sh -upgrade`

9. When the registration script completes, press F3 to exit QSH.

**Related tasks**

“Upgrading policies from Release 8.5 or 8.5.1” on page 1219

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.

Disabling or enabling meetings on a Sametime Community server after upgrading on IBM i:

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

**About this task**

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.

Follow these steps to use the CHGLSTDOM command to disable meetings on a particular server.

**Procedure**

1. On any IBM i command line, type the following and press F4:
   
   CHGLSTDOM

2. On the Change Sametime on Domino display, set Web Conferencing to *NO and press Enter.

**What to do next**

If you decide to enable Web Conferencing on the server later, run the CHGLSTDOM command again, specifying *YES for Web Conferencing.

**Related concepts**

“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 127

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.

**Related tasks**

“Running the community server installation program on IBM i” on page 680

Run the installation program on the machine where you plan to install a Sametime Community Server.

**Upgrading a Sametime 8.5 or 8.5.1 Community Server cluster on IBM i:**

Upgrade a cluster of IBM Lotus 8.5 Sametime Community Servers running on IBM i.

**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 IBM i:**
Upgrade a single, non-clustered IBM Sametime Community Server running on IBM i.

Related tasks

“Disabling or enabling meetings on an IBM i Sametime Standard server” on page 744
Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

Verifying the system host name for the clustered Community Server:

During the IBM Sametime Community Server startup, Sametime attempts to resolve the main system host name in addition to the Sametime server host name. The upgraded server will not start if Sametime cannot resolve the system host name to an IP address. Prior to Sametime 8.5, only the host name for the Sametime server was checked.

About this task

Verify that either the local IBM i host table (CFGTCP, option 10) or the DNS contain a fully qualified host name for the system and that the host name resolves to the correct IP address. If necessary, update the local IBM i host table or the DNS.

Checking supported releases of Lotus Domino and Sametime on the clustered Community Server:

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 for the clustered Community Server:**

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 146. 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>
</tbody>
</table>
Table 146. Sametime server data to back up (continued)

<table>
<thead>
<tr>
<th>Data to back up</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<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 $\text{STprevious_versionBU}$. For example, the subdirectory name is $\text{ST751BU}$ if you upgraded from Sametime 7.5.1, and $\text{ST80BU}$ 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>(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>meetingserver.ini</td>
<td>(Sametime Standard only)</td>
</tr>
<tr>
<td>All recorded meeting files (.rap)</td>
<td>(Sametime Standard only)</td>
</tr>
</tbody>
</table>

Pre-accepting the Sametime software agreements on IBM i on the clustered Community Server:

If you do not pre-accept the IBM Sametime software agreements, the installation process will restore the product to the system, but then stop and wait for you to accept the agreements before completing the installation. Skip this step if you are installing from a downloaded image.

Procedure

1. Insert the Sametime DVD into the optical drive of your system.
2. Enter the following command on an IBM i command line:
   
   `GO LICPGM`  
   
   The Work with Licensed Programs display appears.
3. From the Work with Licensed Programs (LICPGM) menu, select option 5 (Prepare for install) and press Enter. The Prepare for Install display appears.
4. Type 1 in the option field next to Work with software agreements. Press Enter. When the Work with Software Agreements display appears, you see all IBM licensed programs that require software agreement acceptance and whether the agreement has been accepted. Only licensed programs that are not yet installed appear on this display. The software agreements for Sametime will not appear in the list until you restore them from the DVD in a later step.
5. Press F22 (shift-F10) to restore the Software Agreements from the Sametime DVD.
   
   For the Device parameter, specify the name of your optical drive (For example, OPT01). Press Enter to restore the Sametime software agreements to the system.
6. If you are installing from physical media (not virtual optical media), the following message is displayed after the Software agreements are restored:
   
   Waiting for reply to message on message queue QSYSOPR

Chapter 4. Migrating and upgrading 1161
You can sign on to another session to respond to the message or ask the system operator to respond.

To view and respond to the message from another session:

a. Enter the following command on an IBM i command line:
   WRKMSGQ QSYSOPR

b. Select option 5 to display the messages in the QSYSOPR message queue.

c. Locate the following message in the queue:
   Load the next volume in optical device OPT01. (X G)

d. The Sametime software agreements have already been restored. If you want to restore more software agreements from another DVD, insert the next DVD and respond with G. When the software agreements have been restored, the message is issued again. When you are done, respond to the message with X.

7. The Work with software agreements display now shows the restored licenses for products that are not yet installed.
   • If you are using the DVD for the Entry version of Sametime, you will see an entry for Licensed Program 5724J23, option *BASE.
   • If you are using the DVD for Sametime Standard, you will see two entries for Licensed Program 5724J23: one entry for *BASE and another entry for Option 1.

8. For each entry for Licensed Program 5724J23, type 5 in the option field and press Enter to display the Software Agreement. Then press F14 (Accept) to accept the terms of the software agreement.

   Note: In some unusual situations, the following message may be issued when you attempt to display the Software Agreement:

   CPDB6D6 - Software agreement documents are missing. If this occurs, repeat step 5 to restore the Software Agreements again and continue with the remaining steps in this procedure.

Running the upgrade on the clustered Sametime 8.5 or 8.5.1 Community Server on IBM i:

Upgrade an IBM Sametime 8.5 Community Server running on IBM i by installing the new release over the existing product.

Before you begin

Before you can upgrade a Sametime Community Server, the Sametime System Console must be upgraded and running.

About this task

Use the IBM i command line to install the community server programs.

Procedure

1. Log in to the server using a profile with *ALLOBJ and *SECAADM special authorities.

2. From the IBM i command line, run the appropriate command for installing from a downloaded image or physical media.

   Installing from a downloaded image
a. Use the RSTLCPGM command to install from the save files you created when you downloaded the installation package.
   This example uses the save files MYLIB/Q5724J23IM and MYLIB/Q5724J23WC. (For Sametime Entry, the second RSTLCPGM command is not needed.)
   RSTLCPGM LICPGM(5724J23) DEV(*SAVF) OPTION(*BASE) LNG(2924) SAVF(MYLIB/Q5724J23IM)
   RSTLCPGM LICPGM(5724J23) DEV(*SAVF) OPTION(1) SAVF(MYLIB/Q5724J23WC)

b. When you are prompted to accept the Sametime software agreement, you must accept it in order to continue.

**Installing from physical media**

Insert the Sametime disk in your system optical drive and run the RSTLCPGM command, specifying the correct name of the optical device. (For Sametime Entry, the second RSTLCPGM command is not needed.)

RSTLCPGM LICPGM(5724J23) DEV(OPT01) OPTION(+BASE) LNG(2924)
RSTLCPGM LICPGM(5724J23) DEV(OPT01) OPTION(1)

The system loads the Sametime programs to the appropriate libraries and /QIBM directories. You will see status messages as the system installs the software.

**Updating registration of a clustered IBM i Sametime server with the Sametime System Console after upgrading:**

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

**Before you begin**

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server’s registration information, verify that you have completed the following tasks.

**Sametime Community Server**

- The community server must already be registered with the Sametime System Console.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.

**Sametime Proxy Server**

- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

**Sametime Meeting Server**

- The meeting server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
• The LDAP server must be started.

About this task

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server's registration information with the console.

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

- console.properties
- productConfig.properties

Procedure

1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.
   - **Community Server**
     The console directory is a subdirectory of the Sametime Community server data directory.
   - **Proxy Server**
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.
   - **Meeting Server**
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.

3. Verify the following values in the console.properties file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.

<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 SSCSSEnabled 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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/WebSphere/AppServer/V7/SametimeWAS/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>
</tbody>
</table>
Table 147. console.properties settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 “true.”</td>
</tr>
</tbody>
</table>

4. Now update the productConfig.properties file with the values needed for the server you are updating. Then save and close the file. Required values not listed below are filled in automatically.

- **Sametime Community Server**
  - The information from the original registration should already be in the file. If the **DepName** is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

- **Sametime Proxy Server**
  - **WASPassword**: Specify the password associated with the WASUserID.

- **Sametime Meeting Server**
  - **DBAppPassword**: Specify the password associated with the database ID.
  - **WASPassword**: Specify the password associated with the WASUserID.
  - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server. Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH

7. Run the cd shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:
   - **Sametime Community Server**
     - registerSTServerNode.sh -upgrade
   - **Other servers**
     - registerProduct.sh -upgrade

9. When the registration script completes, press F3 to exit QSH.

**Related tasks**

“Upgrading policies from Release 8.5 or 8.5.1” on page 1219

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.

*Disabling or enabling meetings on a clustered Sametime Community server after upgrading on IBM i:*

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

**About this task**

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.

Follow these steps to use the CHGLSTDOM command to disable meetings on a particular server.

Procedure
1. On any IBM i command line, type the following and press F4:
   CHGLSTDOM
2. On the Change Sametime on Domino display, set Web Conferencing to *NO and press Enter.

What to do next

If you decide to enable Web Conferencing on the server later, run the CHGLSTDOM command again, specifying *YES for Web Conferencing.

Related concepts
“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 127
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.

Related tasks
“Running the community server installation program on IBM i” on page 680
Run the installation program on the machine where you plan to install a Sametime Community Server.

Updating registration of a Community Server cluster on IBM i with the System Console:

After upgrading a cluster of IBM Sametime Community servers on IBM i that was previously registered with the Sametime System Console, update the registration information on the console.

Before you begin

Make sure of each these servers is ready for the cluster registration task:
• The cluster is already registered with the Sametime System Console.
If you have never registered the cluster with the Sametime System Console, follow the instructions in Registering a Community Server cluster on IBM i instead.

- Each of the upgraded Sametime Community Servers in the cluster has been registered with the Sametime System Console and the registration information has been updated since the servers were upgraded.

For information about updating individual servers, see Updating registration of an IBM i Sametime server with the Sametime System Console.

- Each of the upgraded Sametime Community Servers in the cluster 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

Follow these steps to run the registerSTCluster.sh registration utility from one of the servers in the cluster.

Procedure

1. From an IBM i command line, run the following command to start the QShell Interpreter:

   `QSH`

2. Navigate to the server's `sametime_server_data_directory/console` directory; for example: `cd /stserver/data/console`.

3. Run the shell script using the following command:

   `registerSTCluster.sh -upgradeCluster`

4. 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>Type the full path to the Sametime Community Server data directory containing notes.ini file (for example, <code>/stserver/data</code>), and press Enter.</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>

5. When the registration script completes, press F3 to exit QSH.

   The utility registers the cluster, generating a log file called `ConsoleUtility.log` and storing it in the `consoles/logs` directory.

6. Restart the Sametime Community Server where you ran the registration utility.

Upgrading a stand-alone Sametime Community Mux from Sametime 8.0.x or 7.5.1:
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_BYTES_SENT=0

   Close and save the file, then restart the server.

**Upgrading a stand-alone Conversion Server from Sametime 8.0.x or 7.5.1:**

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 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 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 8.5 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 Sametime 8.5 or 8.5.1 Proxy Server on IBM i

Follow the instructions for your operating system to upgrade one or more Sametime Proxy Servers running on IBM i.

Upgrading a single Sametime 8.5 or 8.5.1 Proxy Server on IBM i:

Upgrade a single, non-clustered IBM Sametime Proxy Server running on IBM i.

Before you begin

Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

About this task

Upgrading a single, non-clustered Sametime Proxy Server involves preparing a response file and then upgrading the server software.

Preparing the Sametime Proxy Server installation file for upgrading on IBM i:

Follow these steps to customize the response.properties file to prepare for installing the Sametime Proxy Server on IBM i.

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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

2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:
cd /MySametimePackages

c. Run the following shell command, specifying the name of the .zip file:
   
   ajar -x name_of_installation_package

d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:
   
   /MySametimePackages/SametimeProxyServer/IBMi/stii_stp/licenses

   For DVD:
   
   /qopt/volume_id/IBMi/stii_stp/licenses

4. Navigate to the program image directory; for example:
   
   /MySametimePackages/SametimeProxyServer/IBMi/stii_stp

   For DVD:
   
   /qopt/volume_id/IBMi/stii_stp

5. Make a copy of the stp.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     
     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.
   
   - Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

   There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Meeting Server. This is necessary for live names to work correctly in meeting rooms.

Example

“Default Sametime Proxy Server installation file on IBM i” on page 748

Using the default Sametime Proxy Server installation file for upgrading on IBM i:

The response.properties file contains settings used to install or upgrade a Sametime Proxy Server on IBM i.

The default content for the response.properties file for installing the Sametime Proxy Server follows:

```
# Sametime 8.5.2 Proxy Server Installation Properties file for IBM i
#
# Preparing to Install
```

Chapter 4. Migrating and upgrading  1171
# This file is used for either installing a new Sametime 8.5.2 Proxy Server or
# upgrading a Sametime Proxy Server to Sametime 8.5.2.
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime Proxy Server on IBM i and
# running the installation program.
#
# The Information Center is available online from the Lotus Sametime documentation library:
#
#   http://www.ibm.com/developerworks/lotus/documentation/sametime
#
# License Acceptance
#
# By changing the silentInstallLicenseAcceptance property in this response file
# to "true", you agree that you have reviewed and agree to the terms of the
# IBM International Program License Agreement accompanying this program, which
# is located at CD_ROOT\IBM\stii_stp\licenses.
#
# If you do not agree to these terms, do not change the value or otherwise
# download, install, copy, access, or use the program and promptly return the
# program and proof of entitlement to the party from whom you acquired it to
# obtain a refund of the amount you paid.
#
# Valid values for silentInstallLicenseAcceptance:
#   true - Accept the license terms continue with product installation.
#   false - Decline the license terms and do not install the product.
#
# silentInstallLicenseAcceptance=false
#
# Installation Type
#
# Set this value to the type of installation you wish to perform.
# The setting determines the WAS nodes that are created during installation.
#
# Valid values for install.type:
#   Cell - (default) Cell installation, recommended for new deployments.
#      Creates both a deployment manager node and a primary application
#      server node with the Sametime Proxy Server installed. The primary
#      node is federated into the deployment manager's cell.
#      If the cell installation already exists, both the deployment manager
#      node and the primary application server node are upgraded. Secondary
#      nodes must be upgraded separately.
#   PN - Primary Node installation.
#      Creates a primary application server node with the Sametime Proxy
#      Server installed or upgrades an existing primary application server
#      node to Sametime 8.5.2.
#      For new installations, the primary node must be federated into the
#      Deployment Manager's cell when registering the node with the
#      Sametime System Console.
#   SN - Secondary Node installation.
#      Creates a secondary application server node with the Sametime Proxy
#      Server installed or upgrades an existing secondary application server
#      node to Sametime 8.5.2.
#      For new installations, the node is federated into the Deployment
#      Manager's cell specified by the Secondary Node Properties (later in
#      this file). After installation, this node may be clustered with the
#      primary node in the cell.
#      When upgrading a secondary node, the node's federation and clustering
#      status is not changed.
#
# install.type=Cell
# Websphere Settings

These values are used when configuring the Websphere Application Server nodes.

- **stwas.was.hostname** - (required) For new installs, specify the fully qualified hostname that your WAS server will use. For upgrades, specify the fully qualified hostname of the existing WAS server.
- **stwas.was.admin.id** - (required) For new installs, specify the user ID that you will use to log into the Deployment Manager's Integrated Solutions Console once security is enabled. This name must not exist as a user in any LDAP directory that you plan to connect to the server. For upgrades, specify the user ID that you use to log into the Deployment Manager's Integrated Solutions Console.
- **stwas.was.admin.password** - (required) The password associated with the user ID specified for 'stwas.was.admin.id'

---

# Secondary Node Settings

These settings are used only for Secondary Node installations (SN). For new installations, the settings specify the cell that the secondary node should be federated into. For upgrades, the settings specify the cell that the existing secondary node is already federated into. The Deployment Manager for the cell must be started before running a secondary node install or upgrade.

- **stwas.sn.dm.hostname** - (required for 'SN' install) The fully qualified hostname of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade). The Deployment Manager must be running and listening on this hostname or the install will fail.
- **stwas.sn.dm.soap.port** - (required for 'SN' install) The soap port of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade). Deployment Manager must be running and listening for SOAP connections on this port or the install will fail.

---

# STATIC Websphere Settings

These settings are used by the installer to control how Websphere is configured during installation. The values have been set specifically for installing the Sametime Proxy Server. DO NOT CHANGE this settings unless instructed to do so by IBM Support.

### DO NOT CHANGE ###

- **stwas.was.installlocation**
- **stwas.was.profilelocation**
- **stwas.was.dmprofile.default**
- **stwas.was.serverprofile.default**
- **stwas.was.snsprofile.default**

---

Chapter 4. Migrating and upgrading 1173
stwas.was.appserver=STProxyServer
### DO NOT CHANGE ###

# Sametime Community Server Information

# These settings are used for new installs to specify the Sametime Community Server that the Proxy Server will connect to.
# The settings in this section are not used for upgrade installations.

# stp.sametime.community.server.hostname - (required) The fully qualified host name of the Sametime Community Server
# stp.sametime.community.server.hostname=

# stp.sametime.community.server.port - (required) The server-to-server connection port of the Sametime Community Server
# stp.sametime.community.server.port=1516

#
### End of File ###

Upgrading a Sametime 8.5 or 8.5.1 Proxy Server on IBM i:

Upgrade an IBM Sametime Proxy Server running on IBM i.

**Before you begin**

Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

**Upgrading Cell deployment**

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

**Upgrading Primary or Secondary Nodes**

Make sure the Deployment Manager for the node has been upgraded and is running. This is required to successfully upgrade the node.

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation, except the Deployment Manager for the node. The Deployment manager must be running even if it resides on the same system as the node and shares the same WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

**Procedure**

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:

   QSH
4. Run the cd shell command to change directories, specifying the fully qualified path to the installation kit directory; for example:
   
   cd /MySametimePackages/SametimeProxyServer/IBMi/stii_stp

   For DVD:
   
   cd /qopt/volume_ID/IBMi/stii_stp

5. Start the installation with the following shell command:
   
   install_stp.sh
   
   -Dinstall.response.file=path_and_name_of_customized_response.properties_file

6. When the installation completes, press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STPROXY_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STPROXY_20091215_0307.log

Note: If the primary node and secondary node share the same WebSphere Application Server installation with the Deployment Manager, the log from the primary node and secondary node upgrade may contain error CWUPI0049E. This error occurs if the node upgrade attempts to install WebSphere Application Server fixes when a server is running. It indicates that the WebSphere Application Server installation is not fully up-to-date. Check the logs from the Deployment Manager upgrade to determine if a problem occurred when installing the WebSphere Application Server fixes. Correct the problem and re-run the Deployment Manager upgrade. If this was the only error, it is not necessary to re-run the node upgrade.

Updating registration of an IBM i Sametime Proxy Server with the Sametime System Console after upgrading:

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

Before you begin

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server’s registration information, verify that you have completed the following tasks.

Sametime Community Server
The community server must already be registered with the Sametime System Console.

The community server must be started.

The Sametime System Console must be started.

The LDAP server must be started.

**Sametime Proxy Server**

- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

**Sametime Meeting Server**

- The meeting server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The LDAP server must be started.

**About this task**

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server's registration information with the console.

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

- console.properties
- productConfig.properties

**Procedure**

1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.
   - **Community Server**
     The console directory is a subdirectory of the Sametime Community server data directory.
   - **Proxy Server**
     
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.
   - **Meeting Server**
     
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.

3. Verify the following values in the console.properties file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.
Table 148. `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 “false.”</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 “HTTP transport port.” The default profile name is STSCAppProfile.</td>
</tr>
<tr>
<td></td>
<td>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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 “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 “true.”</td>
</tr>
</tbody>
</table>

4. Now update the `productConfig.properties` file with the values needed for the server you are updating. Then save and close the file.

   Required values not listed below are filled in automatically.

   • Sametime Community Server
     – The information from the original registration should already be in the file. If the DepName is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

   • Sametime Proxy Server
     – WASPassword: Specify the password associated with the WASUserID.

   • Sametime Meeting Server
     – DBAppPassword: Specify the password associated with the database ID.
     – WASPassword: Specify the password associated with the WASUserID.
     – LDAPBindPwd: Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server.
   Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   QSH

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   • Sametime Community Server
     registerSTServerNode.sh -upgrade

   • Other servers
registerProduct.sh -upgrade

9. When the registration script completes, press F3 to exit QSH.

Related tasks
“Upgrading policies from Release 8.5 or 8.5.1” on page 1219
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.

Upgrading a cluster of Sametime 8.5 or 8.5.1 Proxy Servers on IBM i:

Upgrade a cluster of IBM Sametime 8.5 Proxy Servers running on IBM i.

About this task
Upgrading a cluster of Sametime Proxy Servers requires you to upgrade the Deployment Manager and all nodes, then update the configuration information in the Sametime System Console. The Sametime System Console must be upgraded first, before upgrading the other servers in a Sametime deployment.

Upgrading the Sametime 8.5 or 8.5.1 Proxy Server application on IBM i:

Upgrade the IBM Sametime 8.5 or 8.5.1 Proxy Server application on a computer running IBM i.

About this task
The Sametime System Console must be upgraded first, before upgrading the other servers in a Sametime deployment. Upgrade the Proxy Server cluster components in the following order:
1. Deployment Manager (Sametime System Console or Proxy Cell deployment)
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.

The instructions for upgrading the Proxy Server application vary according to the server’s operating system:

Upgrading a Sametime 8.5 or 8.5.1 Proxy Server node on IBM i:

Upgrade an IBM Sametime Proxy Server running on IBM i.

Before you begin
Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

Upgrading Cell deployment
Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

Upgrading Primary or Secondary Nodes
Make sure the Deployment Manager for the node has been upgraded and is running. This is required to successfully upgrade the node.

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation, except the Deployment Manager for the node. The Deployment manager must be running even if it resides on the same system as the node and shares the same WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

**Procedure**

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   ```
   QSH
   ```
4. Run the cd shell command to change directories, specifying the fully qualified path to the installation kit directory; for example:
   ```
   cd /MySametimePackages/SametimeProxyServer/IBMi/stii_stp
   ```
   For DVD:
   ```
   cd /qopt/volume_ID/IBMi/stii_stp
   ```
5. Start the installation with the following shell command:
   ```
   install_stp.sh
   ```
   -Dinstall.response.file=path_and_name_of_customized_response.properties_file
6. When the installation completes, press F3 to exit QSH.

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

```
/QIBM/UserData/Lotus/stii/logs
```

The log name contains the date and time in this form:

```
install_STPROXY_yyyymmdd_hhmm.log
```

For example, this log was created at 3:07 A.M. on December 15, 2009:

```
install_STPROXY_20091215_0307.log
```

**Note:** If the primary node and secondary node share the same WebSphere Application Server installation with the Deployment Manager, the log from the primary node and secondary node upgrade may contain error CWUPI0049E. This error occurs if the node upgrade attempts to install WebSphere Application Server fixes when a server is running. It indicates that the WebSphere Application Server installation is not fully up-to-date. Check the logs from the Deployment Manager upgrade to determine if a problem occurred when installing the WebSphere
Application Server fixes. Correct the problem and re-run the Deployment Manager upgrade. If this was the only error, it is not necessary to re-run the node upgrade.

*Updating registration of an IBM i Sametime Proxy Server node with the Sametime System Console after upgrading:*

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

**Before you begin**

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server's registration information, verify that you have completed the following tasks.

**Sametime Community Server**

- The community server must already be registered with the Sametime System Console.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.

**Sametime Proxy Server**

- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

**Sametime Meeting Server**

- The meeting server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The LDAP server must be started.

**About this task**

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server's registration information with the console.

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

- console.properties
- productConfig.properties
Procedure

1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.

   - **Community Server**
     The console directory is a subdirectory of the Sametime Community server data directory.

   - **Proxy Server**
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.

   - **Meeting Server**
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.

3. Verify the following values in the console.properties file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.

   **Table 149. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>SSCPPassword</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. Now update the productConfig.properties file with the values needed for the server you are updating. Then save and close the file.

Required values not listed below are filled in automatically.

   - **Sametime Community Server**
- The information from the original registration should already be in the file. If the **DepName** is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

- **Sametime Proxy Server**
  - **WASPassword**: Specify the password associated with the WASUserID.

- **Sametime Meeting Server**
  - **DBAppPassword**: Specify the password associated with the database ID.
  - **WASPassword**: Specify the password associated with the WASUserID.
  - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server. Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```
   QSH
   ```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   - **Sametime Community Server**
     ```
     registerSTServerNode.sh -upgrade
     ```

   - **Other servers**
     ```
     registerProduct.sh -upgrade
     ```

9. When the registration script completes, press **F3** to exit QSH.

**Related tasks**

“Upgrading policies from Release 8.5 or 8.5.1” on page 1219

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.

**Ensuring connections between the Proxy Server and the Community Server:**

Add the IBM Sametime Proxy server's IP address to the Deployment Manager's `stproxyconfig.xml` file to ensure that the Sametime Community Server accepts connections.

**About this task**

If the Sametime Proxy server is installed on a computer with multiple active IP addresses, you must add each Sametime Proxy Server's IP address to the Deployment Manager's `stproxyconfig.xml` file to ensure that the server is recognized by the Sametime Community Servers in the deployment; otherwise the Community Servers may reject connections from the Proxy Servers.

**Procedure**

1. Add the Proxy Server's IP address to the `stproxyconfig.xml` file used by the cluster's Deployment Manager:
   a. On the Deployment Manager, locate the `stproxyconfig.xml` file, stored in the following directory:

      ```
      /qibm/UserData/WebSphere/AppServer/v7/SametimeWAS/profiles/StPDMgrProfile/config/cells/ProxyCell_Name/nodes/Proxy_Node_Name/servers/STProxyServer
      ```
b. Edit the file and add a localip setting with the IP address that corresponds to
the host name of the current Proxy Server:
For example:
<configuration>
  <server>
    <host>stcommunityserver.example.com</host>
    <port>1516</port>
    <clusterlist />
    <maxconnections>-1</maxconnections>
    <localip>192.0.2.0</localip>
  </server>
</configuration>
c. Save and close the file.
d. Restart the Proxy Server.

2. Repeat Step 1 for every Sametime Proxy Server in the cluster.

3. Synchronize the nodes in the cluster with the Deployment Manager:
   a. Log in to the Deployment Manager's Integrated Solutions Console as the
      WebSphere administrator.
   b. Click System Administration > Nodes.
   c. Select every node in the cluster.
   d. Click Full Resynchronize.

Starting servers in the upgraded Sametime Proxy Server cluster on IBM i:

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. Update the
registration of all upgraded IBM i Sametime servers if they were previously
registered with the Sametime System Console.

Procedure
1. On the server hosting the Deployment Manager, start QSH, navigate to the
   Deployment Manager profile's /bin directory (app_server_root/profiles/
   profile_name/bin) and start the cluster's Deployment Manager:
   startManager dmgr
2. On each node in the cluster, start QSH, navigate to the node profile's /bin
directory and start the following servers:
   a. WebSphere Application Server should already be running, but if it is not,
      start it now:
      startServer server1
   b. Start the node agent:
      startNode
   c. If a WebSphere proxy server is hosted on this node, start it now:
      startServer WAS_proxy_server_name
   d. Start the Sametime Proxy Server:
      startServer STProxy_Server_name
   e. Repeat for every node in the cluster.

Updating registration of a Sametime Proxy Server cluster on IBM i:
After all of the nodes in a cluster have been upgraded, run the registration utility to update the cluster's configuration information on the IBM Sametime System Console.

**Before you begin**

Before you update the cluster information, verify that you have completed the following tasks.
- All of the nodes in the cluster have been upgraded.
- The Sametime System Console must be started.
- All of the nodes in the cluster must be started.
- The Community Server that the Proxy Servers connect to must already be registered with the Console and must be started.

**About this task**

Working from the deployment manager server for the cluster that you upgraded, follow these steps to update properties files and run the registration utility to update the cluster's registration information with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use CTRL+Click to open the topic in a new browser tab or window so you can keep it open for reference:
- `console.properties`
- `productConfig.properties`

**Procedure**

1. On the computer where the Deployment Manager for the cluster is running, navigate to the console directory.
   - Sametime System Console Deployment Manager as cluster Deployment Manager:
     `/QIBM/UserData/Lotus/stii/STCONSOLE/STCONSOLE_date_time/console`
     The `STCONSOLE_date_time` indicates when the Sametime System Console Server was installed.
   - Proxy Server Cell Deployment Manager as cluster Deployment Manager
     `/QIBM/UserData/Lotus/stii/STProxy/STProxy_date_time/console`
     The `STProxy_date_time` indicates when the Proxy Server was installed.

2. In the console directory, make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

3. Verify the following values in the `console.properties` file and add the Sametime System Console password. After making changes, save and close the file.

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>The fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</table>

*Table 150. console.properties settings for the Deployment Manager*
Table 150. *console.properties* settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>The HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSL 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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>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>A value of “true” connects to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>The HTTPS port used by the Sametime System Console server if SSCSSL is set to &quot;true.&quot;</td>
</tr>
</tbody>
</table>

4. Now update the password settings in the productConfig.properties file. The specific settings to update depends on the install type of the Deployment Manager. After making changes, save and close the file.

   - Sametime System Console Deployment Manager as cluster Deployment Manager
     - **DBAppPassword**: Specify the password associated with the database ID.
     - **WASPassword**: Specify the password associated with the WebSphere Application Server user ID.
   - Proxy Server Cell Deployment Manager as cluster Deployment Manager
     - **WASPassword**: Specify the password associated with the WebSphere Application Server user ID.

5. From an IBM i command line, run the following command to start the QShell Interpreter:

   QSH

6. Run the cd shell command, specifying the fully qualified path to the console directory you used in Step 1.

7. Run the registration utility to update the cluster configuration information:

   registerProduct.sh -upgradeCluster

8. When the script completes, press F3 to exit QSH.

**Upgrading Sametime 8.5 or 8.5.1 Meeting Server on IBM i**

Follow the instructions for your operating system to upgrade one or more Sametime Meeting Servers running on IBM i.

**Upgrading a single Sametime 8.5 or 8.5.1 Meeting Server on IBM i:**

Upgrade a single, non-clustered IBM Sametime 8.5 Meeting Server running on IBM i.
Before you begin

Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

About this task

Upgrading a single, non-clustered Sametime Meeting Server involves preparing a response file and then upgrading the server software.

Preparing the Sametime Meeting Server installation file for upgrading on IBM i:

Follow these steps to customize the response.properties file to prepare for installing the Sametime Meeting Server on IBM i.

Before you begin

You should have completed the preparation steps in “Preparing to install Sametime on IBM i.”

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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

2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:
      cd /MySametimePackages
   c. Run the following shell command, specifying the name of the .zip file:
      ajar -x name_of_installation_package
   d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:
   /MySametimePackages/SametimeMeetingServer/IBM/i/stii_stms/licenses
For DVD:
/qopt/volume_ID/IBM/i/stii_stms/licenses

4. Navigate to the program image directory, for example:
/MySametimePackages/SametimeMeetingServer/IBM/i/stii_stms

For DVD:
/qopt/volume_ID/IBM/i/stii_stms

5. Make a copy of the stms.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
   - For the database.db.user.id and database.db.user.password settings in the properties file, specify the user profile and password you created to be the owner of the Meeting Server database schemas.
   - Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Sametime Meeting Server. This is necessary for live names to work correctly in meeting rooms.

Example

"Default meeting server installation file for IBM i" on page 774

Related tasks

"Preparing to install Sametime on IBM i" on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Using the default Sametime Meeting Server installation file for upgrading on IBM i:

The response.properties file contains settings used to install or upgrade a Sametime Meeting Server on IBM i.

The default content for the response.properties file for installing the Sametime Meeting Server follows:

```
# Sametime 8.5.2 Meeting Server Installation Properties file for IBM i
# Preparing to Install
# This file is used for either installing a new Sametime 8.5.2 Meeting Server or
# upgrading a Sametime Meeting Server to Sametime 8.5.2.
```
# Consult the Lotus Sametime 8.5.2 Information Center for detailed information
# about preparing to install or upgrade a Sametime Meeting Server on IBM i and
# running the installation program.
#
# The Information Center is available online from the Lotus Sametime documentation
# library:
#
# http://www.ibm.com/developerworks/lotus/documentation/sametime
#
# License Acceptance
#
# By changing the silentInstallLicenseAcceptance property in this response file
# to "true", you agree that you have reviewed and agree to the terms of the
# IBM International Program License Agreement accompanying this program, which
# is located at CD_ROOT\IBM\stii_stms\licenses.
#
# If you do not agree to these terms, do not change the value or otherwise
# download, install, copy, access, or use the program and promptly return the
# program and proof of entitlement to the party from whom you acquired it to
# obtain a refund of the amount you paid.
#
# Valid values for silentInstallLicenseAcceptance:
#   true - Accept the license terms and continue with product installation.
#   false - Decline the license terms and do not install the product.
#
silentInstallLicenseAcceptance=false
#
# Installation Type
#
# Set this value to the type of installation you wish to perform.
# The setting determines the WAS nodes that are created or upgraded during
# installation.
#
# Valid values for install.type:
#   Cell - (default) Cell installation, recommended for new deployments.
#       Creates both a deployment manager node and a primary application
#       server node with the Sametime Meeting Server installed. The primary
#       node is federated into the deployment manager's cell.
#       If the cell installation already exists, both the deployment manager
#       node and the primary application server node are upgraded. Secondary
#       nodes must be upgraded separately.
#   PN - Primary Node installation.
#       Creates a primary application server node with the Sametime Meeting
#       Server installed or upgrades an existing primary application server
#       node to Sametime 8.5.2.
#       For new installations, the primary node must be federated into the
#       Deployment Manager's cell when registering the node with the
#       Sametime System Console.
#   SN - Secondary Node installation.
#       Creates a secondary application server node with the Sametime Meeting
#       Server installed or upgrades an existing secondary application server
#       node to Sametime 8.5.2.
#       For new installations, the node is federated into the Deployment
#       Manager's cell specified by the Secondary Node Properties
#       (later in this file). After installation, this node may be clustered
#       with the primary node in the cell.
#       When upgrading a secondary node, the node's federation and clustering
#       status is not changed.
#
install.type=Cell
#
# Websphere Settings
# These values are used when configuring the WebSphere Application Server nodes.

## stwas.was.hostname - (required)
For new installs, specify the fully qualified hostname that your WAS server will use.
For upgrades, specify the fully qualified hostname of the existing WAS server.

## stwas.was.admin.id - (required)
For new installs, specify the user ID that you will use to log into the Deployment Manager’s Integrated Solutions Console once security is enabled. This name must not exist as a user in any LDAP directory that you plan to connect to the server.
For upgrades, specify the user ID that you use to log into the Deployment Manager’s Integrated Solutions Console.

## stwas.was.admin.password - (required)
The password associated with the user ID specified for ‘stwas.was.admin.id’

### DO NOT CHANGE ###

```bash
stwas.was.hostname=
stwas.was.admin.id=
stwas.was.admin.password=
```

#### Secondary Node Settings

These settings are used only for Secondary Node installations (SN).
For new installations, the settings specify the cell that the secondary node should be federated into.
For upgrades, the settings specify the cell that the existing secondary node is already federated into.
The Deployment Manager for the cell must be started before running a secondary node install or upgrade.

These values are ignored if not installing or upgrading a secondary node.

## stwas.sn.dm.hostname - (required for ‘SN’ install)
The fully qualified hostname of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade).
The Deployment Manager must be running and listening on this hostname or the install will fail.

## stwas.sn.dm.soap.port - (required for ‘SN’ install)
The soap port of the Deployment Manager for the cell that the secondary node will be federated into (new install) or is already federated into (upgrade).
The Deployment Manager must be running and listening for SOAP connections on this port or the install will fail.

### DO NOT CHANGE ###

```bash
stwas.sn.dm.hostname=
stwas.sn.dm.soap.port=
```

#### STATIC Websphere Settings

These settings are used by the installer to control how Websphere is configured during installation. The values have been set specifically for installing the Sametime Meeting Server.
DO NOT CHANGE this settings unless instructed to do so by IBM Support.

### DO NOT CHANGE ###

```bash
stwas.was.installlocation=/QIBM/ProdData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.profilelocation=/QIBM/UserData/WebSphere/Appserver/v7/SametimeWAS
stwas.was.dprofile.default=STMDMgrProfile
stwas.was.sprofile.default=STMAppProfile
stwas.was.sserverprofile.default=STMAppProfile
stwas.was.snserverprofile.default=STMSNAppProfile
stwas.was.appserver=STMeetingServer
```

### DO NOT CHANGE ###
# Database Settings

# These settings define the database that will be used for the Sametime Meeting
# Server.
# For new installations, they control how the database resources are configured
# in the Websphere Application Server.
# For upgrades, they allow the installer to connect to the database resources.

#
# database.db.hostname - (required) The fully qualified hostname of the system
# where the database is running.
# database.db.user.id - (required) The user ID that will be used when making a
# connection to the database.
# database.db.user.password - (required) The password for the user ID specified
# by database.db.user.id.

database.db.hostname=
database.db.user.id=
database.db.user.password=

# STATIC Database Settings

# These settings are used by the installer to control how database connections are
# configured during installation. The values have been set specifically for
# installing the Sametime Meeting Server.
# DO NOT CHANGE these settings unless instructed to do so by IBM Support.

### DO NOT CHANGE ###
database.db.type=db2_iseries
database.db.name=STMS
database.db.port=50000
### DO NOT CHANGE ###

# LDAP Settings

# These values are used for new installs to define the LDAP server that the
# Sametime Meeting Server will connect to.
# The settings in this section are not used for upgrade installations.

#
# ldap.hostname - (required) The fully qualified hostname of the LDAP server.
# ldap.port - (required) The port used to connect to the LDAP server.
# ldap.displayname - (required) Attribute for the displayname in Websphere
# Identity Manager. The default value is "cn".
# ldap.loginfield - (required) Indicates the attribute name used for login. The
# default value is "mail".
# ldap.basedn - The starting point for LDAP searches of the directory service.
# ldap.binddn - Specifies the Bind distinguished name (DN) that the meeting
# server will use to authenticate with the LDAP server. If not
# specified, the meeting server will use anonymous access.
# ldap.binddn.password - (required if ldap.binddn is set) Specifies the password
# that the meeting server will use to authenticate with the LDAP server.
# ldap.skip.ldap.config - If set to "true", the LDAP will not be configured
# during installation and you will need to complete the configuration
# manually. Only change this setting if you need LDAP to connect using
# SSL.
Upgrading a Sametime 8.5 or 8.5.1 Meeting Server on IBM i:

Upgrade an IBM Sametime 8.5 or 8.5.1 Meeting Server running on IBM i.

Before you begin

Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

Upgrading Cell deployment

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

Upgrading Primary or Secondary Nodes

Make sure the Deployment Manager for the node has been upgraded and is running. This is required to successfully upgrade the node.

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation, except the Deployment Manager for the node. The Deployment manager must be running even if it resides on the same system as the node and shares the same WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

Procedure

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH

4. Run the cd shell command to change directories, specifying the fully qualified path to the installation kit directory; for example:
   
   cd /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   
   For DVD:
   
   cd /qopt/volume_ID/IBMi/stii_stms

5. Start the Meeting Server installation with the following shell command:
   
   install_stms.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file

Chapter 4. Migrating and upgrading  1191
6. When the script completes, press f3 to exit QSH.

**Results**

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STMEETINGS_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STMEETINGS_20091215_0307.log

**Note:** If the primary node and secondary node share the same WebSphere Application Server installation with the Deployment Manager, the log from the primary node and secondary node upgrade may contain error CWUPI0049E. This error occurs if the node upgrade attempts to install WebSphere Application Server fixes when a server is running. It indicates that the WebSphere Application Server installation is not fully up-to-date. Check the logs from the Deployment Manager upgrade to determine if a problem occurred when installing the WebSphere Application Server fixes. Correct the problem and re-run the Deployment Manager upgrade. If this was the only error, it is not necessary to re-run the node upgrade.

**Updating registration of an IBM i Sametime Meeting Server with the Sametime System Console after upgrading:**

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

**Before you begin**

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server's registration information, verify that you have completed the following tasks.

**Sametime Community Server**

- The community server must already be registered with the Sametime System Console.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.

**Sametime Proxy Server**

- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
• The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

Sametime Meeting Server
• The meeting server must already be registered with the Sametime System Console.
• The Sametime System Console must be started.
• The LDAP server must be started.

About this task

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server’s registration information with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:
• console.properties
• productConfig.properties

Procedure
1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.
   • Community Server
     The console directory is a subdirectory of the Sametime Community server data directory.
   • Proxy Server
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.
   • Meeting Server
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.
2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.
3. Verify the following values in the console.properties file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.

Table 151. console.properties settings

| SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
Table 151. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>

4. Now update the productConfig.properties file with the values needed for the server you are updating. Then save and close the file.

   Required values not listed below are filled in automatically.

   • **Sametime Community Server**
     - The information from the original registration should already be in the file. If the **DepName** is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

   • **Sametime Proxy Server**
     - **WASPassword:** Specify the password associated with the WASUserID.

   • **Sametime Meeting Server**
     - **DBAppPassword:** Specify the password associated with the database ID.
     - **WASPassword:** Specify the password associated with the WASUserID.
     - **LDAPBindPwd:** Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server.

   Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   QSH

7. Run the cd shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   • **Sametime Community Server**
     registerSTServerNode.sh -upgrade

   • **Other servers**
     registerProduct.sh -upgrade

9. When the registration script completes, press F3 to exit QSH.
Related tasks

“Upgrading policies from Release 8.5 or 8.5.1” on page 1219

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.

Upgrading a cluster of Sametime 8.5 or 8.5.1 Meeting Servers on IBM i:

Upgrading a cluster of IBM Sametime 8.5 or 8.5.1 Meeting Servers running on IBM i. 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 upgrade the Deployment Manager and all nodes, then update the configuration information in the Sametime System Console. The Sametime System Console must be upgraded first, before upgrading the other servers in a Sametime deployment.

Upgrading the Sametime 8.5 or 8.5.1 Meeting Server application on IBM i:

Upgrade the IBM Sametime 8.5 or 8.5.1 Meeting Server application on a computer running IBM i.

About this task

The Sametime System Console must be upgraded first, before upgrading the other servers in a Sametime deployment. Upgrade the Meeting Server cluster components in the following order:

1. Deployment Manager (Sametime System Console or Meeting Cell deployment)
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.

The instructions for upgrading the Meeting Server application vary according to the server’s operating system:

Upgrading a Sametime 8.5 or 8.5.1 Meeting Server node on IBM i:

Upgrade an IBM Sametime 8.5 or 8.5.1 Meeting Server running on IBM i.

Before you begin

Upgrade the Sametime System Console first, before upgrading the other servers in a Sametime deployment.

Upgrading Cell deployment

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

Upgrading Primary or Secondary Nodes
Make sure the Deployment Manager for the node has been upgraded and is running. This is required to successfully upgrade the node.

Stop all of the WebSphere Application Server servers on the system that use the Sametime WebSphere Application Server installation, except the Deployment Manager for the node. The Deployment manager must be running even if it resides on the same system as the node and shares the same WebSphere Application Server installation. For more information, see the Command reference for starting and stopping servers.

Procedure
1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```sh
   QSH
   ```

4. Run the cd shell command to change directories, specifying the fully qualified path to the installation kit directory; for example:

   ```sh
cd /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   ```

   For DVD:
   ```sh
cd /qopt/volume_ID/IBMi/stii_stms
   ```

5. Start the Meeting Server installation with the following shell command:

   ```sh
   install_stms.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file
   ```

6. When the script completes, press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

```text
install_STMEETINGS_yyyyyymmdd_hhmm.log
```

For example, this log was created at 3:07 A.M. on December 15, 2009:

```text
install_STMEETINGS_20091215_0307.log
```

**Note:** If the primary node and secondary node share the same WebSphere Application Server installation with the Deployment Manager, the log from the primary node and secondary node upgrade may contain error CWUPI0049E. This error occurs if the node upgrade attempts to install WebSphere Application Server fixes when a server is running. It indicates that the WebSphere Application Server installation is not fully up-to-date. Check the logs from the Deployment Manager upgrade to determine if a problem occurred when installing the WebSphere Application Server fixes. Correct the problem and re-run the Deployment Manager upgrade. If this was the only error, it is not necessary to re-run the node upgrade.
Updating registration of an IBM i Sametime Meeting Server node with the Sametime System Console after upgrading:

If the IBM i Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

Before you begin

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Verifying the Community Server is configured with the LDAP server host name and Registering an upgraded Community Server on IBM i with the System Console instead.

Before updating the server’s registration information, verify that you have completed the following tasks.

**Sametime Community Server**
- The community server must already be registered with the Sametime System Console.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.

**Sametime Proxy Server**
- The proxy server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.

**Sametime Meeting Server**
- The meeting server must already be registered with the Sametime System Console.
- The Sametime System Console must be started.
- The LDAP server must be started.

About this task

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server’s registration information with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure

1. On the Sametime server you plan to update with the Sametime System Console, navigate to the console directory.
   - Community Server
The console directory is a subdirectory of the Sametime Community server data directory.

- **Proxy Server**
  
  `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`

  The *date* and *time* indicate when the Proxy Server was installed.

- **Meeting Server**
  
  `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`

  The *date* and *time* indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with different names of the `console.properties` and `productConfig.properties` files.

3. Verify the following values in the `console.properties` file that were specified when the server was registered originally. For the Community Server, the encrypted System Console password should already be in the properties file. For the Proxy Server and Meeting Server, you will need to add the System Console password. After making changes, save and close the file.

   **Table 152. `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 <code>AboutThisProfile.txt</code> 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>On IBM i, look for the <code>AboutThisProfile.txt</code> file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</td>
</tr>
<tr>
<td>SSCPassword</td>
<td>Enter the WebSphere Application Server password associated with the <code>SSCUserName</code>.</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. Now update the `productConfig.properties` file with the values needed for the server you are updating. Then save and close the file.

   Required values not listed below are filled in automatically.

   - **Sametime Community Server**
     - The information from the original registration should already be in the file. If the `DepName` is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console.

   - **Sametime Proxy Server**
     - **WASPPassword**: Specify the password associated with the WASUserID.

   - **Sametime Meeting Server**
- **DBAppPassword**: Specify the password associated with the database ID.
- **WASPassword**: Specify the password associated with the WASUserID.
- **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.

5. If you are registering a Sametime Community Server, start the server. Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```
   QSH
   ```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   - **Sametime Community Server**
     ```
     registerSTServerNode.sh -upgrade
     ```
   - **Other servers**
     ```
     registerProduct.sh -upgrade
     ```

9. When the registration script completes, press **F3** to exit QSH.

**Related tasks**

“Upgrading policies from Release 8.5 or 8.5.1” on page 1219

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.

Starting servers in the upgraded Sametime Meeting Server cluster on IBM i:

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. Update the registration of all upgraded IBM i Sametime servers if they were previously registered with the Sametime System Console.

**Procedure**

1. On the server hosting the Deployment Manager, start QSH, navigate to the Deployment Manager profile’s /bin directory (\app_server_root\profiles\profile_name\bin) and start the cluster’s Deployment Manager:

   ```
   startManager dmgr
   ```

2. On each node in the cluster, start QSH, navigate to the node profile’s /bin directory and start the following servers:

   a. WebSphere Application Server should already be running, but if it is not, start it now:
      ```
      startServer.bat server1
      ```
   
   b. Start the node agent:
      ```
      startNode
      ```
   
   c. If a WebSphere proxy server is hosted on this node, start it now:
      ```
      startServer.bat WAS_proxy_server_name
      ```
   
   d. Start the Sametime Meeting Server:
      ```
      startServer.bat Meeting_Server_name
      ```
   
   e. Repeat for every node in the cluster.
### Updating registration of a Sametime Meeting Server cluster on IBM i:

After all of the nodes in a cluster have been upgraded, run the registration utility to update the cluster's configuration information on the IBM Sametime System Console.

### Before you begin

Before you update the cluster information, verify that you have completed the following tasks.
- All of the nodes in the cluster have been upgraded.
- The Sametime System Console must be started.
- All of the nodes in the cluster must be started.
- The LDAP server must be started.

### About this task

Working from the Deployment Manager server for the cluster that you upgraded, follow these steps to update properties files and run the registration utility to update the cluster's registration information with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use **CTRL+Click** to open the topic in a new browser tab or window so you can keep it open for reference:
- `console.properties`
- `productConfig.properties`

### Procedure

1. On the computer where the Deployment Manager for the cluster is running, navigate to the `console` directory.
   - Sametime System Console Deployment Manager as cluster Deployment Manager: `/QIBM/UserData/Lotus/stii/STCONSOLE/STCONSOLE_date_time/console`
     The `STCONSOLE_date_time` indicates when the Sametime System Console Server was installed.
   - Meeting Server Cell Deployment Manager as cluster Deployment Manager: `/QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console`
     The `STMEETINGS_date_time` indicates when the Meeting Server was installed.

2. In the console directory, make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

3. Verify the following values in the `console.properties` file and add the Sametime System Console password. After making changes, save and close the file.

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>The fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</table>

*Table 153. console.properties settings for the Deployment Manager*
Table 153. console.properties settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHTTPPort</td>
<td>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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</td>
</tr>
<tr>
<td>SSCUserName</td>
<td>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>A value of “true” connects to the Sametime System Console using a secure connection.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>The HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to “true.”</td>
</tr>
</tbody>
</table>

4. Now update the password settings in the productConfig.properties file. The specific settings to update depends on the install type of the Deployment Manager. After making changes, save and close the file.
   - Sametime System Console Deployment Manager as cluster Deployment Manager
     - **DBAppPassword**: Specify the password associated with the database ID.
     - **WASPassword**: Specify the password associated with the WebSphere Application Server user ID.
   - Meeting Server Cell Deployment Manager as cluster Deployment Manager
     - **DBAppPassword**: Specify the password associated with the database ID.
     - **WASPassword**: Specify the password associated with the WebSphere Application Server user ID.
     - **LDAPBindPwd**: Specify the password associated with the LDAP BindDN.

5. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```
   QSH
   ```

6. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

7. Run the registration utility to update the cluster configuration information:

   ```
   registerProduct.sh -upgradeCluster
   ```

8. When the script completes, press F3 to exit QSH.

**Upgrading Sametime 8.5 or 8.5.1 Gateway on IBM i**

Follow the instructions for your operating system to upgrade one or more Sametime Gateway servers running on IBM i.
**What to do next**

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.
- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

**Upgrading a single Sametime 8.5 or 8.5.1 Gateway server on IBM i:**

Upgrade a single, non-clustered IBM Sametime Gateway server running on IBM i.

**About this task**

Upgrading a single, non-clustered Sametime Gateway server requires upgrading the server software, applying IBM WebSphere Application Server interim fixes, and registering the upgraded server with the Sametime System Console.

**What to do next**

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.
- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

**Installing WebSphere iFixes before upgrading Sametime Gateway server on IBM i:**

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.
Upgrading a Sametime 8.5 or 8.5.1 Gateway server on IBM i:

Upgrading a Sametime 8.5 or 8.5.1 Gateway server on IBM i:

Before you begin:

Before you begin:

Stop all the cluster components including the Deployment Manager, the application server on the primary node, the second node, the SIP Proxy server, and the node agents.

About this task:

About this task:

Upgrade cluster components in the following order:
1. Primary Node
2. Secondary Nodes
3. Deployment Manager

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:

Procedure:

1. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the `WRKSYSVAL` command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. Download the installation package for the Sametime Gateway server.
   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
```

4. From an IBM i command line, run the following command to start the QShell Interpreter:

```bash
QSH
```

5. Run the cd shell command, specifying the fully qualified path to the installation kit directory.

6. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as c:\TMP.

7. Extract the contents of part_number.exe to the temporary directory c:\TMP.

8. Navigate to the folder: c:\TMP\SametimeGateway.

9. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

**Important:** If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.

- To run the installer in wizard mode, type the following command:
  ```bash
  installi5OS.bat
  ```
- To run the installer in console mode, perform these steps:
  a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
  b. Start a QSHELL session.
  c. Navigate to the /TMP/SametimeGateway directory and type the following command:
  ```bash
  install.sh -console
  ```

**Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

```bash
install.sh -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

10. Select the language to be used for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed.

11. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.

12. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.

13. Select **Upgrade a server**, and then click **Next**.

14. On the same panel, review the location of the Sametime Gateway node to upgrade. If the location is correct, click **Next**.
Note: If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for *.pid file, delete the file, and continue from this step.

15. Deployment Manager upgrade only: On the “Cluster configuration” screen, verify that the correct cluster name appears.

   Tip: To obtain the cluster name from the Integrated Solutions Console, click Servers > Clusters. The default cluster name is “SametimeGatewayCluster”.

16. On the “Cluster configuration” screen, enter the WebSphere Application Server installation root path. This path is the same as the path that you specified during the original installation.

17. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, /QIBM/proddata/websphere/AppServer/v7/nd
   This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.

18. On the “WebSphere Application Server credential” screen, use the same administrative user ID and password that you created when you install the Deployment Manager and the primary node.

19. Verify the DB2 properties; these should not change for an upgrade.
   Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

20. Click Next to see the Sametime Gateway installation summary.
21. Review the installation summary settings and, if necessary, click Back to make changes.

22. Click Install to begin the installation process (new files are installed during an upgrade).

A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click Finish. To view the installation log, open the log file at stgw_server_root\logs\installlog.txt

Updating registration of an IBM i Gateway server with the Sametime System Console:

If the IBM i Sametime Gateway you upgraded was registered with the Sametime System Console in a previous release, update its registration information now.

Before you begin

If the upgraded server was never registered with the Sametime System Console, follow the instructions in Registering a new Gateway with the System Console instead.

Before updating the server's registration information, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be started.
- The Gateway database must be started.
- The Community Server that the Gateway server connects to must be started.

About this task

Working from the Sametime server that you upgraded, follow these steps to update properties files and run the registration utility to update the server's registration information with the console.

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

- console.properties
- productConfig.properties

Procedure

1. On the Sametime Gateway server you plan to update with the Sametime System Console, navigate to the /qibm/userdata/STGateway/ProfileName/console directory.

   The ProfileName is the one you specified when you installed the Gateway.

2. In the console directory, make backup copies with different names of the console.properties and productConfig.properties files.
3. Verify the following values in the `console.properties` file that were specified when the server was registered originally. If you make changes, save and close the file.

**Table 154. 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; 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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>

4. Now update the `productConfig.properties` file with the values needed for the server you are updating. Then save and close the file. Required values not listed below are filled in automatically.

**Table 155. productConfig.properties settings**

| InstallType | Specify "Cell" as the installation type since this is a non-clustered server. |
| DepName | If the DepName is missing, update it to exactly match the correct deployment name for this server on the Sametime System Console. |
| NodeIP | Specify the IP address of the server being registered. |
| WASAdminPassword | Specify the password associated with the WASUserID |
| LDAPBindPassword | Specify the password associated with the LDAPBindDN. |
| DB2AdminPassword | Specify the password associated with the database ID. |
| CommunityServerHost | Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console. |
| CommunityServerPort | Specify the port for the Community Server. |
| LDAPHost | Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console. |
Table 155. productConfig.properties settings (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

5. Run the registration utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: `QSH`
   b. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.
   c. Run the shell script to register the server: `registerProduct.sh -upgrade`
   d. When the registration script completes, press **F3** to exit QSH.

   The utility updates the server registration with the Sametime System Console, generating a log file called `ConsoleUtility.log` and storing it in the `ConsoleUtility.log` directory.

6. When the registration script completes, press **F3** to exit QSH.

Upgrading a cluster of Sametime 8.5 or 8.5.1 Gateway servers on IBM i:

Upgrade a cluster of IBM Sametime Gateway servers running on IBM i.

About this task

Upgrading a cluster of Sametime Gateway 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, start the cluster, register the upgraded cluster with the Sametime System Console, and then run the clustering guided activity to update configuration information.

What to do next

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

Installing WebSphere iFixes before upgrading Sametime Gateway node on IBM i:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.
About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Preparing the Sametime 8.5 or 8.5.1 Gateway cluster for an upgrade on IBM i:

Before upgrading servers in a cluster of IBM Sametime Gateway servers running on IBM i, prepare the cluster by stopping the Deployment Manager as well as servers running on each node.

Procedure

1. Stop the cluster:
   a. On the Deployment Manager, log in to the Integrated Solutions Console.
   b. Click Servers > Clusters > WebSphere application server clusters.
   c. In the list of clusters, click the checkbox to select your Gateway cluster.
   d. At the top of the list, click the Stop button.
2. Stop the SIP Proxy server:
   a. On the Deployment Manager, click Servers > Server Types > WebSphere proxy servers.
   b. In the list of proxy servers, click the checkbox to select your SIPProxyServer.
   c. At the top of the list, click the Stop button.
3. Stop the node agents:
   a. On the Deployment Manager, click System administration > Node agents.
   b. In the list of node agents, select all the node agents in the cluster.
   c. At the top of the list, click the Stop button.
4. Stop the Deployment Manager:
   a. Log in to the server with a user profile that has the *ALLOBJ and *SECADM authorities.
   b. Start QSH.
   c. Navigate to the stgw_profile_root/bin directory for the Deployment Manager.
   d. Run the following command:
      ```
      stopManager dmgr -username WAS_admin_username -password WAS_admin_password.
      ```

Upgrading a Sametime 8.5 or 8.5.1 Gateway node on IBM i:
Upgrade the IBM Sametime Gateway cluster members and Deployment Manager running on IBM i.

**Before you begin**

Before you can upgrade a Sametime Gateway server, the Sametime System Console must be upgraded and running.

Stop all the cluster components including the Deployment Manager, the application server on the primary node, the second node, the SIP Proxy server, and the node agents.

**About this task**

Upgrade cluster components in the following order:

1. Primary Node
2. Secondary Nodes
3. Deployment Manager

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. Log in to the server using a profile with *ALLOBJ and *SECADM special authorities.

2. Use the `WRKSYSVAL` command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.

3. Download the installation package for the Sametime Gateway server.
   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

4. From an IBM i command line, run the following command to start the QShell Interpreter:
QSH

5. Run the cd shell command, specifying the fully qualified path to the installation kit directory.

6. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as c:\TMP.

7. Extract the contents of part_number.exe to the temporary directory c:\TMP.

8. Navigate to the folder: c:\TMP\SametimeGateway.

9. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

**Important:** If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.

- To run the installer in wizard mode, type the following command:
  `installi5OS.bat`
- To run the installer in console mode, perform these steps:
  a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
  b. Start a QSHELL session.
  c. Navigate to the /TMP/SametimeGateway directory and type the following command:
     `install.sh -console`

**Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

`install.sh -console -V BypassWasInfoCheck=true`

Because your input will not be verified during installation, you should take extra care when typing values.

10. Select the language to be used for the installation and click OK. The Sametime Gateway Welcome screen is displayed.

11. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully.

12. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click Next to proceed with the installation. If you accepted the terms, the Installation Type dialog is displayed.

13. Select Upgrade a server, and then click Next.

14. On the same panel, review the location of the Sametime Gateway node to upgrade. If the location is correct, click Next.

**Note:** If you see the warning the following warning: “The Sametime Gateway has running servers. Stop all active application servers before upgrading” then
make sure all servers are stopped. If you receive this warning, and you are sure that there are no servers running (the only JAVA process in the process list is the installer itself), then search the WebSphere installation root directory for *.pid file, delete the file, and continue from this step.

15. Deployment Manager upgrade only: On the "Cluster configuration" screen, verify that the correct cluster name appears.

   **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters.** The default cluster name is "SametimeGatewayCluster".

16. On the "Cluster configuration" screen, enter the WebSphere Application Server installation root path. This path is the same as the path that you specified during the original installation.

17. In the WebSphere Application Server location screen, specify the directory where WebSphere Application Server 7.0 ND was installed, for example, /QIBM/proddata/websphere/AppServer/v7/nd

   This value should be the same as the installLocation option in the response file used to install WebSphere Application Server.

18. On the "WebSphere Application Server credential" screen, use the same administrative user ID and password that you created when you install the Deployment Manager and the primary node.

19. Verify the DB2 properties; these should not change for an upgrade.

   Provide the application and schema user credentials when prompted; this information will not be needed for a Deployment Manager upgrade.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

20. Click **Next** to see the Sametime Gateway installation summary.

21. Review the installation summary settings and, if necessary, click **Back** to make changes.
22. Click **Install** to begin the installation process (new files are installed during an upgrade).

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process runs in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes to complete; the second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete. When the upgrades are complete, the wizard displays a message indicating a successful installation.

23. Read the summary and click **Finish**. To view the installation log, open the log file at `stgw_server_root/logs/install/installlog.txt`

*Registering an upgraded Sametime Gateway cluster on IBM i with the System Console:*

After upgrading an IBM Sametime Gateway cluster on IBM i, register it with the Sametime System Console, which allows you to manage all Sametime servers from a central location.

**Before you begin**

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

**About this task**

Working from the cluster's Deployment Manager, Primary Node, and Secondary Nodes, follow these steps to update `console.properties` and `productConfig.properties` files. Then run the registration utility on the nodes and the Deployment Manager to register them with the 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 the topic in a new browser tab or window so you can keep it open for reference:

- `console.properties`
- `productConfig.properties`

**Procedure**

1. On the Deployment Manager, navigate to the `stgw_server_root/qibm/userdata/stgateway/dmgrprofilename/console` directory.
   
   **Note:** If a cluster's Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager's profile.

2. Make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

3. Update the Deployment Manager's `console.properties` file:
   a. Open the file for editing.
   b. Update the file with the following values:
Table 156: console.properties settings for the Deployment Manager

<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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWS/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>SSCHTTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to &quot;true.&quot;</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

4. Update the Deployment Manager's productConfig.properties file:
   a. Open the file for editing.
   b. Update the file with the following required values.

Table 157: productConfig.properties settings for the Deployment Manager

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;DM&quot; because you are working in the Deployment Manager's profile right now.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 157. productConfig.properties settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

5. On the Primary Node machine, navigate to the stgw_server_root/qibm/userdata/stgateway/PrimaryNodeProfileName/console directory.

6. Edit the Primary Node's console.properties file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 158. console.properties settings for the Primary Node

<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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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 '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>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

7. Edit the Primary Node's productConfig.properties file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.
Table 159. productConfig.properties settings for the Primary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;PN&quot; because you are now working in the Primary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

8. On the Secondary Node machine, navigate to the stgw_server_root/q1bm/userdata/stgateway/SecondaryNodeProfileName/console directory.

9. Edit the Secondary Node's console.properties file with the following values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.

Table 160. console.properties settings for the Secondary Node

<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>
Table 160. `console.properties` settings for the Secondary Node (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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

10. Edit the Secondary Node's `productConfig.properties` file with the following required values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.

Table 161. `productConfig.properties` settings for the Secondary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;SN&quot; because you are now working in the Secondary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 161. `productConfig.properties` settings for the Secondary Node (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

11. Run the registration utility on the Primary Node.
   a. Log on to the Primary Node machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/PrimaryNodeProfileName/console` directory.
   c. Run the registration utility.
      
      **Already registered**
      registerProduct.sh -upgrade
      
      **First-time registration**
      registerProduct.sh
      
   d. When the registration script completes, press `F3` to exit QSH.

12. Run the registration utility on the Secondary Node.
   a. Log on to the Secondary Node machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/SecondaryNodeProfileName/console` directory.
   c. Run the registration utility.
      
      **Already registered**
      registerProduct.sh -upgrade
      
      **First-time registration**
      registerProduct.sh
      
   d. When the registration script completes, press `F3` to exit QSH.

13. Run the registration utility on the Deployment Manager.
   a. Log on to the Deployment Manager machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/dmgrprofilenname/console` directory.
   c. Run the registration utility.
      
      **Already registered**
      registerProduct.sh -upgradeCluster
      
      **First-time registration**
      registerProduct.sh
      
   d. When prompted for the cluster's name, type the name you assigned the cluster when you created it, and press `Enter`.
   e. When the registration script completes, press `F3` to exit QSH.

14. Start the Sametime Gateway cluster, if it is not already running.

   **Starting servers in the upgraded Sametime Gateway server cluster on IBM i:**

   In an IBM Sametime deployment, start the servers in the upgraded cluster of Sametime Gateway Servers.
Before you begin

Upgrade all nodes in the cluster before you start the cluster. Update the registration of all upgraded IBM i Sametime servers if they were previously registered with the Sametime System Console.

Procedure

1. Apply WebSphere Application Server fixes to the cluster's SIP proxy server as described in Installing WebSphere iFixes for Sametime Gateway.
2. On the server hosting the Deployment Manager, start QSH, navigate to the Deployment Manager profile’s /bin directory (stgw_profile_root/bin) and start the cluster's Deployment Manager:
   startManager dmgr
3. On the primary node in the cluster, start QSH, navigate to the node profile’s /bin directory (stgw_profile_root/bin) and start the following servers:
   a. Start the node agent:
      startNode
   b. Repeat for every secondary node and the SIP proxy node in the cluster.
4. Log on to the Integrated Solutions Console on the Deployment Manager as a user with administrative privileges.
5. Click Servers > Clusters > WebSphere application server clusters.
6. Select the SametimeGatewayCluster and click Start.
7. Click Servers > Server Types > WebSphere proxy servers.
8. Select the SIPProxyServer and click Start if it is not already started.

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.
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 217
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.

**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 RMVLSSTDOM 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 162. 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 STprevious_versionBU. 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>
<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:
         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:
```
mount /dev/cdrom /cdrom
```

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:
   - 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:
     ```ini
     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.:
     ```ini
     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 (c:\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_BYTES_SENT=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 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 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 8.5 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>
<tr>
<td>Group authorization</td>
<td>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.</td>
</tr>
<tr>
<td>Nested group expansion</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Set to Yes to enable Directory Assistance for the LDAP Directory.</td>
</tr>
</tbody>
</table>

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. 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. 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>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>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</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, 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</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>Choose the option that suits your environment.</td>
</tr>
<tr>
<td>server’s certificate</td>
<td></td>
</tr>
<tr>
<td>Advanced options</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>Setting</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</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. For more information on running the name conversion utility, see “Mapping the user ID to a unique directory attribute” on page 208.

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 148
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="(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s))"/>
         </StorageDetails>
       </Storage>
       <Details>
         <Detail Id="MailAddress" FieldName="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>
     </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>
   ```

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 593

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
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:
   &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

**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**

  `db2 connect to STSC`

  `db2 -tf createSchedTable.ddl`
db2cmd

db2 connect to STSC

db2 -tf createSchedTable.ddl

**Related tasks**

“Installing DB2 on Linux or Windows” on page 129

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.

**Linux:** 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:
         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

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 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:
  ```
  ! () . ? [ ] _ ` ~
  ```

- **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. 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 584

**Related tasks**

“Uninstalling a WebSphere-based Sametime server on AIX, Linux, Solaris, or Windows” on page 606

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 582

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.
   
   http://serverhostname.domain:port/ibm/console
   
   For example:
   
   http://sametime.example.com:8700/ibm/console
   https://sametime.example.com:8701/ibm/console

   IBM: 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

   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. 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 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.

What to do next

“Connecting to an LDAP server” on page 143

Related tasks

“Starting the Sametime System Console” on page 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

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 68

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 143

Related tasks

“Starting the Sametime System Console” on page 582

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.

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 93
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 582
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 Authorized 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, setup 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 163. Person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object class</strong></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><strong>LDAP user search base</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Policy ID for users and groups** | 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.                                                                                                                                                             |
| **Display name**              | 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.                                                                                                                                                        |
| **Similar name distinguisher** | 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.                                                                                                                                                        |
| **Email address**             | 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.                                                                                                                                                                         |
| **Home Sametime server**      | 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. |
| **Membership attribute**      | Enter the attribute that specifies which groups a user belongs to if your LDAP server supports this feature.                                                                                                                                                                                                                             |

b. Enter the search and authentication attributes of an LDAP person entry.
Table 164. 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 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 &quot;Display Name&quot; 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 <strong>must be set to mail and must be listed first.</strong> 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 165. 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>
</tbody>
</table>
Table 165. Group attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group membership attribute</td>
<td>Specifies the name of the attribute in the group entry that contains the 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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Starting and stopping the Deployment Manager on IBM i” on page 917
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Enabling encryption between Sametime and the LDAP server” on page 1435
Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

Related reference
“LDAP directory settings” on page 148
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 588
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 93
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 582
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>
<thead>
<tr>
<th>Table 166. console.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCHostName</td>
</tr>
<tr>
<td>SSCHTTPPort</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SSCUserName</td>
</tr>
<tr>
<td>SSCPassword</td>
</tr>
<tr>
<td>SSCSSLEnabled</td>
</tr>
<tr>
<td>SSCHTTPSPort</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>
<thead>
<tr>
<th>Table 167. productConfig.properties settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
</tr>
<tr>
<td>NodeHostName</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:
**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>
<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.

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 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.

About this task

Important: 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.

Related concepts

“Configuring a Sametime Proxy Server” on page 1650
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** &gt; **Install Sametime Proxy Server**.

**Related tasks**

“Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine” on page 257

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 582

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.

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 234

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.

Linux: 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
      ```

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 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.

8. 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 Install.

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

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

13. 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.

14. Select IBM Sametime Proxy Server as the feature to install and select Use Sametime System Console to install. Click Next.

15. 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.

16. 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.

17. Click Validate to log in to the Sametime System Console.

   The button name changes to Validated after you log in.

18. When you are logged in, click Next.

19. Select the Sametime Proxy Server deployment plan you created earlier with the Sametime System Console guided activity. Then click Next.

20. Review the deployment settings, then click Next.

21. Review the summary, then click Install to start the installation.

22. Click Exit to close the Installation Manager.

23. 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 />
       <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

**Related tasks**

“Guided activity: Preparing to install a Sametime Proxy Server” on page 233

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 582

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 606

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.

**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://servername.domain:port/stwebclient/index.jsp`

   Replace `servername.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 `servername.domain` with the fully qualified domain name of the server.
      
      `http://servername.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 584
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\n    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".
    <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">
        ...
        <wccmProperty name="com.ibm.ssl.keyStore" wccmPropertyName="keyFileName" wccmPropertyGroup="SecurityPropertyGroup" wccmDefault="C:/WebSphere/">
        <wccmProperty name="com.ibm.ssl.trustStore" wccmPropertyName="trustFileName" wccmPropertyGroup="SecurityPropertyGroup" wccmDefault="C:/WebSphere/">
        ...
    </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, 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.

Related tasks

“Configuring a Sametime Meeting Server” on page 1675
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.
   - \textbf{AIX, Linux, or Solaris}
     Open the IBM DB2 folder on the desktop and click \textit{Control Center}.
   - \textbf{Windows}
     Click \textit{Start} > \textit{Programs} > \textit{IBM DB2} > \textit{General Administration Tools} > \textit{Control Center}.
6. Find the database name to verify that the new database was created.

\textbf{Related tasks}
“Installing DB2 on Linux or Windows” on page 129
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 \textit{serverhostname.domain} with the fully qualified domain name of the Sametime System Console server.
   \texttt{http://serverhostname.domain:8700/ibm/console}
   For example:
   \texttt{http://sametime.example.com:8700/ibm/console}
   \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:
   \texttt{/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 582

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 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 257

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 582

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 420

*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.

**Linux:** 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`

4. Navigate to the folder where you stored the downloaded files and start the installation program by running one of the following commands:
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. 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. 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 581

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 606

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.

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 168. 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
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 1417
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 from Sametime 8.0.x and 7.5.1 on IBM i

Upgrade from previous releases of IBM Sametime on the IBM i 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)
- Sametime Entry (release 8.5)
- Sametime Standard (release 8.5)

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 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 IBM i

Upgrade one or more IBM Sametime servers running on IBM i.

Upgrading from Sametime 8.0.x and 7.5.1 on IBM i:

Upgrade from previous releases of IBM Sametime on the IBM i 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)
- Sametime Entry (release 8.5)
- Sametime Standard (release 8.5)

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 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.

Removing meeting rooms from Enterprise Meeting Server on IBM i:

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 IBM i:

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 on IBM i:

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 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.
   You must upgrade to at least IBM i 5.4 before installing Sametime. IBM i 5.4 or later is required for Sametime and IBM i 6.1 is required for supporting IPv6 addressing.
   Consider other Lotus Domino servers and related Lotus products that may be running on the same system in your upgrade plans. Make sure that your currently installed server releases, and product releases, are all supported on the new operating system level. For up-to-date details about which combinations of Domino, Sametime, and other Lotus Domino related product releases are supported on current IBM i releases, see the Lotus Software for IBM i Compatibility Guide.
   For information on Sametime system requirements, see the system requirements at the following web address:

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 each Lotus Domino server hosting Sametime 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 or later, continue to the next step.
   Otherwise, install a supported level of Lotus Domino and run the UPDDOMSVR command to update each Lotus Domino server hosting Sametime before proceeding.

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.

Verifying the system host name prior to upgrading on IBM i:

During the IBM Sametime Community Server startup, Sametime attempts to resolve the main system host name in addition to the Sametime server host name. The upgraded server will not start if Sametime cannot resolve the system host name to an IP address. Prior to Sametime 8.5, only the host name for the Sametime server was checked.
About this task

Verify that either the local IBM i host table (CFGTCP, option 10) or the DNS contain a fully qualified host name for the system and that the host name resolves to the correct IP address. If necessary, update the local IBM i host table or the DNS.

Backing up the Sametime data prior to upgrading on IBM i:

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>
<thead>
<tr>
<th>Table 169. Sametime server data to back up</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data to back up</strong></td>
</tr>
<tr>
<td>names.nsf</td>
</tr>
<tr>
<td>notes.ini</td>
</tr>
<tr>
<td>da.nsf</td>
</tr>
<tr>
<td>vpuserinfo.nsf</td>
</tr>
<tr>
<td>sametime.ini, stconfig.nsf</td>
</tr>
</tbody>
</table>
Table 169. Sametime server data to back up (continued)

<table>
<thead>
<tr>
<th>Data to back up</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>All customized data files, templates or</td>
<td></td>
</tr>
<tr>
<td>applications (.ntf, .mdm, .scr, .bmp,</td>
<td></td>
</tr>
<tr>
<td>.mac, .smi, .tbl)</td>
<td></td>
</tr>
<tr>
<td>All ID files, desktop.dsk, and</td>
<td></td>
</tr>
<tr>
<td>pubnames.ntf</td>
<td></td>
</tr>
<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>

Pre-accepting the Sametime software agreements prior to upgrading on IBM i:

If you do not pre-accept the IBM Sametime software agreements, the installation process will restore the product to the system, but then stop and wait for you to accept the agreements before completing the installation. Skip this step if you are installing from a downloaded image.

Procedure
1. Insert the Sametime DVD into the optical drive of your system.
2. Enter the following command on an IBM i command line:
   
   GO LICPGM

   The Work with Licensed Programs display appears.
3. From the Work with Licensed Programs (LICPGM) menu, select option 5 (Prepare for install) and press Enter. The Prepare for Install display appears.
4. Type 1 in the option field next to Work with software agreements. Press Enter.

   When the Work with Software Agreements display appears, you see all IBM licensed programs that require software agreement acceptance and whether the agreement has been accepted. Only licensed programs that are not yet installed appear on this display. The software agreements for Sametime will not appear in the list until you restore them from the DVD in a later step.
5. Press F22 (shift-F10) to restore the Software Agreements from the Sametime DVD.

   For the Device parameter, specify the name of your optical drive (For example, OPT01). Press Enter to restore the Sametime software agreements to the system.
6. If you are installing from physical media (not virtual optical media), the following message is displayed after the Software agreements are restored:

   Waiting for reply to message on message queue QSYSOPR

   You can sign on to another session to respond to the message or ask the system operator to respond.

   To view and respond to the message from another session:
   a. Enter the following command on an IBM i command line:
      
      WRKMSGQ QSYSOPR

   b. Select option 5 to display the messages in the QSYSOPR message queue.

   c. Locate the following message in the queue:
      
      Load the next volume in optical device OPT01. (X G)
d. The Sametime software agreements have already been restored. If you want to restore more software agreements from another DVD, insert the next DVD and respond with G. When the software agreements have been restored, the message is issued again. When you are done, respond to the message with X.

7. The Work with software agreements display now shows the restored licenses for products that are not yet installed.
   - If you are using the DVD for the Entry version of Sametime, you will see an entry for Licensed Program 5724J23, option *BASE.
   - If you are using the DVD for Sametime Standard, you will see two entries for Licensed Program 5724J23: one entry for *BASE and another entry for Option 1.

8. For each entry for Licensed Program 5724J23, type 5 in the option field and press Enter to display the Software Agreement. Then press F14 (Accept) to accept the terms of the software agreement.

   **Note:** In some unusual situations, the following message may be issued when you attempt to display the Software Agreement:

   CPDB6D6 - Software agreement documents are missing. If this occurs, repeat step 5 to restore the Software Agreements again and continue with the remaining steps in this procedure.

**Upgrading the Sametime server application on IBM i:**

Run the installation program on the computer where you plan to upgrade an IBM Sametime server.

**About this task**

Use the IBM i command line to install the Sametime Community Server.

**Procedure**

1. Make sure you have backed up the recommended files to a directory outside of your Sametime directory structure or to physical media before proceeding.
2. Sign on to your server with a user profile that has the *ALLOBJ and *SECADM special authorities.
3. Stop the IBM Lotus Domino server that will run Sametime. Stop all existing Sametime servers.
4. From the IBM i command line, run the appropriate command for installing from a downloaded image or physical media.

**Installing from a downloaded image**

   a. Make sure that you have downloaded the community server installation package and created save files.
   b. Use the RSTLICPGM command to install from the save files you created when you downloaded the installation package.
      
      This example uses the save files MYLIB/Q5724J23IM and MYLIB/Q5724J23WC.
      
      RSTLICPGM LICPGM(5724J23) DEV(*SAVF) OPTION(*BASE) LNG(2924) SAVF(MYLIB/Q5724J23IM)
      RSTLICPGM LICPGM(5724J23) DEV(*SAVF) OPTION(1) SAVF(MYLIB/Q5724J23WC)
   c. When you are prompted to accept the Sametime software agreement, you must accept it in order to continue.

**Installing from physical media**
a. Make sure you have pre-accepted the license agreement as explained in the previous task.
b. Insert the Sametime disk in your system optical drive and use the LODRUN command:
   
   LODRUN DEV(*OPT) DIR('/os400')
   
   The system loads the Sametime programs to the appropriate libraries and /QIBM directories. You will see status messages as the system installs the software.

Results

All of your existing Sametime servers are upgraded during the install process. Check the job log to verify that all of your Sametime servers were upgraded successfully. You should see the following message for each Sametime server that was successfully upgraded on your system:

Upgrade successful for Sametime server server_name

What to do next

Refresh the design of your Sametime databases by either waiting for the nightly Design server task to run or by forcing an immediate refresh with the LOAD DESIGN command, as described in the following steps.

1. On any IBM i command line, type the following command and press Enter:

   WRKDOMCSL

2. On the "Work with Domino Console" display, type the name of your Sametime server and press Enter.

3. At the command prompt, type the following Lotus Domino subcommand and press Enter:

   LOAD DESIGN

In addition, 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. For more information, see Disabling or enabling meetings on an IBM i Sametime Standard server.

Related tasks

“Starting and stopping Domino and a Sametime Community Server on IBM i” on page 927
Learn how to start and stop a Sametime Community Server running on IBM i.

“Installing a Domino server in a new domain on IBM i” on page 671
Follow these steps to set up a Lotus Domino server in a new Lotus Domino domain.

Migrating data from pre-7.5 releases of Sametime on IBM i:

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 on IBM i:

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.

Running the privacy migration utility on IBM i:

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.

About this task

To run the privacy information migration utility after upgrading Sametime, 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 your Sametime 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. Stop the Sametime server.
3. From any IBM i command line, start the QShell Interpreter:

   QSH

4. Run the following shell command:

   cd <sametime_server_data_directory>

5. To migrate privacy information for all of your Sametime users, run the following shell command:

   upgrade_privacy <sametime_server_data_directory>

   To migrate privacy information for a specified subset of your Sametime users, run the following shell command:

   upgrade_privacy <sametime_server_data_directory> <upgrade_util_filter_file>
6. Check the vpuserinfo.nsf<time_stamp>.log file that has the latest time stamp to verify that the utility ran successfully. You can exit the QShell session and browse for the file, or run the following shell command to display the contents:

```bash
cat vpuserinfo* .log
```

Disabling or enabling meetings on an IBM i Sametime Standard server after upgrading from version 8.0 or 7.5.1:

Disable meetings on any IBM i Sametime Standard server that you plan to use as a Sametime Entry server.

About this task

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.

Follow these steps to use the CHGLSTDOM command to disable meetings on a particular server.

Procedure

1. On any IBM i command line, type the following and press F4:

```bash
CHGLSTDOM
```

2. On the Change Sametime on Domino display, set Web Conferencing to *NO and press Enter.

What to do next

If you decide to enable Web Conferencing on the server later, run the CHGLSTDOM command again, specifying *YES for Web Conferencing.
Related concepts
“Planning for a mixed-license environment of Sametime Entry, Sametime Standard, and Sametime Advanced servers” on page 127
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.

Related tasks
“Running the community server installation program on IBM i” on page 680
Run the installation program on the machine where you plan to install a Sametime Community Server.

Upgrading a stand-alone Community Mux from version 8.0 or 7.5.1:
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_BYTES_SENT=0
```

Close and save the file, then restart the server.

**Upgrading a remote Conversion Server from version 8.0 or 7.5.1:**

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 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 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 8.5 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 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 for upgrading a Sametime 8.0 or 7.5.1 deployment on IBM i:**

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 on IBM i

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.

Migrating a Domino Directory to LDAP format on IBM i:

If your existing IBM LotusSametime server is using a native Lotus Domino Directory for user authentication, you will need to convert it to use LDAP protocol so that it can be registered with the Sametime System Console.

Before you begin

Previous releases of Sametime allowed the use of the native Lotus Domino Directory for user authentication. Starting in release 8.5, the Sametime System Console requires access to an LDAP directory, so if you want to register your Community Server with the System Console, you must migrate the Lotus Domino Directory to LDAP format. For more information, see Planning for an LDAP directory and the "Directory considerations" section of Planning a Community Server installation for more information.

Note: If you migrate convert the existing Lotus Domino Directory to LDAP format, the directory can no longer be hosted on the same Lotus Domino server as the Community Server.
About this task

Follow these steps to migrate the Lotus Domino directory to LDAP format.

Procedure
1. Shut down the Sametime services but keep the Lotus Domino services active as described in Starting and stopping a Sametime server on IBM i while Domino is running.
2. Specify LDAP connection information on IBM i.
3. Start the Sametime server.
4. Run the name change task.
5. Configure the LDAP Directory settings in the LDAP document using a Lotus Notes client or the Sametime Administration Tool.

   Note: The Connectivity section should already be completed. Verify that the information in the other sections is correct: Basics, Authentication, Searching, and Group Contents. If necessary, update them for your LDAP directory.
6. Restart the Sametime server.

What to do next

Next, you may need to complete these additional tasks to complete the configuration of your converted LDAP directory:

Changing LDAP connection information for servers on IBM i:

Use the CHGLSTDOM command to change LDAP directory information on IBM i.

About this task

Follow these steps to re-configure an IBM i Sametime server to connect to an LDAP directory instead of a Domino directory:

Procedure
1. On any IBM i command line, type the following and press F4:
   
   CHGLSTDOM

2. On the "Change Sametime on Domino" display, set Directory Type to *LDAP and press Enter.
3. Complete the following fields describing your LDAP server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the fully qualified host name of the LDAP server that Sametime will use. Do not specify the TCP/IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the IP port that Sametime will use. The default IP port for LDAP connections is 389.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind distinguished name (DN)</td>
<td>Enter the distinguished name of the LDAP directory entry that the Sametime server will use when binding to the LDAP directory. This is an optional parameter. If not specified, you must ensure the LDAP server is configured appropriately for anonymous access from a Sametime server.</td>
</tr>
<tr>
<td>Bind password</td>
<td>If you specified a <strong>Bind distinguished name (DN)</strong>, enter the password associated with it.</td>
</tr>
<tr>
<td>Administrator name (DN)</td>
<td>Enter the distinguished name of an LDAP administrator who has authority to browse the LDAP directory. It is used when configuring policies. This parameter is optional and defaults to the same value as the Bind distinguished name.</td>
</tr>
</tbody>
</table>

4. Press **Enter** to run the command.

**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.

### Related tasks

- “Configuring the Sametime Community Server to support IPv6 addressing on IBM i” on page 699
- Configure settings to establish connectivity and resolve addresses when using IPv6 addressing on the IBM Sametime community server.

### Configuring the LDAP Directory settings:

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.

### Before you begin

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

### About this task

You must configure the LDAP Directory settings on the LDAP document in the Configuration database to ensure that the Sametime server can search and authenticate against entries in the LDAP directory. Use the Sametime Administration Tool to enter LDAP Directory settings; the tool then writes the values to the LDAP document in the Sametime Configuration database (`stconfig.nsf`) and updates the Directory Assistance database.
Follow these steps to configure the LDAP settings using the Sametime Administration Tool.

**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. For descriptions of the settings, see “LDAP directory settings” on page 148.
4. Click **Save & Close**.
5. Restart the Sametime Community Server to enable your settings.

**Specifying 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 1308
- “Collect Person Settings” on page 1308
- “Collect Group Settings” on page 1310

**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 170. 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>
| 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. |
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment</strong>&lt;br&gt;<strong>Name</strong> for this LDAP connection</td>
<td>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.</td>
<td>Sample deployment name: ST_LDAP</td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>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.</td>
<td>Sample host name ldap1.example.com</td>
</tr>
<tr>
<td><strong>Port</strong> of the LDAP server</td>
<td>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.</td>
<td>Default 389</td>
</tr>
<tr>
<td><strong>Bind distinguished name (DN) and Password</strong></td>
<td>If you have selected <strong>Authenticated Access</strong>, 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. &lt;br&gt;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. &lt;br&gt;If you use a person entry for the authenticated user, the Sametime server must have access to the following attributes: &lt;br&gt;- person name &lt;br&gt;- person description &lt;br&gt;- home Sametime server &lt;br&gt;- email address &lt;br&gt;- location &lt;br&gt;- telephone number &lt;br&gt;- title &lt;br&gt;- photo (if used for business card) &lt;br&gt;- object class &lt;br&gt;- Any LDAP directory entry attribute that is specified in any search filter in the Collect Person Settings section of the guided activity. &lt;br&gt;If you use a Group entry for the authenticated user, the Sametime server must have access to the following attributes: &lt;br&gt;- group name &lt;br&gt;- group description (if this setting is not empty) &lt;br&gt;- group members &lt;br&gt;- ObjectClass &lt;br&gt;- Any LDAP directory entry attribute that is specified in any search filter in the Collect Group Settings section of the guided activity.</td>
<td>If you use a person entry for the authenticated user, the Sametime server must have access to the following attributes: &lt;br&gt;- person name &lt;br&gt;- person description &lt;br&gt;- home Sametime server &lt;br&gt;- email address &lt;br&gt;- location &lt;br&gt;- telephone number &lt;br&gt;- title &lt;br&gt;- photo (if used for business card) &lt;br&gt;- object class &lt;br&gt;- Any LDAP directory entry attribute that is specified in any search filter in the Collect Person 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 171. 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>Detected LDAP</td>
<td>For stconfig.nsf, edit the ldapservr</td>
<td>Sample Base distinguished name:dc=example,dc=com</td>
</tr>
<tr>
<td>Base DNs</td>
<td>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: DC=austin,DC=ibm,DC=com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Base object when searching for group entries: 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>LDAP user search</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>search base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure advanced</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>
<tr>
<td>LDAP settings</td>
<td></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 172. Collect Person Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</th>
</tr>
</thead>
</table>
Table 172. Collect Person Settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Comments and sample values</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. 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.</td>
<td>Sample authentication attributes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mail;cn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mail;cn;uid</td>
</tr>
<tr>
<td></td>
<td>Consider an LDAP person entry containing the following attributes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• mail: <a href="mailto:jlock@example.com">jlock@example.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• cn: James Lock</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the authentication attribute is mail, the user authenticates with <a href="mailto:jlock@example.com">jlock@example.com</a>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the authentication attribute is cn, the user authenticates with James Lock.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></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 (;).</td>
<td>Sample search attributes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mail;cn;uid</td>
</tr>
<tr>
<td>Object Class</td>
<td>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.</td>
<td>The value is set automatically to a default value based on the type of LDAP directory detected.</td>
</tr>
</tbody>
</table>

Person attributes
Table 172. 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></td>
</tr>
<tr>
<td></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>
<td></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>
<tr>
<td></td>
<td>If you have installed multiple Sametime servers, each user’s person entry in an LDAP directory must contain a field in which a user’s home server is specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can either:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add a new field to the LDAP directory to store the name of each user’s home server. This field must be in the person entry of every Sametime user in the LDAP directory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use a field that exists in the person entries of each Sametime user, such as the email address.</td>
<td></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 173. 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 |

<table>
<thead>
<tr>
<th>Group Attributes</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Displays a group’s name in Sametime user interfaces.</td>
<td>Sample display name: cn</td>
</tr>
</tbody>
</table>
| 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 |
| membership       | 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 144

This activity takes you through the steps for identifying users and groups in an LDAP directory that need access to IBM Sametime.

**Setting up the Sametime System Console for an expanded deployment on IBM i:**

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 an expanded deployment on IBM i:

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.

Preparing the console installation file for an expanded deployment on IBM i:

Follow these steps to customize the response.properties file to prepare for installing the Sametime System Console on IBM i.

Before you begin

You should have completed the preparation steps in "Preparing to install Sametime on IBM i."

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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

2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSE
   b. Run the cd shell command, specifying the fully qualified path to the installation package directory; for example:
      cd /MySametimePackages
   c. Run the following shell command, specifying the name of the .zip file:
ajar -x name_of_installation_package

d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image; for example:
   /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc/licenses
   For DVD:
   /qopt/volume_ID/IBMi/stii_ssc/licenses

4. Navigate to the program image directory; for example:
   /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc
   For DVD:
   /qopt/volume_ID/IBMi/stii_ssc

5. Make a copy of the ssc.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   • For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
   • For the database.db.user.id and database.db.user.password settings in the properties file, specify the user profile and password you created to be the owner of the Sametime System Console database schemas.
   • Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms.

Example

“Default console installation file for IBM i” on page 645

Related tasks

“Preparing to install Sametime on IBM i” on page 642

Follow these steps to prepare IBM i for Sametime server installations.

Creating the System Console database schemas and tables for an expanded deployment on IBM i:

Run the script to create the database schema for the IBM Sametime System Console on IBM i.

Before you begin

You should have prepared the console installation file as described in “Preparing the console installation file on IBM i.”

About this task

On the IBM i system where you will install the Sametime System Console, follow these steps to create the database schema and tables:
Procedure

1. Log in with a user profile that has *ALLOBJ and *SECADM special authorities. These authorities are required to create the database schemas. The database schemas will be created on the system specified in your copy of the ssc.default.response.properties file and owned by the user profile specified in the file.

2. From an IBM i command line, run the following command to start the QShell Interpreter:

   ```bash
   QSH
   ```

3. Run the `cd` shell command, specifying the fully qualified path to the installation kit directory; for example:

   ```bash
   cd /MySametimePackages/SametimeSystemConsole/IBMi/stii_ssc
   ```

   For DVD:
   ```bash
   cd /qopt(volume_ID)/IBMi/stii_ssc
   ```

4. If the SSC schema does not already exist on the system, run the following shell command to create the required database schemas and tables. The command also creates the POLICY schema if it does not exist.

   ```bash
   setupDB_ssc.sh -install.response.file=path_and_name_of_custom_response.properties_file
   ```

5. When the script completes, press F3 to exit QSH.

Results

If the database schema creation was not successful, look at the script log for more information about what occurred during the attempt. Fix the problem, then try running the script again. The script log is stored in the following location.

   ```bash
   /QIBM/UserData/Lotus/stii/logs
   ```

The log name contains the date and time in this form:

   ```bash
   ssc_dbsetup_yyyymmdd_hhmm.log
   ```

For example, this log was created at 3:07 A.M. on December 15, 2009:

   ```bash
   ssc_dbsetup_20091215_0307.log
   ```

Related tasks

"Preparing to install Sametime on IBM i" on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Installing the console for an expanded deployment on IBM i:

Run the install script to set up the IBM Sametime System Console on IBM i.

Before you begin

If you intend to install from a downloaded image, you should have downloaded the console server installation package. For all installations, you should have completed the preparation steps. The database schemas required for the System Console (SSC and POLICY) should already exist.

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 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.

About this task

Follow these steps to install the Sametime System Console and WebSphere Application Server.

Procedure

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   ```
   QSH
   ```
4. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:
   ```
   /MySametimePackages/SametimeSystemConsole/IBM/i/stii_ssc
   ```
   For installing from DVD:
   ```
   cd /qopt/volume_ID/IBM/i/stii_ssc
   ```
5. Start the Sametime System Console installation with the following shell command:
   ```
   install_ssc.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file
   ```
   When the script completes, a summary of the results is displayed. Make a note of the URL for connecting to the Integrated Solutions Console. The "Admin port" displayed is the port you must use when logging in to the system console.
6. Press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STCONSOLE_yyyymmd_d hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STCONSOLE_20091215_0307.log

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Increasing the WebSphere Application Server usage limit for running an expanded Sametime deployment on IBM i:
Use the Change License Information command to allow an unlimited number of users for the WebSphere Application Server installation. Changing the usage limit in this manner is acceptable provided you are in compliance with the terms of your Sametime license and are only using WebSphere Application Server for running Sametime.

**About this task**

If you install more than one Sametime server that uses WebSphere Application Server on the same system, this task only needs to be done once. Following the recommended installation sequence, the first server that uses WebSphere Application Server is the Sametime System Console. Other servers that use WebSphere Application Server are the Sametime Meeting Server, Sametime Proxy Server, and Sametime Gateway.

**Procedure**

1. Sign on to the system with a user profile that has *ALLOBJ special authority.
2. From any IBM i command line, run the following command (on one line):
   ```
   CHGLICINF PRIDID(5733W70) LICTRM(V7) FEATURE(5102) USGLMT(*NOMAX) THRESHOLD(*USGLMT)
   ```

**Results**

The usage limit is changed to *NOMAX.

If the following message is displayed, type G.

CPA9E1B: Usage limit increase must be authorized.
   Press help before replying (C G)

After you respond to the CPA9E1B message, you must respond to the same message on the QSYSOPR message queue:

1. Run the DSPMSG QSYSOPR command to see the message in the QSYSOPR message queue.
2. When the message is displayed, type G.

**Logging in to the console after expanding the deployment on IBM i:**

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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

*Logging in to the Sametime system console in an expanded deployment on IBM i:*
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 `servername.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.
   
   `http://servername.domain:port/ibm/console`

   For example:
   
   `http://sametime.example.com:8700/ibm/console`
   `https://sametime.example.com:8701/ibm/console`

   **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`

   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. 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 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.

**What to do next**

"Connecting to an LDAP server" on page 143

**Related tasks**

"Starting the Sametime System Console" on page 582

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

*Logging in to the console for a cell profile in an expanded deployment on IBM i:*

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 `servername.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 `servername.domain` with the fully qualified domain name of the server.
     
     `http://servername.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 `servername.domain` with the fully qualified domain name of the server.
     
     `http://servername.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 `servername.domain` with the fully qualified domain name of the server.
     
     `http://servername.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 68
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 an expanded deployment on IBM i:

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 `servername.domain` with the fully qualified domain name of the Sametime System Console server.
   Specify port 8700 for all platforms except IBM i.
   
   `http://servername.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://servername.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 143

Related tasks

“Starting the Sametime System Console” on page 582

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

Connecting to an LDAP server in an expanded deployment on IBM i:

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 93
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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Sametime prerequisite: Connecting to an LDAP server in an expanded deployment on IBM i:

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 174. Person attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object class</strong></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><strong>LDAP user search base</strong></td>
<td>Specifies which ID to search for when the administrator selects <strong>User ID</strong> as the search criteria for managing policies.</td>
</tr>
<tr>
<td><strong>Policy ID for users and groups</strong></td>
<td>Specifies which ID to search for when the administrator selects <strong>User ID</strong> as the search criteria for managing policies.</td>
</tr>
<tr>
<td><strong>Display name</strong></td>
<td>Displays a user's name in Sametime user interfaces. The attribute must not be the same as the one you use for <strong>Similar name distinguisher</strong> or <strong>Email address</strong> due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td><strong>Similar name distinguisher</strong></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 <strong>Display name</strong> or <strong>Email address</strong> due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>Contains the user's email address in the field. The attribute must not be the same as the one you use for <strong>Display name</strong> or <strong>Similar name distinguisher</strong> due to WebSphere Application Server configuration rules.</td>
</tr>
<tr>
<td><strong>Home Sametime server</strong></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><strong>Membership attribute</strong></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 175. 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`. |

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 176. 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LDAP group search base</th>
<th>Displays a group’s name in Sametime user interfaces.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td></td>
</tr>
<tr>
<td>Similar name distinguisher</td>
<td>Differentiates between two groups that have the same common name (cn) attribute.</td>
</tr>
</tbody>
</table>
Table 176. Group attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

“Starting and stopping the Deployment Manager on IBM i” on page 917
The Deployment Manager manages the Sametime System Console and all Sametime Server cells.

“Enabling encryption between Sametime and the LDAP server” on page 1435
Configure SSL encryption between an IBM Sametime server and an LDAP server by enabling the LDAPS protocol.

Related reference
“LDAP directory settings” on page 148
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 588
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 in an expanded deployment on IBM i:

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 93
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 582
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 in an expanded deployment on IBM i:

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.

Verifying the Community Server is configured with the LDAP server host name:

Before registering an upgraded IBM Sametime server to a Sametime Community Server on IBM i, verify that the Sametime Community Server is configured to use the fully qualified host name of the LDAP server. If it is configured with an IP address, the command to register the Community Server with the System Console will fail.

**About this task**

Follow these steps to confirm that the LDAP server is configured with a fully qualified host name.

**Procedure**

1. Open the Administration Tool on the Sametime community server and click LDAP directory. If the LDAP server is specified using an IP address, change it to the fully qualified host name of the LDAP server.

2. Open the directory assistance database. (The directory assistance database is usually called da.nsf but it may be different. You can verify the name by checking the Basics tab in the Sametime server document.)
   
   Open the LDAP document. If the LDAP server is specified using an IP address, change it to the fully qualified host name of the LDAP server and save the document.

**Related tasks**

“Creating a Directory Assistance document” on page 1234

The Directory Assistance database on the Sametime server must contain a Directory Assistance document that enables the Sametime server to access the LDAP server.

**Registering an upgraded Community Server on IBM i with the System Console:**

After upgrading an IBM Sametime server to a Sametime Community Server on IBM i, 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**

Verify the upgraded Community Server is configured with the LDAP server host name.

Then make sure the following servers are ready for the registration task:

- The Sametime 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.
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, /stserver/server.cer).
   b. From an IBM i command line, run the following command to start the
      QShell Interpreter:
      QSH.
   c. Run the following shell command to navigate to the directory where Java is
      installed:
      cd /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/bin
   d. Now run the following command (on a single line) to import the SSL
      certificate:
      keytool -import -alias certificate_name -file file_containing_certificate
      -storepass changeit -keystore ../lib/security/cacerts
   e. Press F3 to exit QShell.

2. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's sametime_server_data_directory/
      console directory.
   b. Make backup 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 177. 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 SSSLEnabled 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWA5/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>
</tbody>
</table>
Table 177. console.properties settings (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCSSEnabled</td>
<td>Change this value to &quot;true&quot; to connect to the Sametime System Console using a secure connection. Note: If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to &quot;false.&quot; Otherwise the registration will fail.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSEnabled 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.

   The only required value in this file is

   **DepName**: Provide a descriptive name for your deployment; it must be a unique deployment name on the Sametime System Console.

5. Run the registerSTServerNode.sh registration 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 register the server: `registerSTServerNode.sh`

   d. As the registration utility runs, you will be prompted to enter the following information:

<table>
<thead>
<tr>
<th>Location of notes.ini file</th>
<th>Type the full path to the directory containing the notes.ini file (for example, /stserver/data), and press Enter.</th>
</tr>
</thead>
<tbody>
<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>

   e. When the registration script completes, press F3 to exit QSH.

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

6. Modify the sametime.ini file:

   a. Navigate to the Sametime data directory and open the samtime.ini file in a text editor.

   b. In the [Policy] section of the file, locate the following setting:

      ```
      ST_DB_LDAP_ALLOW_SEARCH_ON_DN=1
      ```

   c. Move (do not copy) this line to the [Directory] section of the file.

   d. Save and close the file.

7. (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.

8. 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 an upgraded Community Server cluster on IBM i with the System Console:

After upgrading a cluster of IBM Sametime servers on IBM i, 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 of each 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. Complete the following steps for each server in the cluster to verify each server document's Net Address field:

   a. From a Lotus Notes client, open the Server document for the Sametime Community Server you are working on.
   b. Click the Ports tab.
   c. Click the Notes Network Ports tab and check the Net Address field:
      This field should contain the fully qualified host name of the current Sametime Community Server. If the field contains an IP address change it now.
   d. Click Save if you made a change, and then click Close to close the Server document.
   e. If you changed the Server document, restart the server.
   f. Remember to repeat this task for every server in the cluster.

3. Now run the registerSTCluster.sh registration utility from one of the servers in the cluster:

   a. From an IBM i command line, run the following command to start the QShell Interpreter: QSH
   b. Navigate to the server's sametime_server_data_directory/console directory; for example: cd /stserver/data/console.
   c. Run the shell script using the appropriate command below:

      Upgrading from 8.5
      registerSTCluster.sh -upgradeCluster

      Upgrading from 8.0.x and 7.5.1
d. 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>Type the full path to the Sametime Community Server data directory containing notes.ini file (for example, /stserver/data), and press Enter.</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>

e. When the registration script completes, press F3 to exit QSH.

The utility registers the cluster, generating a log file called ConsoleUtility.log and storing it in the consoles/logs directory.

4. Restart the Sametime Community Server where you ran the registration utility.

### Installing a Sametime Proxy Server in an expanded deployment on IBM i:

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.

### About this task

**Important:** 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.

### Related concepts

"Configuring a Sametime Proxy Server“ on page 1650
Configure connection settings to enable the IBM Sametime Proxy Server to communicate with other servers in the deployment.

*Preparing the Sametime Proxy Server installation file for an expanded deployment on IBM i:*

Follow these steps to customize the response.properties file to prepare for installing the Sametime Proxy Server on IBM i.
About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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

2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:
      cd /MySametimePackages
   c. Run the following shell command, specifying the name of the .zip file:
      ajar -x name_of_installation_package
   d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:
   /MySametimePackages/SametimeProxyServer/IBMi/stii_stp/licenses
   For DVD:
   /qopt/volume_id/IBMi/stii_stp/licenses

4. Navigate to the program image directory; for example:
   /MySametimePackages/SametimeProxyServer/IBMi/stii_stp
   For DVD:
   /qopt/volume_id/IBMi/stii_stp

5. Make a copy of the stp.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
     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.
Be sure to change the silentInstallLicenseAcceptance setting to true to indicate your agreement with the license terms. There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Meeting Server. This is necessary for live names to work correctly in meeting rooms.

Example

“Default Sametime Proxy Server installation file on IBM i” on page 748

Installing a Sametime Proxy Server for an expanded deployment on IBM i:

Run the install script to set up the Sametime Proxy Server on IBM i.

Before you begin

If you intend to install from a downloaded image, you should have downloaded the proxy server installation package. For all installations, you should have completed the preparation steps.

About this task

Follow these steps to install the Sametime Proxy Server and WebSphere Application Server.

Procedure

1. Log in using a profile with *ALLOBJ and *SECADM special authorities.
2. Use the WRKSYSTR command to check the setting for the QVFYOBJRST system value and change it if necessary. The setting must be 3 or lower to install the Sametime software.
3. From an IBM i command line, run the following command to start the QShell Interpreter:
   QSH
4. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:
   /MySametimePackages/SametimeProxyServer/IBM/i/stii_stp
   For DVD:
   cd /qopt/volume_ID/IBM/i/stii_stp
5. Start the installation with the following shell command:
   install_stp.sh
   -Dinstall.response.file=\path_and_name_of_customized_response.properties_file
6. When the installation completes, press F3 to exit QSH.
7. If the Sametime Proxy server is installed on a system with multiple active IP addresses, follow these steps. 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.
1) Find the stproxyconfig.xml file in the Proxy Server's deployment manager profile configuration in this location:
/qibm/UserData/WebSphere/AppServer/v7/SametimeWAS/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 />
    <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 logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

`install_STPROXY_YYYYmmdd_hhmm.log`

For example, this log was created at 3:07 A.M. on December 15, 2009:

`install_STPROXY_20091215_0307.log`

**What to do next**

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

If you have installed both the Sametime Meeting Server and the Sametime Proxy Server on the same system, you must update the table of Host Aliases associated with the Sametime Proxy Server's `default_host` virtual host so that it does not use the same host name and IP address as the Sametime Meeting Server. Follow the steps in Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine.
Related tasks
“Starting and stopping servers running on WebSphere Application Server” on page 581
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.
“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Registering a non-clustered Sametime Proxy Server with the Sametime System Console for an expanded deployment on IBM i:

After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

Before you begin

Before you register the server, verify that you have completed the following tasks.

Sametime Community Server
• The community server must be configured to use an LDAP directory.
• The community server must be started.
• The Sametime System Console must be started.
• The LDAP server must be started.
• The LDAP server must be connected to the Sametime System Console.

Sametime Proxy Server
• The Sametime System Console must be started.
• The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.
• When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

Sametime Meeting Server
• The Sametime System Console must be started.
• The LDAP server must be started.
• The LDAP server must be connected to the Sametime System Console.
• The Meeting Server database (STMS) must be connected to the Sametime System Console.
• When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

About this task

Working from the Sametime server that you want to connect with the console, follow these steps to update properties files and run the registration utility to register the server with the console.
During this task you will edit the following files; click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:

- `console.properties`
- `productConfig.properties`

### Procedure

1. On the Sametime server you plan to register, navigate to the console directory.
   - **Community Server**
     The console directory is a subdirectory of the Sametime Community server data directory.
   - **Proxy Server**
     `/QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console`
     The `date` and `time` indicate when the Proxy Server was installed.
   - **Meeting Server**
     `/QIBM/UserData/Lotus/stii/STMETINGS_date_time/console`
     The `date` and `time` indicate when the Meeting Server was installed.

2. In the console directory, make backup copies with 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 178. 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>SSCHTPPort</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>On IBM i, look for the AboutThisProfile.txt file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></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>

4. Now update the `productConfig.properties` file with the values needed for the server you are registering. Then save the file.

   Required values not listed below are filled in automatically.

   - **Sametime Community Server**
- **DepName**: Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.

**Sametime Proxy Server**
- **WASPassword**: Specify the password associated with the WASUserID.
  If you are registering a primary node, you must specify additional values for the cell where the node will be added:
  - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
  - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

**Sametime Meeting Server**
- **DBAppPassword**: Specify the password associated with the database ID.
- **WASPassword**: Specify the password associated with the WASUserID.
- **LDAPBindPwd**: Specify the password associated with the LDAPBindDN.
  If you are registering a primary node, you must specify additional values for the cell where the node will be added:
  - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
  - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

5. If you are registering a Sametime Community Server, start the server.
   Otherwise, proceed to the next step.

6. From an IBM i command line, run the following command to start the QShell Interpreter:
   ```
   QSH
   ```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:
   - **Sametime Community Server**
     ```
     registerSTServerNode.sh
     ```
     When prompted, specify the following information:
     - Full path to the Sametime Community server data directory where the `notes.ini` file is located.
     - The Community Server Administrator ID and password.
   - **Sametime Proxy Server**
     ```
     registerProduct.sh
     ```
     If registering a primary node, run the following command: `registerProduct.sh -federateNode`
   - **Sametime Meeting Server**
     ```
     registerProduct.sh
     ```
     If registering a primary node, run the following command: `registerProduct.sh -federateNode`

9. When the registration script completes, press **F3** to exit QSH.

*Verifying a Sametime Proxy Server installation for an expanded deployment on IBM i:*

Open the Sametime Web client to verify that the installation was successful.
About this task

Follow these steps to verify the installation.

Procedure

1. Using a browser, log in to the Sametime Proxy Server application with the following command:
   ```
   http://serverhostname.domain:port/stwebclient/index.jsp
   ```
   Replace `serverhostname.domain` with your server name and add the port number.

   Tip: To verify the HTTP port number being used by the 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:
   ```
   /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs/AboutThisProfile.txt
   ```
   For example:
   ```
   http://stproxy1.example.com:9081/stwebclient/index.jsp
   ```

2. Log in to the Sametime Client and verify that you can create or view contacts.

Related tasks

"Logging in to the console" on page 584

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 on IBM i 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.

**Setting up a Sametime Meeting Server for an expanded deployment on IBM i:**

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 the Sametime Meeting Server for an expanded deployment on IBM i:*

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, 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.

**Related tasks**

“**Configuring a Sametime Meeting Server**” on page 1675
This section describes how to configure a Sametime Meeting Server.

*Preparing the Sametime Meeting Server installation file for an expanded deployment on IBM i:*

Follow these steps to customize the response.properties file to prepare for installing the Sametime Meeting Server on IBM i.
Before you begin

You should have completed the preparation steps in "Preparing to install Sametime on IBM i."

About this task

Skip the first two steps if you are installing from physical media.

Procedure

1. Download the installation package if you have not already done so.
   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

2. Extract the installation files to the directory where you stored the installation package.
   a. From an IBM i command line, run the following command to start the QShell Interpreter:
      QSH
   b. Run the following shell command, specifying the fully qualified path to the installation package directory; for example:
      
   c. Run the following shell command, specifying the name of the .zip file:
      ajar -x name_of_installation_package
   d. Press F3 to exit QSH.

3. Review the IBM International Program License Agreement and ensure that you agree to its terms before proceeding. The agreement is stored in the licenses subdirectory of the program image:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms/licenses
   For DVD:
   /qopt/volume_ID/IBMi/stii_stms/licenses

4. Navigate to the program image directory, for example:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   For DVD:
   /qopt/volume_ID/IBMi/stii_stms

5. Make a copy of the stms.default.response.properties file, using a name of your choosing. Store the copy in a location on the system that the installation program can access.

6. Customize your copy of the response.properties file with the settings appropriate for your specific installation.
   - For the stwas.was.admin.id setting, choose a user name for the WebSphere Application Server administrator that does not contain any spaces.
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.

- For the `database.db.user.id` and `database.db.user.password` settings in the properties file, specify the user profile and password you created to be the owner of the Meeting Server database schemas.
- Be sure to change the `silentInstallLicenseAcceptance` setting to `true` to indicate your agreement with the license terms.

There are special considerations if you are planning to install both the Sametime Meeting Server and the Sametime Proxy Server on the same system. You will need to define a separate host name and IP address in addition to the default system host name and IP address. After both servers have been installed, you will be directed to update the Host Alias table for the Sametime Proxy Server so that it does not use the same host name and IP address as the Sametime Meeting Server. This is necessary for live names to work correctly in meeting rooms.

Example

"Default meeting server installation file for IBM i" on page 774

Related tasks

"Preparing to install Sametime on IBM i" on page 642

Follow these steps to prepare IBM i for Sametime server installations.

Creating the Meeting Server database schemas and tables for an expanded deployment on IBM i:

Run the script to create the database schemas for the IBM Sametime Meeting Server on IBM i.

Before you begin

You should have prepared the Meeting Server installation file as described in "Preparing the Meeting Server installation file on IBM i."

About this task

On the IBM i system that will install the Sametime Meeting Server, follow these steps to create the database schema and tables:

Procedure

1. Log in with a user profile that has *ALLOBJ and *SECADM special authorities. These authorities are required to create the database schemas. The database schemas will be created on the system specified in your copy of the stms.default.response.properties file and owned by the user profile specified in the file.
2. From an IBM i command line, run the following command to start the QShell Interpreter:
   
   QSH
3. Run the `cd` shell command, specifying the fully qualified path to the installation kit directory; for example
   
   /MySametimePackages/SametimeMeetingServer/IBM/i/stii_stms
For DVD:

/qopt/volume_ID/IBM/i/stii_stms

4. The POLICY schema is shared by the Meeting Server and the System Console.
   If the POLICY schema already exists, the Meeting Server database setup script
   will only create the MTG schema.
   
   setupDB_stms.sh -Dinstall.response.file=path_and_name_of_custom_response.properties_file

5. When the script completes, press F3 to exit QSH.

Results

If the database schema creation was not successful, look at the script log for more
information about what occurred during the attempt. Fix the problem, then try
running the script again. The script log is stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

stms_dbsetup_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

stms_dbsetup_20091215_0307.log

Related tasks

“Preparing to install Sametime on IBM i” on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Installing a Sametime Meeting Server for an expanded deployment on IBM i:

Run the database schema and install scripts to set up the Sametime Meeting Server
on IBM i.

Before you begin

If you intend to install from a downloaded image, you should have downloaded
the meeting server installation package. For all installations, you should have
completed the preparation steps. The database schemas required for the Meeting
Server (MTG and POLICY) should already exist.

About this task

Follow these steps to install the Sametime Meeting Server and WebSphere
Application Server.

Procedure

1. Log in using a profile with *ALLOBJ and *SECAADM special authorities.
2. Use the WRKSYSVAL command to check the setting for the QVFYOBJRST system
   value and change it if necessary. The setting must be 3 or lower to install the
   Sametime software.
3. From an IBM i command line, run the following command to start the QShell
   Interpreter:
   
   QSH
4. Run the cd shell command, specifying the fully qualified path to the installation kit directory; for example:
   /MySametimePackages/SametimeMeetingServer/IBMi/stii_stms
   For DVD:
   cd /qopt/volume_ID/IBMi/stii_stms
5. Start the Meeting Server installation with the following shell command:
   install_stms.sh -Dinstall.response.file=path_and_name_of_customized_response.properties_file
6. When the script completes, press F3 to exit QSH.

Results

If the installation was not successful, look at the installation logs for more information about what occurred during the installation attempt. Fix the problem, then try installing again. The installation logs are stored in the following location.

/QIBM/UserData/Lotus/stii/logs

The log name contains the date and time in this form:

install_STMEETINGS_yyyymmdd_hhmm.log

For example, this log was created at 3:07 A.M. on December 15, 2009:

install_STMEETINGS_20091215_0307.log

What to do next

If this is the first installation of WebSphere Application Server on this system, follow steps for increasing the WebSphere Application Server usage limit. This task needs to be done only once on a system.

If you have installed both the Sametime Meeting Server and the Sametime Proxy Server on the same system, you must update the table of Host Aliases associated with the Sametime Proxy Server's default_host virtual host so that it does not use the same host name and IP address as the Sametime Meeting Server. Follow the steps in Deploying Sametime Proxy Server and Sametime Meeting Server on the same machine.

Related tasks

"Preparing to install Sametime on IBM i" on page 642
Follow these steps to prepare IBM i for Sametime server installations.

Connecting the Sametime Meeting Server to a DB2 database for an expanded deployment on IBM i:

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 582
When started, the Sametime System Console runs as a task in the WebSphere Application Server administrative console.

Sametime prerequisite: Connecting the Sametime Meeting Server to a DB2 database for an expanded deployment on IBM i:

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**.

**Registering a non-clustered Sametime Meeting Server with the Sametime System Console for an expanded deployment on IBM i:**

After installing a Sametime Community Server, Sametime Proxy Server, or Sametime Meeting server on IBM i, register it with the Sametime System Console to allow you to manage all Sametime servers from a central location. If you are registering a Proxy Server or Meeting Server primary node (PN), you must federate the PN into an existing cell during registration.

**Before you begin**

Before you register the server, verify that you have completed the following tasks.

**Sametime Community Server**

- The community server must be configured to use an LDAP directory.
- The community server must be started.
- The Sametime System Console must be started.
- The LDAP server must be started.
- The LDAP server must be connected to the Sametime System Console.
Sametime Proxy Server
- The Sametime System Console must be started.
- The Community Server that the Proxy Server connects to must be registered with the Sametime System Console.
- When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

Sametime Meeting Server
- The Sametime System Console must be started.
- The LDAP server must be started.
- The LDAP server must be connected to the Sametime System Console.
- The Meeting Server database (STMS) must be connected to the Sametime System Console.
- When you are registering a primary node and adding it to a cell, both the primary node and the deployment manager for the cell must be started.

About this task
Working from the Sametime server that you want to connect with the console, follow these steps to update properties files and run the registration utility to register the server with the console.

During this task you will edit the following files; click the topic titles below to see details on each file. Use Ctrl+Click to open the topic in a new browser tab or window so you can keep it open for reference:
- console.properties
- productConfig.properties

Procedure
1. On the Sametime server you plan to register, navigate to the console directory.
   - Community Server
     The console directory is a subdirectory of the Sametime Community server data directory.
   - Proxy Server
     /QIBM/UserData/Lotus/stii/STPROXY/STPROXY_date_time/console
     The date and time indicate when the Proxy Server was installed.
   - Meeting Server
     /QIBM/UserData/Lotus/stii/STMeetings/STMEETINGS_date_time/console
     The date and time indicate when the Meeting Server was installed.
2. In the console directory, make backup copies with 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 179. console.properties settings

   | SSCHostName     | Provide the fully qualified host name of the Sametime System Console server. |
Table 179. 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; 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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>

4. Now update the productConfig.properties file with the values needed for the server you are registering. Then save the file. Required values not listed below are filled in automatically.

   - **Sametime Community Server**
     - **DepName**: Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.

   - **Sametime Proxy Server**
     - **WASPassword**: Specify the password associated with the WASUserID. If you are registering a primary node, you must specify additional values for the cell where the node will be added:
       - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
       - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

   - **Sametime Meeting Server**
     - **DBAppPassword**: Specify the password associated with the database ID.
     - **WASPassword**: Specify the password associated with the WASUserID.
     - **LDAPBindPwd**: Specify the password associated with the LDAPBindDN. If you are registering a primary node, you must specify additional values for the cell where the node will be added:
       - **WASDMHost**: Specify the fully qualified hostname of the deployment manager for the cell.
       - **WASDMSoapPort**: Specify the soap port of the deployment manager for the cell.

5. If you are registering a Sametime Community Server, start the server. Otherwise, proceed to the next step.
6. From an IBM i command line, run the following command to start the QShell Interpreter:

```
QSH
```

7. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.

8. Run the appropriate shell script to register the server:

   - **Sametime Community Server**
     
     ```
     registerSTServerNode.sh
     ```
     
     When prompted, specify the following information:
     
     - Full path to the Sametime Community server data directory where the `notes.ini` file is located.
     - The Community Server Administrator ID and password.

   - **Sametime Proxy Server**
     
     ```
     registerProduct.sh
     ```
     
     If registering a primary node, run the following command:
     ```
     registerProduct.sh -federateNode
     ```

   - **Sametime Meeting Server**
     
     ```
     registerProduct.sh
     ```
     
     If registering a primary node, run the following command:
     ```
     registerProduct.sh -federateNode
     ```

9. When the registration script completes, press **F3** to exit QSH.

**Verifying a Sametime Meeting Server installation for an expanded deployment on IBM i:**

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_nameSTMProfile1` 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/STAppProfile/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 URL redirects to migrate meetings for an expanded deployment on IBM i:**

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 for an expanded deployment on IBM i:**

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 toolbar, 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>
<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><code>/stconf.nsf/frmConference*</code></td>
<td><code>[http://host_name/stmeetings/*]</code></td>
</tr>
<tr>
<td>Only redirect users that access the Welcome page in the meeting center on the upgraded Sametime server.</td>
<td><code>/stcenter.nsf*</code></td>
<td><code>[http://host_name/stmeetings/*]</code></td>
</tr>
<tr>
<td>Redirect URL that lead directly to individual meetings.</td>
<td><code>/stconf.nsf/meeting/*</code></td>
<td><code>[http://host_name/stmeetings/migration.jsp?mid=*]</code></td>
</tr>
</tbody>
</table>
Table 180. URL redirect options for various user scenarios (continued)

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Incoming URL path</th>
<th>Redirection URL</th>
</tr>
</thead>
<tbody>
<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</td>
<td>/stconf.nsf/</td>
<td>[http://invited_server_host_name/stmeetings/migration.jsp?mid=*]</td>
</tr>
<tr>
<td>document needs to be directed at a single Sametime Meeting Server</td>
<td>WebLookupMeeting?</td>
<td></td>
</tr>
<tr>
<td>where the rooms will be created. This avoids creating additional</td>
<td>OpenAgent&amp;mid=*</td>
<td></td>
</tr>
<tr>
<td>Meeting Servers each time a redirect from the invited server is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>encountered.</td>
<td></td>
<td></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 for an expanded deployment on IBM i:

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 on IBM i:

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.

**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 181. Migrating policy settings

<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>
<tr>
<td>Allow telephony</td>
<td>Media manager</td>
<td>Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings.</td>
</tr>
<tr>
<td>Allow changes to preferred numbers</td>
<td>Media manager</td>
<td>Allow changes to preferred numbers</td>
</tr>
<tr>
<td>Allow changes to the permanent call routing rule</td>
<td>Media manager</td>
<td>Allow changes to the permanent call routing rule</td>
</tr>
<tr>
<td>Allow use of Offline status in call routing rules</td>
<td>Media manager</td>
<td>Allow use of “Offline” status in call routing rules</td>
</tr>
<tr>
<td>Allow user to create instant meetings and breakout sessions</td>
<td>Meetings</td>
<td>Allow user to create instant (nonpersistent) meeting rooms</td>
</tr>
<tr>
<td>Allow Sametime IP audio and video for instant meetings and breakout sessions</td>
<td>Meetings (Sametime Classic Meetings only)</td>
<td>Allow Sametime IP audio and video in instant meetings and breakout sessions</td>
</tr>
<tr>
<td>Allow participation in meeting room chats</td>
<td>Meetings</td>
<td>Meeting room group chats</td>
</tr>
<tr>
<td>Allow screen sharing</td>
<td>Meetings</td>
<td>Allow screen sharing</td>
</tr>
</tbody>
</table>

* 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.
<table>
<thead>
<tr>
<th>Pre-8.5 Setting</th>
<th>New Policy</th>
<th>New Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to control another user's shared screen</td>
<td>Meetings</td>
<td>Allow user to control another user's shared screen</td>
</tr>
<tr>
<td></td>
<td>Meetings (Sametime Classic Meetings only)</td>
<td>Allow user to control another user's shared screen</td>
</tr>
<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 with Audio only selected. If Allow client to client voice call was not 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 Manager server setting.</td>
<td>Sametime System Console &gt; Sametime Servers &gt; Sametime Media Manager &gt; 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 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 Manager setting.</td>
<td>Sametime System Console &gt; Sametime Servers &gt; Sametime Media Manager &gt; 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 images</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>
</tbody>
</table>
Table 181. 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 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>
<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 integrated clients</td>
<td>Instant messaging</td>
<td>Allow all Sametime Connect features to be used with integrated clients</td>
</tr>
</tbody>
</table>

Upgrading from Sametime Gateway 8.0.x and 7.5.1

Upgrade IBM Sametime Gateway and IBM WebSphere Application Server from release 8.0.x or 7.5.1.

Before you begin

You must upgrade the WebSphere Application Server as well as the Sametime Gateway software. IBM DB2 does not require upgrading, but you will need to run scripts that update the database schema.

Upgrade WebSphere Application server and Sametime Gateway by installing them directly over your earlier version. If you have multiple instances of Sametime Gateway installed on a single computer, you must upgrade each instance in turn.

About this task

Sametime Gateway 8.5.1 can upgrade directly only from release 8.5 or release 8.0.2; if you are using an earlier release of the Gateway, you must either upgrade to 8.0.2 or 8.5, or else install release 8.5.1 as a new deployment.

Backing up data: It is recommended that you take a complete snapshot of the environment prior to upgrading (for example, create a ghost image, pull out a mirrored disk (RAID-1) before starting, or creating a VMWare snapshot). If a full backup of this sort is not available, then a rollback from an upgrade failure might not be possible. To help expedite a new fresh install (in case of an unrecoverable upgrade failure) backup the following directories, prior to the upgrade:

- Linux:
  `/opt/IBM/WebSphere`
  `/opt/.ibm/`

- Windows:
  `\Program Files\IBM\WebSphere\`

Preserving certificates: You can preserve your CA certificates that you had signed and used on the old installation as long as you are using the same host name. When upgrading the server, certificates are automatically preserved for you.

Upgrading clusters: When upgrading a cluster, you must know the cluster name when you upgrade the Deployment Manager server. To view the cluster name in
Before you upgrade the product software, you will need to remove the cluster and then remove all nodes from the Deployment Manager. After you have upgraded all instances of the product, you will recreate the cluster.

**Upgrading the DB2 server**
The edition of IBM DB2 that is used in this release of IBM Sametime is not compatible with the edition used in earlier releases, so you should not upgrade the DB2 server used by your Sametime Gateway deployment.

**About this task**
Previous releases of Sametime Gateway used the Enterprise edition of the DB2 database server. This release of Sametime uses the Limited Use edition; you cannot migrate from the Enterprise edition to the Limited Use edition.

If you are upgrading your Sametime Gateway deployment, you should retain your existing DB2 installation for it. The new installation program will upgrade the database schema automatically; when the upgrade is complete, the database will be ready for use.

**Note:** You will still need to install DB2 9.7 Limited Use edition for the Sametime System Console and the Sametime Meeting Server, but an upgraded Sametime Gateway server cannot use it.

**Upgrading Sametime Gateway servers**
Upgrade an existing IBM Sametime Gateway stand-alone or clustered server.

**What to do next**
After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

**Backing up the Sametime Gateway environment:**
IBM recommends that you back up your IBM Sametime Gateway environment before you start the upgrade process.

**About this task**
For each Sametime Gateway server, back up the full file system, so that it can be rolled back in case the upgrade fails. There is no option to backup and rollback specific directories; the whole file system should be backed up. If Sametime Gateway is installed on a Virtual Machine, you can take a snapshot before continuing any farther.

**Upgrading a stand-alone Sametime Gateway server:**
Upgrading a stand-alone IBM Sametime Gateway server requires upgrading the IBM WebSphere Application Server application as well as the Sametime Gateway application. The installation program upgrades both applications to the newest version. After you have finished upgrading the server, you will need to register it with the Sametime System Console so it can be administered from that central location.

About this task

When the installation program installs the newer version of WebSphere Application Server on a computer, it overwrites most of the previous version; however, it leaves the AppServer directory intact and creates a new AppServer7 directory. This is because the original AppServer directory is still needed on an upgraded server, for the following reasons:

- Not all profiles on a server will necessarily be upgraded to Sametime release 8.5, and the AppServer directory is still needed for those profiles that are not being upgraded.
- Of the profiles that are upgraded, the active profile will exist under AppServer7 but there will still be a backup profile under the original AppServer directory.
- Once a server is upgrade to release 8.5, all server administration operations must be performed underneath the AppServer7/profiles/Profile_Name tree.

What to do next

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway:

- Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Configure LDAP for Sametime Gateway (IBM i)
- Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
- Connect servers to Sametime Gateway (IBM i)
- Set up SSL
- Other optional configuration steps

Upgrading all profiles on a Sametime Gateway server:

Upgrading an existing Sametime Gateway server involves upgrading the IBM WebSphere Application Server as well as the IBM Sametime Gateway server for every instance of the product that is installed on the computer.

Upgrading Sametime Gateway on Windows:

Upgrade IBM Sametime Gateway on Microsoft Windows. The installation wizard upgrades both Sametime Gateway and IBM WebSphere Application Server to the latest versions.

Before you begin

Stop all instances of Sametime Gateway and WebSphere Application Server on the current computer.

About this task

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately.
(this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and the latest release of Sametime Gateway.

**Procedure**

1. Create the temporary file folder `\TMP\WASCD`
2. From the installation media, copy the WebSphere Application Server installation image `part_number.exe` to the folder `\TMP\WASCD`.
   Information about downloading packages for Sametime is located at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
3. Open a command window and navigate to the folder `\TMP\WASCD`.
4. Extract all files to the temporary directory `\TMP\WASCD`. When you are done extracting the files, you should have a `\TMP\WASCD\ifpackage` folder with WAS and JDK folders inside the `ifpackage` folder.
5. From the installation media, copy the Sametime Gateway installation image `part_number.exe` to the `\TMP` folder.
6. In the `\TMP` folder, create a subfolder called `SametimeGateway`.
7. Extract the files in `part_number.exe` into the `\TMP\SametimeGateway` folder.
8. Open a command window and type the following command:
   • For wizard mode: `install.bat`
   • For console mode: `install.bat -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   `install.bat -V BypassWasInfoCheck=true`

   Because your input will not be verified during installation, you should take extra care when typing values.
9. Select the language for the installation wizard and click **OK**.
10. At the Welcome screen, click **Next**.
11. Read the Software License Agreement and select the appropriate radio button option to accept the terms; then click **Next**.
12. Select **Upgrade an existing instance of Sametime Gateway**.
13. On the same screen, review the location of the Sametime Gateway instance to upgrade. If the location is correct, click **Next**.

   **Important:** If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.
14. Type or click **Browse** to select the path to where you extracted the WebSphere Application Server installation files from the CD, and click **Next**. Do not use quotation marks. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `C:\TMP\WASCD\ifpackage` but do not use `C:\TMP\WASCD\ifpackage\WAS` or `C:\TMP\WASCD\ifpackage\JDK`.

15. If you are upgrading the Deployment Manager server, type the name of the existing cluster. **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is `RTCGW_Cluster`.

16. Click **Next** to enter database properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server (typically 50000).</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created.</td>
</tr>
<tr>
<td></td>
<td>If you used the default database name, type <code>STGW</code>. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

17. Review the installation summary settings and, if necessary, click **Back** to make changes.

18. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process is in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes. The second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete.

   When the upgrades are complete, the wizard displays a message indicating a successful installation.

19. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be `dmgr` (the deployment manager instance). Then click **Finish**.

   To view the installation log, click **View log file** or open the log file at `stgw_server_root\logs\installlog.txt`. 

---

Chapter 4. Migrating and upgrading 1359
Installing WebSphere iFixes for the upgraded Sametime Gateway server on Windows:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Upgrading Sametime Gateway on AIX, Linux, or Solaris:

Upgrade IBM Sametime Gateway running on IBM AIX, Linux, or Sun Solaris. The installation wizard upgrades both Sametime Gateway and IBM WebSphere Application Server to the latest versions.

Before you begin

Stop all instances of Sametime Gateway and WebSphere Application Server on the current computer.

About this task

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and Sametime Gateway 8.5.

Procedure

1. Create the temporary file folder /TMP/WASCD.
2. From the installation media, copy the WebSphere Application Server installation image for your operating system to /TMP/WASCD.
   Information about downloading packages for Sametime is located at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
3. Open a command window and navigate to the directory /TMP/WASCD.
4. Run the following command to extract the files:
   
   ```
   gunzip -c part_number.tar.gz | tar -xvf -
   ```

   When you are done extracting the files, you should have the following folder:
   `/TMP/WASCD/ifpackage`

   Verify that you have WAS and JDK folders inside the ifpackage folder.

5. From the installation media, copy the Sametime Gateway installation image `part_number.tar` to the temporary directory `/TMP`.

6. In the `/TMP` directory, create a subdirectory called `SametimeGateway`.

7. Extract the following file into the `/TMP/SametimeGateway` directory:
   `unzip part_number.tar`

8. Navigate to the folder `/TMP/SametimeGateway` and type one of the following commands:
   - For wizard mode: `./install.sh`
   - For console mode: `./install.sh -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:

   ```
   ./install.sh -V BypassWasInfoCheck=true
   ```

   Because your input will not be verified during installation, you should take extra care when typing values.

9. Select the language for the installation wizard and click OK. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

10. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click Next to proceed with the installation.

11. Select **Upgrade an existing instance of Sametime Gateway**.

12. On the same panel, review the location of the Sametime Gateway instance to upgrade. If the location is correct, click Next.

   **Important:** If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.

13. Type or click **Browse** to select the path to where you extracted the WebSphere Application Server installation files from the CD.

   This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/NAS` or `/TMP/WASCD/ifpackage/JDK`. 

   "Chapter 4. Migrating and upgrading 1361"
14. If you are upgrading the Deployment Manager server, type the name of the existing cluster. **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters.** The default cluster name is `SametimeGatewayCluster`.

15. Click **Next** to verify the database properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server (typically 50001).</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created.</td>
</tr>
<tr>
<td></td>
<td>If you used the default database name, type <code>STGW</code>. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

16. Review the installation summary settings and, if necessary, click **Back** to make changes.

17. Click **Install** to begin copying files.

A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process is in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes. The second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete.

When the upgrades are complete, the wizard displays a message indicating a successful installation.

18. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be ‘dmgr’ (the deployment manager instance). Then click **Finish**.

To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`.

*Installing WebSphere iFixes for the upgraded Sametime Gateway server on AIX, Linux, or Solaris:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.
About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Upgrading a Sametime Gateway server on IBM i:

Upgrading an IBM Sametime Gateway server on IBM i is a two-step process. First you must upgrade the previous version of IBM WebSphere Application Server, and then you upgrade Sametime Gateway on the same computer.

Upgrading WebSphere Application Server on IBM i:

Upgrade IBM WebSphere Application Server on IBM i before you upgrade IBM Sametime Gateway. The installation wizard upgrades WebSphere Application Server to the latest version.

Before you begin

Stop all instances of Sametime Gateway and WebSphere Application Server on the current computer.

You must have *ALLOBJ and *SECADM authorities to successfully complete the upgrade.

About this task

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and Sametime Gateway 8.5.

Procedure

1. Create the temporary file folder /TMP/WASCD on a computer that can connect to the IBM i system.
2. Copy the file part_number.zip to the temporary folder /TMP/WASCD.
Information on downloading packages for Sametime is located at the following web address:
https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

3. Open a command window and navigate to the folder /TMP/WASCD.
4. Extract all files to the temporary directory /TMP/WASCD. When you are done extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS and JDK folders inside the ifpackage folder.
5. Copy the ifpackage folder to the IFS of the IBM i system.
6. In the folder you copied to the IFS of the IBM i system, edit the file ifpackage/WAS/responsefile.nd.txt
7. Accept the license to install. Read the comments in the file regarding License Acceptance and then set the value of silentInstallLicenseAcceptance to true. For example:
   -OPT silentInstallLicenseAcceptance="true"
8. Set the option installType to installAndPatch. For example:
   -OPT installType="installAndPatch"
9. Set the option installLocation to the location of the WebSphere Application Server to be updated. For example:
   -OPT installLocation="/QIBM/ProdData/WebSphere/AppServer/V61/ND"
10. Save the file.
11. Start a QSHELL session.
12. Before running the install to update the product, the classes directory from the installation location must be removed. You can do this by issuing a move (mv) command.
   /QIBM/ProdData/WebSphere/AppServer/V61/ND/classes /tmp/was_classes
13. Navigate to the ifpackage/WAS directory.
14. Run the following command:
   install -options responsefile.nd.txt
15. When the installation is successful, you will see a message such as this:
   install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS

Installing WebSphere iFixes for the upgraded Sametime Gateway server on IBM i:

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

**Upgrading Sametime Gateway on IBM i:**

Upgrade IBM Sametime Gateway on an IBM i server. The installation wizard upgrades Sametime Gateway to the latest version.

**Before you begin**

Upgrade IBM WebSphere Application Server on this computer before attempting to upgrade Sametime Gateway.

Stop all instances of Sametime Gateway on the current computer.

You must have *ALLOBJ and *SECADM authorities to successfully complete the upgrade.

**About this task**

IBM i allows multiple instances of Sametime Gateway to be installed on a single IBM i system. If a Sametime Gateway server is running while you install a new Sametime Gateway server, the running server must be restarted before you can use the Integrated Solutions Console to administer Sametime Gateway.

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and Sametime Gateway 8.5.

**Procedure**

1. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as /TMP.
   
   Information on downloading packages for Sametime is located at the following web address:
   
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

2. In the /TMP directory, create a subdirectory called SametimeGateway.

3. Extract the contents of part_number.exe to the /TMP/SametimeGateway directory.


5. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

**Important:** If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.
To run the installer in wizard mode, type the following command:

`installi5OS.bat`

To run the installer in console mode, perform these steps:

a. Copy the directory `/TMP/SametimeGateway` to the IFS of the IBM i system.
b. Start a QSHELL session.
c. Navigate to the `/TMP/SametimeGateway` directory and type the following command:

```
install.sh -console
```

**Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:

```
install.sh -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

6. Select the language for the installation and click **OK**. The Sametime Gateway Welcome screen is displayed. If you are installing in wizard mode, you can launch the Sametime Information Center from this panel. Click **Next** to continue with the installation.

7. Click **Next** to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click **Next** to proceed with the installation.

8. Select **Upgrade an existing instance of Sametime Gateway**. The installation wizard displays the location of the installed Sametime Gateway server on this machine. Change the location of the existing Sametime Gateway server to the `stgw_server_root` of the server you’d like to upgrade, if necessary, then click **Next**.

**Important:** If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.

9. If you are upgrading the Deployment Manager server, type the name of the cluster to which Sametime Gateway belongs.

**Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is `RTCGW_Cluster`.

10. Click **Next** to enter database properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: <code>server1.example.com</code></td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, <code>STGW</code>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

11. Review the installation summary settings and, if necessary, click **Back** to make changes.

12. Click **Install** to begin copying files. A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This upgrade takes about 10 to 20 minutes to complete. When the upgrade is complete, the wizard displays a message indicating a successful installation.

13. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be ‘dmgr’ (the deployment manager instance). Then click **Finish**.

   To view the installation log, open the log file at `stgw_server_root\logs\installlog.txt`.

*Registering the upgraded server with the Sametime System Console:*

After you have upgraded an IBM Sametime Gateway server, you must register it with the Sametime System Console so you can administer the Gateway from the console.

*Registering an upgraded Sametime Gateway server with the System Console:*

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

**Before you begin**

Before you register the server, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
• The Gateway database must be connected to the System Console and must be started.
• The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the server that you want to connect to the console, follow these steps to update properties files and run the registration utility.

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 the topic in a new browser tab or window so you can keep it open for reference:
• console.properties
• productConfig.properties

Procedure

1. On the Sametime Gateway server, navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.
2. In the console directory, make backup copies (using different names) of the console.properties and productConfig.properties files.
3. Update the console.properties file with the following values, and then save and close the file.

<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 path is: 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>

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 183. productConfig.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;Cell&quot; as the installation type since this is a non-clustered server.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

5. Set the application server path in the registration utility:
   a. Navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory and open a command window.
   b. Open the registration utility file for editing.
      AIX, Linux, Solaris
      registerProduct.sh
      Windows
      registerProduct.bat
   c. Locate the following statement:
      SET PATH=../../WebSphere/AppServer/java/bin
   d. Change it to reflect IBM WebSphere Application Server version 7:
      SET PATH=../../WebSphere/AppServer7/java/bin
   e. Save and close the file.

6. Run the registration utility.
   AIX, Linux, Solaris
   • Already registered
     registerProduct.sh -upgrade
   • First-time registration
     • registerProduct.sh
Windows
• Already registered
  registerProduct.bat -upgrade
• First-time registration
  registerProduct.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 also be generated.

7. Start the Sametime Gateway server, if it is not already running.

Registering an upgraded Gateway server on IBM i with the System Console:

After upgrading an IBM Sametime Gateway server on IBM i, you must register it again with the Sametime System Console, which allows you to manage all Sametime servers from a central location.

Before you begin

Before you register the server, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.
• The Gateway server must be registered with the Sametime System Console.
• The Sametime System Console must be started.
• The LDAP server must be connected to the System Console and must be started.
• The Gateway database must be connected to the System Console and must be started.
• The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the server that you want to connect with the console, follow these steps to update properties files and run the registration utility.

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 the topic in a new browser tab or window so you can keep it open for reference:
• console.properties
• productConfig.properties

Procedure
1. Working on the Sametime Gateway server, navigate to the
   /qibm/userdata/STGateway/ProfileName/console directory.
   The ProfileName is the one you specified when you installed the Gateway.
2. In the console directory, make backup copies (using different names) of the
   console.properties and productConfig.properties files.
3. Update the console.properties file with the following values, and then save
   and close the file.

| SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
Table 184. 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>On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>SSCCSSLEnabled</td>
<td>Change this value to “true” to connect to the Sametime System Console using a secure connection. <strong>Note:</strong> If the Sametime System Console was installed using a host name that is different from the system host name, make sure this value is set to “false.” Otherwise the registration will fail.</td>
</tr>
<tr>
<td>SSCHTTPSPort</td>
<td>Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to “true.”</td>
</tr>
</tbody>
</table>

4. Update the productConfig.properties file with the following values, and then save and close the file.

Only the required values in this file are listed here:

Table 185. productConfig.properties settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;Cell&quot; as the installation type since this is a non-clustered server.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 185. `productConfig.properties` settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to <code>true</code> for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

5. Now run the `registerProduct.sh` registration utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: `QSH`
   b. Run the `cd` shell command, specifying the fully qualified path to the console directory you used in Step 1.
   c. Run the shell script to register the server: `registerProduct.sh`
   d. When the registration script completes, press `F3` to exit QSH.
      The utility registers the server, generating a log file called `ConsoleUtility.log` and storing it in the `consoles/logs` directory. If the registration is successful, a `console.pid` will also be generated.

6. Start Sametime Gateway server, if it is not already running.

Upgrading a cluster of Sametime Gateway servers:

Upgrading a cluster of IBM Sametime Gateway server requires you to remove all nodes from the cluster before upgrading each instance of the Sametime Gateway server on every node. The installation program upgrades the IBM WebSphere Application Server and the Sametime Gateway applications to the newest version. After you have finished upgrading the nodes, you will need to recreate the cluster by federating the nodes to the Deployment Manager. Finally, you will register the cluster with the Sametime System Console so it can be administered from that central location.

About this task

When the installation program installs the newer version of WebSphere Application Server on a node, it overwrites most of the previous version; however, it leaves the `AppServer` directory intact and creates a new `AppServer7` directory. This is because the original `AppServer` directory is still needed on an upgraded server, for the following reasons:

- Not all profiles on a server will necessarily be upgraded to Sametime release 8.5, and the `AppServer` directory is still needed for those profiles that are not being upgraded.
- Of the profiles that are upgraded, the active profile will exist under `AppServer7` (on IBM i, `AppServer/V7`), but there will still be a backup profile under the original `AppServer` directory.
- Once a server is upgrade to release 8.5, all server administration operations must be performed underneath the `AppServer7/profiles/Profile_Name` tree (on IBM i, the `AppServer/V7/profiles/Profile_Name` tree).

Make sure you upgrade the following servers in your cluster:
• Deployment Manager
• Primary Node
• Secondary Node (release 8.5 supports only one Secondary Node in a Sametime Gateway cluster)
• SIP proxy server
• XMPP proxy server

What to do next

After upgrading, you can perform other required and optional configuration tasks for Sametime Gateway.
• Configure LDAP for Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Configure LDAP for Sametime Gateway (IBM i)
• Connect servers to Sametime Gateway (AIX, Linux, Solaris, and Windows)
• Connect servers to Sametime Gateway (IBM i)
• Set up SSL
• Other optional configuration steps

Removing the Sametime Gateway nodes from the cluster:

Before you can upgrade the instances of IBM Sametime Gateway in a clustered deployment, you must remove the nodes from the cluster. IBM WebSphere is installed during the product upgrade, but it cannot be upgraded on a node that is federated to the cluster’s Deployment Manager. After you complete the upgrade for every node in the cluster, you will by federate the nodes to the Deployment Manager.

About this task

Removing nodes from the Sametime Gateway cluster involves manually removing the nodes in the Deployment Manager’s Integrated Solutions Console settings, and then running a utility that updates additional settings for you.

Procedure
1. Log in to the Deployment Manager’s Integrated Solutions Console as the IBM WebSphere administrator.
2. Stop the cluster that you want to upgrade:
   Because the SIP proxy server and the XMPP proxy server function as part of the cluster, you need to stop them as well.
   a. Click Servers > Clusters.
   b. In the clusters table, click the check box next to the cluster’s name, and then click the Stop button at the top of the table.
      Wait for the cluster’s status to update before proceeding.
   c. Now click Servers > Proxy servers.
   d. In the proxy servers table, click the check box next to the SIP proxy server associated with the cluster, and then click the Stop button at the top of the table.
   e. Finally, click Servers > Application servers.
   f. In the application servers table, click the check box next to the XMPP proxy server associated with the cluster, and then click the Stop button at the top of the table.
3. Now uninstall all Sametime Gateway Enterprise Applications:
   a. Click **Applications > Application Types > Enterprise applications**.
   b. In the applications table, click the check box for every Sametime Gateway application, and click **Uninstall**.

   **Important**: Do not delete the ivtApp and query applications.
   c. Click OK.
   d. Save the change by clicking **Save** in the Messages’ box at the top of the page.

4. Now remove nodes:
5. Still working on the Deployment Manager, click **System administration > Nodes**.
6. On the Nodes page, select the check box beside each node that you want to remove.
   If you are upgrading, remove all nodes. The nodes can only be uninstalled one at a time. The Deployment Manager node cannot be removed.
7. At the top of the table, click the **Remove Node** button.
   If you cannot remove the nodes by clicking Remove Node, remove the node from the configuration by clicking **Force Delete**.
8. Type the Deployment Manager user name and password, and click **OK**.
9. Save your change by clicking the **Save** link in the "Messages" box at the top of the page.

**Upgrading all profiles on a Sametime Gateway node:**

Upgrading an existing Sametime Gateway server involves upgrading the IBM WebSphere Application Server as well as the IBM Sametime Gateway server for every instance of the product that is installed on the computer.

**Upgrading a Sametime Gateway node on Windows:**

Upgrade IBM Sametime Gateway on Microsoft Windows. The installation wizard upgrades both Sametime Gateway and IBM WebSphere Application Server to the latest versions.

**Before you begin**

Stop all instances of Sametime Gateway and WebSphere Application Server on the current computer.

**About this task**

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and the latest release of Sametime Gateway.
Procedure

1. Create the temporary file folder `\TMP\WASCD`.
2. From the installation media, copy the WebSphere Application Server installation image `part_number.exe` to the folder `\TMP\WASCD`.
   Information about downloading packages for Sametime is located at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
3. Open a command window and navigate to the folder `\TMP\WASCD`.
4. Extract all files to the temporary directory `\TMP\WASCD`. When you are done extracting the files, you should have a `\TMP\WASCD\ifpackage` folder with WAS and JDK folders inside the `ifpackage` folder.
5. From the installation media, copy the Sametime Gateway installation image `part_number.exe` to the `\TMP` folder.
6. In the `\TMP` folder, create a subfolder called `SametimeGateway`.
7. Extract the files in `part_number.exe` into the `\TMP\SametimeGateway` folder.
8. Open a command window and type the following command:
   - For wizard mode: `install.bat`
   - For console mode: `install.bat -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   `install.bat -V BypassWasInfoCheck=true`

   Because your input will not be verified during installation, you should take extra care when typing values.
9. Select the language for the installation wizard and click **OK**.
10. At the Welcome screen, click **Next**.
11. Read the Software License Agreement and select the appropriate radio button option to accept the terms; then click **Next**.
12. Select **Upgrade an existing instance of Sametime Gateway**.
13. On the same screen, review the location of the Sametime Gateway instance to upgrade. If the location is correct, click **Next**.

   **Important:** If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.
14. Type or click **Browse** to select the path to where you extracted the WebSphere Application Server installation files from the CD, and click **Next**.
   Do not use quotation marks. This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `C:\TMP\WASCD\ifpackage` but do not use `C:\TMP\WASCD\ifpackage\WAS` or `C:\TMP\WASCD\ifpackage\JDK`.
15. If you are upgrading the Deployment Manager server, type the name of the existing cluster. **Tip:** To obtain the cluster name from the Integrated Solutions Console, click **Servers > Clusters**. The default cluster name is `RTCWW_Cluster`.
16. Click **Next** to enter database properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server (typically 50000).</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

17. Review the installation summary settings and, if necessary, click **Back** to make changes.

18. Click **Install** to begin copying files.

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process is in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes. The second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete.

   When the upgrades are complete, the wizard displays a message indicating a successful installation.

19. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be ‘dmgr’ (the deployment manager instance). Then click **Finish**.

   To view the installation log, click **View log file** or open the log file at `stgw_server_root\logs\installlog.txt`.

*Installing WebSphere iFixes for the Sametime Gateway node on Windows:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.
Procedure
1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3 iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in Installing WebSphere Application Server updates.

Upgrading a Sametime Gateway node on AIX, Linux, or Solaris:

Upgrade IBM Sametime Gateway running on IBM AIX, Linux, or Sun Solaris. The installation wizard upgrades both Sametime Gateway and IBM WebSphere Application Server to the latest versions.

Before you begin

Stop all instances of Sametime Gateway and WebSphere Application Server on the current computer.

About this task

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster's Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile's install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and Sametime Gateway 8.5.

Procedure
1. Create the temporary file folder /TMP/WASCD.
2. From the installation media, copy the WebSphere Application Server installation image for your operating system to /TMP/WASCD.
   Information about downloading packages for Sametime is located at the following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
3. Open a command window and navigate to the directory /TMP/WASCD.
4. Run the following command to extract the files:
   gunzip -c part_number.tar.gz | tar -xvf -
   When you are done extracting the files, you should have the following folder:
   /TMP/WASCD/IFpackage
   Verify that you have WAS and JDK folders inside the IFpackage folder.
5. From the installation media, copy the Sametime Gateway installation image part_number.tar to the temporary directory /TMP.
6. In the /TMP directory, create a subdirectory called SametimeGateway.

7. Extract the following file into the /TMP/SametimeGateway directory:
   `unzip part_number.tar`

8. Navigate to the folder /TMP/SametimeGateway and type one of the following commands:
   - For wizard mode: `.install.sh`
   - For console mode: `.install.sh -console`

   **Attention:** If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6-format address, add the following option to your install command to work around an IPv6-related issue with the installer:
   `./install.sh -V BypassWasInfoCheck=true`

   Because your input will not be verified during installation, you should take extra care when typing values.

9. Select the language for the installation wizard and click OK. The Sametime Gateway Welcome screen is displayed. You can launch the Sametime information center from this panel.

10. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Read the license agreement carefully. Select the appropriate radio button option to accept the terms if you agree with the statement and click Next to proceed with the installation.

11. Select Upgrade an existing instance of Sametime Gateway.

12. On the same panel, review the location of the Sametime Gateway instance to upgrade. If the location is correct, click Next.

   **Important:** If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.

13. Type or click Browse to select the path to where you extracted the WebSphere Application Server installation files from the CD.

   This directory should contain the WAS and JDK subdirectories. It is very important that you select the parent directory and not the subdirectory. For example: use `/TMP/WASCD/ifpackage` but do not use `/TMP/WASCD/ifpackage/WAS` or `/TMP/WASCD/ifpackage/JDK`.

14. If you are upgrading the Deployment Manager server, type the name of the existing cluster. **Tip:** To obtain the cluster name from the Integrated Solutions Console, click Servers > Clusters. The default cluster name is SametimeGatewayCluster.

15. Click Next to verify the database properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>The Fully qualified host name or TCP/IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the database server (typically 50001).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database that you created. If you used the default database name, type STGW. Case does not matter.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

16. Review the installation summary settings and, if necessary, click **Back** to make changes.

17. Click **Install** to begin copying files.
   
   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. The upgrade process is in two stages. The first stage upgrades Sametime Gateway and takes 5 to 20 minutes. The second stage upgrades WebSphere Application Server and takes another 15 to 20 minutes to complete.
   
   When the upgrades are complete, the wizard displays a message indicating a successful installation.

18. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be 'dmgr' (the deployment manager instance). Then click **Finish**.
   
   To view the installation log, click **View log file** or open the log file at `stgw_server_root/logs/installlog.txt`.

*Installing WebSphere iFixes for the Sametime Gateway node on AIX, Linux, or Solaris:*

Install required IBM WebSphere Application Server updates on the IBM Lotus Gateway server.

**About this task**

After you install or upgrade the Sametime Gateway, add the WebSphere Application Server updates, which are included in the product package.

**Procedure**

1. Download the package containing the WebSphere iFixes to the Sametime Gateway server.
The iFixes are included in the following package: IBM WebSphere V7.0.0.3
iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
Multilingual.

2. Install the WebSphere Update Installer as described in Installing the WebSphere
Application Server Update Installer.

3. Use the WebSphere Update Installer to install the iFixes as described in
Installing WebSphere Application Server updates.

**Upgrading a Sametime Gateway node on IBM i:**

Upgrading an IBM Sametime Gateway server on IBM i is a two-step process. First
you must upgrade the previous version of IBM WebSphere Application Server, and
then you upgrade Sametime Gateway on the same computer.

**Upgrading WebSphere Application Server on an IBM i Sametime Gateway node:**

Upgrade IBM WebSphere Application Server on IBM i before you upgrade IBM
Sametime Gateway. The installation wizard upgrades WebSphere Application
Server to the latest version.

**Before you begin**

Stop all instances of Sametime Gateway and WebSphere Application Server on the
current computer.

You must have *ALLOBJ and *SECADM authorities to successfully complete the
upgrade.

**About this task**

Upgrade all Sametime Gateway instances in your deployment. If a server has
multiple instances of the Gateway, you must upgrade every instance separately
(this is likely to be the case when you upgrade a cluster). Each upgrade will
require you to run the Gateway installation program again, specifying the target
instance to be upgraded during each run. Note that the server hosting a cluster's
Deployment Manager also hosts the Primary Node; it is important to make sure
you upgrade the Deployment Manager first; then when you upgrade the Primary
Node, you specify that profile's install path instead.

When you are finished upgrading, your server will contain WebSphere Application
Server Network Deployment 7 and Sametime Gateway 8.5.

**Procedure**

1. Create the temporary file folder /TMP/WASCD on a computer that can connect to
the IBM i system.

2. Copy the file part_number.zip to the temporary folder /TMP/WASCD.
   Information on downloading packages for Sametime is located at the
   following web address:
   https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128

3. Open a command window and navigate to the folder /TMP/WASCD.

4. Extract all files to the temporary directory /TMP/WASCD. When you are done
   extracting the files, you should have a /TMP/WASCD/ifpackage folder with WAS
   and JDK folders inside the ifpackage folder.

5. Copy the ifpackage folder to the IFS of the IBM i system.
6. In the folder you copied to the IFS of the IBM i system, edit the file
   ifpackage/WAS/responsefile.nd.txt
7. Accept the license to install. Read the comments in the file regarding License
   Acceptance and then set the value of silentInstallLicenseAcceptance to true.
   For example:
   
   -OPT silentInstallLicenseAcceptance="true"
8. Set the option installType to installAndPatch. For example:
   -OPT installType="installAndPatch"
9. Set the option installLocation to the location of the WebSphere Application
   Server to be updated. For example:
   -OPT installLocation="/QIBM/ProdData/WebSphere/AppServer/V61/ND"
10. Save the file.
11. Start a QSHELL session.
12. Before running the install to update the product, the classes directory from the
    installation location must be removed. You can do this by issuing a move (mv)
    command.
    
    /QIBM/ProdData/WebSphere/AppServer/V61/ND/classes /tmp/was_classes
13. Navigate to the ifpackage/WAS directory.
14. Run the following command:
    install -options responsefile.nd.txt
15. When the installation is successful, you will see a message such as this:
    
    ISMPLogSuccessMessageAction, msg1, INSTCONFSUCCESS.

Installing WebSphere iFixes for the Sametime Gateway node on IBM i:

Install required IBM WebSphere Application Server updates on the IBM Lotus
Gateway server.

About this task

After you install or upgrade the Sametime Gateway, add the WebSphere
Application Server updates, which are included in the product package.

Procedure

1. Download the package containing the WebSphere iFixes to the Sametime
   Gateway server.
   The iFixes are included in the following package: IBM WebSphere V7.0.0.3
   iFixes for Sametime V8.5.1 Windows, AIX, Linux x86, zLinux, Solaris, IBM i
   Multilingual.
2. Install the WebSphere Update Installer as described in Installing the WebSphere
   Application Server Update Installer.
3. Use the WebSphere Update Installer to install the iFixes as described in
   Installing WebSphere Application Server updates.

Upgrading the Sametime Gateway application on IBM i:

Upgrade IBM Sametime Gateway on an IBM i server. The installation wizard
upgrades Sametime Gateway to the latest version.
Before you begin

Upgrade IBM WebSphere Application Server on this computer before attempting to upgrade Sametime Gateway.

Stop all instances of Sametime Gateway on the current computer.

You must have *ALLOBJ and *SECADM authorities to successfully complete the upgrade.

About this task

IBM i allows multiple instances of Sametime Gateway to be installed on a single IBM i system. If a Sametime Gateway server is running while you install a new Sametime Gateway server, the running server must be restarted before you can use the Integrated Solutions Console to administer Sametime Gateway.

Upgrade all Sametime Gateway instances in your deployment. If a server has multiple instances of the Gateway, you must upgrade every instance separately (this is likely to be the case when you upgrade a cluster). Each upgrade will require you to run the Gateway installation program again, specifying the target instance to be upgraded during each run. Note that the server hosting a cluster’s Deployment Manager also hosts the Primary Node; it is important to make sure you upgrade the Deployment Manager first; then when you upgrade the Primary Node, you specify that profile’s install path instead.

When you are finished upgrading, your server will contain WebSphere Application Server Network Deployment 7 and Sametime Gateway 8.5.

Procedure

1. From the installation media, copy the Sametime Gateway installation image (part_number.exe) to a temporary directory such as /TMP.
   Information on downloading packages for Sametime is located at the following web address: https://www-304.ibm.com/support/docview.wss?rs=477&uid=swg24029128
2. In the /TMP directory, create a subdirectory called SametimeGateway.
3. Extract the contents of part_number.exe to the /TMP/SametimeGateway directory.
5. You can run the installer in wizard mode or in console mode. Use the wizard mode if you are installing from a PC to the IBM i system.

   Important: If you are installing on an IPv6–enabled server, you must use the second option below to install using the console.
   • To run the installer in wizard mode, type the following command:
     installi5OS.bat
   • To run the installer in console mode, perform these steps:
     a. Copy the directory /TMP/SametimeGateway to the IFS of the IBM i system.
     b. Start a QSHELL session.
     c. Navigate to the /TMP/SametimeGateway directory and type the following command:
        install.sh -console
Attention: If one or more of the DNS addresses in your environment (for example: WebSphere Application Server installation host name, DB2 host name, or LDAP host name) refers to an IPv6–format address, add the following option to your install command to work around an IPv6–related issue with the installer:

```
install.sh -V BypassWasInfoCheck=true
```

Because your input will not be verified during installation, you should take extra care when typing values.

6. Select the language for the installation and click OK. The Sametime Gateway Welcome screen is displayed. If you are installing in wizard mode, you can launch the Sametime Information Center from this panel. Click Next to continue with the installation.

7. Click Next to continue with the installation. The Software License Agreement dialog is displayed. Please make sure to read the license agreement carefully. Select the appropriate radio button option to accept the license agreement if you agree with the statement and click Next to proceed with the installation.

8. Select Upgrade an existing instance of Sametime Gateway. The installation wizard displays the location of the installed Sametime Gateway server on this machine. Change the location of the existing Sametime Gateway server to the stgw_server_root of the server you’d like to upgrade, if necessary, then click Next.

Important: If you are upgrading a server that contains the Deployment Manager and the Primary Node for a cluster, you must upgrade the Deployment Manager first. Note that the installer default instance path may not be the deployment manager instance and may point to STgatewayPrimary node instead of STgateway node. If that is the case, change the path to be correct for the original installation.

9. If you are upgrading the Deployment Manager server, type the name of the cluster to which Sametime Gateway belongs.

Tip: To obtain the cluster name from the Integrated Solutions Console, click Servers > Clusters. The default cluster name is RTCGW_Cluster.

10. Click Next to enter database properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Fully qualified domain name of the machine on which you are installing WebSphere Application Server. For example: server1.example.com</td>
</tr>
<tr>
<td>Schema name</td>
<td>The name of the schema you created when preparing the Sametime Gateway environment. For example, STGW.</td>
</tr>
<tr>
<td>Application user ID</td>
<td>A database user ID that has permission to connect to the database and read or write records. The application user ID is often the same as the schema owner user ID.</td>
</tr>
<tr>
<td>Application password</td>
<td>The password for the application user. The application password is often the same as the schema owner password.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Schema user ID</td>
<td>The ID for the user that has appropriate permissions to create tables in the database. You may need to get this information from the database administrator. The schema user ID is often the same as the application user ID.</td>
</tr>
<tr>
<td>Schema password</td>
<td>The password for the schema owner. You may need to get this information from the database administrator. The schema password is often the same as the application password.</td>
</tr>
</tbody>
</table>

11. Review the installation summary settings and, if necessary, click **Back** to make changes.

12. Click **Install** to begin copying files.

   A progress screen is displayed and the activity is logged to the Sametime Gateway log file. This upgrade takes about 10 to 20 minutes to complete. When the upgrade is complete, the wizard displays a message indicating a successful installation.

13. Read the summary and verify that the server name is correct. In a cluster where you are upgrading the first instance, the server name MUST be 'dmgr' (the deployment manager instance). Then click **Finish**.

   To view the installation log, open the log file at `stgw_server_root\logs\installlog.txt`.

**Re-installing the Gateway administration portlet:**

During the Deployment Manager upgrade process, the IBM Sametime Gateway administration portlet is removed and must be manually re-installed. This task is needed only if your configuration includes a Deployment Manager, SIP, and XMPP proxy servers on the same operating system; otherwise, skip this task.

**Re-installing the Gateway administration portlet on the Deployment Manager:**

During the Deployment Manager upgrade process, the IBM Sametime Gateway administration portlet is removed and must be manually re-installed. This task is needed only if your configuration includes a Deployment Manager, a SIP proxy server, and an XMPP proxy server installed on the same computer; otherwise, skip this task.

**Before you begin**

Upgrade the Deployment Manager, the Primary node, the Secondary node, the SIP proxy server, and the XMPP server.

**About this task**

During the Deployment Manager upgrade process, the Sametime Gateway administration portlet is removed. Complete these steps on the Deployment Manager to re-install the portlet:
Procedure
1. Log in to the Deployment Manager's Integrated Solutions Console as the IBM WebSphere administrator.
2. Open the wsadmin console:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile/bin`.
      where `app_server_root` is the root directory for the creation of WebSphere Application Server profile directories.
   b. Run the `wsadmin` file to open the console:
      - **Windows**: `wsadmin.bat -conntype NONE`
      - **AIX, Linux, Solaris**: `./wsadmin.sh -conntype NONE`
3. In the wsadmin console, execute the following commands:
   $AdminApp update isclite modulefile {-operation delete -contenturi RTCAdminPortlet.war}
   $AdminConfig save
   quit
4. Delete the following file/directory: `was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war`
5. Now copy a file to replace the one you just deleted:
   Copy this file from the installation image:
   `../setup/installableApps/RTCAdminPortlet.war`
   and paste it in:
   `was_install_root/systemApps/isclite.ear/`
6. Open the wsadmin console again:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile/bin`.
   b. Run the `wsadmin` file to open the console:
      - **Windows**: `wsadmin.bat -conntype NONE`
      - **AIX, Linux, Solaris**: `./wsadmin.sh -conntype NONE`
7. In the wsadmin console, execute the following commands.

   **Note**: Type the command as one continuous line.

   $AdminApp update isclite modulefile {-operation add -contents "was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war" -contenturi RTCAdminPortlet.war -usedefaultbindings -server dmgr -preCompileJSPs -contextroot /ibm/RTCGW -MapWebModToVH {{.* .* admin_host}}}
   $AdminConfig save
   quit
   where `app_server_root` is the absolute path to the WebSphere Application Server install directory.
8. Restart the Deployment Manager.

*Re-installing the Gateway administration portlet on the Deployment Manager on IBM i:*

During the Deployment Manager upgrade process, the IBM Sametime Gateway administration portlet is removed and must be manually reinstalled. This task is needed only if your configuration includes a Deployment Manager, a SIP proxy server, and an XMPP proxy server installed on the same computer; otherwise, skip this task.
Before you begin

Upgrade the Deployment Manager, the Primary Node, the Secondary node, the SIP proxy server, and the XMPP server.

About this task

During the Deployment Manager upgrade process, the Sametime Gateway administration portlet is removed. Complete these steps on the Deployment Manager to re-install the portlet.

Procedure

1. Log in to the Deployment Manager’s Integrated Solutions Console as the IBM WebSphere administrator.
2. Start a QSHELL session.
3. Open the wsadmin console:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile`.
   b. Run the `wsadmin` file to open the console: `wsadmin.sh -conntype NONE`
4. In the wsadmin console, execute the following commands:
   ```
   $AdminApp update isclite modulefile {-operation delete -contenturi RTCAdminPortlet.war}
   $AdminConfig save
   quit
   ```
5. Now delete the following file: `was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war`
6. Now copy a file to replace the one you just deleted:
   Copy this file:
   ```
   app_server_root/profiles/RTCGW_Profile/installableApps/RTCAdminPortlet.war
   ```
   and paste it in:
   `was_install_root/systemApps/isclite.ear/`
7. Open the wsadmin console again:
   a. Navigate to the following directory: `app_server_root/profiles/DMProfile`.
   b. Run the wsadmin file to open the console: `wsadmin.sh -conntype NONE`
8. In the wsadmin console, execute the following commands ($AdminApp should be on one line. It has been formatted to fit this page.):
   ```
   $AdminApp update isclite modulefile {-operation add -contents "was_install_root/systemApps/isclite.ear/RTCAdminPortlet.war" -contenturi RTCAdminPortlet.war -usedefaultbindings -server dmgr -preCompileJSPs -contextroot /ibm/RTCGW -MapWebModToVH {{.* .* admin_host}}}
   $AdminConfig save
   quit
   ```
   where `was_install_root` is the absolute path to the WebSphere Application Server install directory.
9. Restart the Deployment Manager.

Federating the primary node into the cell after upgrading:

After you create the primary node you must add the primary node to the Deployment Manager’s cell.
Federating the primary node into the cell after upgrading on Windows:

Add the primary node to the Deployment Manager’s cell. Adding the primary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager’s Integrated Solutions Console. You will not be able log into the primary node’s Integrated Solutions Console after this step.

Before you begin

Expected state: the Deployment Manager is running.

About this task

Procedure

1. Make sure that the system clocks on the Deployment Manager and the primary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the primary node to make sure the host name is resolvable.
3. On the primary node, open a command window and navigate to the stgw_profile_root\bin directory. If the Deployment Manager and the primary node are installed on the same machine, the default profile directory is RTCGW_Profile1 (not RTCGW_Profile).
4. Run the following command to add the primary node to the Deployment Manager’s cell:
   
   addNode.bat DM_hostname DM_port_number -includeapps
   
   Where DM_hostname is the host name of the Deployment Manager server. For example:
   
   addNode.bat gateway_dm.example.com 8879 -includeapps
   
   Port 8879 is the default port on which the Deployment Manager listens.

   Note: If you are upgrading the server, the Deployment Manager, the default port on which the Deployment Manager listens changes after the upgrade. The list of default ports can be found under stgw_profile_root\logs\AboutThisProfile.txt of the deployment manager profile. To verify which port is used by the Deployment Manager for SOAP communication, open System Administration > Deployment manager > Ports and note the value of SOAP_CONNECTOR_ADDRESS.
5. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:
   
   Node MyserverNodePrimary has been successfully federated.
6. To verify that the primary node has joined the Deployment Manager’s cell, log into the Integrated Solutions Console using your administrative user ID and password and click Servers > Application servers. Make sure you can see the primary node’s information.
   
   If you already logged in, you must log out and then log in again before you can see changes.

Federating the primary node into the cell after upgrading on AIX, Linux, and Solaris:
Add the primary node to the Deployment Manager's cell on AIX, Linux, or Solaris platforms. Adding the primary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console. You will not be able log into the primary node's Integrated Solutions Console after this step.

Before you begin

Expected state: the Deployment Manager is running.

Procedure

1. Make sure that the system clocks on the Deployment Manager and the primary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the primary node to make sure the Deployment Manager host name is resolvable.
3. On the primary node, open a command window and navigate to the \stgw_profile_root\bin directory.
4. Run the following command to add the primary node to the Deployment Manager's cell:
   ```bash
   ./addNode.sh DM_hostname DM_port_number -includeapps
   ```
   Where `DM_hostname` is the host name of the Deployment Manager server. For example:
   ```bash
   ./addNode.sh gateway_dm.example.com 8879 -includeapps
   ```
   Note: After upgrading, the default port on which the Deployment Manager listens is changing. The list of default ports can be found under `stgw_profile_root\logs\AboutThisProfile.txt` of the deployment manager profile (for example, RTCGW_Profile).
5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:
   ```
   Node MyserverNodePrimary has been successfully federated.
   ```
   Port 8879 is the default port on which the Deployment Manager listens.
6. To verify that the primary node has joined the Deployment Manager's cell, log into the Integrated Solutions Console using your administrative user ID and password and click **Servers** > **Application servers**. Make sure you can see the primary node's information.
   If you already logged in, you must log out and then log in again before you can see changes.

   **Federating the primary node into the cell after upgrading on IBM i:**

   Add the primary node to the Deployment Manager's cell on IBM i. Adding the primary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console. You will not be able log into the primary node's Integrated Solutions Console after this step.

   Before you begin

   Expected state: the Deployment Manager is running.
Procedure

1. Make sure that the system clocks on the Deployment Manager and the primary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the primary node to make sure the host name is resolvable.

3. Log in to the IBM i system where the Deployment Manager node is installed as a user with administrative privileges.

4. On the IBM i command line, run the STRQSH (Start Qshell) command.

5. Navigate to the `stgw_profile_root\bin` directory for the Deployment Manager profile.

6. Run the following command to obtain the `SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number as you will need it to add nodes to the cluster:
   
   `dspwasinst`

7. Log in to the IBM i system, where the primary node is installed, with administrative privileges.

8. On the IBM i command line, run the STRQSH (Start Qshell) command.

9. Navigate to the `stgw_profile_root\bin` directory for the primary node profile.

10. Run the following command to add the primary node to the Deployment Manager’s cell:

    `addNode DM_server_host_name DM_SOAP_port -includeapps -username WAS_Admin_username_on_DM -password WAS_Admin_password_on_DM`

    Where:
    - `DM_server_host_name` is the resolvable host name of the Deployment Manager.
    - `DM_SOAP_port` is the port that the Deployment Manager's SOAP port is listening on.
    - `WAS_Admin_username_on_DM` is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
    - `WAS_Admin_password_on_DM` is the password associated with that WebSphere Application Server administrator account on the Deployment Manager.

    For example:

    `addNode gateway_dm.acme.com 8880 -includeapps -username wasadmin -password waspassword`

11. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

    `Node MyserverNodePrimary has been successfully federated.`

12. To verify that the primary node has joined the Deployment Manager's cell, log into the Integrated Solutions Console (http://localhost:9060/ibm/console) using your administrative user ID and password and click **Servers > Application servers**. Make sure you can see the primary node's information. If you already logged in, you must log out and then log in again before you can see changes.

**Federating secondary nodes into the cell after upgrading:**

Add secondary nodes to the Deployment Manager's cell to create a network deployment of Sametime Gateway servers.
About this task

In this release, a Sametime Gateway cluster can support only two nodes: one Primary Node and one Secondary Node.

Federating secondary nodes into the cell after upgrading on Windows:

Add a secondary node to the Deployment Manager's cell. Adding secondary nodes to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

Before you begin

Expected state: the Deployment Manager is running.

Procedure

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.
3. On the secondary node, open a command window and navigate to the \stgw_profile_root\bin directory.
4. Run the following command to add a secondary node to the Deployment Manager's cell. Note the omission of the -includeapps qualifier.

   addNode.bat DM_hostname DM_port_number

   Where DM_hostname is the host name of the Deployment Manager server. For example:

   addNode.bat gateway_dm.example.com 8879

   Port 8879 is the default port on which the Deployment Manager listens.

   Note: To verify which port is used by the Deployment Manager for SOAP communication, open System Administration > Deployment manager > Ports and note the value of SOAP_CONNECTOR_ADDRESS.
5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

   Node Machine22NodeSecondary has been successfully federated.
6. For each additional secondary node, repeat the preceding steps.
7. Restart the Deployment Manager by typing the following commands. Wait for the first command to finish before starting the Deployment Manager:

   stopManager
genstartManager

What to do next

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers” on page 505.

Federating secondary nodes into the cell after upgrading on AIX, Linux, and Solaris:
Add a secondary node to the Deployment Manager's cell. Adding a secondary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

**Before you begin**

Expected state: the Deployment Manager is running.

**Procedure**

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.
2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.
3. On secondary node, open a command window and navigate to the `stgw_profile_root/bin` directory.
4. Run the following command to add a secondary node to the Deployment Manager's cell. Note the omission of the `-includeapps` qualifier.
   ```
   ./addNode.sh DM_hostname DM_port_number
   ```
   Where `DM_hostname` is the host name of the Deployment Manager server. For example:
   ```
   ./addNode.sh gateway_dm.example.com 8881
   ```
5. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:
   ```
   Node Machine22NodeSecondary has been successfully federated.
   ```
6. For each additional AIX, Linux, or Solaris secondary node, repeat the preceding steps.
7. Restart the Deployment Manager by typing the following commands on the Deployment Manager machine. Wait for the first command to finish before starting the Deployment Manager:
   ```
   ./stopManager.sh
   ./startManager.sh
   ```

**What to do next**

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers” on page 505.

**Federating secondary nodes into the cell after upgrading on IBM i:**

Add the secondary node to the Deployment Manager's cell on IBM i. Adding the secondary node to the cell allows a central point of administration for the network deployment by using the Deployment Manager's Integrated Solutions Console.

**Before you begin**

Expected state: the Deployment Manager is running.
Procedure

1. Make sure that the system clocks on the Deployment Manager and the secondary node are within five minutes of each other and set for the same timezone. Federation fails if the clocks are not synchronized within five minutes.

2. Ping the Deployment Manager node from the secondary node to make sure the Deployment Manager host name is resolvable.

3. Log in to the IBM i system where the Deployment Manager node is installed with administrative privileges.

4. On the IBM i command line, run the STRQSH (Start Qshell) command.

5. Navigate to the `stgw_profile_root/bin` directory for the Deployment Manager profile.

6. Run the following command to obtain the `SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number as you will need it to add nodes to the cluster:

```
dspwasinst
```

7. Log into the secondary node.

8. On the IBM i command line, run the STRQSH (Start Qshell) command.

9. Navigate to the `stgw_profile_root/bin` directory for the secondary node profile.

10. Run the following command to add the secondary node to the Deployment Manager’s cell. Note the omission of the `-includeapps` qualifier.

```
addNode DM_server_host_name DM_SOAP_port -username WAS_Admin_user_name_on_DM -password WAS_Admin_password_on_DM
```

where:

- `DM_server_host_name` is the resolvable host name of the Deployment Manager.
- `DM_SOAP_port` is the port that the Deployment Manager’s SOAP port is listening on.
- `WAS_Admin_user_name_on_DM` is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
- `WAS_Admin_password_on_DM` is the password associated with the WebSphere Application Server administrator account.

For example:

```
addNode gateway_dm.example.com 8880 -username wasadmin -password waspassword
```

11. When prompted, provide the Deployment Manager’s administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:

```
Node Machine22NodeSecondary has been successfully federated.
```

12. For each additional IBM i secondary node, repeat the preceding steps.

13. Navigate to the `stgw_profile_root/bin` directory for the Deployment Manager profile.

14. Restart the Deployment Manager by typing the following commands. Wait for the first command to finish before starting the Deployment Manager:

```
./stopServer.sh dmgr -username username -password password
./startServer.sh dmgr
```
What to do next

When you have finished installing and federating secondary nodes into the Deployment manager, continue with the cluster configuration as instructed in the topic, “Creating a cluster and proxy servers” on page 505.

Recreating the cluster:

Create a new cluster of IBM Lotus Sametime Gateway servers. If you are upgrading an existing Sametime Gateway cluster, you must still complete this task because you removed the cluster before upgrading the nodes.

Before you begin

Expected state: the Deployment Manager is running and nodes are stopped.

About this task

The instructions that follow describe steps for setting up a horizontal cluster, the most common cluster configuration. The Primary Node already has the primary server installed, so no additional server is needed on that computer. To add servers to the horizontal cluster, create one cluster member for each secondary node (computer).

Note: This release supports only one Secondary Node on a cluster.

Procedure

1. Delete the old cluster:
   a. Click Servers > Clusters > WebSphere Application Server Clusters.
   b. In the clusters table, click the check box in front of the old cluster, and then click the Delete button at the top of the table.
   c. Click OK.
   d. Save the change by clicking Save in the "Messages" box at the top of the page.

2. Create a new cluster:
   a. Click Server > Clusters > WebSphere application server clusters, and then click New.
   b. Enter the cluster name, for example SametimeGatewayCluster, and then click Next.
   c. Enter the primary node name as the member name, for example RTCGWServer.
   d. Click Create the member by converting an existing application server, and then click Next.
   e. In the next screen you can add more members into the cluster by entering a member name, verifying the node, and clicking Add Member. Click Next.
   f. Review the summary and click Finish.
   g. Click Save.

3. Assign the gateway applications to the new cluster:
   a. Click Applications > WebSphere enterprise applications, and then click Sametime Gateway Authorization controller.
   b. Under Modules section, click Manage Modules.
   c. Select all modules by clicking the Multiple Selection button
d. Click the cluster name in the Cluster and servers box, and click **Apply**.
e. Repeat these steps for the following applications: Sametime Gateway Core, Sametime Gateway Event logger, Sametime Gateway User locator.

4. Assign the XMPP proxy application to the new proxy node:
   a. Click **Applications > WebSphere enterprise applications** and then click **Sametime Gateway XMPP Proxy**
   b. Under Modules section, click **Manage Modules**
   c. Select all modules by clicking the **Multiple Selection** button
   d. Click the XMPPProxyServer name from the Cluster and servers box and click **Apply**.

5. Restart the Deployment manager.

Registering the upgraded Sametime Gateway cluster:

After you finish creating the cluster of IBM Sametime Gateway servers, register the cluster with the Sametime System Console so you administer it from there. Register the cluster as a whole; during the process, individual nodes are registered automatically.

Registering an upgraded Sametime Gateway cluster with the System Console:

After upgrading an IBM Sametime Gateway cluster 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**

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on AIX, Linux, Solaris, and Windows section of this information center.

- The Sametime System Console must be started.
- The LDAP server must be connected to the System Console and must be started.
- The Gateway database must be connected to the System Console and must be started.
- The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

**About this task**

Working from the cluster's Deployment Manager, Primary Node, and Secondary Nodes, follow these steps to update console.properties and productConfig.properties files. Then run the registration utility on the nodes and the Deployment Manager to register them with the console.

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

- console.properties
- productConfig.properties

**Procedure**

1. On the Deployment Manager, navigate to the `stgw_server_root/IBM/WebSphere/STgateway/console` directory.
Note: If a cluster's Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager's profile.

2. Make backup copies (using different names) of the console.properties and productConfig.properties files.

3. Update the Deployment Manager's console.properties file:
   a. Open the file for editing.
   b. Update the file with the following values:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</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 path is: 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>
   c. Verify that the remaining settings are appropriate for the Deployment Manager.
   d. Save and close the file.

4. Update the Deployment Manager's productConfig.properties file:
   a. Open the file for editing.
   b. Update the file with the following required values:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;DM&quot; because you are working in the Deployment Manager's profile right now.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUser ID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
</tbody>
</table>
Table 187. productConfig.properties settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

5. On the Primary Node machine, navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
6. Edit the Primary Node's console.properties file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 188. console.properties settings for the Primary Node

<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 path is: 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>
7. Edit the Primary Node's `productConfig.properties` file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;PN&quot; because you are now working in the Primary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to <code>true</code> for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>


9. Edit the Secondary Node's `console.properties` file with the following required values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.

<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>
Table 190. `console.properties` settings for the Secondary Node (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 <code>AboutThisProfile.txt</code> 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 path is: <code>C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt</code></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 <code>wasadmin</code>.</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>

10. Edit the Secondary Node’s `productConfig.properties` file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 191. `productConfig.properties` settings for the Secondary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;SN&quot; because you are now working in the Secondary Node’s profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
</tbody>
</table>
Table 191. productConfig.properties settings for the Secondary Node (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

11. Run the registration utility on the Primary Node.
   a. Log on to the Primary Node machine.
   b. Navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
   c. (AIX, Linux, and Solaris) Edit the registerProduct.sh file to change the SET PATH= statement to reflect IBM WebSphere Application Server version 7.
      SET PATH=../../WebSphere/AppServer7/java/bin
      Then save the file.
   d. At a command prompt, run the registration utility.
      AIX, Linux, Solaris
      • Already registered
        registerProduct.sh -upgrade
      • First-time registration
        registerProduct.sh
      Windows
      • Already registered
        registerProduct.bat -upgrade
      • First-time registration
        registerProduct.bat

12. Run the registration utility on the Secondary Node.
   a. Log on to the Secondary Node machine.
   b. Navigate to the stgw_server_root/IBM/WebSphere/STGWServerCell/console directory.
   c. (AIX, Linux, and Solaris) Edit the registerProduct.sh file to change the SET PATH= statement to reflect IBM WebSphere Application Server version 7.
      SET PATH=../../WebSphere/AppServer7/java/bin
      Then save the file.
   d. At a command prompt, run the registration utility.
      AIX, Linux, Solaris
      • Already registered
        registerProduct.sh -upgrade
      • First-time registration
        registerProduct.sh
      Windows
      • Already registered
        registerProduct.bat -upgrade
      • First-time registration
registerProduct.bat

13. Run the registration utility on the Deployment Manager.
   a. Log on to the Deployment Manager machine.
   b. Navigate to the stgw_server_root/IBM/WebSphere/STgateway/console directory.
   c. Run the registration utility.
      AIX, Linux, Solaris
      • Already registered
        registerProduct.sh -upgradeCluster
      • First-time registration
        registerProduct.sh
      Windows
      • Already registered
        registerProduct.bat -upgradeCluster
      • First-time registration
        registerProduct.bat
   d. When prompted for the cluster's name, type the name you assigned the cluster when you created it, and press Enter.

14. Start the Sametime Gateway cluster, if it is not already running.

Registering an upgraded Sametime Gateway cluster on IBM i with the System Console:

After upgrading an IBM Sametime Gateway cluster on IBM i, register it with the Sametime System Console, which allows you to manage all Sametime servers from a central location.

Before you begin

Before you register the cluster, verify that you have completed the following tasks, which are described in the Installing on IBM i section of this information center.
   • The Sametime System Console must be started.
   • The LDAP server must be connected to the System Console and must be started.
   • The Gateway database must be connected to the System Console and must be started.
   • The Community Server that the Gateway server connects to must already be registered with the Console and must be started.

About this task

Working from the cluster's Deployment Manager, Primary Node, and Secondary Nodes, follow these steps to update console.properties and productConfig.properties files. Then run the registration utility on the nodes and the Deployment Manager to register them with the 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 the topic in a new browser tab or window so you can keep it open for reference:
   • console.properties
   • productConfig.properties
Procedure

1. On the Deployment Manager, navigate to the `stgw_server_root/qibm/userdata/stgateway/dmgrprofilename/console` directory.

   **Note:** If a cluster's Primary Node is installed on the same server as the Deployment Manager, make sure you are working in the Deployment Manager's profile.

2. Make backup copies (using different names) of the `console.properties` and `productConfig.properties` files.

3. Update the Deployment Manager's `console.properties` file:
   a. Open the file for editing.
   b. Update the file with the following values:

<table>
<thead>
<tr>
<th><strong>Table 192. console.properties settings for the Deployment Manager</strong></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>
<tr>
<td><strong>SSCSSLEnabled</strong></td>
</tr>
<tr>
<td><strong>SSCHTTPSPort</strong></td>
</tr>
<tr>
<td><strong>OfferingVersion</strong></td>
</tr>
</tbody>
</table>
   c. Verify that the remaining settings are appropriate for the Deployment Manager.
   d. Save and close the file.

4. Update the Deployment Manager's `productConfig.properties` file:
   a. Open the file for editing.
   b. Update the file with the following required values:

<table>
<thead>
<tr>
<th><strong>Table 193. productConfig.properties settings for the Deployment Manager</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>InstallType</strong></td>
</tr>
</tbody>
</table>
Table 193. *productConfig.properties* settings for the Deployment Manager (continued)

<table>
<thead>
<tr>
<th>Settings</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

c. Verify that the remaining settings are appropriate for the Deployment Manager.
d. Save and close the file.

5. On the Primary Node machine, navigate to the `stgw_server_root/qibm/userdata/stgateway/PrimaryNodeProfileName/console` directory.

6. Edit the Primary Node's `console.properties` file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 194. *console.properties* settings for the Primary Node

<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 SSCSSEnabled 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 &quot;HTTP transport port.&quot; The default profile name is STSCAppProfile. On IBM i, look for the AboutThisProfile.txt file in the following location: <code>/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs/AboutThisProfile.txt</code></td>
</tr>
</tbody>
</table>
Table 194. `console.properties` settings for the Primary Node (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 <code>wasadmin</code>.</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>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

7. Edit the Primary Node's `productConfig.properties` file with the following required values. Verify that the remaining settings are appropriate for the Primary Node, then save and close the file.

Table 195. `productConfig.properties` settings for the Primary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;PN&quot; because you are now working in the Primary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>


9. Edit the Secondary Node's `console.properties` file with the following values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.
### Table 196. console.properties settings for the Secondary Node

<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. On IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/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>
<tr>
<td>OfferingVersion</td>
<td>8.5.2.0</td>
</tr>
</tbody>
</table>

10. Edit the Secondary Node's productConfig.properties file with the following required values. Verify that the remaining settings are appropriate for the Secondary Node, then save and close the file.

### Table 197. productConfig.properties settings for the Secondary Node

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallType</td>
<td>Specify &quot;SN&quot; because you are now working in the Secondary Node's profile.</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>NodeIP</td>
<td>Specify the IP address of the server being registered.</td>
</tr>
<tr>
<td>WASAdminPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPassword</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DB2AdminPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
<tr>
<td>CommunityServerHost</td>
<td>Specify the fully qualified host name (not the IP address) of the Community Server registered with the Sametime System Console.</td>
</tr>
<tr>
<td>CommunityServerPort</td>
<td>Specify the port for the Community Server.</td>
</tr>
<tr>
<td>LDAPHost</td>
<td>Specify the fully qualified host name (not the IP address) of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPPort</td>
<td>Specify the port of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
</tbody>
</table>
Table 197. productConfig.properties settings for the Secondary Node (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindDN</td>
<td>Specify the Bind Distinguished Name of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN value.</td>
</tr>
<tr>
<td>LDAPBaseDN</td>
<td>Specify the search base of the LDAP server that was registered with the Sametime System Console.</td>
</tr>
<tr>
<td>isFederated</td>
<td>Set the value to true for a primary or secondary node. The registration utility cannot run without this value.</td>
</tr>
</tbody>
</table>

11. Run the registration utility on the Primary Node.
   a. Log on to the Primary Node machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/PrimaryNodeProfileName/console` directory.
   c. Run the registration utility.
      - **Already registered**
        `registerProduct.sh -upgrade`
      - **First-time registration**
        `registerProduct.sh`
   d. When the registration script completes, press F3 to exit QSH.

12. Run the registration utility on the Secondary Node.
   a. Log on to the Secondary Node machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/SecondaryNodeProfileName/console` directory.
   c. Run the registration utility.
      - **Already registered**
        `registerProduct.sh -upgrade`
      - **First-time registration**
        `registerProduct.sh`
   d. When the registration script completes, press F3 to exit QSH.

13. Run the registration utility on the Deployment Manager.
   a. Log on to the Deployment Manager machine and start the QShell Interpreter.
   b. Navigate to the `stgw_server_root/qibm/userdata/stgateway/dmgrprofilename/console` directory.
   c. Run the registration utility.
      - **Already registered**
        `registerProduct.sh -upgradeCluster`
      - **First-time registration**
        `registerProduct.sh`
   d. When prompted for the cluster’s name, type the name you assigned the cluster when you created it, and press Enter.
   e. When the registration script completes, press F3 to exit QSH.

14. Start the Sametime Gateway cluster, if it is not already running.

_Federating the Sametime Gateway cluster’s proxy server node into the cell:_
After you install the SIP and XMPP proxy server node, you must federate the node into the Deployment Manager's cell so that the proxy server becomes part of the cluster.

**Before you begin**

Expected state: The Deployment Manager is running.

**About this task**

To federate or add the proxy server node into the cell, you run the `addnode` command on the proxy server node and specify the hostname of the Deployment Manager.

**Procedure**

1. Log into the proxy server node’s operating system.
2. **IBM i** only: On the command line, run the STRQSH (Start Qshell) command.
3. Synchronize the system clocks on the Deployment Manager and the proxy node so that they are within five minutes of one another and are set for the same time zone.
   
   Federation fails if the clocks are not synchronized within five minutes of each other.

4. On the proxy server node, open a command window and navigate to the `stgw_profile_root\bin` directory.
5. **IBM i** only: Run the following command to obtain the `SOAP_CONNECTOR_ADDRESS` port number. Make a note of the port number as you will need it to add nodes to the cluster:
   
   ```
   dspwasinst
   ```

6. Run the following command to add the proxy server node to the Deployment Manager’s cell:
   
   **AIX, Linux, and Solaris:**
   
   ```
   ./addNode.sh DM_server_host_name DM_port_number -includeapps
   ```

   **Windows**
   
   ```
   addNode.bat DM_hostname DM_port_number -includeapps
   ```

   **IBM i:**
   
   ```
   addNode DM_server_host_name DM_SOAP_port -username WAS_Admin_user_name_on_DM -password WAS_Admin_password_on_DM
   ```

   where:
   
   - `DM_server_host_name` is the resolvable host name of the Deployment Manager.
   - `DM_SOAP_port` is the port that the Deployment Manager's SOAP port is listening on.
   - `WAS_Admin_user_name_on_DM` is the user ID of the WebSphere Application Server administrator account on the Deployment Manager.
   - `WAS_Admin_password_on_DM` is the password associated with the WebSphere Application Server administrator account.

   For example:
   
   ```
   addNode gateway_dm.example.com 8879 -includeapps -username wasadmin -password waspassword
   ```

7. When prompted, provide the Deployment Manager's administrative user ID and password. Wait for the operation to complete before proceeding. Look for a success message similar to the following when complete:
Node MyProxyNode has been successfully federated.

8. Verify that the proxy servers are installed correctly:
   a. Log into the Integrated Solutions Console.
      If you already logged in, you must log out and then log in again before you can see changes.
   b. Click Servers > Server Types > WebSphere proxy servers. You should see the SIP proxy server.
   c. Click Servers > Server Types > WebSphere application servers. You should see the XMPP proxy server.

Recreating the SIP proxy server:

After you upgrade and federate the SIP proxy server, it will fail to start. Correct this problem by deleting the SIP proxy server and recreating it manually.

Before you begin

Upgrade the SIP proxy server by installing the new version of IBM WebSphere Application Server, and then federate the SIP proxy server to the cell.

About this task

Procedure

1. On the cluster’s Deployment Manager, log into the Integrated Solutions Console as the WebSphere administrator.
2. Click Servers > Server Types > Websphere Proxy Servers.
3. In the proxy servers table, click the checkbox next to the SIP proxy server, and then click the Delete button at the top of the table.
4. Click OK.
5. Save the change by clicking the Save link in the "Messages" box at the top of the page.
7. Click the New button at the top of the proxy servers table.
8. In the dialog box, select the node where the SIP proxy server was previously installed.
9. Type a name for the new server (for example, SipProxyServer), and then click Next.
10. Deselect HTTP, and then click Next.
11. Select the default server template, and then click Next.
12. Review the summary, and then click Finish.
13. Save the change by clicking the Save link in the "Messages" box at the top of the page.
14. Now apply WebSphere Application Server iFixes as explained in Installing WebSphere iFixes for Sametime Gateway.

Note: The instructions for applying the iFixes are valid for all operating systems.
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 126
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**
  - In this release, 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.
  - Clients running this release of Sametime can only establish audio and video connections with clients running Release 8.5.1 or later.
  - 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 who have not yet upgraded, do not use these new 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 provides 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 198. Client versions

<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.
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 and 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.
3. 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.
<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 sever 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.

Upgrading 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.
Chapter 5. 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 1055

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 -acgqw -d /tmp/ibm5/gsk8 GSKIt8.gskcrypt32.ppc.rte \
      GSKIt8.gskssl32.ppc.rte \
      GSKIt8.gskcrypt32.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 -i vh /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 gsk8ssl32 gsk8cry64 gsk8ssl64
      ```
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 gsk8crypt32.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 199. Defining the new JAVA_HOME environment variable

<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 gsikm.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 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>
</table>
| Password             | Type the password that you will use to  
|                      | access the keystore. You will need this  
|                      | password later in the procedure. |
| Confirm password     | Type the password again to confirm it. |
| 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/sunsap`

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:
   - Verify that **Base64-encoded ASCII data** is selected as the "Data type".
   - Set the Certificate file name to the name of the text file (for example, CA.txt) into which you copied the certificate.
   - Set the **Location** to the location to which you transferred the CA.txt file in the previous procedure (for example, `/local/notes/data`).
   - 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)
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. From an IBM i command line, run the following command to start qshell:
   ```bash
   strqsh
   ```

2. From qshell, run the following keytool command:
   ```bash
   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:
   ```bash
   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:
   ```bash
   keytool -list -storepass keystore_password
   -keystore keystore_path_and_filename
   ```

   Example:
   ```bash
   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:
   ```
   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:
   ```
   [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:
   ```
   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:
   ```
   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:
   ```
   [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:
   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 showing a connection from a client to a HTTPS proxy to a Community Services multiplexer to a Sametime server]

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](http://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

---

Chapter 5. Configuring 1433
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><strong>Host</strong></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><strong>Community port</strong></td>
<td>443</td>
</tr>
<tr>
<td><strong>Use proxy</strong></td>
<td>Select this setting.</td>
</tr>
<tr>
<td><strong>Use HTTPS proxy</strong></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 1440
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, xIC.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><strong>Note:</strong></td>
<td>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>
</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:
   ```
   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, the keystore is called "stkeys.jks" 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 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><strong>Channel encryption</strong></td>
<td>Select <strong>SSL</strong>.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specify the same port that appears in the <strong>LDAP SSL port</strong> field of the &quot;LDAP Directory - Connectivity” 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><strong>Accept expired SSL certificates</strong></td>
<td>Select <strong>Yes</strong> (the default setting) to accept a certificate from the LDAP directory server, even if the certificate has expired. For tighter security, select <strong>No</strong> 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. |
### Verify server name with remote server's certificate

<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 <strong>Enabled</strong> (the default setting) to verify the server name with the remote server’s certificate. If <strong>Enabled</strong> 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 <strong>Disabled</strong> (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 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**.
   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:
      ```plaintext
      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"/>
   `...g
   
   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"/>
   `...g
   
   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 1422
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 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.

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.

**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:
      
      ```text
      /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:

   ```text
   /opt/IBM/WebSphere/AppServer/profiles/<xxxxSTPDMProfilex>/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 Layer (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 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 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:
   a. Navigate to 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.
   b. Navigate to 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 582
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 582

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-----
ZZZZ3zCCAkigAwIBAgIDB5iRMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
MR4wDgZQQKEwdFcXpZmF4MS50KwywDQQLERyFrcXvPZmF4F1NlY3VyZSB2ZXJ0
aW52Y2F0ZSBbXRXZzPdhKhhcNMDcwNJE4MTkwMDI3KwhcNMDgwNJE4MTkwMDI3
WjB0BwMQwCQYDVQQEwJVUZZzZwgaAIUECBEFVGV4XzZzZwZgnAnBgNVAcTBaTkF1c3R
bJEMMmAoGA1UEChMDSUJNMR4wDgYDVQQLEwzdBw8wJjCwHgYDVR0MDAYGAYGgExz
EydGNnYXR1LmxvdHZlZmVtCBAzANBIGQIwCgYDVQQDExFydGNNYXRlLmxvdHZlZmVtC
GANBIGQIwCgYDVQQDExFydGNNYXRlLmxvdHZlZmVtCw8wCQYDVQQDExFydGNNYXRl
-----END CERTIFICATE-----
```

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 your server. For example, the following screen capture shows a certificate chain where an intermediary CA, VeriSign Class 3 Secure Server CA, issued a certificate for

```
-----BEGIN CERTIFICATE-----
ZZZZ3zCCAkigAwIBAgIDB5iRMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
MR4wDgZQQKEwdFcXpZmF4MS50KwywDQQLERyFrcXvPZmF4F1NlY3VyZSB2ZXJ0
aW52Y2F0ZSBbXRXZzPdhKhhcNMDcwNJE4MTkwMDI3KwhcNMDgwNJE4MTkwMDI3
WjB0BwMQwCQYDVQQEwJVUZZzZwgaAIUECBEFVGV4XzZzZwZgnAnBgNVAcTBaTkF1c3R
bJEMMmAoGA1UEChMDSUJNMR4wDgYDVQQLEwzdBw8wJjCwHgYDVR0MDAYGAYGgExz
EydGNnYXR1LmxvdHZlZmVtCBAzANBIGQIwCgYDVQQDExFydGNNYXRlLmxvdHZlZmVtC
GANBIGQIwCgYDVQQDExFydGNNYXRlLmxvdHZlZmVtCw8wCQYDVQQDExFydGNNYXRl
-----END CERTIFICATE-----
```

Chapter 5. Configuring 1467
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 582
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 582
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 582
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-----
      ZZZZ3zCCAkigAwIBAgIDB5iRMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
      MRAwDgZQQKQewdFcYnZmF4MS0wKxYDVQQL9R4DFkgZSBDZXJ0aWZpY2F0aW9u
      aW5zdGFuZ3RhdGlvb3hwaWQhIEhpc3RlZxIICnEp
      -----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...

1. 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.
   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 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 **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 CHAIN > 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 $gw_profile_root\bin directory and use the following commands:
    AIX, Linux, and Solaris
    ./$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.

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.
   a. Open the *names.nsf* file on the Domino server for the Sametime Community Server.
   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. 

3. Click **Security > Global security > WEP and SIP Security > Single Sign-on (SSO)**.

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) 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, samtetimeserver.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
LTPA keys from the WebSphere server and import the LTPA keys to the Domino server. See the WebSphere Information Center documentation for details.

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, sametimeserver.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</td>
<td>This field is required.</td>
</tr>
<tr>
<td></td>
<td>GOllerman</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Community (or domain) name is appended to the first entry in the user name field by default.</td>
<td></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:
   
   
   *
   
   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 *
   
   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 1491.

**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 1417
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 1485
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 1488
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></td>
<td></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>General</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enable logging to a text file.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Path to log text file</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>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></td>
<td></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>Number of people in all screen sharing/whiteboard meetings exceeds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of people in one active screen sharing/whiteboard meeting exceeds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>Settings</td>
<td>Capacity Warnings - Sharing in Scheduled Meetings</td>
<td>Number of active screen sharing/whiteboard meetings exceeds</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of people in all screen sharing/whiteboard meetings exceeds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of people in one active screen sharing/whiteboard meeting exceeds</td>
<td></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>Community services network</td>
<td>Switches</td>
<td>Required restart</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address for server connections</td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td>Port number</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address for client connections</td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td>Port number (default 1533)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address for HTTPS tunneled client connections</td>
<td>Host name (if empty, service will bind to all host names on server)</td>
<td>Port number</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></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Meeting Services network

<table>
<thead>
<tr>
<th></th>
<th>Address for server connections</th>
<th>Host name (if empty, service will bind to all host names on server)</th>
<th>Port number (default 1503)</th>
<th>Address for HTTPS tunneled client connections</th>
<th>Host name (if empty, service will bind to all host names on server)</th>
<th>Port number (default 8081)</th>
<th>Yes</th>
<th></th>
</tr>
</thead>
<tbody>
<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>
<td></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></td>
<td></td>
<td></td>
<td></td>
<td>Yes</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>
<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>
<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>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8081 or 80)</td>
<td>Yes</td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Token server port (default 9094)</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Services Network</td>
<td></td>
<td></td>
<td></td>
<td>Yes</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>
<td></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>Interactive Audio/Video Network</td>
<td></td>
<td></td>
<td>TCP tunneling address for client connections</td>
<td>Yes</td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 8084)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia Processor (MMP) UDP port numbers start at :49252</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia Processor (MMP) UDP port numbers end at :65535</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia control address</td>
<td>Yes</td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port number (default 9093)</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>
<td></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>Reverse Proxy Support</td>
<td></td>
<td></td>
<td>Enable Reverse Proxy Discovery on the client</td>
<td>Yes</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>Connecting Meeting Servers</td>
<td></td>
<td>Connecting Meeting Servers</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Function in Admin</td>
<td>Sub - Function</td>
<td>Details - Setting</td>
<td>Details - Setting</td>
<td>Required restart</td>
<td>Comments</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>
<td></td>
</tr>
<tr>
<td>Community services</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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>How often to poll for new names added to the Sametime Community Directory (minutes): (60)</td>
<td>Yes</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>How often to poll for new servers added to the Sametime Community (minutes): (60)</td>
<td>Yes</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum user and server connections to the Community server: (20000)</td>
<td>Yes</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>General</td>
<td>Display the &quot;Launch Sametime Connect for the desktop&quot; link on the Sametime Home page.</td>
<td>No</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>
<td></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></td>
<td></td>
<td></td>
<td>Allow users to transfer files to each other.</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum file size allowed (KB):1000</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Features</td>
<td></td>
<td></td>
<td>Allow users to send announcements (unencrypted one-way messages).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sametime Connect for Browsers</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>
<td></td>
<td></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>
<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>
<td></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>Display Name Settings for Anonymous Access to Meetings or other Virtual Places</td>
<td></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.) Default domain for anonymous users: Guest Default name: User</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.) Default domain for anonymous users: Guest Default name: User</td>
<td>Yes</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>
<td></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>Community Services</td>
<td></td>
<td>Directory Searching and Browsing</td>
<td>Users cannot browse or search the Directory. Users can type names (resolve users and groups) to add them to an awareness list. Users can browse the directory (see a list of names) or type names (resolve users and groups). Users can browse the directory to see group content and names, or type names (resolve user and groups).</td>
<td>No</td>
<td></td>
<td></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. After a meeting, add the names of participants to the meeting document</td>
<td>No</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>
<td></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>When people start or schedule a meeting</td>
<td>Allow people to choose the Screen Sharing tool in meetings:</td>
<td></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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Participants can share their screen if the moderator permits or view a shared screen.</td>
<td></td>
<td>Participants can view the shared screen only.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Force Screen Sharing to use 8-bit color.</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow people to choose the whiteboard tool in meetings</td>
<td>Allow people to save whiteboard annotations as attachments to the meeting.</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow people to enable the “Send Web Page” tool in meetings</td>
<td></td>
<td></td>
<td></td>
<td>No</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>
<td></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></td>
<td></td>
<td></td>
<td>Allow people to choose the Polling tool in meetings</td>
<td>No</td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Save recorded meetings in the following location</td>
<td>No</td>
<td></td>
<td></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>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow people to schedule Recorded Meeting Broadcast meetings.</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encrypt all Sametime meetings</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Require all scheduled meetings to have a password</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**When People Start an Instant Meeting or Schedule a Meeting**

It does work in Meeting center, but doesn’t affect the instant meeting.
<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>Meeting Services</td>
<td>Connection Speed Settings</td>
<td>When People Schedule a Meeting</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>Allow people to choose Sametime IP Audio (in addition to or instead of telephone) in meetings.</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allow people to choose Sametime IP Video in meetings.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switching</td>
<td></td>
<td>Time to wait for silence before switching to next speaker (100 - 500 ms): 250</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time to wait before switching to next video (500 - 4000 ms): 2000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recorded Meeting</td>
<td></td>
<td>Connection Speed Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast Meetings</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>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 supported</th>
<th>SOCKS 5 proxy supported</th>
<th>HTTP proxy supported</th>
<th>HTTPS proxy supported</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.
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:

```
Http[s]://hostname:port/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 1544.

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 sting "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/Http[s]://proxy.ibm.com/st01/CommunityCBR/
```

The mapping rules on the reverse proxy must translate these URLs to:

```
```

**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:

   ```
   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:

   ```
   ```

   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.
### Port Description

<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 1552
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 200
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 1552
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 1552
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 1561
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
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 Notes.</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>
</tbody>
</table>
Setting | Value
---|---
Group expansion | 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.

3. Select the Rules tab and enter these settings.

Setting | Value
---|---
Rule # | 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.

Enabled | Choose one:
- No to disable a specific rule.
- Yes to enable a specific rule.

By default, the first rule is enabled.

Trusted for Credentials | Choose Yes to allow Domino to use this Directory to authenticate web clients.

4. Select the Replicas tab and do the following:
**Setting**

<table>
<thead>
<tr>
<th>Database Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
</tr>
<tr>
<td>Open the replica of the secondary directory, and then click <strong>Edit &gt; Copy As Link &gt; Database Link</strong>.</td>
</tr>
<tr>
<td>Select the <strong>Database links</strong> field, and then click <strong>Edit &gt; Paste</strong>.</td>
</tr>
<tr>
<td>For example, assume you are creating the Directory Assistance document in the Directory Assistance database on the Sametimeserver1/East server and you have replicated the directory file named sametimeserver2west.nsf to the Sametimeserver1/East server. In this example, you must open the sametimeserver2west.nsf file and copy the file as a Database Link. Paste this Database Link into the <strong>Database links</strong> field in the Directory Assistance Document you are creating in the Directory Assistance database on the Sametimeserver1/East server.</td>
</tr>
<tr>
<td>Conversely, when creating a Directory Assistance Document on the Sametimeserver2/West server, you would open the directory file sametimeserver1east.nsf, copy the file as a Database Link, and paste the link into the <strong>Database links</strong> field.</td>
</tr>
</tbody>
</table>

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</strong> &gt; <strong>Notes Network Ports</strong> section of the Server document. The Port_0 field is required. 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</strong> &gt; <strong>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</strong> &gt; <strong>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</strong> &gt; <strong>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</strong> &gt; <strong>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:

\[
\text{(Type = "Person") \mid (Type = "Group") \mid (Type = "Server" \text{ and Sametime = "1")}
\]

### 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/mmpi</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 224
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 198
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 1574
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 198
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 232

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 1483

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 198

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 198

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 **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.

**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 **Use 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 198

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
     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 1574
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 198
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 following way:

- 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. Users 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 tasks
“Configuring preferences for the Sametime embedded client for Lotus Notes” on page 1586
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.
• 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 1581

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 1585

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:
   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 1582
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 1583
If you want to change the update interval for managed preferences, you can update the existing settings XML file.
“Discontinuing managed preferences” on page 1584
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 200. Accessibility Preferences - com.ibm.collaboration.realtime.accessibility plugin 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>useAcc</td>
<td>Boolean. Default is false.</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. Default is false.</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. Default is false.</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. Default is false.</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. Default is false.</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 201. 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</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>
<tr>
<td></td>
<td>Default is true.</td>
<td></td>
<td></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 202. 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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>Boolean</td>
<td>Specify wether or not to enable auto status change for meetings scheduled in user's calendar.</td>
<td>8.0 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
<td></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>
<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>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 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>
<td>8.0 and later</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 203. 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 204. 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 204. 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 204. 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>save.file.location</td>
<td>A string of a valid path on the computer.</td>
<td>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:DocumentsuserSavedChats</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.chat.logging/root.location=\SametimeTranscripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Linux, com.ibm.collaboration.realtime.chat.logging/root.location=SametimeTranscripts</td>
<td></td>
</tr>
<tr>
<td>prompt.save</td>
<td>Boolean</td>
<td>If using mail service for logging, specify whether to display a confirmation after manually saving chats to the mail file.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>reset.user.resets.logging.prefs</td>
<td>Boolean. Default is false.</td>
<td>Specify whether to prompt user to reset logging preferences after resetting user.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>firsttime.askprefs</td>
<td>Boolean. Default is true.</td>
<td>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.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

### Table 205. 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 205. 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 206. 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>escclous</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</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>warnNewMessageArrived Threshhold</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</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</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 206. 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 207. 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 208. 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.</td>
<td>7.5.1 and later</td>
</tr>
</tbody>
</table>

...
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<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</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</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</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 208. 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>proxy UserName</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>proxy Password</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>proxy ResolvesLocally</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. Default is 900000.</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.</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.</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.</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.</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.</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.</td>
<td>Specifies whether by default to always edit the status message when changing status to do not disturb.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>showActionToolBar</td>
<td>Boolean.</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.</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.</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.</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.</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.</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. Default is true.</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>autoSyncDefaultCommunity</td>
<td>Boolean. Default is true.</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. Default is true.</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. Default is false.</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. Default is 60.</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. Default is true.</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. Default is false.</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 209. 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 limitPublicGroupSubscriptions 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, employees_Active,employees_All). 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 limitPublicGroupSubscriptions 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 210. 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>
### Table 210. 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><code>external.application.use.custom.mail</code></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><code>external.custom.browser</code></td>
<td>String</td>
<td>Specifies the custom browser on Linux.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td><code>external.application.mail</code></td>
<td>String</td>
<td>Specifies the default mail application.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td><code>external.application.use.default.mail</code></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><code>external.custom.mail</code></td>
<td>String</td>
<td>Specifies the user mail application on Linux.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td><code>disableHostnameWarning</code></td>
<td>Boolean</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 211. 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><code>allowTransferToAnonymous</code></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 211. 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>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. 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. For Linux, com.ibm.collaboration.realtime.filetransfer/saveFileLocation=SametimeFileTransfer.</td>
<td>7.5.1 and later</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:

```plaintext
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:

```plaintext
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="toolboxvisibleMaster" 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 &quot;Do not automatically detect location changes&quot; 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 212. 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 213. 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>autoReconnectInterval</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 213. 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. Default is false.</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. Default is true.</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 214. 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. Should be a valid path for Lotus Notes.</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 215. 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. 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>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>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 215. 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 216. 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 86100000 (23 hours and 55 minutes).</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Variable type</td>
<td>Description</td>
<td></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 217. 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 218. 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 219. 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 219. 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:

```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 220. 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</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</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</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</td>
<td>For hiding all legacy meeting UI.</td>
<td>8.5 and later</td>
</tr>
</tbody>
</table>
Table 221. Meeting Preferences - com.ibm rtc meetings shelf release 8.5 x and higher

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<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 &quot;false&quot; 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 &quot;false&quot; 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>
</tbody>
</table>
Table 221: 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>loginByToken</td>
<td>Boolean.</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 “false” 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 “false” to skip meeting alerts.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td>meetings.showMeetingAlertMins</td>
<td>String. 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 221. 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 to use when inviting another user to a room. Otherwise, the default room configured in preferences is used for invitations.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>

### Table 222. 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>lastServerConnectionOnly</td>
<td>boolean</td>
<td>The default value of false disables peer-to-peer connections when screen sharing. Setting the value to &quot;true&quot; allows peer-to-peer connections.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>
| lastScreenSharingSlider    | string        | Sets the position of the sharing quality slider on the screen sharing host dialog:  
• 1 - Fastest speed, possibly reducing quality  
• 2 - Middle, balance between speed and quality (default)  
• 3 - Best quality, possibly reducing speed                                                                                   | 8.5.1 and later |
| maximumP2PConnections      | integer       | The maximum number of peer-to-peer connections that can be accepted when hosting a screen sharing session.                                                                                               | 8.5 and later |

### Table 223. 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 meeting server configuration page and when the user logs in. Do not set this value to &quot;false&quot; if clients connect to older Meeting Servers because it can cause policy validation issues in the client.</td>
<td>8.5.2 and later</td>
</tr>
</tbody>
</table>
Table 224. 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</td>
<td>By default, if the user name in a meeting room is the full canonical name</td>
<td>8.5.1.1 and later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(&quot;cn=name/ou=org unit/o=org&quot;), the name is truncated. Set this flag to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;false&quot; to prevent the conversion from occurring.</td>
<td></td>
</tr>
</tbody>
</table>

Table 225. 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</td>
<td>Set this parameter to &quot;true&quot; to disable the polling tool. This entry is</td>
<td>8.5.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>superseded by a server policy introduced in release 8.5.2. For clients</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>connecting to older servers, this preference can be used to disable the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tool.</td>
<td></td>
</tr>
</tbody>
</table>

Related tasks
"Preparing servers running on WebSphere Application Server for single sign-on" on page 1485
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 226. 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</td>
<td>This stores one of four possible values of which corner of the user’s</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>screen the alert bubble will appear.</td>
<td></td>
</tr>
<tr>
<td>pref_alertbubble_window_width</td>
<td>Positive integer</td>
<td>Stores the width in pixels of the alert bubble.</td>
<td>7.5.1 and</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td></td>
<td>later</td>
</tr>
<tr>
<td>pref_alertbubble_window_height</td>
<td>Positive integer</td>
<td>Stores the height in pixels of the alert bubble.</td>
<td>7.5.1 and</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td></td>
<td>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_alertbubble_window_edge_padding</td>
<td>Positive integer value</td>
<td>Stores the amount in pixels that the alert bubble's top and bottom edge will be from the edge of the desktop.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_show</td>
<td>String value, &quot;standard&quot; = show standard OS window, &quot;less&quot; or others = show alert bubble for an alert</td>
<td>Determines whether to show the alert bubble or a standard OS window for an alert.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_close_alerts</td>
<td>Boolean. TRUE = automatically close alert, FALSE = do not automatically close alert</td>
<td>Determines whether to automatically close an alert after it appears.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_close_alerts_delay</td>
<td>Positive integer value</td>
<td>If alerts are set to automatically close, this is the delay amount in seconds before the alert is closed.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_animation</td>
<td>String value, &quot;none&quot; = no window animation, &quot;slide&quot; = animate using slide effect, and &quot;fade&quot; = animate using fade effect. The default value is &quot;slide&quot;</td>
<td>Specify the Alert bubble animation type.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_bring_window_to_front</td>
<td>Boolean</td>
<td>The default value, whether to Bring the Popup window to front.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_alertbubble_flash_taskbar</td>
<td>Boolean</td>
<td>The default value, whether to Flash the taskbar to indicate new Popup window.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_0_playsound</td>
<td>Boolean</td>
<td>Determines whether one on one chat events play a sound.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_1_playsound</td>
<td>Boolean</td>
<td>Determines whether invitations to multi-party chat events play a sound.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_2_playsound</td>
<td>Boolean</td>
<td>Determines whether announcement events play a sound.</td>
<td>7.5.1 and later</td>
</tr>
<tr>
<td>pref_event_3_playsound</td>
<td>Boolean</td>
<td>Determines whether Invitations to Sametime Classic online meeting play a sound.</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_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 \ 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 \ or / instead. For example, com.ibm.collaboration.realtime.alertmanager/pref_event_7_soundfile=C:\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 226: 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 227: 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 users 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>
</tbody>
</table>
Table 227. 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>isCaseInsensitive</td>
<td>Boolean</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>
</tbody>
</table>

Chapter 5. Configuring 1627
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
</table>
| userInfoReplaces         | Boolean. Default is false. | 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 > 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. | 7.5.1 and later |
Table 227. 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. <strong>Tip:</strong> 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 231
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 228. 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 228. 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 229. 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 230. 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 230. 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 <code>true</code> 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 <code>true</code>, it is not necessary to also set enableTelephonyStatus to <code>true</code>. 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 <code>true</code> so nonusers can see telephony presence for Sametime Unified Telephony users.</td>
<td>8.5.1 and later</td>
</tr>
</tbody>
</table>
### Table 230. 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</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 Adapter, 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 231. 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. 0 for &quot;Image View&quot; or 1 for &quot;List View&quot;</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>
</tbody>
</table>
Table 231. Telephony, Audio, and Video Preferences - com.ibm.collaboration.realtime.telephony.ui release 8.5 and higher (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<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>ext_avc” or “st_avc”. If set to ”st_avc”, 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. Default is false.</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 TCSPi 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 231. Telephony, Audio, and Video Preferences - com.ibm.collaboration.realtime.telephony.ui release 8.5 and higher (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Variable type</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>videoCallActionProviderId</td>
<td>String</td>
<td>For Multiple TCSP service providers, this value specifies the video service</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provider ID selected by user to initiate video calls</td>
<td></td>
</tr>
<tr>
<td>extensionDelimiters</td>
<td>String</td>
<td>Comma-delimited list of delimiter used when a phone number contains an</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extension.</td>
<td></td>
</tr>
<tr>
<td>nationalPrefixes</td>
<td>String</td>
<td>Comma-delimited list of national prefixes.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>internationalPrefixes</td>
<td>String</td>
<td>Comma-delimited list of international prefixes.</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Update preferences:

The following table lists the update preferences for the IBM Sametime Connect client and Sametime embedded client for Lotus Notes.

Table 232. 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</td>
<td>8.5.2 and later</td>
</tr>
<tr>
<td></td>
<td></td>
<td>completed. Prompts immediately by default.</td>
<td></td>
</tr>
</tbody>
</table>
Table 232. 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. restart.now.or.later - user is presented with a restart dialog with Restart Now and Wait x minutes buttons. restart.on.next.login - user is presented with an info message that the plug-in updates will be effected on next restart. restart.now.no.prompt - the client is restarted automatically when update is completed without any user interaction. Default is restart.now.or.later.</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>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:

```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 233. `<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 234. `<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 234. `<managed-community-action>` attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>createNewConfig</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."

<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.

<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.

<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 id="acct.sales.usma.example.com" host="acct.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-community-action type="update" managed-community-id="acct.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":
      - AddType .jad text/vnd.sun.j2me.app-descriptor
      - AddType .jar application/java-archive
      - AddType .alx application/octet-stream
      - AddType .cod application/octet-stream
      - AddType .sisx application/octet-stream
      - AddType .cab application/vnd.ms-cab-compressed
      - AddType .cfg text/Sametime
   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, sometime.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
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 1417
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 1485
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 1490
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 TCSP (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 1417
  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 1485
  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 have a WebSphere Application Server anonymous user, follow these steps to create one:

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 ID to be used as the anonymous user ID (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**.
4. Under Additional Properties, click **Interceptors**.
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 TCSPi adapters

IBM Sametime supports the use of up to two external TCSPi adapters; for example, one to support audio, and another for video.

**How do external TCSPi adapters work?**
IBM Sametime supports the use of up to two external TCSPi adapters.

The Sametime Media Manager supports a single internal TCSPi adapter called "Sametime Audio/Video Conferencing". In addition, you can deploy up to two external TCSPi adapters; for example, one to support audio, and another for video.

Telephony Conferencing Service Provider Interface (TCSPi) is a protocol used to establish audio and video calls. The TCSPi service provider in Sametime Media Manager provides telephony and audio/video services, which are implemented by the TCSPi adapters hosted on the server's Conference Manager component. All new TCSPi 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" TCSPi 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:

![TCSPi Adapter Diagram]

**Limitations on using external adapters**

Limitations on deploying external adapters:

- You can deploy one external TCSPi adapter for audio/telephony within a given community.
- You can deploy one external TCSPi adapter for video within a given community – the adapter will implicitly support audio as well.
- You can deploy a maximum of two external TCSPi 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 235. Client-Server compatibility with external TCSPi adapters*

<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 235. 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/Rethink** 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).
Note: For details on compatibility between Sametime servers and clients, see the "Client-Server compatibility when external adapters are deployed" section in “How do external TCPI adapters work?” on page 1657

Configuring Sametime Bandwidth Manager

Configure the bandwidth manager to control bandwidth usage within a network managed by IBM Sametime Bandwidth Manager, defining sites, links between them, call rates that control bandwidth utilization, and policies that apply the rates to various classes of user.

Configuring bandwidth manager modules

Use the Configuration page to add or remove individual IBM Sametime Bandwidth Manager modules.

About this task

The bandwidth manager comprises three different modules:

- **Bandwidth Pool Manager:** Manages bandwidth allocations.
- **Media Session Controller:** Implements the business logic of the bandwidth management component (such as user lookup and application of policies).
- **SIP Frontend:** Handles incoming SIP requests and acts as SIP proxy.

Several instances of the same module type can be set up to improve scalability; use the Configuration tab to add or remove individual modules.

Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime System Console > Servers > Bandwidth Manager**.
3. Click the **Configuration** tab.
4. Scroll down to the modules table (it appears below the property settings).
5. Do one of the following:
   - Delete a module by selecting the module in the table, and then clicking the **Delete** button.
   - Add a module by clicking the **New** button and entering the following information before clicking **OK**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component type</strong></td>
<td>The type of the component instance: Bandwidth Pool Manager, Media Session Controller, or SIP Frontend.</td>
</tr>
<tr>
<td><strong>Server name</strong></td>
<td>The full IBM WebSphere Application Server name of the server where this component was installed, in the following format -- &quot;CELL/NODE/SERVER&quot; (for example, Websphere302Node01Cell1\Websphere302Node01\server1).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP URI</td>
<td>The HTTP URL of this particular instance of the component, in the following format <a href="http://HOSTNAME:HTTPPORT/APPLICATIONPATH/">http://HOSTNAME:HTTPPORT/APPLICATIONPATH/</a> where HOSTNAME is the hostname or IP address of the WebSphere Application Server server where the component is installed. HTTPPORT is the HTTP port configured for this server.</td>
</tr>
<tr>
<td>Cluster HTTP URI</td>
<td>The common HTTP URL for all instances of the given component type on the cluster (for a single server installation use the same value as for the &quot;HTTP URI&quot; field).</td>
</tr>
<tr>
<td>SIP URI</td>
<td>The SIP Address of the bandwidth management component of this particular instance of the &quot;SIP Frontend&quot; (leave it blank for other types). It should be defined in the following format sip:HOSTNAME:SIPPORT where HOSTNAME is hostname or IP address of the WebSphere Application Server where the component is installed. SIPPORT is SIP Port configured for this server. This value should match the destination address as configured in the SIP Proxy routing rule.</td>
</tr>
<tr>
<td>Cluster SIP URI</td>
<td>The common SIP address for all instances of &quot;SIP Frontend&quot; on the cluster (for single server installation use the same value as for &quot;SIP URI&quot;). This value should match the destination address as configured in the SIP Proxy routing rule.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the current instance. This is an integer value used only for &quot;Bandwidth Pool Manager&quot; components to determine which instance will be acting as primary and which will be running as secondary servers. The lower number means higher priority).</td>
</tr>
</tbody>
</table>

6. Save your changes by clicking the Save link in the "Messages" box at the top of the page.

**Setting properties for the bandwidth manager**

Use the Configuration page to define properties that determine how the IBM Sametime Bandwidth Manager handles SIP requests.

**About this task**

The properties you define here apply to the bandwidth manager as a whole; the individual modules have additional properties that you define when adding those modules.
Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click Sametime Servers > Bandwidth Manager.
3. Click the Configuration tab.
4. The configuration properties appear at the top of the page.
5. Provide values for the deployment environment’s properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Controller regex</td>
<td>Accept the default value. The value is a regular expression used to recognize if an incoming SIP request is coming from the Sametime Media Manager server’s Conference Manager component.</td>
</tr>
<tr>
<td>SIP server URI</td>
<td>The URI to be used as the From header for SIP messages sent between servers within the bandwidth manager deployment. Any valid SIP URI can be used. This value is not used for routing.</td>
</tr>
<tr>
<td>Inactive Session Timeout (Hours)</td>
<td>Set '0' for No Timeout</td>
</tr>
<tr>
<td>Initial call rate for unmanaged calls (kbps)</td>
<td>The initial call rate is a value in Kbps that is applied to all unmanaged calls. It provides an overall call rate policy for such calls.</td>
</tr>
<tr>
<td>Ignored user id prefix (regex)</td>
<td>Accept the default value for the ignored user ID prefix. The value is a regular expression that defines prefixes for user identifiers used in From headers in SIP INVITE messages. The prefix is removed and ignored before looking up users IDs in the Federated Repository.</td>
</tr>
<tr>
<td>Allow calls that exceed bandwidth capacity</td>
<td>If you set the value to Yes, calls that would otherwise be restricted are allowed to exceed available bandwidth capacity. This setting also affects calls that have no route during ICE re-INVITE, as well as calls to unmanaged destinations.</td>
</tr>
<tr>
<td>Identify organizational units as groups</td>
<td>If you set the value to Yes, organizational units in LDAP can be used as groups in policy definitions.</td>
</tr>
</tbody>
</table>

6. Click Apply to save your changes, or Reset to cancel them and revert to the previous settings.
7. Save your changes by clicking the Save link in the "Messages" box at the top of the page.

Configuring sites

In a network managed by IBM Sametime Bandwidth Manager, sites are configured with properties whose settings help determine the bandwidth used for audio and video calls.
Before you begin

Before creating and configuring a site, it is recommended that you create a model of your physical network topology. The network topology model should include all the sites on your enterprise network, and the links between them. This model will help you to create and configure individual sites in terms of their interactions with other sites. For more information, see “Modeling your network topology” on page 107.

Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click Sametime System Console > Servers > Bandwidth Manager.
3. Click the Sites tab.
4. Click the Configuration tab.
5. Click New to create a new site.
   - Click Edit to modify site information, or Delete to remove a site from bandwidth management.
6. Provide values for the site’s properties on the Configuration page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Country</td>
<td>Enter a name for the site’s country. Country names can be up to 64 Unicode characters in length, including upper- and lowercase letters, numbers, spaces, and symbols. The region, country, and city values for a site can be used later as filters to specify groups of sites, providing a built-in organization to simplify site administration.</td>
</tr>
<tr>
<td>City</td>
<td>Enter a name for the site’s city. City names can be up to 64 Unicode characters in length, including upper- and lowercase letters, numbers, spaces, and symbols. The region, country, and city values for a site can be used later as filters to specify groups of sites, providing a built-in organization to simplify site administration.</td>
</tr>
<tr>
<td>Category</td>
<td>Use this field denote a custom category to help identify the site; for example branch office, region HQ, or corporate HQ. Later, this can be used to create your own groupings of sites to simplify administration.</td>
</tr>
<tr>
<td>Site type</td>
<td>Select one of the following types of sites: Regular, Cloud, or VPN. For more information, see “Site types” on page 13.</td>
</tr>
<tr>
<td>IP ranges</td>
<td>Specify one or more IP addresses, or ranges of addresses, for the site. Click <strong>Add</strong> to add the specified IP address(es).</td>
</tr>
<tr>
<td></td>
<td>There are three ways to specify an IP range value:</td>
</tr>
<tr>
<td></td>
<td>• Adding a single IP address, such as 192.168.0.1.</td>
</tr>
<tr>
<td></td>
<td>• Adding a range by specifying a starting IP address and ending IP address separated by a hyphen, as in 192.168.0.2-192.168.0.10.</td>
</tr>
<tr>
<td></td>
<td>• Adding a range by specifying an entry such as 192.168.0.1/N, where N is the number of bits that identify the network. This notation is referred to as CIDR (Classless Inter-Domain Routing).</td>
</tr>
<tr>
<td></td>
<td>To remove IP addresses from the site, select them in the list by clicking them and then click <strong>Remove</strong>. For more information, see IP ranges.</td>
</tr>
<tr>
<td>Maximum bandwidth</td>
<td>Define the maximum bandwidth available for calls to or from this site in Kbps or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td></td>
<td>This setting is optional; the default value is unlimited. If specified, whenever the bandwidth utilized equals or exceeds the specified value, then future calls are prevented until the current bandwidth used is less than the specified maximum bandwidth.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Peak utilization | The default peak utilization controls how much bandwidth is available to the site during heavy usage periods. The default value is 100%; type an integer between 0 and 100 to modify the available percentage. This setting is optional; use it when you want the bandwidth available on the site during periods of heavy usage to be less than the normal maximum bandwidth.

Reflector | If a reflector is available, click this option.

Links | A link is the connection between this site and a destination. The links table lists the links for this site and the properties for those links that require bandwidth monitoring. Click the name of a link to open the configuration page for configuring the link's properties. For more information, see "Links to other sites."

7. Click the OK button at the bottom of the page.
8. Save your changes by clicking the Save link in the "Messages" box at the top of the page.

**Links to other sites**

Links are defined as properties of the sites they connect. A link can be created, configured, or modified from the site configuration screen of either of the sites that it connects within the network managed by IBM Sametime Bandwidth Manager.

The table at the bottom of the site configuration screen contains a row for each link that has been defined for that site. To add a new link to the site definition, click the New button in the Links table to open the link configuration screen.

The user-defined properties of links are configured by providing values for the fields and controls on the link configuration screen. The properties are described below:

- **Destination site name**: This value is selected from a list that includes all sites that have been defined for this network.
- **Distance**: By default, all links are given a distance of 10. By modifying this value, you can ensure that the call route represented in your network topology model matches the actual route for calls that routed through this link.
- **Link type**: There are two types of links, physical and virtual. These are explained in the section below.

Additional properties of physical links:
- **Maximum bandwidth**: Click the radio button for either Unlimited or Kbps. For Kbps, specify a value between 1-1,000,000 Kbps.
- **Peak utilization**: This value determines when a bandwidth pool is considered to be highly utilized.

**Two types of links: physical and virtual**

Links can be either physical or virtual. A physical link connects two sites.
Virtual links are used when a single physical link to a site such as the Internet or a WAN cloud is used to provide access to multiple other sites. For example, a single physical connection is used to connect sites A, B, and C to the internet.

Network administrators can then leverage the physical link to create connections to other sites via the Internet. Using the nominal capacity value on a virtual link, administrators can dedicate bandwidth to each site using the shared physical connection to the internet.

So there is not a one-to-one correspondence between physical and virtual links but a one-to-many. The administrator, when creating a virtual link, selects the physical link with which it is associated. When calls are routed over the virtual link, they actually use bandwidth from that physical link. This also allows multiple virtual links to consume bandwidth on a single physical link. So in the example above, calls from Site A to Site C and Site A to Site B will both utilize bandwidth on the physical link from Site A to the Internet.

**Configuring call rate policies**

In an IBM Sametime Bandwidth Manager deployment, you can define call rates to be used during periods of normal utilization, and call rates to be used during periods of peak utilization. Combine these call rates with different classes of users and different locations to create *call rate policies*.

**Creating a call rate policy**

In a network managed by IBM Sametime Bandwidth Manager, use the New Call Rate Policy page to define call rate policies that can be applied to users or endpoints.

**Procedure**

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click *Sametime System Console > Servers > Bandwidth Manager*.
3. Click the *Call Rate Policies* tab.
4. Click *New* to open the *Configuration* page.
To disable an existing call rate policy, click the checkbox in the **Select** column for the policy, and then click **Disable**.

5. Provide values for the call rate policy's properties on the **Configuration** page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Select to enable the call rate policy. The default call rate policy cannot be disabled.</td>
</tr>
<tr>
<td>Party 1: Site attribute</td>
<td>Select one of the following values. For all values except <strong>Any Site</strong>, you must also select an additional value for the selected site attribute. For example, if you select <strong>City</strong>, select a City from the list of available configured sites.</td>
</tr>
</tbody>
</table>
|                             | • **Any Site**  
|                             | • **Category**  
|                             | • **City**  
|                             | • **Country**  
|                             | • **Region**  
|                             | • **Site Name**  |
| Party 1: User Source        | Select one of the following values. For all values except **Any User**, you must also provide an additional value as described below.  
|                             | • **Any User**  
|                             | • **Bandwidth Management Groups**  
|                             | Select a bandwidth management group from the list of available defined groups.  
|                             | • **IP Address**  
|                             | Enter a valid IP address.  
|                             | • **User Directory**  
|                             | Click **Find User** and select a user or group from the resulting page.  |
| Party 2: Site attribute     | Select one of the following values. For all values except **Any Site**, you must also select an additional value for the selected site attribute. For example, if you select **City**, select a City from the list of available configured sites.  |
|                             | • **Any Site**  
|                             | • **Category**  
|                             | • **City**  
|                             | • **Country**  
|                             | • **Region**  
|                             | • **Site Name**  |
| Option                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Party 2: User Source         | Select one of the following values. For all values except Any User, you must also provide an additional value as described below.  
  - Any User  
  - Bandwidth Management Groups  
    Select a bandwidth management group from the list of available defined groups.  
  - IP Address  
    Enter a valid IP address.  
  - User Directory  
    Click Find User and select a user or group from the resulting page.  
| Normal Call Rate             | Select one of the following:  
  - Audio and Video and enter the call rate in Kbps  
  - Audio only and enter the call rate in Kbps  
| Peak Utilization Call Rate   | Select one of the following:  
  - Audio and Video and enter the call rate in Kbps  
  - Audio only and enter the call rate in Kbps  
  - Busy Signal to prevent new calls from being initiated during peak utilization periods  

6. Click the OK button.  
7. Save your changes by clicking the Save link in the "Messages" box at the top of the page.  

**Ordering call rate policies**  
In a network managed by IBM Sametime Bandwidth Manager, call rate policies are listed in order on the Call Rate Policies page. The order is significant because the policies are evaluated in that sequence, and the first matching policy is used to determine the call rate used for a call.  

**About this task**  
By default, call rate policies are listed from newest to oldest, with the exception of the default policy, which is always listed last as the lowest priority. To change the order of call rate policies, perform the following steps.  

**Procedure**  
1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.  
2. Click Sametime System Console > Servers > Bandwidth Manager.  
3. Click the Call Rate Policies tab.  
4. Click the checkbox in the Select column for the policy you want to move.
5. Click the **Move Up** or **Move Down** button repeatedly until the policy appears in the desired position.

**Call rate policy examples**

To understand how call rate policy works in a network managed by IBM Sametime Bandwidth Manager, review the examples in this section.

This section provides examples of typical call rate policies, showing the settings as they appear on the **Call Rate Policies** screen, beginning with a simple call rate policy and progressing to more complex examples that illustrate the concepts involved in configuring call rate policies.

**Example 1: One site with one class of user:**

Example 1 shows the simplest case: a single policy that specifies the normal call rate for all users in all sites within a network managed by IBM Sametime Bandwidth Manager.

For the simplest scenario, assume there is only one call rate policy for the enterprise network. It specifies the normal call rate for all users in all sites. Administrators use it to restrict bandwidth use uniformly across all calls.

For this example, assume administrators want to:
- limit calls to 384 kbps
- prevent additional calls when a the peak utilization bandwidth condition is reached

The required policy would be:

<table>
<thead>
<tr>
<th></th>
<th>Party 1</th>
<th>Party 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>User</td>
<td>Site</td>
</tr>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

This is the default policy included in the bandwidth management module by default.

**Example 2: Two sites with one class of user:**

Example 2 shows a scenario where different call rates are applied for calls between certain sites, where bandwidth is limited within a network managed by IBM Sametime Bandwidth Manager.

A second scenario considers two different sites or groups of sites. In this scenario, all users are treated uniformly, but different sites are considered to enforce different call rates within the sites or between the sites.

For example, consider the example where administrators allow
- 384 kbps normal call rate for video calls within North America and within Europe
- 128 kbps normal call rate for video calls across the Atlantic
- For all calls, force 16 kbps audio-only calls when peak utilization bandwidth conditions exist

The required policies are:
Example 3: One site with two classes of users:

Example 3 shows a scenario where different classes of users are assigned different call rates within a network managed by IBM Sametime Bandwidth Manager.

The next scenario considers two different classes of users. In this scenario, traffic in all sites and between all sites is treated uniformly, but different classes of users are considered to enforce different call rates between these different users.

As a first example, assume administrators want to allow all calls involving VIPs (VIP to anyone) to run at 384kb/s but calls between standard users to be 16 kbps audio-only calls.

The required policies are:

<table>
<thead>
<tr>
<th>Order</th>
<th>User</th>
<th>Site</th>
<th>User</th>
<th>Site</th>
<th>Normal Call Rate</th>
<th>Peak utilization Call Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>NA</td>
<td>Any</td>
<td>NA</td>
<td>Video call, 384 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>EMEA</td>
<td>Any</td>
<td>EMEA</td>
<td>Video call, 384 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>EMEA</td>
<td>Any</td>
<td>NA</td>
<td>Video call, 128 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Video call, 384 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
</tbody>
</table>

In a second example, administrators want to allow all calls between VIPs to run at 384kb/s, but all other calls to be 16kbps audio-only:

<table>
<thead>
<tr>
<th>Order</th>
<th>User</th>
<th>Site</th>
<th>User</th>
<th>Site</th>
<th>Normal Call Rate</th>
<th>Peak utilization Call Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VIP</td>
<td>Any</td>
<td>VIP</td>
<td>Any</td>
<td>Video call, 384 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Audio-only call, 16 Kbps</td>
<td>Audio-only call, 16 Kbps</td>
</tr>
</tbody>
</table>

Example 4: Two sites with two classes of users:

Example 4 combines two different sites with two different classes of users within a network managed by IBM Sametime Bandwidth Manager.

The fourth scenario combines two different sites with two different classes of users. Not only do call policies differ based on the classes of users involved in the call, policies also take into account the sites where the users are located.

As a first example, consider a scenario with the following business objectives:

- Calls within the US and within Europe are allowed to use 384 kbps for video
- Calls between the US and Europe are limited to 256 kbps for video
- All VIP-to-VIP video calls use 384 kbps
- All VIPs continue to place calls as normal when peak utilization bandwidth conditions exist
• All other users will use audio-only when peak utilization bandwidth conditions exist

The required policies for this example are:

<table>
<thead>
<tr>
<th>Party 1</th>
<th>Party 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>User</td>
</tr>
<tr>
<td>1</td>
<td>VIP</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
</tr>
</tbody>
</table>

In the next example, consider a scenario with the following business objectives:
• All video calls within Europe or within the US that involve VIPs are allowed to run at 384 kbps
• All other video calls within those regions, US and Europe, are limited to 256 kbps
• Between the regions, VIP-to-VIP video calls are allowed to run at 256 kbps
• Between regions, all other video calls are limited to 192 kbps
• All VIPs continue to place calls as normal when peak utilization bandwidth conditions exist
• All other users will use audio-only when peak utilization bandwidth conditions exist

The required policies for this example are:

<table>
<thead>
<tr>
<th>Order</th>
<th>Party 1</th>
<th>Party 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Site</td>
<td>User</td>
</tr>
<tr>
<td>VIP</td>
<td>US</td>
<td>VIP</td>
</tr>
<tr>
<td>VIP</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>US</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

### Configuring groups for Sametime Bandwidth Manager

Call rate policies can be applied to either endpoints, or to users, within network managed by IBM Sametime Bandwidth Manager. If you choose to use groups, they can be Sametime user groups, groups created specifically for use with bandwidth management, or a mixture of the two.

### About this task

To create a group of users or endpoints (a room or home network), perform the following steps.

### Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click **Sametime System Console > Servers > Bandwidth Manager**.
3. Click the **Groups** tab.
4. To configure a group, click **New** to create a new group or click the name of an existing group in the list to modify its group information.
To remove a group from bandwidth management, select an existing group and click Delete.

5. Configure a group’s site properties on the site details page. Provide a name and, optionally, a description for the group. The name is required, and must be unique within the bandwidth manager deployment.

If you deployed a cluster of bandwidth managers, make sure you have not used this name on another node.

6. Assign members to the group. Add members from user directories or enter IP addresses for meeting rooms or home networks.

a. To add members to the group by their names, click the Individual users and groups radio button. Select User in the Search by list. Optionally, narrow your search by entering a first or last name in the Search for text box. Click the Search button to find members, and click the Add button to assign them to the new group.

b. To add members to the group by adding the members of an existing Sametime group, click the Individual users and groups radio button. Select Groups in the Search by list. Optionally, narrow your search by entering the name of an existing Sametime group in the Search for text box. Click the Search button to find a Sametime group, and click the Add button to assign the members of the Sametime group to the new bandwidth management group.

c. To add an endpoint to the group by IP address, click the IP Address radio button. Enter the IP address in the text field. Click the Add button to add the endpoint to the group.

d.

7. Click Apply or Ok to create the group.

Click Reset to clear the Assign Members fields, or click Cancel to discard all new configuration settings for this group.

Creating a reflector policy

Configure reflector policies to indicate to the Bandwidth Manager where reflectors are deployed in your network and which sites make use of them.

About this task

Reflector policies include the following information:

- Whether the particular reflector policy is enabled
- Site or group of sites requiring a reflector to access other sites
- Site where the reflector is used and deployed
- Site or group of sites accessible using the reflector. This can include a single site, group of sites, any site, or any site other than the one that requires the reflector

Follow these steps to create a reflector policy.

Procedure

1. On the server hosting the bandwidth manager, open the IBM WebSphere Application Server Integrated Solutions Console and log in as the WebSphere administrator.
2. Click Sametime System Console > Servers > Bandwidth Manager.
3. Click the Reflector Policies tab.
4. Click New to open the Configuration page.
To disable an existing reflector policy, click the checkbox in the Select column for the policy, and then click Disable. Disabling a policy is useful if you are troubleshooting problems or making configuration changes during operational hours. When a policy is in a disabled state, no calls are initiated, terminated, or routed using the policy.

5. Provide values for the reflector policy's properties on the Configuration page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Select when you are ready to enable the reflector policy. The default status for the policy is disabled. This default status allows you to configure all the attributes of a policy before putting it into operation.</td>
</tr>
<tr>
<td>Site Reflector</td>
<td>Select the site where the reflector is hosted. The list of sites contains only those sites that have been enabled for the reflector.</td>
</tr>
<tr>
<td>Party 1: Location</td>
<td>Select the location type for the users who are using the reflector to connect to other users. For all values except Any Site, you must also select an additional value for the selected site attribute. For example, if you select City, select a City from the list of available configured sites.</td>
</tr>
<tr>
<td>Party 2: Location</td>
<td>Select the location type for the users that are accessed by the reflector. For all values except Any Site or Any Other, you must also select an additional value for the selected site attribute. For example, if you select City, select a City from the list of available configured sites.</td>
</tr>
</tbody>
</table>

6. Click the OK button.

7. Save your changes by clicking the Save link in the "Messages" box at the top of the page.
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 1417
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 1485
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.
   
   \$PATH=$PATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export \$PATH
   \$LIBPATH=$LIBPATH:/opt/IBM/WebSphere/STMeetingsServer/stellent
   export \$LIBPATH
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 I 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)
   ```

   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.

Configuring a Sametime Gateway

Configure one or more IBM Sametime Gateway servers.
Related tasks

“Working with Sametime servers that are enabled for SSL” on page 1417
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 1485
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 LDAP for Sametime Gateway” on page 540
Configure Sametime Gateway to use the LDAP directory used by the local Sametime environment. If you did not connect to LDAP when you installed Sametime Gateway, or you did connect to LDAP but now want to create a secure connection, use these procedures. Sametime Gateway must look up names and groups in the LDAP directory to grant users and groups access to external communities.

“Connecting servers to Sametime Gateway” on page 551
To complete IBM Sametime Gateway setup, you connect servers to the Sametime Gateway by performing some configuration steps on the local Sametime server, adding the local community to the Sametime Gateway, registering your Sametime Gateway server with AOL so that Sametime Gateway can connect to the AOL clearinghouse, and then, after you complete your registration, adding the AOL clearinghouse community to the Sametime Gateway. Finally, you want to note the port numbers so you can provide these ports to external communities.

Installing and configuring event logging

The Sametime Software Developer Kit includes a sample ear file that you can install to view the event log. The event log may contain content logging, instant messaging logging, or subscription logging events, depending on what you enable.

Before you begin

The event logging feature is available only for a clustered deployment. When you configure the Lotus Sametime Gateway cluster, the Common Event Infrastructure data source is installed automatically on IBM AIX, Linux, Microsoft Windows, and Solaris. If you are using IBM i, you must install this data source yourself before you can enable event logging.

About this task

For complete details regarding functionality and how to read the logging codes in the event log, see the Sametime Gateway Integration Guide included in the Lotus Sametime Software Development Kit.

Creating an activation specification for event logging

Before you install the Sametime Gateway samples ear file that is available from the Sametime Software Developer’s Kit, you must create an activation specification in WebSphere Application Server. The samples ear file contains an application that makes reading the event log possible.
Before you begin

The event logging feature is available only for a clustered deployment. When you configure the Lotus Sametime Gateway cluster, the Common Event Infrastructure data source is installed automatically on IBM AIX, Linux, Microsoft Windows, and Solaris. If you are using IBM i, you must install this data source yourself before you can enable event logging.

About this task

Follow these steps to create an activation specification.

Procedure

1. From the Integrated Solutions Console, click Service Integration > Buses.
2. Select CommonEventInfrastructure_Bus, and then click Destinations.
3. Select the destination with one of the following names:
   - Single server installation: node.server.CommonEventInfrastructureTopicDestination where node is the node name and server is the Sametime Gateway server name.
   - Cluster: cluster_name.CommonEventInfrastructureTopicDestination where cluster_name is the name of the cluster.
4. Click Publication Points.
5. Using a text editor, copy and paste the long name for use later. For example (the following is all on one line but split over two lines here for printing purposes):
   dibby.RTCGWServer.CommonEventInfrastructureTopic
   Destination@dibby.RTCGWServer-CommonEventInfrastructure_Bus
6. From the Integrated Solutions Console, click Resources > JMS > Activation Specifications.
7. In scope, select one of the following:
   - For single server installations, select the server level. For example:
     Node=dibby, Server=RTCGWServer
   - For cluster installations, select the cluster: RTCCluster.
8. Click New.
9. With Default messaging provider selected, click OK.
10. Type any name in the Name field. For example:
    CEI_Topic_ActivationSpec
11. For the JNDI Name, type:
    jms/cei/TopicActivationSpec
12. For the Destination type, select Topic.
13. For the Destination JNDI Name, type the following:
    jms/cei/notification/AllEventsTopic
14. For the Bus name, select CommonEventInfrastructure_Bus.
15. For the Subscription durability, select Non-durable.
16. For the Subscription name field, paste the long name that you copied in Step 5. For example (the following is all on one line but split over two lines here for printing purposes):
    dibby.RTCGWServer.CommonEventInfrastructureTopic
    Destination@dibby.RTCGWServer-CommonEventInfrastructure_Bus
17. For the **Client identifier** field, paste the portion that comes before the @ symbol. For example:
   
   `dibby.RTCGWServer.CommonEventInfrastructureTopicDestination`

18. For the **Durable subscription home** field, paste the portion that comes after the @ symbol. For example:
   
   `dibby.RTCGWServer.CommonEventInfrastructure_Bus`

19. Click **OK**, and then **Save**.

**Creating the message store for event logging (clusters only)**

This procedure creates a message store for event logging for use by Sametime Gateway clusters.

**Procedure**

1. In the Integrated Solutions Console, click **Service Integration > Buses**.
2. Click the **CommonEventInfrastructure_Bus**.
3. Under Topology, click **Messaging engines**.
4. Click the messaging engine name.
5. On the Configuration panel, under Additional properties, click **Message store**.
6. In the **Authentication alias** field, select `cell_name/RTCDBUser`, where `cell_name` is the name of your cluster's cell.
7. Click **OK**, and then **Save**.

**Installing the event logging application**

To view the event log, you must install the event logging application included in the Sametime Gateway samples ear file. While Sametime Gateway does ship with an event logger that sends events to a database, you must install a sample ear file to view those events.

**Before you begin**

The Sametime Software Development Kit includes a samples ear file (`rtc_gatewaySamplesEAR.ear`) that you install as a regular J2EE application in WebSphere Application Server. Once the ear file is installed and the event logger is enabled, Sametime Gateway event logger can then send easy to read output to the `trace.log` file. For complete details regarding installation, configuration, and the functionality of the sample Logger Event Consumer, see the Sametime Gateway Integration Guide included with the Sametime SDK.

**About this task**

The sample application sends the name and value pairs of extendedDataElements in any event that is captured with extensionName RtcGatewayLoggerEvent to the `trace.log` file. The sample Logger Event Consumer distributed with the SDK only writes information when diagnostic trace is enabled. Review the topic "Setting a diagnostic trace" for more information. Logging for the samples must be enabled and set to **All Message and Trace Levels** for `com.ibm.collaboration.realtime.sample`.

The installation of the sample application on a node in a cluster binds the application to the cluster. There's no need to install the `rtc_gatewaySamplesEAR.ear` file on every node.
Procedure

1. From the Integrated Solutions Console, click **Applications > Install New Application**.
2. Browse to the Sametime Software Development Kit and locate the file: `...\samples\rtc_gatewaySamplesEAR.ear`
3. Accept the defaults provided by WebSphere Application Server and click **Next**.
4. Click **Next** again to go to the **Bind listeners for message-driven beans** panel.
5. Select the EJB module.
6. Select **Activation Specification**.
7. In the **Target Resource JNDI Name** field, type:
   
   jms/cei/TopicActivationSpec
8. For the **Destination JNDI Name**, type:
    
    jms/cei/notification/AllEventsTopic
9. In the **Activation spec authentication alias** field, type one of the following entries:
   
   - Single server installations: type your primary administrative user name that you created when you enabled administrative security.
   - Cluster installations: type `CommonEventInfrastructureJMSAuthAlias`.
10. Click **Next**.
11. Check the summary, click **Finish**.
12. Click **Save**.
13. From the Integrated Solutions Console, click **Applications > Enterprise Applications**.
14. Select **rtc.gatewaySamplesEAR**.
15. Click **Start**.
16. If you are installing the sample ear file on a cluster, complete the following substeps, otherwise skip this step:
   a. Install the rtc_gatewaySamplesEAR.ear on the Deployment Manager node.
   b. Synchronize your changes to all nodes in the cluster. Click **System Administration > Nodes**.
   c. Select all nodes in the cluster, then click **Full Resynchronize**.
   d. Open a command window.
   e. 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**
      
      ```bash
      ./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
      ```
   f. Restart the node agents.

2) Click System Administration > Node agents .

3) Select all node agents, and then click Restart.

17. Click Sametime Gateway > Message Handlers.

18. Select the Event logger, and click the Move Down button to make the event logger the last message handler in the list.

19. Select the User locator message handler and click the Move Up button to make the user locator the first message handler in the list.

20. Select the newly installed Event logger and click Enable.

Uninstalling the event logging application:

Uninstall the event logging application, which is part of the Sametime Gateway samples ear file, by first disabling the event logging message handler, then stopping the enterprise application, and finally uninstalling the application.

Procedure
1. From the Integrated Solutions Console, click Sametime Gateway > Message Handlers.

2. In the list of message handlers, select the event logger, helloworld, chatlog, and presblock.

3. Click Disable.

4. Click Applications > Enterprise Applications.

5. Select rtc_gatewaySamplesEAR.ear from the list and click Stop, and then Uninstall.

Logging events
Complete these steps to enable content, instant messaging, or presence logging. To actually view the log results, you must install the sample ear file.

About this task

When you first install Sametime Gateway, event logging is enabled. But to begin logging events, you must enable at least one custom property for the event logger. You can record three types of events: the actual content of an instant messaging session, instant messaging data, and presence (or subscription) data. Each type of event records basic information such as when a session starts and stops, when an instant message is sent, when a presence subscription is created or released, and when a presence notification takes place.

Event logging for content, instant messaging, and presence is disabled (set to 0) by default. Values 0 or 1 and true or false are acceptable.

Expected state:
• Single server: the Sametime Gateway server is started.
• Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure
1. In the Integrated Solutions Console, click Sametime Gateway > Message Handlers.
2. Click the event logger plugin in the table.
3. Click **Custom properties**.
4. Select one of the following properties:
   - `enableContentLogging`
   - `enableImLogging`
   - `enablePresenceLogging`
5. Set the value as follows:

<table>
<thead>
<tr>
<th>Values</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 OR false</td>
<td>disabled</td>
</tr>
<tr>
<td>1 OR true</td>
<td>enabled</td>
</tr>
</tbody>
</table>

6. Click **OK**. You cannot view logged events until you install the sample application that logs information to `trace.log`. See the sample ear file and Sametime Gateway Integration Guide included in the Sametime Software Development Kit.

**What to do next**

### Configuring Sametime Gateway properties

You can put limits on sessions and subscriptions, and specify blacklist domains to check when Sametime Gateway receives a subscription request. You can also add or edit custom properties for communities, connections, translation protocols, or message handlers.

#### Setting the blacklist domains
You can specify the DNS blacklisted sites to check when the Sametime Gateway receives a subscription request. A blacklisted domain is an email address domain that you do not want to give access through Sametime Gateway.

**About this task**

**Expected state:**
- **Single server**: the Sametime Gateway server is started.
- **Cluster**: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Gateway Properties**.
2. Type the blacklist domain names. Use Fully qualified domains names or TCP/IP addresses separated by a comma, semicolon, or space. Wildcards using an asterisk in the left-most subdomain position are allowed. For example, `*.spamalot.com` is allowed.
3. Click **Apply**.

#### Setting a session timeout for an external community

Setting a session timeout applies to the instant messaging capability only. By default, the session timeout is set on the translation protocol only and disabled at the external community level. Note that setting a community session to timeout may cause instant messaging sessions to expire, terminate, or be lost.
About this task

If the session timeout property is set for a community, the community value takes precedence over the translation protocol value.

You can set a session timeout on communities that use the following translation protocols:
- SIP for Sametime Gateway
- SIP for legacy Sametime Gateway
- SIP for AOL
- SIP for Microsoft Office Collaboration Server (OCS)

The session timeout does not apply to the VP or XMPP translation protocols.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure
1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. Select a community to view the community properties.
3. At the top, click Custom Properties.
4. In this is the first time you are setting the session timeout at the community level, click New, otherwise click session_timeout to edit the custom property.
5. Type session_timeout as the name for the property.
6. Type an interval, in seconds, in the Value field, for example: 3600.
7. Click OK, and then Save.
8. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

Setting a session timeout for a translation protocol
A session timeout applies to instant messaging sessions only, not presence, and to the following translation protocols: SIP for Sametime Gateway, SIP for AOL, SIP for OCS (Office Communications Server), and SIP for legacy Sametime Gateway. By default, this property is set on the translation protocol, but you can set the property at the community level.

About this task

The session timeout does not apply to VP or other protocols.

By default, after 60 minutes of inactivity, Sametime Gateway removes session records. The next instant message that the user types in the same instant messaging window is considered to be the start of a new instant messaging session. Starting a new session is internal to Sametime Gateway. Session timeouts are transparent to users.

If the property is defined for a community, the community value takes precedence over translation protocol value.

Expected state:
- Single server: the Sametime Gateway server is started.
• Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Translation Protocols**.
2. Select a translation protocol: SIP for Sametime Gateway, SIP for AOL, SIP for OCS, or SIP for legacy Sametime Gateway.
3. Under Additional properties, click **Custom Properties**.
4. Select **session_timeout**.
5. Type a new session timeout in the **Value** field. The default timeout is 3600 seconds (60 minutes).
6. Click **OK**, and then **Save**.
7. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

**Setting a subscription timeout for an external community**

Setting a subscription timeout applies only to the presence capability when connecting to a community using the SIP for legacy Sametime Gateway protocol. The subscription timeout cancels or re-subscribes a SIP-based presence session.

**About this task**

By default, the subscription timeout is set on the translation protocol only. You can set the same property on an external community, allowing fine-grained control on a community basis. If the property is defined for a community, the community value takes precedence over the translation protocol value.

Subscription timeout applies to only to the SIP for legacy Sametime Gateway translation protocol. The subscription timeout does not apply to VP or other protocols.

Expected state:

• Single server: the Sametime Gateway server is started.

• Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. Select a community that uses SIP for legacy Sametime Gateway to view the community properties.
3. At the top, click **Custom Properties**.
4. If this is the first time you are setting the subscription timeout at the community level, click **New**, otherwise click **subscription_timeout** to edit the custom property.
5. Type **subscription_timeout** as the name for the property.
6. Type an interval in seconds in the **Value** field, for example: 3600.
7. Click **OK**, and then **Save**.
8. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.
Setting an internal subscription timeout for an external community

Setting an internal subscription timeout allows you to define a subscription timeout if an external community does not set a timeout through the SIP Expires header. An internal subscription timeout also overrides any existing subscription timeout defined by an external community.

About this task

Use the custom property incomingSubscribeDefaultExpiration to determine when an external community should renew its subscription.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. Select a community to view the community properties.
3. At the top, click Custom Properties.
4. If this is the first time you are setting the inbound subscription timeout, click New, otherwise click incomingSubscribeDefaultExpiration to edit the custom property.
5. Type incomingSubscribeDefaultExpiration as the name for the property.
6. Type an interval in seconds in the Value field, for example: 1800.
7. Click OK, and then Save.
8. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

Setting subscription timeouts for a translation protocol

Setting a subscription timeout applies only to the presence capability. The subscription timeout cancels or re-subscribes a SIP for legacy Sametime Gateway presence session.

About this task

By default, the subscription timeout is set on the translation protocol only. You can set the same property on a community, allowing fine-grained control on a community basis. If the property is defined for a community, the community value takes precedence over the translation protocol value.

Subscription timeout applies to the SIP for legacy Sametime Gateway protocol. The subscription timeout does not apply to VP, XMPP, or other protocols.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Translation Protocols.
2. Select a translation protocol from the list.
3. Under Additional properties, click **Custom Properties**.
4. Select **subscription timeout**.
5. Type a new subscription timeout in the **Value** field. The default subscription timeout is 3600 seconds (60 minutes).
6. Click **OK**, and then **Save**.
7. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster.

**Customizing the error message for when instant messaging fails**

You can create and display custom text for users when an instant message fails.

**Before you begin**

You must create the external community first before you specify the custom error message.

**About this task**

You can set a custom property at the community level to display a specific error message that users see when they are unable to connect to a user in an external community. Without specifying the custom property, user always see a default message "Your message has not been delivered. Please verify that the recipient is online." The steps below describe how to create a custom error message to provide additional feedback to users when trying to connect to a specific community.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. From the list of communities, select an external community.
3. Click **Custom Properties**.
4. Click **New** to create a new custom property.
5. In the **Name** field, type **IM failure message**.
6. In the **Value** field, type the custom error message to display to users when sending an instant message fails.
7. Click **Apply**.
8. Restart the Sametime Gateway server.

**Updating AOL, Office Communications Server, or Google host addresses**

Complete these steps to update the server IP addresses that Sametime Gateway uses to determine when SIP requests originate from AOL Instant Messenger, Office Communications Server, or Google Talk.

**Before you begin**

Update host or IP addresses only after new addresses have been published by IBM.

**About this task**

Sametime Gateway uses a custom property called **server** to store Fully qualified domain names (FQDN) or host IP addresses of instant messaging services. The property enables Sametime Gateway to determine when a SIP request is coming
from AOL Instant Messenger or Office Communications Server, or when an or XMPP request is coming from Google Talk. The property is pre-set when you add an external community that uses one of the aforementioned services, so if a FQDN or a host IP addresses changes, you must update the custom property for any community that relies on that service.

Note that you can change only the custom property at the community level after you create the connection to a community.

**Procedure**

1. Log into the Integrated Solutions Console (http://localhost:9060/ibm/console), and click Sametime Gateway > Communities.
2. Click a community that uses the translation protocol that you want to update:

<table>
<thead>
<tr>
<th>Translation protocol</th>
<th>Instant messaging provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for AOL</td>
<td>AOL Instant Messenger</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>Office Communications Server</td>
</tr>
<tr>
<td>XMPP</td>
<td>Google Talk</td>
</tr>
</tbody>
</table>

3. Click Custom properties.
4. Click servers.
5. In the Value field, edit the host names or IP addresses.
6. Click OK.
7. Repeat the preceding steps for other communities that use the same translation protocol (SIP for AOL, SIP for OCS, or XMPP).
8. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.

**Adding custom properties**

You can add a custom property for a community, connection, translation protocol, or message handler. You can view or edit existing properties, or specify new properties that are needed to configure third-party elements used by the Sametime Gateway.

**About this task**

Expected state:

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. Select a community to view the community properties.
3. At the top, click Custom Properties.
4. Click New.
5. Type the name of the custom property in the Name field.
6. Type the value in the Value field.
7. Select Required to enable the custom property.
8. Click OK.
Translation protocol additions:

You can extend the IBM Sametime Gateway by adding translation protocols. Additional translation protocols expand the communities that the Sametime Gateway can connect with.

A new translation protocol permits the Sametime Gateway's ability to connect to additional instant messaging communities. A translation protocol needs to implement the API defined by the Sametime Gateway core. The core exposes an API for use by the translation protocol, and includes documentation on how to use it. Your new translation protocol is responsible for connectivity with the corresponding presence servers. If the presence server supports distribution or failover, the translation protocol is responsible for implementing these features. During deployment, the Sametime Gateway configuration must be updated to be made aware of the existence of the new translation protocol. Restart the Gateway to initiate the new translation protocol.
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.