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. Administering .......................... 1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting and stopping servers.</td>
<td>1</td>
</tr>
<tr>
<td>Sametime component URLs</td>
<td>6</td>
</tr>
<tr>
<td>Adding administrators</td>
<td>9</td>
</tr>
<tr>
<td>Changing the administrator password</td>
<td>10</td>
</tr>
<tr>
<td>Updating your DB2 administrator password</td>
<td>10</td>
</tr>
<tr>
<td>Updating your LDAP Bind password</td>
<td>10</td>
</tr>
<tr>
<td>Updating your WebSphere Application Server administrator password</td>
<td>11</td>
</tr>
<tr>
<td>Managing users with policies</td>
<td>12</td>
</tr>
<tr>
<td>Finding policies associated with a user</td>
<td>13</td>
</tr>
<tr>
<td>Creating new user policies</td>
<td>13</td>
</tr>
<tr>
<td>Assign users and groups to policies</td>
<td>15</td>
</tr>
<tr>
<td>Changing a user policy’s weight</td>
<td>31</td>
</tr>
<tr>
<td>Using nested groups in policy assignments</td>
<td>32</td>
</tr>
<tr>
<td>Administering a Sametime System Console</td>
<td>34</td>
</tr>
<tr>
<td>Backing up the console database</td>
<td>34</td>
</tr>
<tr>
<td>Starting the Sametime System Console so you can administer servers</td>
<td>34</td>
</tr>
<tr>
<td>Administering a Sametime Community Server</td>
<td>35</td>
</tr>
<tr>
<td>Managing administrator access and roles</td>
<td>35</td>
</tr>
<tr>
<td>Managing trusted IP addresses</td>
<td>45</td>
</tr>
<tr>
<td>Managing community services</td>
<td>46</td>
</tr>
<tr>
<td>Managing anonymous access to virtual places</td>
<td>52</td>
</tr>
<tr>
<td>Sending a message to all users</td>
<td>53</td>
</tr>
<tr>
<td>Managing business cards</td>
<td>54</td>
</tr>
<tr>
<td>Changing user names</td>
<td>79</td>
</tr>
<tr>
<td>Changing the IP address of an IBM i Sametime Community Server</td>
<td>98</td>
</tr>
<tr>
<td>Changing the host name of an IBM i Sametime Community Server</td>
<td>98</td>
</tr>
<tr>
<td>Monitoring the Sametime Community Server</td>
<td>100</td>
</tr>
<tr>
<td>Administering a Sametime Proxy Server</td>
<td>107</td>
</tr>
<tr>
<td>Updating Sametime Proxy Server connection properties on the console</td>
<td>107</td>
</tr>
<tr>
<td>Administering a Sametime Media Manager</td>
<td>107</td>
</tr>
<tr>
<td>Updating Sametime Media Manager connection properties on the console</td>
<td>108</td>
</tr>
<tr>
<td>Managing UDP ports for voice chat and video calls</td>
<td>108</td>
</tr>
<tr>
<td>Managing multiple audio and video streams</td>
<td>109</td>
</tr>
<tr>
<td>Changing the SIP transport protocol in the Sametime Media Manager</td>
<td>111</td>
</tr>
<tr>
<td>Managing media encryption and codecs</td>
<td>112</td>
</tr>
<tr>
<td>Managing video bit-rate</td>
<td>113</td>
</tr>
<tr>
<td>Changing the default number of maximum users</td>
<td>114</td>
</tr>
<tr>
<td>Administering a SIP Proxy and Registrar</td>
<td>115</td>
</tr>
<tr>
<td>Updating SIP Proxy and Registrar connection properties on the console</td>
<td>116</td>
</tr>
<tr>
<td>Managing SIP proxy properties</td>
<td>117</td>
</tr>
<tr>
<td>Managing SIP registrar properties</td>
<td>122</td>
</tr>
<tr>
<td>Managing SIP registered bindings</td>
<td>123</td>
</tr>
<tr>
<td>Managing the SIP Proxy and Registrar domains</td>
<td>124</td>
</tr>
<tr>
<td>Administering a Sametime Bandwidth Manager</td>
<td>124</td>
</tr>
<tr>
<td>Monitoring the status of bandwidth manager modules</td>
<td>124</td>
</tr>
<tr>
<td>Monitoring bandwidth usage for individual links</td>
<td>126</td>
</tr>
<tr>
<td>Monitoring bandwidth usage for sites</td>
<td>127</td>
</tr>
<tr>
<td>Monitoring calls for selected links</td>
<td>127</td>
</tr>
<tr>
<td>Monitoring calls for selected sites</td>
<td>128</td>
</tr>
<tr>
<td>Bandwidth Manager statistics</td>
<td>129</td>
</tr>
<tr>
<td>Administering a Sametime Meeting Server</td>
<td>131</td>
</tr>
<tr>
<td>Updating Sametime Meeting Server connection properties on the console</td>
<td>131</td>
</tr>
<tr>
<td>Customizing the Sametime Meeting Server configuration</td>
<td>135</td>
</tr>
<tr>
<td>Tuning sametime polling “Keep Alive” interval for client requests</td>
<td>134</td>
</tr>
<tr>
<td>Administering a Sametime Gateway Server</td>
<td>141</td>
</tr>
<tr>
<td>Updating Sametime Gateway Server connection properties on the console</td>
<td>141</td>
</tr>
<tr>
<td>Maintaining and monitoring Sametime Gateway Reference</td>
<td>145</td>
</tr>
<tr>
<td>Administering a Sametime Gateway Server</td>
<td>145</td>
</tr>
<tr>
<td>Managing users access to external communities</td>
<td>141</td>
</tr>
<tr>
<td>Enabling spam filtering</td>
<td>143</td>
</tr>
<tr>
<td>Setting log files size and rotation for the SIP Proxy and Registrar</td>
<td>147</td>
</tr>
<tr>
<td>Tuning Sametime Media Manager</td>
<td>195</td>
</tr>
<tr>
<td>Limiting participants in a video conference</td>
<td>195</td>
</tr>
<tr>
<td>Setting log files size and rotation for the SIP Proxy and Registrar</td>
<td>197</td>
</tr>
<tr>
<td>Tuning Sametime Bandwidth Manager</td>
<td>198</td>
</tr>
<tr>
<td>Monitoring the dynamic port range to improve Packet Switcher performance</td>
<td>196</td>
</tr>
<tr>
<td>Setting log files size and rotation for the Sametime Bandwidth Manager</td>
<td>198</td>
</tr>
</tbody>
</table>

### Chapter 2. Tuning ............................... 189

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing the number of open files on a Sametime server running Linux</td>
<td>189</td>
</tr>
<tr>
<td>Tuning a Sametime Community Server</td>
<td>189</td>
</tr>
<tr>
<td>Tuning Sametime LDAP settings</td>
<td>189</td>
</tr>
<tr>
<td>Advanced settings to control contact list size</td>
<td>193</td>
</tr>
<tr>
<td>Setting a Sametime Polling “Keep Alive” interval for client requests</td>
<td>194</td>
</tr>
<tr>
<td>Tuning Sametime Media Manager</td>
<td>195</td>
</tr>
<tr>
<td>Limiting participants in a video conference</td>
<td>195</td>
</tr>
<tr>
<td>Modifying the dynamic port range to improve Packet Switcher performance</td>
<td>196</td>
</tr>
<tr>
<td>Setting log files size and rotation for the Sametime Bandwidth Manager</td>
<td>198</td>
</tr>
</tbody>
</table>
Chapter 3. Troubleshooting .... 213

Troubleshooting Sametime clients .......... 213
Logging and tracing on Sametime Connect .... 213
Locating the Sametime Connect workspace .... 216
Troubleshooting audio and video in the
Sametime Connect client .................. 217
Troubleshooting the Sametime web audio-visual
plugin .................................... 217
Troubleshooting meeting invitations ........ 222
Resolving problems with business cards ... 222
Troubleshooting a Sametime System Console 224
Sametime System Console log locations ..... 224
Determining Sametime server status using the
Integrated Solutions Console ............. 224
The console.properties file ............... 225
The productConfig.properties file for
WebSphere-based servers .................. 225
The productConfig file for the Sametime
Community server ....................... 229
Troubleshooting clustering .................. 229
Troubleshooting a Sametime Community Server 230
Troubleshooting general issues in the Sametime
Community Server ....................... 230
Troubleshooting LDAP in Sametime ......... 234
Troubleshooting network issues on the
Sametime Community Server .............. 234
Troubleshooting a Sametime Proxy Server .... 238
Enabling logging and tracing for a Sametime
Proxy Server ................................ 238
Troubleshooting a Sametime Media Manager 239
Setting a diagnostic trace on a Sametime Media
Manager server. ........................... 239

Gathering Sametime Media Manager logs and
traces for IBM Support .................... 241
Troubleshooting a Sametime Bandwidth
Manager using JVM logs ................... 241
Troubleshooting video quality ............... 242
Troubleshooting Sametime Media Manager
component clusters ....................... 242
Troubleshooting Sametime Bandwidth Manager 244
Setting a diagnostic trace on a Sametime
Bandwidth Manager ....................... 244
Troubleshooting a Sametime Bandwidth
Manager using JVM logs ................... 245
Troubleshooting using the Bandwidth Manager
Monitor and Policy Testing tools .......... 246
Troubleshooting Sametime Bandwidth Manager
clusters .................................. 246
Troubleshooting a Sametime TURN Server .... 247
Troubleshooting a Sametime Meeting Server .... 248
Setting a diagnostic trace on a Sametime
Meeting Server ............................ 248
Gathering Sametime Meeting Server logs and
traces for support ......................... 249
Troubleshooting a Sametime Meeting Server
using JVM logs ............................ 250
Troubleshooting a Sametime Meeting Server
cluster .................................... 250
Troubleshooting a Lotus Sametime Gateway Server 251
Setting a diagnostic trace on Sametime Gateway
Setting a diagnostic trace for specific user names
and domains ............................ 252
Gathering logs and traces for IBM support .... 255
Gathering performance data ................. 256
Troubleshooting installation ................ 258
Troubleshooting WebSphere Application Server 259
Troubleshooting the Sametime Gateway using
JVM logs .................................. 259
Troubleshooting a failed WebSphere Application
Startup .................................... 260
Troubleshooting starting a cluster .......... 260
Troubleshooting secondary node problems .... 261
Troubleshooting connections to external
communities ............................. 262
Troubleshooting message handlers .......... 262
Troubleshooting slow or missing awareness
changes ................................... 263
Troubleshooting XMPP and Google community
connections and awareness ............... 264
Error message severity levels and situations ... 266
Troubleshooting installation or uninstallation .... 267
Troubleshooting a Sametime System Console
installation ................................ 267
Troubleshooting a Sametime Gateway
installation ................................ 268
Registering a Sametime server manually on AIX,
Linux, Solaris, and Windows ............. 269
Manually removing WebSphere Application
Server .................................... 273
Manually removing DB2 data on AIX, Linux,
Solaris, and Windows .................... 275
Unregistering a Sametime server on AIX, Linux,
Solaris, or Windows ..................... 276
Chapter 1. Administering

IBM® Sametime administrators set up and maintain users and their ability to use Sametime features. They also maintain and monitor the servers.

This section contains information about user registration and policies and the tools that you can use to administer the server.

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 1. 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>

Note: The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

### AIX®, Linux, or Solaris

#### Table 2. 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                                     |
| Proxy Server        | ./startNode.sh   
                        | ./startServer.sh STMeetingServer                                       |
| Media Manager       | Linux only:   
                        | ./startNode.sh   
                        | ./startServer.sh STMediaServer                                         |
| Sametime Gateway    | ./startNode.sh   
                        | ./startServer.sh RTCGWServer                                           |
| Sametime Advanced   | ./startNode.sh   
                        | ./startServer.sh STAdvancedServer                                     |

Note: Stop the Deployment Manager last after you have stopped the server. Also note that the server name is case sensitive.

#### Table 3. Stop server commands for AIX, Linux, or Solaris

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime System Console</td>
<td>./stopServer.sh STConsoleServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
</tbody>
</table>
Table 3. Stop server commands for AIX, Linux, or Solaris (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Server</td>
<td>./stopServer.sh STMeetingServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopServer.sh STMeetingHttpProxy</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username</td>
</tr>
<tr>
<td></td>
<td>-password password</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>./stopServer.sh STProxyServer -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>
<tr>
<td>Sametime Gateway</td>
<td>./stopServer.sh RTCGWServer -username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
<tr>
<td>Sametime Advanced</td>
<td>./stopServer.sh STAdvancedServer</td>
</tr>
<tr>
<td></td>
<td>-username username -password password</td>
</tr>
<tr>
<td></td>
<td>./stopNode.sh -username username -password password</td>
</tr>
</tbody>
</table>

Windows

The Start Programs menu is also a convenient way to start and stop Sametime servers running on WebSphere Application Server.

Note: The Deployment Manager must be running for the cell before starting a server. Also note that the server name is case sensitive.

Table 4. 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>
</tbody>
</table>
### Table 4. Start server commands for Windows (continued)

<table>
<thead>
<tr>
<th>Server</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<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 5. 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 6. 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 7. 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 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>
Sametime component URLs

This section lists the URLs for IBM Sametime servers and components.

The following table lists the URLs for logging in to Sametime:

Table 8. Sametime URLs

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
</table>

A single Integrated Solutions Console URL is only applicable if you deploy a cluster and choose to use the Sametime System Console as the Deployment Manager for all Sametime products.

For IBM i, the port number may not be 8700. Use the port that was listed in the Sametime System Console installation results summary. To check the port, open the AboutThisProfile.txt file for the Sametime System Console Deployment Manager Profile and use the setting specified for the "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

The default port is 8700 for all platforms except IBM i.
Table 8. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
</table>

The default port is 9060 for all platforms except IBM i.

For IBM i, the port number may not be 9060. To check the port, open the logs/AboutThisProfile.txt file for the Websphere Application Server profile that is running the ISC for your Gateway server and use the setting specified for the "Administrative console port."

If you have installed a single Sametime Gateway server, this will be the one Sametime Gateway profile you have. If you have a cluster setup, this profile will be the Deployment Manager profile that your Sametime Gateway server has been clustered with.
<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime web client</td>
<td><a href="http://proxyserverhostname.domain:port/stwebclient/index.jsp">http://proxyserverhostname.domain:port/stwebclient/index.jsp</a></td>
<td>Log in with your user name and password.</td>
</tr>
</tbody>
</table>
Table 8. Sametime URLs (continued)

<table>
<thead>
<tr>
<th>Sametime component</th>
<th>URL</th>
<th>Logging in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Room Center</td>
<td><a href="http://meetingserver">http://meetingserver</a> hostname.domain:port/stmeetings</td>
<td>Log in with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>To verify the HTTP port number being used by the Lotus Sametime Meeting Server, open 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 STMAppProfile. For IBM i, look for the AboutThisProfile.txt file in the following location: /QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs/AboutThisProfile.txt</td>
<td></td>
</tr>
<tr>
<td>Sametime Community Server Administrator Tool</td>
<td><a href="http://communityserver">http://communityserver</a> hostname.domain:port/stcenter.nsf</td>
<td>Log in with your Domino® administrator's name and password. Under Administrator Tools, click Administer the server.</td>
</tr>
<tr>
<td></td>
<td>Specify the port number if it is not the default port number 80.</td>
<td></td>
</tr>
</tbody>
</table>

**Adding administrators**

Add yourself or others as administrators for the WebSphere Application Server-based IBM Sametime components.

**About this task**

You must give yourself and users that you designate as administrators the same roles as the wasadmin in order to manage Sametime using the Sametime System Console. The wasadmin ID is the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.

**Procedure**

1. From a browser, enter the URL for the Sametime System Console.
2. Enter the WebSphere Application Server User ID and password that you created when you installed Sametime System Console.
   The default name is wasadmin.
3. Click Applications > Application types > WebSphere enterprise applications.
4. Click Sametime System Console (deployment.ear).
5. Under Detail Properties, click Security role to user/group mapping.
6. Note the roles for wasadmin. For information on the access level of the roles see "Administrative roles" in the WebSphere Application Server information center.
Click Cancel to return to the Integrated Solutions Console.

7. Click Users and Groups.

8. Select either Administrative user or Administrative group to assign yourself and other designated administrators to the Administrator and Admin Security Manager roles, and other roles assigned to wasadmin.

   *Note:* An administrator cannot map users and groups to the administrator roles without having the Admin Security Manager role.

9. Save your changes.

### Changing the administrator password

The following topics explain how to change your administrator passwords.

**Updating your DB2 administrator password**

If you change your administrator password in IBM DB2®, you must update your password in the Sametime System Console, as well as the Meeting Server and, if applicable, Sametime Advanced. If you do not update your password, IBM Sametime stops working.

**Procedure**

1. Log in to the Integrated Solutions Console for the Sametime System Console.
2. Click Resources > JDBC > Data sources.
3. Click the data source in the table.
4. Under Related Items, click JAAS - J2C authentication data.
5. Click your DB2 administrator alias.
6. Under General Properties, type your new password.
7. Click Apply and then click OK.
8. Repeat this procedure for the Sametime Meeting Server and, if applicable, the Sametime Advanced server.
9. Restart the Sametime System Console and Meeting Server or Advanced Server.

   The changed password only takes effect after you restart the server, so be sure to restart the server.

**Updating your LDAP Bind password**

You can change the LDAP Bind password that you defined when you first connected the LDAP server.

**About this task**

Change your LDAP Bind password by running the Connect to LDAP Servers prerequisite in the Sametime System Console. Changing the password updates the Sametime Community Server database, stconfig.nsf and the WebSphere Application Server. Then send the update to any other Deployment Managers in the environment and to the Directory Assistance database on the Sametime Community Server.
Procedure
1. From the Sametime System Console, run the Connect to LDAP Servers prerequisite. Update the LDAP Bind password when you are prompted to do so and save the changes.
   The change updates the LDAP repository configured for WebSphere Application Server.
2. Wait for the next scheduled update task to run, which updates the LDAP Server document in the Sametime Community Server configuration database (stconfig.nsf) with the password change.
3. If the Sametime System Console is the Deployment Manager for all Sametime servers, proceed to the next step.
   If there are other Deployment Managers in the Sametime environment, update the Bind password on each Deployment Manager. Make the change by editing the LDAP repository as described in the WebSphere Application Server information center topic Lightweight Directory Access Protocol repository configuration settings.
   a. From the Notes® client, open the Directory Assistance database (usually named da.nsf) on the Community Server.
   b. Open the Directory Assistance document for the LDAP server.
   c. On the LDAP tab, under Connectivity Settings, update the Administrator password.
   d. Save and close the document.
5. Restart the Community Servers, Deployment Managers, and Application Servers that share the LDAP repository.

Updating your WebSphere Application Server administrator password
You can change your WebSphere Application Server administrator password.

About this task
You can change your WebSphere Application Server administrator (wasadmin) password on the following WebSphere-based Sametime servers. If you change the wasadmin password on any of these servers, then you must also update the wasadmin password for that server that is stored in the Sametime System Console.

- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Gateway Server
- SIP Proxy and Registrar
- FIPS Proxy Server
- Sametime Advanced

The complete Sametime Media Manager installations are listed under both the Media Manager and the SIP Proxy and Registrar administration listings. There is only one entity and changing the connection properties in one place is reflected in the other.
A FIPS Proxy Server uses the same credentials as the Sametime Proxy Server on which it was installed. Changing the credentials in either location affects both administrative connections. The FIPS Proxy Server list depends on a valid server connection, so if the connection information is not correct, the FIPS Proxy server is not be listed. You can correct this by editing the connection properties in the Sametime Proxy Server listing.

**Procedure**

1. Change the wasadmin password of the WebSphere-based Sametime application server.
   a. Log in to the Integrated Solutions Console on the WebSphere-based Sametime application server.
   b. Click **Users and Groups > Manage Users**.
   c. Under Search for Users, select **User ID** in the **Search by** field, and then enter **wasadmin** in the **Search for** field. Click **Search**.
   d. Click **wasadmin** in the results dialog.
   e. Enter a new password in the **Password** and **Confirm Password** fields.
   f. Click **Apply** and then click **OK**.

2. Update the wasadmin password that you changed in the previous step on the Sametime System Console.
   a. Log in to the Integrated Solutions Console for the Sametime System Console.
   b. Click **Sametime System Console > Sametime Servers**.
   c. Click the Sametime application server that has the wasadmin password that you changed in step 1.
   d. Locate the deployment name and click **Edit** under **Connection Properties**.
   e. Enter a new password.
   f. Click **Save** and then click **Done**.

---

**Managing users with policies**

All IBM Sametime users are automatically assigned to default policies. Sametime Instant Messaging, Meetings, and Media Services each has a default policy to be applied to users. You can create additional user policies, and assign users and groups to these policies.

**Before you begin**

If you upgraded from an earlier release, complete the steps for migrating policy assignments before setting any new ones.

**About this task**

When a user authenticates, Sametime applies a default policy if no other policy can be found for that user. You can create new policies that grant or limit access to features, and assign users to these policies. Users can be assigned to more than one policy. If a user belongs to more than one policy, then Sametime uses the policy weight to determine policy precedence. Custom policies can be designed for specific groups in the company, and the default policy can be inherited or assigned. Meetings policy changes take effect immediately, while Instant Messaging and Media Services policy changes take effect within an hour.
There is also an anonymous policy that is assigned by default to users who have not authenticated, and unauthenticated users always receive this policy.

**Note:** If your deployment includes the Sametime System Console, you must manage policies there because all settings made in the legacy Sametime Administration Tool (STCenter.nsf) are ignored. This includes the override all feature, as well. Moreover, there is no automatic migration of policies from the Sametime Administration Tool to the Sametime System Console. You must do this manually because Sametime Administration Tool policies do not map one-to-one to policies in the Sametime System Console.

Do not use the ampersand character (&) in the policy's name or in any one of the values of policy attributes.

### Finding policies associated with a user
You can find all the policies associated with a user for all the IBM Sametime products to which the user has access.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console**.
3. Click **Manage Policies**.
4. Click any user Sametime component. It does not matter which component that you select, because your search results display all the policies for all the Sametime components to which the user has access.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Click **Find Active Policies**.
6. Select the criterion for the user for which you want to find the associated policies in the **Search by** field.
   - User ID
   - Name
   - E-mail address
7. Enter the entire or partial user ID, email address, or name of the user or group in the **Search for** field If you enter partial information, use an asterisk as a wild card character for missing or incomplete information. For example, type `sm*` for all names starting with `sm`.
8. Select the number of listings in the search results in the **Maximum results** field.
9. Click **Search**. The results display the users that match your search criteria.
10. Select a name in the results table, and then click **Find Active Policies** to show the policies for that user.
11. Click **Done**.

### Creating new user policies
You can create user policies, and assign users and groups to these policies.
About this task

You can set policy for users to have access to specific IBM Sametime features, depending upon their level of need. For example, the maximum size for a file being transferred is set by default at 1 megabyte to help manage traffic over the server(s); however, if you have a group that routinely transfers large files for business reasons, you can create a new policy specifically for those users and set the maximum size of files that they can send to a much higher number.

Note: When you create a new policy, it uses the default policy settings as the base settings in the new policy. You can update these settings.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime product for which you want to create a policy.
   • Instant Messaging
   • Meetings
   • Media Manager
5. Click New.
6. Enter a name to use to identify the policy in the Policy Name field.
   
   Note: Do not use the following special characters in the policy's name or in any one of the values of policy attributes:
   • Ampersand (&)
   • Apostrophe (’)
   • Quotation mark (")
   • Greater than character (>)
   • Less than character (<)
7. Specify the features that you want to enable or disable for the users or groups that you will assign to this policy. Some instant messaging features are flagged with IC characters after the field label. This flag indicates that a feature is only available for installed clients. The feature is not available to browser clients.
8. Click OK.

Results

Tip: You can follow these same basic steps to delete or edit a policy. Delete a policy by selecting the policy and then click the Delete button. Edit a policy by clicking the policy name. You cannot delete the anonymous or default policies, but you can edit them. If you edit a policy, you cannot change the policy ID. To do this, you must make a copy of the policy by selecting it and clicking Duplicate, then you can enter a new ID in the copy. Before you delete the original, be sure to reassign the users and groups to the copy and give it the proper policy weight.

What to do next

You can now assign users and groups to this policy.
Assign users and groups to policies

You can assign users and groups to specific user policies to grant or limit access to features in IBM Sametime.

About this task

You cannot assign users to the default or anonymous policies. Authenticated users are automatically assigned to the default policies. Unauthenticated users are assigned to anonymous policies.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime component with the policy to which you want to assign a user or a group.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Select a policy name from the list, and click Assign.
6. Click Add Users or Add Groups.
   At this point you could remove a user from a policy, by selecting the user in the list and then clicking Remove.
7. Select the criterion for searching for the user or group that you want to add to the policy in the Search by field.
   - User ID
   - Name
   - E-mail address
8. Enter user ID, email address, or name or partial name with wildcard characters (asterisks) of the user or group in the Search for field.
9. Select the number of listings on each search results page in the Maximum results field.
10. Click Search. The results display the DN, display name, and email address of the users that matched your search.
11. Select a user and click Assign.
12. Click Done.

Sametime Instant Messaging user policy settings

You can grant or limit access to features in IBM Sametime Instant Messaging by enabling or disabling various policies for users. Instant Messaging policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take affect by editing the REFRESH_RULES_INTERVAL setting in the sametime.ini file.

All unauthenticated users have the anonymous policy, Sametime Instant Messaging Anonymous Policy, applied to them. For authenticated users, the Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match, then the default policy, Sametime Instant Messaging Default Policy, is applied.
In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

Table 9. Chat

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User must set this community as the default server community</td>
<td>Determines if this community can be connected to as a secondary community or if must it be the default community for the Sametime Connect client. When this policy is selected, users must log in to this community before they can log in to other communities. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 9. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to add multiple server communities</td>
<td>If this is checked, community preferences and menus are available to users. When the <strong>Allow user to add multiple server communities</strong> policy is set to <strong>Not selected</strong>, users cannot add their own secondary communities. When the policy becomes enabled, clients cannot log in to any secondary communities that were not set by the administrator. Administrator-defined secondary communities are not impacted by the policy. The client recognizes they are defined by the administrator and allows the user to log into them. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Allow user to add external users using Sametime Gateway communities</td>
<td>Allowing users to connect to external communities such as AIM, OCS, and Google Talk. If this policy is not allowed, the check box and text for adding external users by email address is not available in clients.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow user to save chat transcripts</td>
<td>If this is enabled, users see the File-Save option in the chat window. Chat history capabilities are available. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically save chat transcripts</td>
<td>This is not valid unless Allow user to save chat transcripts is selected. If this is not selected, then users do not see preferences for chat history or the chat history viewer in their clients. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
<td>Applies to Default Community Only?</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Maximum days to save automatically saved chat transcripts</td>
<td>If <strong>Allow to automatically save chat transcripts</strong> is selected, then a value must be entered in this field. Users cannot set a larger value in their clients than the one specified here. This setting does not apply to browser users.</td>
<td>365</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>Limit contact list size</td>
<td>This limits the number of contacts that users can enter in their contact lists.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Contacts</td>
<td>If <strong>Limit contact list size</strong> is selected, then a value must be entered in this field. Specify the number of contacts that users can enter in their contact lists.</td>
<td>500</td>
<td>500</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow all Sametime Connect features to be used with integrated clients</td>
<td>If this is not selected, some Sametime Connect features do not display when Sametime is integrated with other products. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow mobile client</td>
<td>This feature lets users deploy Sametime awareness and chat features mobile device.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 9. Chat (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime update site URL</td>
<td>Provides a URL where users can retrieve updates to features for the Sametime Connect client. This setting does not apply to browser users.</td>
<td>updates.sametime.com</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Table 10. Image Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow custom emoticons</td>
<td>Allows all actions on the preferences palette: new, import, export, add picture, add palettes. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow screen capture and images</td>
<td>Allows pasting and right-click copying of image and screen captures. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
<tr>
<td>Set maximum image size for custom emoticons, screen captures, and inline images</td>
<td>This setting includes images pasted inline through the palette emoticons, cut and paste, screen captures, and print screen. It does not include images sent through file transfer. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not Selected</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 10. Image Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB</td>
<td>If set maximum image size for custom emoticons, screen captures, and inline images is selected, then a value must be entered in this field. Users see a message if they attempt to send a file that is larger than the specified size. This setting does not apply to browser users.</td>
<td>500</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

### Table 11. File Transfer

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to transfer files</td>
<td>Allows user to transfer files to other users. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Maximum file transfer in Kilobytes</td>
<td>Limits the size of the file that can be transferred by the specified value in kilobytes. This setting does not apply to browser users.</td>
<td>1000</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Allow client-to-client file transfer</td>
<td>Allows users to transfer files without passing the files through the Sametime server. These files are not logged. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 11. File Transfer (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use exclude file types transfer list</td>
<td>Limits the types of files that users can transfer. This setting does not apply to browser users.</td>
<td>Not selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Types to exclude from transfer.</td>
<td>If <strong>Use exclude file types transfer list</strong> is selected, then a value must be entered in this field. Type the three-letter extension of each file type, separated by a comma or semicolon. Accepts bmp, gif, txt, pdf, sxi, sxc, sxw file extensions. Comma separated, values, and spaces are acceptable. This setting does not apply to browser users.</td>
<td>exe, com, bat</td>
<td>Blank</td>
<td>No</td>
</tr>
</tbody>
</table>

### Table 12. Plugin Management

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to install plug-in</td>
<td>Allows users to install plugins and updates from the Sametime Connect Tools &gt; Plug-ins menu. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Selected</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 12. Plugin Management (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sametime optional plug-in site URLs. Type the URLs separated by a comma or semicolon</td>
<td>If no value is specified, then the Check for Optional Features item on the Tools &gt; Plug-ins menu not valid. This setting does not apply to browser users.</td>
<td>Blank. Type the URLs separated by a comma or semicolon</td>
<td>Blank</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Meetings user policy settings

You can grant or limit access to features in meetings by enabling or disabling various policies for users. Policy changes take effect immediately.

All unauthenticated IBM Sametime users have the anonymous policy, Sametime Meetings Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match the default policy, Sametime Meetings Default Policy is applied.

Sametime does not allow anonymous users to create meeting rooms. Therefore, any policy that is related to authenticated users or the ability to create meeting rooms, does not apply to anonymous users.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

Note: Although Sametime Classic meetings are still managed on the server itself, you can set user policy for Sametime Classic meetings on the Meetings policy tab in the Sametime Classic Meetings section.

Table 13. General Meeting Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum persistent meeting rooms this user can own</td>
<td>Users are limited to creating this number of meeting rooms per user. When this limit is reached or set to zero, users cannot create more meeting rooms.</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Setting</td>
<td>Purpose</td>
<td>Default Policy</td>
<td>Anonymous Policy</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Allow user to create instant (nonpersistent) meeting rooms</td>
<td>If not selected, user does not see the capabilities for creating instant meetings. User can, still see the capabilities for using an existing room.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Automatically connect to meeting server when logging into Sametime Connect</td>
<td>If not selected the user must manually connect to each meeting room server to view the meetings there. This setting is stored with the client, so that changes in the policy do not take effect until after the next time the user logs in to the server. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching of meeting rooms</td>
<td>If not selected, users can attend meeting rooms only with a direct URL. The meeting room manager interface never shows. Only affects browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow searching of hidden meeting rooms</td>
<td>If selected, the interface allows the user to explicitly search for hidden meeting rooms by exact name. If not selected, the interface for searching for hidden meeting rooms does not appear, and hidden meeting rooms are never returned in search results.</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Show &quot;Scheduled Meetings&quot; view</td>
<td>Determines whether to show the &quot;Scheduled Meetings&quot; view in the shelf. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
</tbody>
</table>
Table 13. General Meeting Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow meetings to be recorded</td>
<td>Allows users to record meetings for rooms they have created. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow meeting content to be downloaded</td>
<td>Allow users to download content from the meeting library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Meeting room group chats</td>
<td><strong>Hidden</strong> - Users cannot see or create group chats. <strong>Read-only</strong> - Users can only read what others have typed into the group chat. <strong>Interactive</strong> - Users can type and read group chats.</td>
<td>Interactive</td>
<td>Interactive</td>
</tr>
<tr>
<td>Allow meeting room polls</td>
<td>Determines whether a presenter can send a poll to meeting participants.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
<tr>
<td>Allow annotations of uploaded content</td>
<td>Determines whether a presenter can use meeting room annotation tools when sharing documents from the meeting room library.</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 14. Meeting Room Library

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum file upload size, in Megabytes</td>
<td>Maximum file upload size for an individual user in megabytes. Users cannot upload a larger file into the library.</td>
<td>50</td>
<td>0</td>
</tr>
</tbody>
</table>
**Table 14. Meeting Room Library (continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum total size of library in Megabytes</td>
<td>Maximum total size in megabytes of files that a meeting room library can hold. When the library contains the maximum size or if the size is set to zero, users cannot upload files to the library. In addition, when the library’s maximum storage capacity has been reached, users may be unable to upload all their files even though their individual file upload size.</td>
<td>200</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 15. Screen Sharing**

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen sharing</td>
<td>Disabled - Users cannot share screens or applications. Share an application - Users can share a specific application. No other applications or their desktops are shared. Entire screen, frame, and applications - Users share their whole screen including any applications that they open on their screens.</td>
<td>Entire screen, frame, and applications</td>
<td>Entire screen, frame, and applications</td>
</tr>
<tr>
<td>Allow user to control another user’s shared screen</td>
<td>Allow others to control a user’s shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Allow peer-to-peer application sharing</td>
<td>Whenever this user hosts screen sharing, peer-to-peer can be used by any viewers that support it.</td>
<td>Selected</td>
<td>Not selected</td>
</tr>
</tbody>
</table>
### Table 15. Screen Sharing (continued)

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce bandwidth limitations.</td>
<td>Any time the user hosts sharing, the experience is limited by the value specified in the Maximum bandwidth size</td>
<td>Not selected</td>
<td>Not selected</td>
</tr>
<tr>
<td>Maximum bandwidth size, in Kilobytes per second:</td>
<td>This is not used unless &quot;Enforce bandwidth limitations&quot; is selected.</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

### Table 16. Sametime Classic Meetings.

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to create instant meetings and breakout sessions.</td>
<td>Lets users start a meeting from the contact list, from an existing chat, and from within a meeting (breakout session).</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow Sametime IP audio and video in instant meetings and breakout sessions.</td>
<td>No Does not allow use of Sametime Internet Protocol audio and video in instant meetings and breakout sessions.</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IP audio only</td>
<td>Allow use of Sametime Internet Protocol audio but not video in instant meetings and breakout sessions.</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IP video only</td>
<td>Allows use of Sametime Internet Protocol video but not audio in instant meetings and breakout sessions.</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 16. Sametime Classic Meetings (continued).

<table>
<thead>
<tr>
<th>Feature list</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow participation in meeting room chats.</td>
<td>Allows participants in the meeting to use the chat window to communicate with any other participant in the meeting.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow screen sharing</td>
<td><strong>No</strong> - Users cannot share screens or applications. <strong>Application only</strong> - Users can share a specific application. No other applications or their desktops are shared. <strong>Entire screen, frame, and applications</strong> - Users share their whole screen including any applications that they open on their screens.</td>
<td>Entire screen, frame, and applications</td>
<td>Not selected</td>
<td>No</td>
</tr>
<tr>
<td>Allow user to control another user's shared screen</td>
<td>Allows others to control a user's shared screen. Any participant can make changes to the shared information. This setting does not apply to browser users.</td>
<td>Selected</td>
<td>Not selected</td>
<td>No</td>
</tr>
</tbody>
</table>

**Media Manager user policy settings**

You can grant or limit access to media features in by enabling or disabling various policies for users. Media Manager policy changes take effect in 60 minutes by default.

You can change the default time that Instant Messaging and Media Manager policies take affect by editing the `REFRESH_RULES_INTERVAL` setting in the `sametime.ini` file.
All unauthenticated users will have the anonymous policy, Media Manager Anonymous Policy, applied to them. For authenticated users, Sametime searches for a user ID or group match, and then applies the highest weighted policy. If there is no match for the default policy, Media Manager Default Policy is applied.

In a deployment with multiple Sametime communities, most policies are applied when a user logs in to any community. However, some policies are only applied when the client logs in to the default community. The following tables flag those policies that are applied only when users log in to their default communities.

**Table 17. Telephony, Audio, and Video**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings</td>
<td>Allows outside vendors to provide audio and video for instant messages and instant meetings. This setting does not apply to browser meetings.</td>
<td>Not selected</td>
<td>Not selected</td>
<td></td>
</tr>
<tr>
<td>Allow changes to preferred numbers</td>
<td>If not selected, user cannot add telephony devices. This gives the administrator control over the devices that can make or receive calls in the system. &quot;Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings&quot; must be selected to specify this setting.</td>
<td>Selected</td>
<td>Selected</td>
<td></td>
</tr>
</tbody>
</table>
Table 17. Telephony, Audio, and Video (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice and video capabilities available through the Sametime Media Server:</td>
<td>Allows users to use computer audio and video in instant messages and instant meetings. Choices are:</td>
<td>Audio and video</td>
<td>Audio and video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Audio only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Audio and video</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This setting does not apply to browser users.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 18. Sametime Unified Telephony

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
<th>Default Policy</th>
<th>Anonymous Policy</th>
<th>Applies to Default Community Only?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow changes to the permanent call routing rule</td>
<td>If this setting is not selected a lock appears next to this rule in the user’s preferences. “Allow access to third-party service provider capabilities from contact lists, instant messages, and meetings” must be selected to specify this setting.</td>
<td>Selected</td>
<td>Selected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This setting does not apply to browser users.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Changing a user policy’s weight

IBM Sametime products implement user policies that have higher weights over policies with lower weights. You can change the weight of policies.

About this task

User policies in Sametime have weights. A policy’s weight determines whether or not its attributes take precedence over the attributes of other policies. For a given user or group assigned two or more policies, Sametime implements the policy with the highest weight. Anonymous policies always have the lowest weight; default policies have the next lowest weight. For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match. If no group matches are found, the default policy applied. You can change the weight of policies by moving them up and down the policy list of a Sametime product.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click the Sametime component with the policy with the weight that you want to change.
   - Instant Messaging
   - Meetings
   - Media Manager
5. Select a Policy ID from the list, and click Move Up or Move Down. Moving the policy up increases its weight; moving the policy down decreases its weight. You cannot change the weight of a default or anonymous policy.
Using nested groups in policy assignments

You can configure whether or not Sametime considers nested groups when it applies policies and how many levels deep that Sametime searches for the highest weighted group.

About this task

For authenticated users, Sametime searches for an exact ID match, and then applies the highest weighted policy. If there is no match for the user ID in any policy, the Sametime applies the highest weighted group match to which the user belongs. By default, Sametime searches through four levels of nested groups when determining the highest weighted policy.

For example, a fourth level assigned group would mean that the group is four levels above the user. In the following example the EMEAGroup is four levels above the user: EMEAGroup (level 4) contains UKGroup (level 3), which contains LondonGroup (level 2), which contains MarketingGroup (level 1), which contains the user.

Follow these steps to change the number of levels of nested groups that Sametime searches for the highest weighted policy. If a policy is assigned to a group higher than the nesting depth, that the default policy is assigned. Entering a large number as the maximum nested group depth can have an impact on performance.

Note: To change the maximum nested group depth for the Sametime Instant Messaging user policy, edit DIR_SEARCH_LEVEL_LIMIT parameter of the Sametime Community Server sametime.ini file.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console.
3. Click Manage Policies.
4. Click Preferences.
5. Enter a numerical value of -1 or greater in the Maximum Nested Group Depth field.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Sametime searches an infinite number of levels of nested groups.</td>
</tr>
<tr>
<td>0</td>
<td>Sametime searches for the user ID directly, and does not look in groups, nested or otherwise.</td>
</tr>
<tr>
<td>1</td>
<td>Sametime searches within groups, but not nested groups (groups within groups).</td>
</tr>
<tr>
<td>2 or greater.</td>
<td>Sametime searches nested groups up to and including the level specified.</td>
</tr>
</tbody>
</table>

6. Enter a number in minutes in the Policy Cache Timeout field. The default value is 30 minutes. The Policy cache stores policy assignments. This cache reduces the number of database operations required to provide policy information. For example, if Sametime calculates that user1 gets policy1, that is
stored in the cache. The next time that something requests user1's policy it does not have to calculate it. The timeout is how long the information stays in the cache.

7. Enter a number in minutes in the Group Membership Cache Timeout field. The default value is 30 minutes. The Group Membership cache stores the group membership information. This cache alleviates potential LDAP load issues due to group membership look-ups. You might want to update this timeout to reflect your site's LDAP administration operating procedures.

8. Click Apply.
9. Restart the servers.

Example

In following examples, use the this group structure:
1. Group1 contains user1
2. Group2 contains user2 and group1
3. Group3 contains user3 and group2
4. Group4 contains user4 and group3
5. Group5 contains user5 and group4
6. Group6 contains user6 and group5

Example 1: Nested group matches

Policy1 has a weight of 2 and is assigned Group6. Nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.

User1 and User2 get the default policy because they are not within the group search depth limit.

Example 2: Nesting has priority over policy weight

Policy1 has a weight of 2 and is assigned Group5. Policy2 has a weight of 3 and is assigned Group6. The nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets policy1 because it is in the 4th group nesting level from Group5.
3. User3 gets policy1 because it is in the 3rd group nesting level from Group5.
4. User4 gets policy1 because it is in the 2nd group nesting level from Group5.
5. User5 gets policy1 because it is in the 1st group nesting level from Group5.
6. User6 gets policy1 because it is in the 4th group nesting level from Group5.

Even though policy2 has a higher weight, it is not assigned to User2, User3, User4, and User5 because they have a lower level policy match.

Example 3: Policy weight breaks ties
Policy1 has a weight of 3 and is assigned to Group6. Policy2 has a weight of 2 and is assigned to Group6. The nesting level is the default of 4.
1. User1 gets the default policy because it is over the nesting level limit.
2. User2 gets the default policy because it is over the nesting level limit.
3. User3 gets policy1 because it is in the 4th group nesting level.
4. User4 gets policy1 because it is in the 3rd group nesting level.
5. User5 gets policy1 because it is in the 2nd group nesting level.
6. User6 gets policy1 because it is in the 1st group nesting level.

Since both Policy1 and Policy2 were at the same level, Policy1 won the tie breaker because it has a higher weight.

---

Administering a Sametime System Console

This section describes how to manage the IBM Sametime System Console.

Backing up the console database

The IBM Sametime System Console database stores information about all the Sametime servers that are connected to it.

About this task

Back up the database regularly to protect the server data and to minimize downtime if you need to restore lost or corrupted data. Follow the instructions in the DB2 information center:

http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp

Starting the Sametime System Console so you can administer servers

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

Before you begin

Verify that the Deployment Manager is running for the cell.

Procedure

1. Open a command window (on IBM i, run QSH command).
2. Navigate to the local app_server_root/profiles/STSCAppProfile profile directory and change to the bin directory.
3. Run the following command. Note that the name of the server is case sensitive:
   AIX, Linux, or Solaris
   .startupNode.sh
   .startupServer.sh STConsoleServer
   Windows
   startNode.bat
   startServer.bat STConsoleServer
   IBM i
   startNode
   startServer STConsoleServer
Administering a Sametime Community Server

This section describes how to manage an IBM Sametime Community Server

About this task

Use the instructions in this section to manage connectivity, community services, anonymous access, and business cards on the Sametime Community Server.

Managing administrator access and roles

Manage administrator access and roles using the Sametime Administration Tool.

Starting the Sametime Administration Tool

You administer Sametime through a web browser application. You must enable Java applets and JavaScript or ActiveX Controls in your browser to use the Sametime Administration Tool.

About this task

To start the Sametime Administration Tool:

Procedure

1. Enter the URL for the Sametime server:
   http://hostname/stcenter.nsf
   where hostname is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime server you want to administer.

   Note: For versions of Sametime that do not support web conferencing, enter the following URL in your browser: http://hostname.

   Note: For Sametime Entry and other Sametime offerings that do not include web conferencing, access the server page by typing http://hostname/ into a browser URL field where hostname is the fully qualified name of your Sametime server.

2. From the Sametime server home page (Sametime Welcome page), click Administer the Server.

3. Enter the administrator name and password specified during the Sametime server installation. The Sametime Administration Tool opens in its own web browser window.

Related concepts

Adding a new Sametime administrator

Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

Adding a Sametime administrator in Domino LDAP

Use the Domino Directory to give a group of administrators access to the Sametime Administration Tool.

A Sametime administrator name and password is specified during the Sametime installation and setup process. The administrator specified during the Sametime server installation and setup can access all features of the Sametime Administration Tool and can provide other administrators with access to the Sametime Administration Tool.
This is the procedure for adding an administrator in Domino. If your Sametime server is configured for LDAP, then you must create the new administrator using your LDAP Directory tools.

Creating a Person document for the administrator:

Administrators must have a Person document in the Domino Directory.

About this task

Follow these steps to create a Person document using the Sametime Administration Tool. If the administrator whom you are adding already has a Person document that contains a last name, user name, and Internet password, skip this procedure.

Procedure

1. From the Sametime server home page, click **Administer the Server**.
2. From the Sametime Administration Tool, click LDAP Directory:
3. Choose **Add Person**.
4. In the Person document, select the Basics tab.
5. Enter the user’s first, middle, and last name in the appropriate fields. Only the last name is required.
6. Enter a name for the user in the User Name field. An entry in this field is required for the user to authenticate with the Sametime server.
   You can use any of the following characters in a user name: A-Z, 0-9, dash (-), period (.), underscore (_), and space. Using other characters can cause unexpected results.
7. Enter an Internet password for the person in the "Internet password" field. An entry in this field is required for the user to authenticate when accessing the Sametime Administration Tool. There are no restrictions on the number of characters used in the Internet password.

   **Password character restrictions**
   In addition to non-English characters, the following characters must not be included in passwords used by Sametime:
   : \ } ' " &
8. Click **Save & Close**. The Person document is added to the Directory.

Creating an Administrators Group document:

Create a group document to hold the names of Sametime administrators.

About this task

Use the Sametime Administration Tool to create an Administrators Group document.

Procedure

1. From the Sametime server home page, click **Administer the Server**.
2. From the Sametime Administration Tool:
   - If you are using a Domino Directory with the Sametime server, select Domino Directory - Domino.
   - If you are using an LDAP directory with the Sametime server, select LDAP Directory.
3. Choose "Add Sametime Administrators - Create a group for the administrators."

4. Click Add Group.

5. Enter a name for the group in the "Group name" field (for example, "Administrators" or "Sametime Administrators").

6. For group type, select Multipurpose.

7. Optional: Enter a description of the group in the Description field.

8. In the Members field, list the names of users you want to access the Sametime Administration Tool.

   Make sure to enter the name exactly as it is entered in the topmost entry of the "User name" field of a user's Person document.


10. Enter the names of the group owners in the Owners field. Generally, the group owner is the administrator creating the group. Only the administrator listed in the Owners field can modify this Group document. If the Owners field is blank, any administrator can modify this Group document.

11. Click Save & Close.

Adding the Administrators Group document to Sametime database ACLs:

Add the Administrators Group document to Sametime database Access Control Lists (ACLs) and provide the Manager access level to the group.

About this task

In addition to ACL access levels, you must also specify the ACL privileges and roles that the Administrators Group (or an individual user) has in each database. Generally, for an Administrators Group, select all ACL privileges and roles.

Note: If you are adding individual user names to Sametime database ACLs instead of a group name, database roles can be used to prevent or allow access to specific features of the Sametime Administration Tool.

Add the Administrators Group to the ACLs of the following Sametime databases.

- **Sametime Configuration (stconfig.nsf)** - Stores the configuration parameters that are set from the Sametime Administration Tool.

- **Domino Directory or Address Book (names.nsf)** - Stores Person and Group documents, ACL settings, and other configuration information for the Domino/Web Application Services.

- **Sametime Log (stlog.nsf)** - Stores logging information.

- **Domino Web Administration (webadmin.nsf)** - Contains the Domino Web Administration client, which includes monitoring features for the HTTP Services and free disk space. This is the full Domino Web Administration client that is included with Domino servers.

Procedure

1. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
2. Choose "Add Sametime Administrators - Give the administrator group Manager access for all appropriate databases, such as stconf.nsf and stcenter.nsf." The Access Control options appear.

3. From the Databases list, select Sametime Configuration (stconfig.nsf).

   **Note:** The database filename appears below the Databases list.

4. Click **Access**.

5. Click **Add**. Enter the Administrators Group document name in the dialog box (for example, "Administrators" or "Sametime Administrators").

   If you are adding individual user names, enter the person's user name in the dialog box. Enter the name as it is entered in the top entry of the "User name" field on the user's Person document.

6. Click **OK**.

7. Select the Administrators Group name (or individual person's name) from the list in the Database Security window.

8. In the User Type drop-down list, select Group (or Person if you are adding an individual user's name).

9. In the Access drop-down list, select Manager.

10. Make sure that all ACL privileges, such as "Create documents" and "Delete documents," are selected.

11. Click **Roles**.

12. If you want the Administrators Group to have access to the full range of administrative functions, select all roles. Click **OK**.

   The roles determine which administration tasks the members of the group can perform. If you are adding individual user names to the ACLs, you can use the roles to control the administrative features that are available to individual administrators. For more information, see Roles in Sametime databases ACLs.

13. Click **Submit**.

14. After adding the Administrators Group to the ACL of the Sametime Configuration database (stconfig.nsf), repeat steps 4 through 14 to add the Administrators Group to the ACL of each of the Sametime databases listed below:

   - Domino Address Book or Domino Directory (names.nsf)
   - Sametime Online Meeting Center (stconf.nsf)
   - Sametime Log (stlog.nsf)
   - Sametime Self Registration (streg.nsf)
   - Domino Web Administration (webadmin.nsf)

**Modifying the Server document of the Sametime server:**

Add the Administrators Group document (or the name of an individual user) to two fields on the Server document.

**Procedure**

1. From the Sametime Administration Tool:

   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.

2. Choose "Add Sametime Administrators - Edit the Server document."
3. Click **Security**.

4. In the "Administrators" field of the Administrators section, type the name of the Administrators Group (or enter the name of an individual user).

   **Note:** Type a group name exactly as it appears in the Group document. If you are entering an individual user name in this field, type the user name exactly as it is entered in the topmost entry of the "User name" field on the Person document. Separate multiple entries in the "Administer the server from a browser" field with commas.

5. In the "Run unrestricted methods and operations" field of the Programmability Restrictions section, type the Administrators Group name (or an individual user's name). Separate multiple entries in this field with commas.

6. Click **Save & Close**.

**Adding and removing names from an Administrators Group document:**

Control access to the Sametime Administration Tool by editing the Group document.

**About this task**

Adding a user's name to the Administrators Group document provides the user with access to the Sametime Administration Tool. Removing a user's name from the Group document revokes the user's access to the Sametime Administration Tool.

**Procedure**

1. From the Sametime server home page, click **Administer the Server**.
2. From the Sametime Administration Tool:
   - If you are using the Domino Directory with the Sametime server, choose Domino Directory - Domino.
   - If you are using an LDAP Directory with the Sametime server, choose LDAP Directory.
3. Choose "Add Sametime Administrators - Create a group for the administrators."
4. Double-click a group name.
5. Select **Edit Group**.
6. In the Members field, add or remove a user's name from the Group document.
   - If you add a user's name, the user must have a Person document in the Domino Directory that contains a last name, user name, and Internet password. Make sure to enter the name exactly as it is entered in the top entry of the "User name" field of a user's Person document.
   - The user must enter a last name or user name and the Internet password from the Person document to access the Sametime Administration Tool.
7. Click **Save & Close**.

**Sametime database default ACL settings**

See the following tables to determine the default ACL settings for Sametime databases.
Table 19. stconfig.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 20. stconf.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 21. names.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Author</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td></td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 22. stpolicy.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>No Access</td>
</tr>
</tbody>
</table>
Table 22. stpolicy.nsf database default ACL settings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td></td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td></td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td></td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td></td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 23. stlog.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Reader</td>
</tr>
<tr>
<td>Create documents</td>
<td></td>
</tr>
<tr>
<td>Delete documents</td>
<td></td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Table 24. stnamechange.nsf database default ACL settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Manager</td>
</tr>
<tr>
<td>Create documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create private agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Create personal folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create shared folders/views</td>
<td>Selected</td>
</tr>
<tr>
<td>Create LotusScript/Java agents</td>
<td>Selected</td>
</tr>
<tr>
<td>Read public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Write public documents</td>
<td>Selected</td>
</tr>
<tr>
<td>Replicate or copy documents</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Roles in Sametime database ACLs

Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.
For example, the Sametime Configuration database (stconfig.nsf) ACL contains three roles: ServerMonitor, ServerAdmin, or DatabaseAdmin. If you assign only the ServerMonitor role to an administrator, the administrator can monitor server memory, disk space, and other server statistics but cannot perform any other administrative functions. Assign all roles to an administrator if you want the administrator to have full access to all administrative functions.

Access Control List (ACL) roles are defined in the following Sametime databases:

**Roles in the Sametime Configuration database (stconfig.nsf):**

The Sametime Configuration database (stconfig.nsf) stores the values for parameters that are available from the Sametime Administration Tool. The roles in this database affect the administrative tasks that an administrator can perform from the Sametime Administration Tool.

The following table lists the commands and features available with the Sametime Administration Tool and the roles that an administrator must be assigned in the stconfig.nsf database to use the Sametime Administration Tool commands and features. If an administrator does not have the appropriate roles, the Sametime Administration Tool does not display the command.

<table>
<thead>
<tr>
<th>Command Group</th>
<th>Command or feature</th>
<th>Role required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message From Administrator</td>
<td>Sends message to all users logged into Community Services</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Monitoring</td>
<td>All monitoring features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Logging</td>
<td>All logging features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Directory</td>
<td>Add directory features</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Configuration</td>
<td>Connectivity, Community Services, Meeting Services, Audio/Video Services</td>
<td>[ServerMonitor] or [SametimeAdmin] or [DatabaseAdmin]</td>
</tr>
<tr>
<td>Help</td>
<td>Online help for administrators</td>
<td>No roles required</td>
</tr>
</tbody>
</table>

**Note:** The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.

**Roles in the Domino Directory (names.nsf):**

The Domino Directory (or Address Book) contains the Person and Group documents that you create and edit when you use the Sametime Administration
Tool. The roles in the Domino Directory determine who can create or edit a particular type of document in the Directory.

The Domino Directory also contains the Server document that you access to provide another user with administrative privileges to the Sametime Administration Tool.

**Note:** If you use Sametime in a Domino environment, the Domino Directory roles function the same as they do on Domino servers.

The Domino Directory contains eight roles. The privileges for each role are listed in this table:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserCreator</td>
<td>Allows an administrator to create Person documents in the Domino Directory</td>
</tr>
<tr>
<td>UserModifier</td>
<td>Allows an administrator to edit all Person documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupCreator</td>
<td>Allows an administrator to create Group documents in the Domino Directory</td>
</tr>
<tr>
<td>GroupModifier</td>
<td>Allows an administrator to edit all Group documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerCreator</td>
<td>Allows an administrator to create Server documents in the Domino Directory</td>
</tr>
<tr>
<td>ServerModifier</td>
<td>Allows an administrator to edit all Server documents in the Domino Directory</td>
</tr>
<tr>
<td>NetCreator</td>
<td>Not used by Sametime</td>
</tr>
<tr>
<td>NetModifier</td>
<td>Not used by Sametime</td>
</tr>
</tbody>
</table>

**Related reference**
Roles in Sametime database ACLs
Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

**Roles in the Sametime Meeting Center (stconf.nsf):**
The Sametime Meeting Center database contains only the Sametime Admin role.
Role Description

Sametime Admin

- Allows an administrator to see hidden meetings displayed in the All Meetings view of the Meeting Center.
- Allows an administrator to see the Hidden Meetings view in the Meeting Center. This view displays only hidden meetings.
- Allows the administrator to alter the meeting details of any meeting. For example, the administrator can delete or change the end time of a meeting that the administrator did not create.
- Allows an administrator to see and use the "Delete the Recording," "Export the Recording," "Replace the Recording," and Import Recording options in the Meeting Center forms. These features enable the administrator to manage the recorded meeting files if the administrator makes the Record and Playback feature available on the Sametime server.

**Note:** The Domino server cannot resolve the user if given the internet address in the person entry that defines the internal ID of a Sametime user. The mail attribute is not supported in this field. The field may be left blank.

**Related reference**

Roles in Sametime database ACLs
Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

**Roles in the Domino Web Administration database (webadmin.nsf):**

The Domino Web Administration database is available on the Sametime server to enable administrators to monitor the HTTP server and access logging information about the Domino Application Services.

The following table defines the roles in the Domino Web Administration database:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerAdmin</td>
<td>A Sametime administrator requires this role to access the Server document when providing other users with access to the Sametime Administration Tool.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServerMonitor</td>
<td>A Sametime administrator requires this role to access the Monitoring - Miscellaneous functions of the Sametime Administration Tool. These monitoring functions enable the administrator to monitor HTTP commands and requests, server memory usage, and free disk space. The Sametime administrator also requires this role to access the Logging - Domino Log functions of the Sametime Administration Tool, which report information about the Domino Application Services.</td>
</tr>
<tr>
<td>DatabaseAdmin</td>
<td>A Sametime administrator requires this role to change database ACLs from the Sametime Administration Tool.</td>
</tr>
<tr>
<td>FileRead</td>
<td>This feature provides access to the Configuration - System Files (read-only) command of the Domino Web Administration Tool. This feature is usually not used with Sametime.</td>
</tr>
<tr>
<td>FileModify</td>
<td>This feature provides access to the Configuration - System Files (read/write) command. This feature is usually not used with Sametime.</td>
</tr>
</tbody>
</table>

Related reference

Roles in Sametime database ACLs
Roles provide a way to define the access an administrator has to the features and settings of the Sametime Administration Tool.

Domino log
To access the Domino log, choose Logging - Domino Log in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

Managing trusted IP addresses

Whenever you install a server that communicates with a community server, you must add the new server's IP address to the community server's settings.

About this task

The community server accepts connections from the Sametime Media Manager, the Sametime Gateway, the Sametime Community Multiplexer, and the Sametime Proxy Server, as well as other servers that are listed in the Community Services page. To ensure that the Sametime Community Server trusts these components when they establish a connection, you must add the trusted server's IP address to the community server.

If you are installing a cluster of media manager servers, gateway servers, or proxy servers, be sure to complete include the IP address of the primary node as well as every secondary node in the cluster (you do not need to include the deployment manager).
You do not need to add the system console's IP address because it is added automatically when you install the community server using a deployment plan or when you register the community server with the system console after installation.

This task must be completed separately for each server within a community server cluster, as well as for multiple non-clustered community servers.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the list of trusted IP addresses that you want to change.
4. Click the **Connectivity** tab.
5. Under **Trusted Servers**, enter the IP address of the server that must connect to the Sametime Community Server in the **New IP Address** field, and click **Add**.

   **Note:**
   - If you have a cluster, type the IP addresses of the primary node and all secondary nodes, separating each address with a comma. Do not include the IP address of the deployment manager.
   - For the media manager, enter the Conference Manager server IP address.
   To delete an IP address from the list, select it and click **Delete Selected**.
6. Click **OK**.
7. Restart the community server for the change to take effect.

**Managing community services**

Community services settings support all online presence (or awareness), instant messaging, and chat features at a server-wide level. These settings supersede any feature settings that you set at the policy level for users or groups. Community services settings carry a greater weight.

**Managing general community services**

The general community services settings control the interaction of the IBM Sametime Community Server with an LDAP directory and the maximum number of users allowed on the server.

**About this task**

These settings must be addressed for each server within a Sametime Community Server cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the **Community Services** tab.
5. Use the following table to set general server-wide settings for users of the Sametime Community Server.
### Table 25. Server-wide settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of entries on each page in dialog boxes that show names in the directory</td>
<td>Controls the number of user and group names that display when a user browses the directory. When an user browses the names and groups in the directory, the directory entries (names and groups) are listed on “pages” in a dialog box. The default is 100 entries per page. It is best to use a setting between 100 and 200 entries. Higher settings cause more data to be transmitted on the network when a user browses the directory.</td>
</tr>
<tr>
<td>How often to poll for new names added to the Sametime community directory (minutes)</td>
<td>Controls how frequently the cache of user names is updated with new information from the directory. The Sametime Community Server maintains a cache that contains information about the users and groups in the community. This cache must be or refreshed periodically to ensure that users who have recently been added to a directory can be displayed in the presence lists of all Sametime clients. The update occurs only if changes are made to the directory during the update interval. The default setting is 60 minutes.</td>
</tr>
<tr>
<td>How often to poll for new servers added to the Sametime community (minutes)</td>
<td>Controls the time interval in which the Sametime Community Server receives an updated list of all Sametime servers. If you have deployed more than one Sametime Community Server, the community services on each server must maintain a list of all other Sametime Community Servers in the Sametime community. Community services uses this list to ensure that users who have different home servers or different home clusters can see each other in presence lists and communicate through instant messaging and chat. The default setting is 60 minutes.</td>
</tr>
<tr>
<td>Maximum user and server connections to the community server</td>
<td>Controls the maximum number of connections allowed to Sametime Community Server. The connections include both client connections and server-to-server connections. A client connection occurs when a user starts the Sametime client. Server-to-server connections occur when you have deployed multiple Sametime Community Servers and different home servers are specified for users. The limit is 20,000 connections.</td>
</tr>
</tbody>
</table>
Table 25. Server-wide settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the authentication type that users can use while logging into the Community server:</td>
<td>Controls the authentication type. When LTPA or Sametime Tokens option is selected, the Sametime Community Server accepts authentication tokens generated by both Single-Sign On (SSO) and the Secrets and Tokens databases on the Sametime Community Server. This option is selected by default. When LTPA only is selected, the Sametime Community Server accepts authentication tokens generated only by SSO (LTPA tokens).</td>
</tr>
<tr>
<td>• LTPA or Sametime token</td>
<td></td>
</tr>
<tr>
<td>• LTPA only</td>
<td></td>
</tr>
</tbody>
</table>

6. Click OK.
7. Restart the Sametime Community Server for settings to take effect.

Saving transcripts of chats and meetings

You can enable the Sametime Community Server to save transcripts from two-way and multiple-user chats and from chats in meetings. Two-way chats are managed with the server’s native Chat Logging application. Multiple-user chats and meeting chats are managed with the Places server application.

Enabling local chat logging:

Each text chat has a transcript, the record of the text messages exchanged between chat partners during a chat session. You can configure the IBM Sametime Community Server to automatically log all chats and announcements, making these transcripts available to users for viewing in their chat history.

Procedure

1. In a text editor, open the sametime.ini file, which is located in the Sametime Community Server installation directory (for example: C:\Program Files\lotus\domino).
2. In the [Config] section, set the value for ST_LOG_ALL_CHATS.
   • ST_LOG_ALL_CHATS=0 is the default behavior, which logs only part of the two-user chats.
   • ST_LOG_ALL_CHATS=1 logs all two-user chats.
3. In the [Config] section, set the value for CHAT_LOGGING_MANDATORY.
   • CHAT_LOGGING_MANDATORY=0 is the default behavior, which makes chat logging optional. If this line is missing, Sametime also uses the default behavior to make chat logging optional.
   • CHAT_LOGGING_MANDATORY=1 enforces chat logging.
4. In the [Config] section, set the value for REMOTE_CHAT_LOGGING to 1.
   • REMOTE_CHAT_LOGGING=0, the default, does not enable remote chat logging.
   • REMOTE_CHAT_LOGGING=1 ensures that a given server can enable remote chat logging for multiple-user chats and chats in meetings.
5. In the [Config] section, set the value for CL_USE_USER_DN. If this setting is not found, the server defaults to using the Sametime user ID as the user’s identifier for a chat log.
   • CL_USE_USER_DN=0 uses the Sametime user ID as the user’s identifier for a chat log.
• **CL_USE_USER_DN=1** uses the user DN and if the DN is not found, uses the Sametime user ID as the user’s identifier for a chat log. The DN may be either the Sametime user ID or another attribute. Announcement originators and recipients can only be identified by their Sametime user IDs. Banning and logging must be done with Sametime user IDs rather than DNs. Do not set the value to 1 if that behavior does not work for your environment.

6. In the [ST_BB_NAMES] section, set the value for **ST_CHAT_LOG**. The StChatLogFile library (or libstchatlogfile.so on AIX, Linux, and Solaris platforms) is a sample of how to implement a chat logging black box using the Sametime SDK.

   - **ST_CHAT_LOG=N/A**
     
     The default of N/A means that Sametime does not attempt to load any chat logging black box. If you do not want StChatLog.dll to be used by Sametime, leave the default of N/A; do not remove the line.

   - **ST_CHAT_LOG=File**
     
     The value `File` describes the suffix to an StChatLog base name of the chat logging black box library. For example, to load your StChatLogMyCustom.dll file, set the value to `ST_CHAT_LOG=MyCustom`.

   **Note**: The StChatLogFile sample is not supported, and is not recommended for use in deployment environments.

7. Close and save the file.

8. Log in to the Integrated Solutions Console.

9. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.

10. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.

11. Click the **Community Services** tab.

12. In the Server Features section, under **Enable chat logging**, select one of the following choices:
   - **Always**
     
     With mandatory logging, the sametime.ini file must have this value to classify the server as a mandatory chat logging server:
     
     `CHAT_LOGGING_MANDATORY=1`
   - **When available**
     
     When logging is enabled when it is available, the sametime.ini file must have these values to allow remote chat logging:
     
     - `REMOTE_CHATLOGGING=1`
     - `CHAT_LOGGING_MANDATORY=0` (or is not provided)
   - **Never**
     
     With logging set to Never, the sametime.ini file must have these values to allow remote chat logging for other servers:
     
     - `REMOTE_CHATLOGGING=1`
     - `CHAT_LOGGING_MANDATORY=0` (or is not provided)

13. Click **OK**.

14. Restart the Sametime Community Server for settings to take effect.
What to do next

To find out more IBM Sametime chat logging and how to extend its features, see this article in the Sametime wiki: New features of IBM Sametime 8.x chat logging and how to extend its SDK.

Enabling remote chat logging for places:

Mandatory chat logging server settings on a user’s home server determine if chat logging is mandatory for this server’s users. If a user has access to multiple-user chats or chats in meetings on servers that do not require mandatory logging, set up the server that manages a given n-way chat as a remote chat logging server to fulfill the mandatory chat logging requirement. Remote logging handles chat logs for multiple-user chats and chats in meetings if a local Chat Logging service is disabled (either Never chat logging mode is defined or a local Chat Logging service is down). The two-way chats are logged on the home server of the chat participants. If two-way chat participants have different home servers, the chat is logged on both servers. Mandatory chat logging configuration requires all servers in the distributed environment to be running Sametime 8.5.2.

About this task

A home server with mandatory chat logging must have the following settings to be recognized by remote logging servers:

- The server logging mode is set to Always in the Community Services tab in the Sametime System Console (or STRICT if set in stconfig.nsf).
- CHAT_LOGGING_MANDATORY=1 flag is set in the [Config] section of the sametime.ini file.

All servers involved in remote logging must be configured like this:

- The server logging mode is set to When available or Never in the Community services tab in the Sametime System Console (or OFF or RELAX if set in stconfig.nsf).
- REMOTE_CHATLOGGING=1 flag is set in the [Config] section of the sametime.ini file.

In most cases, the n-way chat logging is logged on users’ home servers. The one exception is if a user whose home server is set to mandatory chat logging joins a chat that is already being logged on a remote chat logging server. In that case, the n-way chat continues to be logged only on that server in Always logging mode. N-way chats are not logged on multiple servers.

Other chat logging settings are determined by the server’s chat logging black box. If chat logging fails, for example, if there is a database error, the chat log for a mandatory chat user is destroyed.

Allowing users to transfer files to each other

Community Services allow users to transfer files to each other over the network while using Sametime Connect.

About this task

When you enable this feature, you should also set a file size limit and virus scanning preference.
Computer viruses can be spread through transferred files. To protect against this possibility, users should have current third-party anti-virus software installed. The Virus scan files setting should be enabled and set to scan all files.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. In the Server Features section, click Allow users to transfer files to each other.
6. To increase or decrease the size of files that users can transfer, enter a value in the Maximum file transfer size, in Kilobytes field.
7. Under Virus scan files, select one of the following choices:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>If scanning cannot be done, the file is not transferred</td>
</tr>
<tr>
<td>When available</td>
<td>The file is sent with a message that the file was not scanned, allowing the user to decide how to handle the file, or it is not sent if scanning reveals a virus</td>
</tr>
<tr>
<td>Never</td>
<td>Files are not scanned</td>
</tr>
</tbody>
</table>

8. Click OK.
9. Restart the Sametime Community Server for settings to take effect.

**Allowing users to send announcements**

Community Services allows users to send unencrypted announcements to others who are online in the Sametime Community.

**About this task**

When you enable this feature users can:

- Send unencrypted announcements to anyone who is online in Sametime Connect or in an online meeting. To receive an announcement, a user must be online, and in either active or away status. Users who are offline or have a status of "do not disturb" do not receive announcements.
- Allow the recipients of the announcement to respond to the announcement, or prevent them from responding.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Community Services tab.
5. In the Server Features section, click Allow users to send announcements (unencrypted one-way messages).
6. Click OK.
7. Restart the Sametime Community Server for settings to take effect.

Managing anonymous access to virtual places

The Sametime Software Development Kit provides developers with the capability to build applications that create virtual places. Anonymous users can enter a virtual place and have awareness of other users in the same virtual place.

About this task

This capability to have awareness of other users in the same virtual place is sometimes called place-based awareness. Place-based awareness differs from community-wide awareness. With community-wide awareness, users can have awareness of any user in the community who is online. IBM Sametime Connect provides users with community-wide awareness functionality. Anonymous users are not allowed to have community-wide awareness in any Sametime clients.

The Anonymous users can enter virtual places field controls the ability of anonymous users to enter virtual places created by custom-built applications created with the Sametime Software Development Kit. For more information on virtual places, see the IMWC Directory and Database Access Toolkit documentation available from IBM developerWorks® at http://www.ibm.com/developerworks/lotus/downloads/toolkits.html.

Enter information for anonymous access to a virtual place. Each attendee who accepts the default name has a number added to the end (For example, User1, User2).

This task must be completed separately for each server within a Sametime Community Server cluster.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
4. Click the Anonymous tab.
5. Click the Anonymous users can enter virtual places

Note: The following fields do not take effect unless the Anonymous users can enter virtual places field is selected.

6. If you want to let an anonymous user have a unique display name when accessing a Sametime application that includes awareness, click Users of Sametime applications (databases such as stconf.nsf or websites) can specify a display name so that they do not appear online as "anonymous." A display name entry dialog box appears when a user accesses the Sametime application. This display name allows the anonymous user to be individually identified in any presence lists in the Sametime application.

Note: The ACL settings of the application must allow anonymous access, too.
7. If you want to have a domain name automatically appended to the display name entered by the user at the name entry dialog box, click **Default domain for anonymous users**.

8. If you want a name to appear by default in the name entry dialog box, click **Default name**. For instance, if the **Default name** field contains the entry User the first person entering a meeting sees User displayed by default in the name field of the name entry dialog box. If the person accepts the default and enters the application, the person is identified as User1 in any presence list in the application.

9. Specify the level of access that an anonymous user of an application enabled with Sametime technology has to the directory. You can limit an anonymous user's ability to view names in the directory. For example, you might prevent anonymous users from browsing all names in a directory or searching for names in the directory.
   - **Users cannot browse or search the Directory**
     Anonymous users cannot search or browse the directory.
   - **Users can type names to add them to an awareness list**
     Anonymous users can type text in an user search interface to search for person or group entries in the directory. However, users cannot view or browse a list containing all entries in the directory. Users might perform such searches to add users to a presence list.
   - **Users can browse the directory (see a list of names) or type names (resolve users and groups)**
     Anonymous users can type text in an user search interface and search for group or person entries in the directory. Anonymous users can also browse lists that contain all entries in the directory. When this option is selected, anonymous users can see all group and name entries in the directory, but cannot see the content of a group entry (the list of names within a group entry). Users cannot browse the LDAP directory on the LDAP server.
   - **Users can browse the directory to see group content and names, or type names**
     Anonymous users have all searching and browsing privileges described for the **Users can browse the directory (see a list of names) or type names (resolve users and groups)** setting above. In addition, users can search and browse within group entries in the directory and access the user and group names that are specified within group entries in the directory.

10. Click **OK**

11. Restart the Sametime Community Server for settings to take effect.

**Sending a message to all users**

Use the Sametime Administration Tool to simultaneously send a single message to all users currently logged in to Community Services from any Sametime client.

**About this task**

Follow these steps to send a message to all users currently logged in to Community Services.

**Procedure**

1. Open a browser and navigate to the Sametime Community Server.
   Type the following address:
   http://host_name/servlet/auth/admin
where *host_name* is the fully qualified host name of the server; for example:

http://commsvr1.example.com/servlet/auth/admin

2. From the Sametime home page, click **Administer the Server**.
3. Log in as the Sametime administrator.
4. Select **Message From Administrator**.
5. Enter the message in the text box provided.
6. Click **Send**. You receive a confirmation that your message was sent.

**Managing business cards**

You can configure the IBM Sametime Community Server so that business card information about an individual displays when a user hovers over a name in a chat window or a contact list.

**About this task**

Business card can access user information from any of three types of storage repositories: the native Domino directory, the LDAP directory (including Domino LDAP), or a custom Notes application. Each repository stores user information differently, so to facilitate user searches, Sametime provides a search engine, called a black box, for each storage type.

Since there are three different storage types, Sametime provides three different black boxes to search for user information (one per storage type). These are:

- LDAP – used to search a LDAP directory
- Notes – used to search a native Domino directory
- Notes_custom_db – used to search a customized Notes application

Using information in the LDAP server or the native Domino directory, you can choose the fields that represent the information that you want to display in the business card. The available fields are:

- Photo
- Name
- Company
- E-mail address
- Telephone
- Address or location
- Title

You can set up or change the details you want to retrieve by changing the values for these fields on the main Business Card page.

**Configuring business cards using an LDAP directory**

Follow these steps to configure the business card using an LDAP directory. Domino LDAP is considered an LDAP directory.

**Before you begin**

Before you start setting up your business cards, be sure the following conditions are true for your site.

- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
• Sametime authentication is configured to use an LDAP directory
• The LDAP server is running and accessible by the Sametime Community Server
• All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account and password
• The Sametime Community Server is running
• For Domino LDAP only: To allow anonymous users to access required user details, you can edit the All Servers document in names.nsf. Under the LDAP tab, all LDAP attributes that you want to be retrieved by anonymous users should be added to the list of Anonymous Users Can Query.

About this task

This task must be completed separately for each server within a Sametime Community Server cluster.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server with the business card information that you want to add or change.
4. Click the Business Card tab.
5. In the Business Card Contents section, select the attribute you want displayed in users’ business cards, and then click Add to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click Remove.
6. Under Attribute Definition, choose Attribute Values that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose User Defined. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

Domino LDAP does not contain the postalAddress field. The value retrieved for this LDAP attribute is the concatenation of City, State/Province, and Country. Also, Domino LDAP contains a hidden field for the ou attribute. This field cannot be set through the Domino LDAP, and a third-party LDAP management tool can be used to add a value to it.

7. If you select User Defined for an Attribute Value, then enter an attribute to map to the Attribute Name.
8. Click OK.
9. Restart the Sametime Community Server.

**What to do next**

**Special considerations**

In a configuration where:

- Sametime is configured with LDAP
- UserInfo is configured to ignore configuration updates
- The Sametime ID is configured to an attribute different then a DN

You must add additional parameters to the *UserInfoConfig.xml* file to correctly support this type of Sametime ID.

1. Open the *UserInfoConfig.xml* file.
2. Locate the `StorageDetail` tag of the relevant LDAP and add the following flags:
   
   ```xml
   UserIdAttribute= <the chosen attribute for userid such as cn>
   PersonObjectClass= <the required object class such as OrganizationalPerson>
   ```
3. Save and close the file.
4. Restart the server.

**Configuring business card photos for Domino LDAP:**

To store photos in Domino LDAP and enable UserInfo to retrieve them, please follow the steps below. A third-party LDAP management tool is required for adding a JPEG Photo field to Domino LDAP. Most LDAP V3-compliant tools will work.

**Before you begin**

Configuring Business Card with an authenticated LDAP bind account is highly recommended. Allowing Anonymous LDAP Schema write access is a security risk and additional security changes to Domino Directory Access Control List may be required to allow anonymous write access to Domino LDAP.

**Procedure**

1. Use Domino Administrator to enable Domino LDAP write access. Within default *Configuration Setting Document LDAP*, click Yes next to Allow LDAP users write access.
2. Using the third party LDAP tool, connect to the Domino LDAP server and bind as a Domino Administrator. Once a successful connection is made, select a user and add an Attribute. The Attribute name for Domino LDAP should be specified as: jpegphoto;binary and the type should be selected as binary. Note the name being used for the attribute. If you use just jpegPhoto or Photo as the name, depending on the LDAP tool, you might not be able to store images in the field. The `-;binary` is required for Domino LDAP to understand the binary data.
3. Use the third party LDAP tool to import the JPEG or GIF photo into the new field.

   **Note:** The size of the image should be smaller then 64kb.

4. Use `ldapsearch` or the LDAP tool to check that the photo has uploaded successfully.
5. Log in to the Integrated Solutions Console.
   a. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
   b. In the **Sametime Community Servers** list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the **Business Card** tab.
   d. In the Business Card Contents section, select the **Photo** attribute, and then click **Add** to include it in the business card.
   e. Under **Attribute Definition**, choose **User Defined** as the attribute value for **Photo**.
   f. In the User Defined column next to **Photo**, type **jpegphoto;binary**.
   g. Click **OK**.

   a. Expand the **Configurations > Servers**, and select the **Configurations** view. Open this document in Edit mode and click the Basic tab. Enable the **Use these settings as the default settings for all servers** option. The LDAP tab appears.
   b. Click the LDAP tab. Click **Choose Fields that Anonymous Users Can Query via LDAP**.
   c. Click **New** in the window that displays.
   d. Type **jpegphoto** in the field and click **OK** to save the value. Click **OK** again to close the window.
   e. **Save** and close the document.

7. Restart the LDAP server. From the server console, type **tell ldap quit** and then **load ldap**.


9. Browse to **UserInfoConfig.xml** file within the Domino Install folder. Under Details section, check to make sure **Photo** field is set to **jpegPhoto;binary**.

   ```xml
   <Detail Id="Photo" FieldName="jpegPhoto;binary" Type="image/jpeg" />
   ```

10. Restart the Sametime Community Server.

**Configuring business card photos for the Sametime browser client:**

Follow these steps to configure the business card photo that displays for users that chat using the IBM Sametime browser client.

**Before you begin**

Enable the **PhotoURL** attribute in your LDAP directory. Refer to the documentation for your LDAP directory.

**Procedure**

1. In the Sametime Community Server, find the **UserInfoConfig.xml** file.
2. Open the file with a text editor, and add the following tag to the Details section:
   
   ```xml
   <Detail Id="PhotoURL" FieldName="PhotoURL" Type="text/plain"/>
   ```
3. Restart the Sametime Community Server.
4. Upload user photos into a web server repository, so that users can access the photos using a URL. For example: http://iddirectory.mycompany.com/userphoto/mybusinesscard.jpg

Verifying business card configuration:

After you have configured your business card feature, you can verify the configuration.

About this task

To display user information, the business card uses an IBM Sametime Community Server application named UserInfo. UserInfo retrieves and delivers user information for each client request to view a user's business card. Follow these instructions to verify your business card configuration.

Procedure

1. Open \lotus\domino\UserInfoConfig.xml in a text editor. When you use an LDAP directory to store user information, the UserInfoConfig.xml should look like this:

```xml
<UserInformation>
    <Resources>
        <Storage type="LDAP">
            <CommonField CommonFieldName="MailAddress"/>
            <StorageDetails HostName="ldap.mycompany.com" Port="389" UserName="username"
                Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2"
                SearchFilter="(&(objectclass=organizationalPerson)|(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s))")="/>
            <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
            <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
            <SslProperties KeyStorePath="/" KeyStorePassword="/"/>
        </StorageDetails>
        <Details>
            <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
            <Detail Id="Name" FieldName="cn" Type="text/plain"/>
            <Detail Id="Title" FieldName="title" Type="text/plain"/>
            <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
            <Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
            <Detail Id="Company" FieldName="ou" Type="text/plain"/>
            <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
        </Details>
    </Resources>
    <ParamsSets>
        <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
        <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    </ParamsSets>
    <BlackBoxConfiguration>
        <BlackBox type="LDAP" name="com.ibm.sametime.userinfo.userinfobb.UserInfoLdapBB" MaxInstances="5"/>
    </BlackBoxConfiguration>
</UserInformation>
```

2. Verify that stconfig.nsf has valid data for the LDAP document and the UserInfo document.

3. Verify that the HTTP server has been restarted after any changes have been made to the xml file.

Configuring business cards using a Domino directory

This task demonstrates how to configure the business card using the Domino directory.

Before you begin

Prerequisites:
IBM Lotus Domino and IBM Sametime Community Server have been installed and configured.
Sametime authentication is configured to use an Domino directory.
The Sametime Community Server is running.

About this task

Note: IBM recommends that you use a third party LDAP directory, and not Domino, because Domino does not have a standard field for photos (a jpegPhoto field). Using a third party LDAP directory avoids unnecessary replacement of the default jpegPhoto field.

Follow these steps to configure the Business Card to display data that is stored in a single data repository—a Domino directory.

Procedure

1. Open an Internet browser and enter this URL into the URL-locater field:

http://example.com/stcenter.nsf, substituting the host name example.com with your server’s actual host name.

2. Click Administer the server, and then log in as Administrator.

3. Click the plus sign next to Configuration to expand the contents, and then click Business Card Setup.

4. In the User Information section, select the entry you want displayed in users’ business cards, and then click Add to move the entry to the right-side list box.

To remove preselected entries, click the entry and click Remove. In most cases, the Attribute name and Attribute value section of the business card interface requires no modification; however, if the information you want displayed in the users’ business cards is not mapped to the default fields provided by the users’ person documents, then you might need to update the Attribute name and Attribute value section. The following table lists the default attribute value that is mapped to each attribute name.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

5. Click Update to save the changes.

To display user information, the business card feature uses a server application called UserInfo which is designed to retrieve and deliver user information for each incoming request from a client to view a specific user’s business card. To ensure this application is configured properly to search the proper data storage, confirm the settings as defined in UserInfo.xml.

6. Open the UserInfoConfig.xml file in a text editor. The file is located in the Domino program directory (\\lotus\domino\UserInfoConfig.xml). Here is a section of the UserInfoConfig file edited for XYZ’s scenario:
<UserInformation>
<Resources>
<Storage type="NOTES">
<CommonField CommonFieldFieldName="MailAddress"/>
<Details>
  <Detail Id="Location" FieldName="Location" Type="text/plain"/>
  <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
  <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain"/>
  <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
  <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
  <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
</Details>
</Storage>
</Resources>

<ParamsSets>
<Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
<Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
</ParamsSets>

<BlackBoxConfiguration>
<BlackBox type="NOTES" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesBB">
  MaxInstances="4"/>
</BlackBoxConfiguration>
</UserInformation>

What to do next

There might be specific configurations where the names in the Domino directory include commas (,). By default, these special characters are treated as LDAP separators. In order to treat them as regular characters, add the following flag to UserInfoConfig.xml:

<UseUnformattedNotesNames />

This setting take affect after the server is restarted.

Photos in the Domino directory:

The Domino directory does not have a standard field for photo, but photos can be retrieved from the Domino Name and Address Book (NAB) as follows:

1. Add a rich text field or rich-text lite field to the Person form of the Name and Address Book in Domino.
   a. Open names.nsf in Domino Designer.
   b. Open the Person form.
   c. Click the section where you want to add the field. A sub-form will open.
   d. In the sub-form, click where you want to add the field.
   e. Select Create > field from the menu, and edit the field’s properties.
   f. Add the name to the field and select Rich Text as the type.
   g. Save the form.

2. To store photo information in the newly-added rich-text field, choose either:
   - Import--click on the rich text field and choose Create > Picture. This adds the file contents to the field.
   - Attach--save the image file in the rich text field as an attachment.
3. Using the Sametime Administration tool, go to the Business Card Attribute page.
4. In the text box for the Photo attribute, type the name of the rich text field that you added to the Name and Address Book, above, matching the case, then click Update.
5. Restart the Sametime server.

Photo types used by Domino are .jpeg and .gif.

**Configuring business cards to use two repositories**

For retrieving business card information, you can set up a dual repository:

When you set up dual repositories, you set up a primary repository and a secondary repository:

**Primary repository** – The first storage repository search by the UserInfo application to retrieve user information; must always be the Sametime directory.

**Secondary repository** – The second storage repository searched by the UserInfo application to retrieve user information.

**Note:** The primary storage can never be of the same type as the second repository; for example, the primary and secondary storage cannot both be a Domino directory.

There are a variety of ways you can use dual repositories:
- The dual repository with Domino/LDAP directories
- The dual repository with LDAP/ Domino directories
- The dual repository with Domino/Custom Notes databases
- The dual repository with LDAP/Custom Notes databases

**Configuring a dual repository with LDAP and a native Domino Directory:**

For retrieving business card information, you can set up a dual repository of a LDAP directory and a native Domino Directory.

**Before you begin**

This section describes how to configure the business card using two storage repositories: LDAP directory as the primary storage, a native (non-LDAP) Domino Directory as the secondary storage.

**About this task**

These directions assume the following:
- Lotus Domino & IBM Sametime Community Server have already been installed & configured to run properly
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- All LDAP attributes needed by business card accessible for query via anonymous connection or using a specific bind account/password
- The Sametime Community server is running
- Business card information can be retrieved from your Sametime directory
A Notes database based off of the Domino directory template (pubnames.ntf) has been created and contains person documents for each corresponding user account defined in the Sametime directory. (In our example, this database is named bcardstorage.nsf; and the user accounts correspond to the accounts in the Sametime directory by users' email address.

**Procedure**

1. Using Lotus Notes, open your Directory Assistance database (typically da.nsf). If such a database does not exist, you must create one based upon the Directory Assistance template.

2. Click **Add Directory Assistance** to add an additional directory assistance document, and then specify the secondary storage. See the sample Directory Assistance document for the bcardstorage.nsf below:

   **DIRECTORY ASSISTANCE**

   ![Directory Assistance Interface]

   Naming contexts (Rules) tab

   **Note:** For Business Card purposes, the secondary storage does NOT have to be trusted for credentials.
Replicas tab

3. Once you have completed the changes, save and close the document. The resultant Directory Assistance database may show the following:

<table>
<thead>
<tr>
<th>Database links:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Replica</strong></td>
</tr>
<tr>
<td><strong>Database links:</strong></td>
</tr>
<tr>
<td><strong>Domain</strong></td>
</tr>
<tr>
<td>Replicas</td>
</tr>
<tr>
<td>Replicas2</td>
</tr>
<tr>
<td>Replicas3</td>
</tr>
<tr>
<td>Replicas4</td>
</tr>
</tbody>
</table>

**Note:** The directory assistance database must be listed on the Basics tab of the Sametime server document in the Directory assistance database name field. If it is not listed, fill in the field, and restart the Sametime server to effect that change.

4. Log in to the Integrated Solutions Console.

5. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.

6. In the **Sametime Community Servers** list, click the deployment name of the server with the business card information that you want to add or change.

7. Click the **Business Card** tab.

8. In the Business Card Contents section, select the attribute you want displayed in users’ business cards, and then click **Add** to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click **Remove**.

9. Under **Attribute Definition**, choose **Attribute Values** that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose **User Defined**. The following table lists the default attribute value that is mapped to each attribute name.
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

10. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.

11. In the **Attribute Definition** table, change the **Attribute Value** for the attributes that will be retrieved from the secondary storage to **User Defined** and leave the **User Defined** field blank. For example, if you are retrieving users' Telephone and Title information from the Domino Directory; therefore, change the values for the Telephone & Title attributes to **User Defined**, and leave the **User Defined** field blank, and then click **OK** to save the changes.

**Note:** These values are blank to ensure they are retrieved from the secondary repository (the Domino Directory) and not from the primary repository, which is the LDAP directory.

12. Modify the UserInfoConfig.xml file located in the Domino program directory (`\lotus\domino\UserInfoConfig.xml`) using a text editor. The.UserInfo application fetches and delivers user information for each incoming client request (an user's request to view a particular user's business card). When you are using an LDAP directory as primary storage and a Domino Notes directory as secondary storage, make the following modifications. Add an additional Storage tag of Notes type within the Resources tag:

```xml
<Storage type="NOTES">
    <CommonField CommonFieldName="MailAddress"/>
    <Details>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
    </Details>
</Storage>
</Resources>
</Storage>
```

**Note:** The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are retrieving Title and Telephone information from Domino.

13. To ensure Telephone and Title fields come from Domino, remove the following from the Details tag of the LDAP storage type:

```xml
<Detail Id="Title" FieldName="title" Type="text/plain"/>
<Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>
```

14. Add the following to the `<BlackBoxConfiguration>` section. Make sure it is listed after the LDAP blackbox as the order defines the search order:

```xml
```
Note: Since Sametime is the storage to be searched first by the UserInfo application, and the LDAP directory is the Sametime directory, the NOTES black box must be listed after the LDAP black box.

15. Once these changes are made, the UserInfoConfig.xml looks like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="LDAP">
      <StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username"
        Password="password" SslEnabled="false" SslPort="636"
        BaseDN="o=ibm" Scope="2"
        SearchFilter="(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)
          (sn=%s)(mail=%s)))"/>
      <!-- Add another StorageDetails tag to support another ldap server.
      The listing order implies the searching order -->
      <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE -->
      <SslProperties KeyStorePath="" KeyStorePassword=""/>
      <Details>
        <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
        <Detail Id="Name" FieldName="cn" Type="text/plain"/>
        <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="ou" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
  <BlackBoxConfiguration>
    <BlackBox type="LDAP" name="com.ibm.sametime.userinfo.userinfobb.UserInfoLdapBB"
      MaxInstances="5"/>
    <BlackBox type="NOTES" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesBB"
      MaxInstances="4"/>
  </BlackBoxConfiguration>
</UserInformation>
```

16. UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user—from multiple sources. By default, the user's email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

17. Restart your Sametime Community and Domino servers to effect the changes.

Results

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and the Domino Directory.

Configuring a dual repository with LDAP and a custom application:
For retrieving business card information, you can set up a dual repository of a LDAP directory and a custom IBM Lotus Notes application.

**Before you begin**

This section describes how to configure the business card using two storage repositories: LDAP with a custom Lotus Notes application repository. Here, we describe how you can set up LDAP as the primary storage, and a custom Lotus Notes application as the second storage.

These directions assume the following:
- Lotus Domino & IBM Sametime Community Server have already been installed & configured to run properly
- Sametime authentication is configured to use an LDAP directory
- The LDAP server is running and accessible by the Sametime Community Server
- Business card information can be retrieved from your Sametime directory
- A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf).
- To use a custom Lotus Notes application as a secondary repository, each user record in the custom application must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).

**About this task**

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the **Sametime Community Servers** list, click the deployment name of the server with the business card information that you want to add or change.
4. Click the **Business Card** tab.
5. In the Business Card Contents section, select the attribute you want displayed in users' business cards, and then click **Add** to include the selected attribute. If you do not want to display any pre-selected information, select each attribute, and then click **Remove**.
6. Under **Attribute Definition**, choose **Attribute Values** that are appropriate for your deployment. Each LDAP directory has its own naming schema, so be sure to confirm that each attribute value selected for display is mapped to the correct LDAP attribute as defined by your LDAP schema. If you prefer to map another attribute value to the attribute name instead of the default value, then choose **User Defined**. The following table lists the default attribute value that is mapped to each attribute name.

   **Table 28. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
</tbody>
</table>
Table 28. Attribute names and values (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo</td>
<td>jpegPhoto</td>
</tr>
<tr>
<td>Address</td>
<td>postalAddress</td>
</tr>
<tr>
<td>Company</td>
<td>ou</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
</tr>
</tbody>
</table>

7. If you select **User Defined** for an **Attribute Value**, then enter an attribute to map to the **Attribute Name**.

8. In the **Attribute Definition** table, change the **Attribute Value** for the attributes that will be retrieved from the secondary storage to **User Defined** and leave the **User Defined** field blank. For example, if you are retrieving users’ Telephone and Title information from the custom Lotus Notes application; therefore, change the values for the Telephone & Title attributes to **User Defined**, and leave the **User Defined** field blank, and then click **Reset** to save the changes.

**Note:** These values are blank to ensure they are retrieved from the secondary repository (the Lotus Notes application) and not from the primary repository, which is the LDAP directory.

9. Modify the **UserInfoConfig.xml** file located in the Domino program directory (\lotus\domino\UserInfoConfig.xml) using a text editor. The **UserInfo** application fetches and delivers user information for each incoming client request (an user’s request to view a particular user’s business card). When you are using an LDAP directory as primary storage and a custom Notes application as secondary storage, make these modifications:

a. Add the following **NOTES_CUSTOM_DB Storage** tag inside the **Resources** tag:

   ```xml
   <Storage type="NOTES_CUSTOM_DB">
   <StorageDetails DbName="bcardstorage.nsf" View="$BCardView"/>
   <Details>
   <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
   <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
   </Details>
   </Storage>
   ```

   **Note:** In the **<StorageDetails>** tag, the following settings are specified:
   - **DbName** = database_path Filename of the custom Notes application (relative path to the domino data directory)
   - **View** = view_name The name of the Notes view that displays the documents containing the user records.
   - The **<Details>** section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Notes application database

b. The attributes Title and Telephone must come from the custom Notes application rather than from LDAP, so remove the following information from the **<details>** tag of the LDAP storage: **<Detail Id="Title" FieldName="title" Type="text/plain"/>** **<Detail Id="Telephone" FieldName="telephoneNumber" Type="text/plain"/>**

c. Add the following information to the **<BlackBoxConfiguration>** section. Make sure it is listed after the LDAP blackbox as the list order defines the
d. The UserInfoConfig.xml now looks like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="LDAP">
      <CommonField CommonFieldName="MailAddress"/>
      <StorageDetails HostName="ldap.austin.ibm.com" Port="389" UserName="username" Password="password" SslEnabled="false" SslPort="636" BaseDN="o=ibm" Scope="2" SearchFilter="(&(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s)))"/>
    </StorageDetails>
    <Details>
      <Detail Id="MailAddress" FieldName="e-mail" Type="text/plain"/>
      <Detail Id="Name" FieldName="cn" Type="text/plain"/>
      <Detail Id="Location" FieldName="postalAddress" Type="text/plain"/>
      <Detail Id="Company" FieldName="ou" Type="text/plain"/>
      <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
    </Details>
  </Storage>
  <Storage type="NOTES_CUSTOM_DB">
    <StorageDetails DbName="bcardstorage.nsf" View="$BCardView"/>
    <Details>
      <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
      <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
    </Details>
  </Storage>
</Resources>
<ParamsSets>
  <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
</ParamsSets>
<BlackBoxConfiguration>
  <BlackBox type="LDAP" name="com.ibm.sametime.userinfo.userinfobb.UserInfoLdapBB" MaxInstances="5"/>
  <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userinfo.userinfobb.UserInfoNotesCustomBB" MaxInstances="4"/>
</BlackBoxConfiguration>
</UserInformation>
```

e. UserInfo must have a common field shared among the various storage repositories to retrieve data for a single user—from multiple sources. By default, the user’s email address is the common attribute, but any unique value may be used. If you prefer to use a different attribute, update the following field:

```
<CommonField CommonFieldName="MailAddress"/>
```

10. Restart the Sametime Community Server and the Lotus Domino server to effect the changes.

What to do next

You have successfully configured the business card to display information for a single user from dual storage repositories: an LDAP directory and a custom Notes application.

Configuring a dual repository with Domino Directory and LDAP:
You can configure Business Card with the use of two (dual) repositories—Domino and LDAP. The primary storage repository is the native (non-LDAP) Domino Directory, and the auxiliary storage is the LDAP directory.

**Before you begin**

These directions assume the following:
- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Sametime authentication is configured to use a Domino directory
- The Sametime Community Server is running
- The LDAP server is running and is accessible by the Sametime Community Server
- All LDAP attributes needed by Business Card are accessible for query via anonymous connection or by using a specific bind account/password
- Business card information can be retrieved from your Sametime directory

**About this task**

Enter this URL in the address window of a browser: http://hostname/stcenter.nsf, using your server's actual host name.

**Procedure**

1. Click **Administer the server**, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click **Business Card Setup**.
3. In the User Information section, select the entry you want displayed in users' business cards, and then click **Add** to move the entry to the right-side list box. To remove preselected entries, click the entry and click **Remove**. The following table lists the default attribute value that is mapped to each attribute name in the **Attribute Names and Attribute Values** section.

   **Table 29. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the **Attribute Names and Attribute Values** section, remove the attribute values for the attributes that will be retrieved from the auxiliary storage. In the following example, the Telephone information is retrieved from the LDAP directory, so delete the value for the Telephone attribute. Removing attributes insures they are pulled from auxiliary storage, and not primary storage.
Table 30. Attribute names and values

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, MiddleInitial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

5. Click **Update** to save the changes.

To display user information, the business card feature uses a server application called **UserInfo** which is designed to retrieve and deliver user information for each incoming request from a client to view a specific user's business card. To ensure this application is configured properly to search the proper data storage, confirm the settings as defined in **UserInfo.xml**.

6. When Domino Directory is primary storage and LDAP is auxiliary storage, make the following modifications:

a. Add the following LDAP `<storage>` tag within the `<Resources>` tag:

```
<Storage type="LDAP">
  <StorageDetails HostName="ldap.austin.ibm.com" Port="389"
                  UserName="username" Password="password" SslEnabled="false"
                  SslPort="636" BaseDN="o=ibm" Scope="2"
                  SearchFilter="(&(objectclass=organizationalPerson)
                              (((cn=%s)(givenname=%s)(sn=%s)(mail=%s))))"/>
  <!-- Add another StorageDetails tag to support another ldap server. The listing order implies the searching order -->
  <!-- Scope: 0=OBJECT_SCOPE 1=ONELEVEL_SCOPE 2=SUBTREE_SCOPE-->
  <SslProperties KeyStorePath="" KeyStorePassword=""/>
  <Details>
    <Detail Id="Telephone" FieldName="telephonenumber" Type="text/plain"/>
  </Details>
</Storage>
```

Update the Storage details tag with the appropriate settings for your LDAP directory. The Details section defines the attributes that Sametime will retrieve from the corresponding storage repository. In this example, we are pulling the **telephonenumber** attribute from the LDAP directory.

b. To ensure the telephone number is retrieved from LDAP, and not from Domino, remove the following from the `<details>` tag of the DominoNotes storage type:

```
<Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
```

After you have made these changes, the **UserInfoConfig.xml** file should look like the below:

```
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="EmailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
    </Details>
  </Storage>
</Resources>
```

70 IBM Sametime: Administration Guide
c. So the UserInfo application can retrieve data for a user from multiple data sources, a common field must be shared among the storage repositories. This field must be unique for its corresponding directory. By default, users’ email address are used as the common attribute. Consequently, users must be uniquely identified by their email addresses. If another attribute is preferred, the following line must be updated to reflect the field for that attribute:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

7. Restart your Sametime server and the Domino server to effect all the changes.

### Configuring a dual repository with Domino Directory and custom:

For retrieving Business Card information, you can set up a dual repository of a Domino Directory and a custom Lotus Notes application.

#### Before you begin

This section describes how to configure the Business Card using two storage repositories: Domino Directory with a custom Lotus Notes repository. Here, we describe how you can set up Domino Directory as the primary storage, and a custom Lotus Notes application as the secondary storage.

These directions assume the following:

- IBM Lotus Domino and IBM Sametime Community Server have been installed and configured
- Business card information can be retrieved from your Sametime directory
- A custom Lotus Notes application based upon any template has been created and contains user records for each corresponding person document defined in the Sametime directory. (In our example, this custom application is named bcardstorage.nsf).
To use a custom Lotus Notes application as an auxiliary repository, each user record in the custom database must have a common field whose unique value matches the value of the same field for the person in the Sametime directory. By default, the common field that is used is the internet email address).

**Procedure**

1. Click **Administer the server**, and then log in as Administrator.
2. Click the plus sign next to Configuration to expand the contents, and then click **Business Card Setup**.
3. In the User Information section, select the entry you want displayed in users' business cards, and then click **Add** to move the entry to the right-side list box.
   
   To remove preselected entries, click the entry and click **Remove**. The following table lists the default attribute value that is mapped to each attribute name in the **Attribute Names and Attribute Values** section.

   **Table 31. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, Middle initial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>OfficePhoneNumber</td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

4. In the **Attribute Names and Attribute Values** section, if the information you want displayed in users' business cards is not mapped to the appropriate attributes used in your company, then you may need to update it.

5. To prepare attributes for use by the auxiliary storage, in the attribute name/attribute value section, remove the values for the attributes that are to be retrieved from the auxiliary storage. In this example, we are retrieving the Telephone information from the custom Notes application; therefore, you should delete the value for the Telephone attribute, and then click **Update** to save the changes. These values are removed to ensure the appropriate values are retrieved from the auxiliary data repository, and not the first.

   **Table 32. Attribute names and values**

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Location</td>
</tr>
<tr>
<td>Company</td>
<td>CompanyName</td>
</tr>
<tr>
<td>Email address</td>
<td>InternetAddress</td>
</tr>
<tr>
<td>Name</td>
<td>FirstName, Middle initial, LastName</td>
</tr>
<tr>
<td>Photo</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>JobTitle</td>
</tr>
</tbody>
</table>

6. Modify the **UserInfoConfig.xml** file located in the Domino program directory (\lotus\domino\UserInfoConfig.xml) using a text editor. The **UserInfo** application fetches and delivers user information for each user's request to view a particular user's business card.
a. Add the following NOTES_Custom_DB Storage tag inside the Resources tag:

```xml
<Storage type="NOTES_CUSTOM_DB">
  <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
  <Details>
    <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
  </Details>
</Storage>
```

**Note:** In the StorageDetails tag, the following settings are specified:
- **DbName** = database_path Filename of the custom Lotus Notes application (relative path to the domino data directory)
- **View** = view_name The name of the Notes view that displays the documents containing the user records
- The Details section defines the attributes that will be retrieved by Sametime from the corresponding storage repository. In this example, we are pulling the telephone attribute from the custom Lotus Notes application.

b. Since the Telephone number must come from the custom Notes application, ensure the information is not retried from the Domino directory by removing the following information from the Details tag of the Notes storage:

```xml
<Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain"/>
```

c. Add the following information to the BlackBox Configuration section. The Notes black box must come first since the listed order defines the search order:

```xml
<BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userinfo.userinfo.bbUserInfoNotesCustomBB" MaxInstances="4"/>
```

**Note:** The Sametime directory must be configured as the primary storage so it can be searched first by the UserInfo application. In this example, the Domino directory is the Sametime directory; therefore, the NOTES_CUSTOM_DB black box is listed AFTER the Notes black box.

Now the UserInfoConfig.xml should look like this:

```xml
<UserInformation>
  <Resources>
    <Storage type="NOTES">
      <CommonField CommonFieldName="MailAddress"/>
      <Details>
        <Detail Id="Location" FieldName="Location" Type="text/plain"/>
        <Detail Id="Title" FieldName="JobTitle" Type="text/plain"/>
        <Detail Id="EmailAddress" FieldName="InternetAddress" Type="text/plain"/>
        <Detail Id="Company" FieldName="CompanyName" Type="text/plain"/>
        <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain"/>
        <Detail Id="Photo" FieldName="jpegPhoto" Type="image/jpeg"/>
      </Details>
    </Storage>
    <Storage type="NOTES_CUSTOM_DB">
      <StorageDetails DbName="bcardstorage.nsf" View="persons"/>
      <Details>
        <Detail Id="Telephone" FieldName="telephone" Type="text/plain"/>
      </Details>
    </Storage>
  </Resources>
  <ParamsSets>
    <Set SetId="0" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
    <Set SetId="1" params="MailAddress,Name,Title,Location,Telephone,Photo,Company"/>
  </ParamsSets>
</UserInformation>
```
7. So the UserInfo application can retrieve data for a single user from multiple sources, a common field must be shared among the storage repositories. By default (though any unique value may be used), the user's email address is the common attribute, so in both storage repositories, users must be uniquely identified by their email addresses. If you want to use a different attribute, you must update this line to show which attribute you plan to use:

```xml
<CommonField CommonFieldName="MailAddress"/>
```

8. Restart the Sametime server and the Domino server to effect all the changes.

What to do next

You have successfully configured the business card to display information for a single user from dual storage repositories: the Domino directory and a custom Notes application.

Additional configurations for black boxes

Though Sametime ships with two black boxes or special implementations already present for configuring with LDAP or Domino, additional black boxes can be configured to retrieve data from more than one resource. A special configuration can be used to designate NOTES as its first box, if Sametime is configured with Domino, and with LDAP as its second black box.

For a Sametime installation that is configured to work with Domino but that can also retrieve data from Domino LDAP, Notes would be listed as the first black box, and LDAP as the second. Each of these special configurations requires manual settings in the UserInfoConfig.xml file.

This version of Sametime includes an additional black box that enables data retrieval from a separate Notes database (other than the Domino directory). This black box should be applied as a part of a special configuration designated to retrieve data from the Sametime directory and from an additional Notes database that contains users' business card details.

See the topic “Retrieving data from a customized database” on page 75 for more information on how to configure data retrieval from the additional Notes database.

A newly-written black box or special implementation can be used to retrieve data from any selected data resource. The black box should be implemented and configured according to the Application Programming Interface (API) and to the instructions published with the Sametime Software Development Kit (SDK).

For 8.5 and 8.5.1 only

To use the customized black box, an additional configuration setting is required. In the sametime.ini file, under the Config section, add the following flag:

```ini
USERINFO_LOAD_SVC_IN_SERVLET=1
```

For additional help with these special configurations, please contact Support.
Retrieving data from a customized database:

For the user data included in the Business Card, Administrators can retrieve details about the user from separate Notes databases that are dedicated to storing user details and that function independently of the Domino directory that is used for Sametime.

About this task

Retrieving user data from customized Notes databases allows you to:

- Retrieve some details from the Sametime Domino directory and the rest from a customized Notes database (Domino)
- Retrieve some details from the LDAP directory Sametime is configured to work with and the rest of the details from an additional Notes database.

An additional black box, which functions as a customized special implementation, is provided to enable data retrieval from the customized Notes database. This 'customized' black box should always be preceded by a call to the black box that handles the Sametime directory. A CommonField tag is used for synchronization between the black boxes. If the common field is defined as MailAddress, then the value retrieved for MailAddress from the first storage (LDAP or Domino) is used as the ID to query for in the customized database. The application first queries the database using the userID received as a parameter; if no record is found, it queries the database again, using the value retrieved for the CommonFieldName as userID. To use the customized database feature:

- Perform the following manual steps:

Procedure

1. Open UserInfoConfig.xml and update the CommonField tag in the first 'storage' section to hold the ID property of a Detail tag that represents the same detail in the different storage types. This detail tag is assigned a different field name in each storage section, but the value in each of these fields should be identical for the specific user. The default value for the Common field tag is "MailAddress." The attributes holding the email address for a user should have the same value in both storages.

2. Using the Administrator's Tool, update the Business Card attribute page with the values to be retrieved from the Sametime directory, leaving blank the field name for items required from the customized database.

3. Remove the Detail tags of the fields you left blank in the set-up page from the first 'storage' section in the UserInfoConfig.xml file.

4. Add an additional 'storage' section to the UserInfoConfig.xml as the second storage. This storage section is a new section added specifically for this feature; it differs from the standard Notes storage section through the additional parameters specified below:

```xml
<Storage type="NOTES_CUSTOM_DB">
  <StorageDetails DbName="" View="$users" />
  <Details>
    <Detail Id="Location" FieldName="Location" Type="text/plain" />
    <Detail Id="Title" FieldName="JobTitle" Type="text/plain" />
    <Detail Id="MailAddress" FieldName="InternetAddress" Type="text/plain" />
    <Detail Id="Telephone" FieldName="OfficePhoneNumber" Type="text/plain" />
    <Detail Id="Company" FieldName="CompanyName" Type="text/plain" />
    <Detail Id="Name" FieldName="FirstName,MiddleInitial,LastName" Type="text/plain" />
  </Details>
</Storage>
```
5. In the newly-added "storage" section, delete the Detail tags of the items that you do not want to retrieve from this database, and update:
   a. The DbName property, including the full path
   b. The view name (if needed)
   c. The mapping of the "Detail" tag so each item is mapped to the correct field name of the new database

6. Add a BlackBox tag to the BlackBoxConfiguration section in UserInfoConfig.xml as a second record:
   <BlackBox type="NOTES_CUSTOM_DB" name="com.ibm.sametime.userinfo.userinfobb.
   UserInfoNotesCustomBB" MaxInstances="4" />

7. Restart StConfiguration and the HTTP task.

What to do next

Note: For complete information on how to use these "black boxes" and on how to use all the storage repositories for LDAP, Sametime, and Domino, see the section in Business Card entitled "Using repositories." This section provides detailed information on how to store and retrieve user data contained in both single and dual repositories.

Mapping a detail to multiple attributes
An optional setting in UserInfoConfig.xml file lets you map a detail to more than one attribute. As a result, the returned value for a detail is composed of a list of attributes retrieved from the storage.

About this task
You can do this by mapping an item to a comma-separated list of attributes.
<Detail Id="Telephone" FieldName="telephoneNumber,mobile" Type="text/plain" />

The response can contain a list of values separated by any character chosen by the administrator. To apply the new separator, edit the UserInfoConfig.xml file.

Procedure
1. Open UserInfoConfig.xml in an editor.
2. Choose the Detail tag that you want to use to retrieve a list of attributes.
3. Complete the FieldName property with the list of attributes to retrieve, separated by commas.
4. Add an additional property: DisplaySeparator. Set its value to the required character that should appear in the response xml between any 2 retrieved attributes values. For example, <Detail Id="Telephone"
   FieldName="telephoneNumber,mobile" Type="text/plain" DisplaySeparator="/"
   />
5. Log in to the Integrated Solutions Console.
   a. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
   b. In the Sametime Community Servers list, click the deployment name of the server with the connectivity information that you want to change.
   c. Click the Business Card tab
   d. Verify that the mapping of this detail (the Telephone detail in the example) is empty.
   e. Click OK.
6. Restart the server.

**UserInfoConfig Debug tracing**

If additional information is needed to trace a problem, tracing information can be collected. To enable trace collection, set the `USERINFO_DEBUG_LEVEL` flag of the `sametime.ini` file.

1. Stop the IBM Sametime Community Server.
2. Set or add this flag in the debug section of `sametime.ini` file:
   ```
   USERINFO_DEBUG_LEVEL=5
   ```
   The trace file will have a name and format like `UserInfo_091021_1818.txt` for the UserInfo Server Application and `UserInfoHTTP_091231_2240.txt` for the UserInfo servlet. You can find the file in the Trace folder.
   
   **Linux and IBM i only**: If you are running Sametime Community Server 8.5.1 on Lotus Domino 8.5.2, then edit the `domino_directory/servlets.properties` file by removing `UserInfoServlet` from the `servletsstartup` line.
3. Restart the Sametime Community Server.
4. When the server is fully started, send an http request using a web browser to activate the servlet.

**Resolving problems with business cards**

If Business Cards are not displaying user information as expected, check the server configuration, then the client, and finally, the business cards themselves.

**Checking the server configuration**

Check and validate the configuration on the storage repository you use with the Sametime Community Server. A configuration problem is the most likely cause of problems with Business Cards. For more information, see the appropriate section in Managing business cards.

**Checking the UserInfo servlet on the client**

The UserInfo servlet on the client receives and responds to client requests. The servlet must be working correctly to provide the requested details for Business Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.

1. Determine the distinguished name (DN) of the user whose Business Card you want to view. Here are sample DNs of the various directory types:
   - Domino directory: `cn=sametime User/O=IBM`
   - Active directory: `cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com`
   - TDS directory: `uid=Sametime user,ou=Austin,o=IBM`
2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:
   ```
   [protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1 &UserId=[User DN]
   ```
   - `[protocol]` = {http, https}
   - `[hostname]` = {Fully qualified hostname of the Sametime server}
   - `[User DN ]` = {The full distinguished name of the user for whose information you are seeking}

**Examples:**

- Domino Directory:
http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
User/O=IBM

- Active Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User,cn=users,dc=austin,dc=ibm,dc=com

- TDS Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime
  user,ou=Austin,o=IBM

Note:
- Do not use spaces in the URL for the UserInfo servlet operation.
  A space is translated into %20 in the URL, and the servlet will not produce a result; for example:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  User/O=IBM

  is translated to:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime
  %20User/O=IBM

  . The characters "%20" are inserted before the word "User" to represent the space.
- The name "UserInfoServlet" is case sensitive.
- Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you've composed into a web browser's address field, and view the result.

You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.

An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:
- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

Checking the client

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.

Checking that Business Cards meet requirements

Finally, verify that the business cards follow these requirements.
- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

Note: Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.
- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage
(the directory used by Sametime for authentication). For example, if Sametime is configured to use the Domino directory, then the secondary storage cannot also be a Domino directory.

Changing user names

After users have been registered in IBM Sametime, you can change their names if their user IDs must change due to a name or location change.

About this task

The name conversion tool or use the AdminP feature should be used for changing user names as needed. To eliminate the need to run name changes in the future, you can migrate older user IDs to a unique directory attribute, which requires you to run the name conversion tool only once. This can be done only for an LDAP directory and only when the names in the directory are already synchronized with Sametime.

Changing names as needed

When you change user or group names in the directory, the change is not reflected in IBM Sametime Community Server databases. In order to synchronize the directory names with the names in the Sametime Community Server databases, you must run the name conversion utility.

About this task

Running the name conversion utility updates Sametime Community Server user or group names with the latest directory changes. The name conversion utility uses a comma-separated value list that you compile to change names, delete names, or convert all names from Domino to Domino LDAP formatted names.

Users create a contact list, a privacy list, and an alert-me-when list in the IBM Sametime Connect client by selecting user names or group names from the Domino or Domino LDAP directory that is used with the IBM Sametime Community server. These contact, privacy, alert-me-when lists are stored in the user information database (vpuserinfo.nsf) on Sametime Community servers. When a user starts the Sametime Connect client, the lists are downloaded from the database to update the lists stored on the client's local computer.

You do not need to run the name conversion utility when you add new users or groups to the Domino or LDAP directory.

Run the name conversion utility manually on a stand-alone Sametime Community server, or on a server in a cluster which will replicate the change throughout the cluster.

Note: Be sure to stop the Domino server before you run the name conversion utility.

Preparing for changing names:

Before you can run the name conversion utility, you need to perform the following tasks:
About this task

You do not need to use the name conversion utility if you add new users or groups to directory. Use the name conversion utility only if you change user names or group names that exist in the directory.

Creating a comma separated value file:

A comma-separated value (CSV) file created in a text editor provides the name conversion utility with the information it needs to make a name change to user contact, privacy, and alert-me-when lists. The CSV file includes the type of change and typically provides details such as the old name and the new name, and optionally, the display name.

Procedure

1. Use a text editor that supports UTF-8 saving format to create a comma-separated file.
2. Create a CSV for only one type of change; you cannot mix name change types in the same CSV.
   - ID
   - ORGANIZATION
   - DELETE
   - LDAP
   - REPORT
3. Name and save the file with an extension of .csv in a directory accessible by the Sametime server. The text file should be saved in UTF-8 format.

Syntax for comma-separated value file used in name change utility:

A CSV file created in a text editor provides the server with the information it needs to make a name change to user contact lists or privacy lists. The CSV file includes the type of change (or descriptor) and typically provides details such as the old name and the new name, and optionally, the display name.

You can create the CSV text file using any text editor. Some spreadsheet programs also allow you to export spreadsheet values to a CSV file. The CSV file should include only the list of comma-separated old name, new name pairs that reflect the changes you have made to the directory. Do not include any header information in your CSV file. Name the file at your discretion. After you create the CSV file, store it in a network location that is accessible from the Sametime server. You must browse to this file to import it when you create the Name Change Task from the Administrator's tool in Sametime.

When you create a CSV file, you must format it correctly following the syntax rules below. CSV files are case-sensitive and sensitive to spaces. You can create multiple CSV files. The CSV file can include only one descriptor:

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Change specified first names, last names, display names, or group names.</td>
</tr>
<tr>
<td>ORGANIZATION</td>
<td>Change the organization name for all users.</td>
</tr>
<tr>
<td>Descriptor</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>LDAP</td>
<td>Changes all contact list information from Domino directory format to LDAP format. For example, a user listed as CN=Maria Smith/OU=Sales/O=IBM changes to CN=Maria Smith,OU=Sales,O=IBM.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Remove specified individual contact names from contact lists and privacy lists.</td>
</tr>
<tr>
<td>REPORT</td>
<td>This feature can be used to confirm a name change in the vpuserinfo.nsf database by taking snapshots before and after the change and comparing them. To use this descriptor, create two CSV files in the trace folder that capture the vpuserinfo.nsf tables for user's contact list, alert me list, and privacy list. The CSV file names will be similar to: ConvertStorage_110308_0548.csv ConvertPrivacy_110308_0548.csv The first file contains the contact list and alert me list. The second file contains the privacy list. This feature is also available for releases prior to release 8.5.2 as a hotfix. See Technote #1469735 for more information.</td>
</tr>
</tbody>
</table>

The second part of the CSV file includes one line for each change that includes the old name, the new name, and, optionally, the new display name.

Changing the user and group IDs.
### CSV File Syntax

**ID**

```
"old ID", "new ID","new display name"
```

... where the [...] indicate that the new display name is optional but if you use it, you must precede it with a comma as in the first example (where 'Maria Brown' is the new display name), and the new display name must immediately follow the comma (if you leave a blank space between the comma and the new display name, the conversion will not work).

### Sample CSV showing changes from a Domino directory:

**Example**

```
ID
"CN=Maria Smith/OU=Sales/O=IBM",
"CN=Maria Brown/OU=Sales/O=IBM",
"Maria Brown"
"CN=John/OU=New York/O=IBM",
"CN=John/OU=Texas/O=IBM"
"52e811 85256500/Old Group",
"52e811 85256500/New Group Name",
"New Group Name"
```

Note that "52e811 85256500" in the example above is replica ID of Domino Directory. Be sure to change the colon in the replica ID to a space. For example: "52e811:85256500" should be "52e811 85256500".

### Changing the organization name.

**CSV File Syntax**

```
ORGANIZATION
"oldOrg","newOrg"
```

**Example**

```
Sample CSV showing changes from a Domino or LDAP directory:

```
ORGANIZATION
"lotus","ibm"
```

Changes all contact list information from Domino directory format to LDAP format (converts forward slashes in the hierarchical name to commas).

**CSV File Syntax**

```
LDAP
```

**Example**

```
Sample CSV:

LDAP
```

You cannot change the format from LDAP to Domino.

Delete specified users and groups.
Verify a name change.

Creating a Name Change task:

Create a name change task on the IBM Sametime Community server.

**Before you begin**

Before you create a name change task, create a comma-separated value (CSV) file of the name changes in the Sametime Community Server directory.

**About this task**

A name change task is not actually a scheduled program; its timestamp merely indicates when the task was created and not when it will be run. The list of tasks is ignored until you run the `stnamechange.cmd` program, which then operates on all of the tasks in the list, using the `.CSV` files specified in the Name Change page.

Follow the steps below to create a name change task.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Community Servers.
3. In the Sametime Community Servers list, click the deployment name of the server where you want to add a name change task. If you want to create a task to run on multiple servers, then click the deployment name of any of the servers on which you want to run the task.
4. Click the Name Change tab.
5. Click New.

   **Note:** If you only want to edit a task, you can click the name of the scheduled task to edit it.

6. Enter a name in the Name of Task field. The name is at your discretion. By default, the name is the date the task is created.
7. Optional: Enter a description for the task.
8. Browse for the CSV file you want to use, and then click OK.
9. The name change task appears in the list of scheduled tasks. All tasks listed here run when the stnamechange.cmd is run.

Results

After you have completed these steps on one Sametime Community server, it is necessary to repeat this process on other servers in a distributed environment.

When you are finished configuring the task, name changes are saved to the stnamechange.nsf file. For a clustered environment, create this task on one server per cluster. All other servers receive the changes through the cluster replication process.

Lotus Domino picks up all valid name change tasks in the stnamechange.nsf file. You choose the servers or cluster on which the name change task runs on a regular basis using general scheduling tools. The application does not run by default; you must run the task manually.

To delete a name change task, on the Name Change page, select the task, and then click Delete. If any name changes are entered incorrectly, you can import a new CSV file.

Running the name conversion utility:

To run a name change task, start the name conversion utility. The name conversion utility uses the CSV file to update user contact and privacy lists with the latest directory changes.

Before you begin

Before you begin, create a comma-separated value file with name changes, and then create a name change task. IBM recommends running the name conversion utility at off-peak hours, and stopping the Domino server before you begin.

About this task

Starting the name conversion utility starts the name change task. You can create many tasks, but name change conversion utility executes only one task at a time. You can have only one name change task scheduled or in progress. If a name change task is scheduled or in progress, you cannot create another name change task until the existing name change task completes.

It is not necessary to run the name change conversion utility on every IBM Sametime Community Server in a cluster. For clusters, the task should run once on one server and then replicated to other servers in the cluster. Note that the All servers option on the Name Change page in the Sametime System Console does not work because of the procedure for replicating across all servers. If you create a Name Change task and select All servers, only the server you are logged on to contains the task—other servers do not. This is viewable in stnamechange.nsf through the Notes client. The correct procedure is to create the name change task on all the servers in the community.

Running the name conversion utility on Windows:

Follow these steps to run the name conversion utility on Microsoft Windows.
Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Type the following command:
   stnamechange.cmd

3. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server.
   Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on UNIX:
Follow these instructions to run the name conversion utility on a UNIX operating system.

Procedure
1. Stop the IBM Sametime Community Server and the Lotus Domino server.
2. Open a new shell and change to the domino data directory.
   cd /domino/notesdata
3. Type the following command:
   ./stnamechange.sh domino_bin_directory domino_data_directory
   For example:
   ./stnamechange.sh /domino/opt/lotus/notes/80020/linux /domino/notesdata
4. When the name change task completes, restart the Sametime Community Server and the Lotus Domino server.
   Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Running the name conversion utility on IBM i:
Follow these instructions to run the name conversion utility on an IBM i operating system.

Procedure
1. Stop the IBM Sametime Community Server.
2. From an IBM i command line, run the "QSH" command. This command starts the QShell interpreter, where the Name Change task is run.
3. Type the following commands:
cd server data directory
stnamechange server data directory domino bin directory

where domino bin directory is an optional parameter. The default directory is /qibm/proddata/lotus/notes, which causes the command to use the latest version of Lotus Domino installed on the system.

If the Sametime Community server is using an earlier release of Domino, specify the appropriate Domino bin directory.

<table>
<thead>
<tr>
<th>Lotus Domino version used by Sametime Community server</th>
<th>Associated domino bin directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino 8.5.2</td>
<td>/qibm/proddata/lotus/domino852</td>
</tr>
<tr>
<td>Domino 8.5.1</td>
<td>/qibm/proddata/lotus/domino851</td>
</tr>
<tr>
<td>Domino 8.5.0</td>
<td>/qibm/proddata/lotus/domino850</td>
</tr>
<tr>
<td>Domino 8.0.2</td>
<td>/qibm/proddata/lotus/domino802</td>
</tr>
<tr>
<td>Domino 8.0.1</td>
<td>/qibm/proddata/lotus/domino801</td>
</tr>
<tr>
<td>Domino 8.0.0</td>
<td>/qibm/proddata/lotus/domino800</td>
</tr>
</tbody>
</table>

4. When the command completes, press F3 to exit QSH.

To verify whether all of the names were changed successfully, view the following files in the /trace subdirectory of the server data directory:

namechange_YYMMDD_XXXX.txt
name_change_summary_report_YYMMDD_XXXX.log

If you encounter problems, add VP_NCSA_TRACE=1 to the Debug section of the sametime.ini file to collect additional debug information when you run the name change utility.

5. Restart the Sametime Community Server.

Restart all Sametime Community Servers in your deployment so they can detect the modified name. If your deployment includes Sametime Unified Telephony, restart all Telephony Application Servers as well.

Name Change task replication:

When you create a name change task, the task is saved in a file called stnamechange.nsf, and this file is replicated to all home IBM Sametime Community Servers so that updates can be made to each server's vpuserinfo.nsf database. The file vpuserinfo.nsf is the Sametime user information database that contains contact lists and privacy lists.

Set up a Domino replication task to replicate stnamechange.nsf among all servers. By default, stnamechange.nsf is replicated to all servers in a cluster, but not between clusters. This step makes it unnecessary to add future tasks to each stnamechange.nsf database in the environment. When a new task is added, all servers get the new information as a result of the replication procedure.

Note that the All servers option on the name change page in the Sametime System Console does not work because of the procedure for replicating across all servers. If you create a name change task and select All servers, only the server you are logged on to contains the task--other servers do not. This is viewable in stnamechange.nsf through the Notes client. The correct procedure is to create the name change task on all the servers in the community.
If several Sametime Community Servers operate as a cluster, create a name change task on only one server in the cluster. The vpuserinfo.nsf database replicates in real time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster. Declaring the task in one cluster can populate all the clusters because you set replica information for the stnamechange.nsf between all the clusters.

Sample deployments

The examples below illustrate how you might run name change tasks in different Sametime Community Server deployments.

Example Deployment 1

In this example, the Sametime community has the following characteristics:

Three Sametime Community Servers are deployed.

None of the servers are clustered.

With this deployment, you must create and run the name change task three times—one on each server. Though you create the task only once, you run it three times, and the run can be scheduled automatically.

Example Deployment 2

In this example, the Sametime community has the following characteristics:

Eight Sametime Community Servers are deployed.

Three Sametime Community Servers operate as Community Services cluster 1.

Three Sametime Community Servers operate as Community Services cluster 2.

Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster.

With this deployment, you must run the name change task four times. You can schedule the tasks to run automatically on one Sametime Community Server in Community Services cluster 1, on one Sametime Community Server on Community Services cluster 2, and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster.

Example Deployment 3

In this example, the Sametime community has the following characteristics:

- Six Sametime Community Servers are deployed
- Three Sametime Community Servers operate as a Community Services cluster
- Two Sametime Community Servers operate as home Sametime Community Servers but are not part of a Community Services cluster
- One Sametime server is not used as a home Sametime server and is not part of a Community Services cluster
With this deployment, you must create the name change task three times. Create the name change task on one of the Sametime Community Servers in the Community Services cluster and on each of the two Sametime Community Servers that operate as home Sametime Community Servers but are not part of a cluster. You do not need to create the name change Task on the Sametime Community Server that is not part of a cluster.

Name Change task status:

This topic describes the status of the name change tasks, how to view tasks in progress, and how to delete a name change task.

After you create a name change task, the task defaults to the Scheduled status. A scheduled task begins executing on the IBM Sametime Community Server at the time specified in the server setting on the Name Change page of the Sametime System Console (Sametime System Console > Sametime Servers > Sametime Community Servers > server_name > Name Change). You cannot edit a name change task that has the Scheduled status. The only way to change a scheduled task is to delete the task and then create a new task in its place.

Once a task begins executing, its status changes from Scheduled to In Progress if any of the servers have the name change task with the status that is in progress or scheduled. You cannot delete a task that is in progress. If all the servers have tasks that are marked Check error log or Disabled, the name change task can be marked Finished.

Finished means the task has completed the name change successfully. At this status level, you can add or delete any task.

Check error log means there were errors incurred while the task was running. At this stage, you can add or delete a task.

Note: The status column provides only the status of the task running on the server being used; it does not provide a summary of the task across servers and clusters of servers.

You can have only one name change task scheduled or in progress on a IBM Sametime Community Server. If a name change task is scheduled or in progress, you cannot create another name change task on the Sametime Community Server until the existing name change task completes.

You cannot delete a task that is marked In Progress. You can delete a task that is marked Scheduled, Finished or Check log status. There is a log file on the server that collects failures in Name Conversion.

- A user name that is changed in the directory but is not yet changed in the vpuserinfo.nsf database will appear as offline in the contact list and privacy list of another user until the name change task executes on the other user's home Sametime Community Server.
- All members of a changed group appear as offline in the contact list and privacy list of a user until the name change task executes on the user's home Sametime Community Server.

You can view the status of the names being changed. The vpuserinfo.nsf database includes a view for name change tasks. The task you are running is not marked complete. If several Sametime Community Servers operate as a Community Services cluster, you view the status of a name change task on only one Sametime Community Server.
Community Server in the cluster. The database replicates in real-time among the servers in the cluster. When the name change task changes the vpuserinfo.nsf database on one server, the changes are automatically replicated to the vpuserinfo.nsf databases on all other servers in the cluster.

Below is an example of viewable statuses. In the example, Servers X, Y, and Z are not clustered, and servers A, B, and C are clustered.

<table>
<thead>
<tr>
<th>Servers</th>
<th>task is created on Server X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server X</td>
<td>task appears in Name Change page</td>
</tr>
<tr>
<td>Server Y</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server Z</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server A</td>
<td>task does NOT appear in Name Change page, but it is in the log file</td>
</tr>
<tr>
<td>Server B</td>
<td>task does NOT appear in the Name Change page, and it does NOT appear in the log file</td>
</tr>
<tr>
<td>Server C</td>
<td>task does NOT appear in the Name Change Status page, and it does NOT appear in the log file</td>
</tr>
</tbody>
</table>

Note: Turn on the sametime.ini flag if you are working locally:
NC_LOCAL_CONVERSION = 1

Changing names with AdminP

This feature allows IBM Sametime to synchronize name change updates made to the IBM Lotus Domino directory via the Domino Administration Process (AdminP) with updates to Sametime User Information database (vpuserinfo.nsf).

Prior to Sametime 8.0.1, when a Lotus Domino Administrator executed name changes through the Lotus Domino Administrator client and the AdminP process, the users' names were changed automatically in the Lotus Domino Directory but were not changed in the corresponding Sametime records. The administrator had to manually generate a CSV text file that contained the renaming information, and run the Sametime name change utility on one or more servers, depending on the configuration.

In Sametime 8.0.1, this process is enhanced, allowing Sametime to update VPUserlnfo.nsf and add a new CSV text file to stnamechange.nsf whenever a change is made in the Domino Directory.

Note: It is still necessary to manually run the name conversion utility even when AdminP integration code is working. The Name Change Integration with AdminP feature creates a new Name Change task and only partially updates vpuserinfo.nsf. For example, it does not update the contact lists that include the old name. For a full update, the Name conversion utility must be executed.
In addition, the AdminP functionality is only available for Sametime servers that use Lotus Domino authentication running on Lotus Domino 8.0.2 or later. If the Sametime server is using LDAP authentication, or if you are using a version of Lotus Domino earlier than 8.0.2, you cannot use the AdminP feature to change names.

**AdminP integration components**

The following components contain the code for the Name change integration with AdminP feature. These components are located under the Domino program directory (by default \Lotus\Domino in Windows):

- StUpdateAdminP.dll -- the code loaded by the AdminP process. This DLL file receives notifications from Domino regarding renaming operations. We will refer to it as the AdminP add-in.
- AdminpUpdate.jar -- the java code executed by the StUpdateAdminP.dll
- NameChangeUtils.jar -- a library that provides services of updating the different Sametime databases. called by AdminUpdate.jar to perform the actual change in vpuserinfo.nsf and stnamechange.nsf

**Known issues with AdminP integration**

Please note the following issues concerning AdminP integration with Sametime:

- This feature is supported starting in Domino 6.0, but is currently not available with Domino 8.0.1.
- In Sametime, this feature is supported starting with release 8.0.1.
- Only name updates are handled; deletions and additions are not supported by AdminP.
- To complete the name change process, you must still execute the name change application (AdminP integration simplifies the process but does not replace it)
- When Sametime databases are being updated as a result of the AdminP operation, warning messages are seen on the Domino console. These messages are not an indication of any issue with the process and should be ignored.

**Enabling AdminP integration:**

The name change AdminP integration will run on one Sametime server in each cluster, is part of a Sametime server installation, and is disabled by default.

**Before you begin**

The name change AdminP integration functionality is only available for Sametime 8.0.1 servers hosted on Microsoft Windows and configured to use IBM Domino Directory for authentication. If your deployment uses an LDAP directory, you must use the Name Conversion utility as in previous releases. For information on the Name Conversion utility, see the topic, “About the Name Conversion utility” in this Sametime information center.

**About this task**

Enable the AdminP integration for your Sametime environment by completing the following steps:
Procedure

1. Remove the comment marker from the following statement in the notes.ini file:
   
   ```
   EXTMGR_ADDINS=StUpdateAdminP.dll
   ```
   
   If there are multiple servers in one community, only perform this step on one server.

2. Using a text editor, open sametime.ini and confirm that the following flags are set as follows:
   
   ```
   ST_JAVA_CLASS_PATH=C:\Lotus\Domino\java;C:\Lotus\Domino\StConfig.jar;
   C:\Lotus\Domino\StConfigXml.jar;C:\Lotus\Domino\AdminpUpdate.jar
   ST_JAVA_JVM_PATH=C:\Lotus\Domino\ibm-jre\jre\bin\classic\jvm.dll
   ST_JAVA_LIB_PATH=C:\Lotus\Domino
   ```
   
   The paths may be different based on your deployment.

   **Note:** Ensure ST_JAVA_CLASS_PATH contains the full path of the AdminpUpdate.jar file (the default path is \Lotus\Domino\AdminpUpdate.jar).

3. If the Sametime community consists of more than one Sametime server, ensure that the following databases are replicated among all of the servers in the community: names.nsf, admin4.nsf.

   A Domino administrator can configure Connection documents to ensure these databases are replicated on a defined schedule. For more information on how to create Connection documents, see the “Scheduling server-to-server replication” topic in the Domino Administrator Help information center.

   Now the environment is setup properly for Sametime to capture name changes carried out by the AdminP.

4. Run the stnamechange.cmd as described in the topic, “Running Name Change Tasks on Sametime servers in a community” in this Sametime information center.

**Specifying an administration server for databases:**

AdminP uses administration servers to manage administrative changes that apply to IBM Domino databases. Either the administrator or the database manager can specify the administration server for a database. Perform this procedure on an as-needed basis.

**Before you begin**

To change the administration server for a Domino database, you must have Manager access to the database or be designated as a Full access administrator on the Security tab of the Server document.

**About this task**

**Procedure**

1. From the IBM Lotus Domino Administrator, open the domain containing the server with the database for which you are setting an administration server.
2. From the **Servers** pane, select the server containing the database you are setting as an administration server.
3. Click the **Files** tab and then select the database to which you are assigning an administration server.
4. From the “Tools” pane, click **Tools** > **Database** > **Manage ACL**.
5. Click **Advanced**.
6. Complete these fields and then click **OK**: 

<table>
<thead>
<tr>
<th>Field</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server</td>
<td>Choose one of these:</td>
</tr>
<tr>
<td></td>
<td>• None -- If you do not want an administration server assigned for the database.</td>
</tr>
<tr>
<td></td>
<td>• Server -- Select a server from the list.</td>
</tr>
<tr>
<td></td>
<td>Choose one of these according to whether you want modifications to the indicated fields to occur during a rename group, rename user, or rename server action; or during a delete server, delete group, or delete user action:</td>
</tr>
<tr>
<td></td>
<td>• Do not modify Names fields -- Names fields are not updated during any of the above rename and delete actions.</td>
</tr>
<tr>
<td></td>
<td>• Modify all Readers and Authors fields -- Reader and Author fields are updated during the rename and delete actions listed above.</td>
</tr>
<tr>
<td></td>
<td>• Modify all Names fields -- All names fields are updated during any of the rename or delete actions listed above.</td>
</tr>
</tbody>
</table>

7. If you will be processing administration requests across domains, complete the procedure in the topic "Creating a Cross-domain Configuration document" in the Domino Administration information center.

*Sample configurations:*

AdminP operates with various configurations of the IBM Sametime server and IBM Domino.

**Sametime and the Domino Directory are hosted on the same machine**

The Sametime and Domino directory are on the same server. When a rename is made the AdminP add-in is notified and the callback updates the relevant databases. After the Name Change Utility is run all users can see each other's updated names.
Two or more Domino servers, each hosting Sametime and a Domino Directory

The Domino directories are replicated between all servers. Names.nsf and admin4.nsf are replicated on all servers. A name change executed on either one of these servers will trigger the AdminP process on both servers. Each AdminP process updates only the database that their administration server matches. This setting avoids replication conflicts.

Domino Directory hosted remotely from Sametime but within the same Domino domain

One or more Sametime servers and Domino directory are in the same domain. Each Sametime server accesses the Domino Directory through the directory assistance feature. Since all are in the same domain and the remote directory is accessed through da.nsf, updates are done on the remote directory and are received on the Sametime server. The Sametime server triggers the update of the databases that set their administration server to be the local server and activate the callback in the AddIns.
Domino Directory hosted remotely from Sametime, in a different Domino domain

This time, the Sametime servers and the Domino directory are in different domains. For rename updates to go from the Domino directory on Domain A to the Sametime servers on Domain B, a cross domain configuration should be applied on these domains. When a name is updated on the directory in domain B, a mail message is sent to domain A (assuming cross domain configuration is applied). This mail message is treated as a request for the AdminP and is added to the admin4.nsf which logs the request for the AdminP process.

Refer to the Domino Administration guide for additional information on cross-domain configuration.

Domino Directory hosted remotely from Sametime, in a different Domino domain, and not serving as primary directory

The Sametime servers and Domino directory are in different domains, and the Domino directory is not the primary directory for the deployment.
As In the previous configuration, the Cross Domain Configuration should be applied and the da.nsf on the Sametime servers should point to the required NAB in the remote Domino server (instead of names.nsf).

Two or more Domino Directories on remote servers, replicated with one or more Sametime servers

The Sametime servers and the Domino directories are in different domains. A Cross Domain Configuration should be applied and the da.nsf on each Sametime server should point to the required NAB in the remote Domino cluster. One server in the Domino environment (domain B) should be defined as the Administration server of the Primary address book for the Domino Domain. The da.nsf of each Sametime server should point to the NAB on this server.

Changing a person's name with AdminP:

You can use the AdminP feature to change a user's name in IBM Sametime.
About this task

To change a name in an environment with the AdminP add-in enabled:

**Procedure**

1. From the IBM Lotus Domino Administrator, click the **People & Groups** tab.
2. In the left-hand column, choose **People** under the selected directory.
3. Select the name that you want to change; for example, "Sara Lester".
4. On the right-hand side, select the **People** tab and choose **Rename**.
5. In the "Rename selected HTTP, POP3, and IMAP people" dialog box, specify the time frame allowed for a user to login with both the old and the new names and click **Next**.
6. Now select a user name, fill in information in the appropriate fields to change the name, and click **Next**.
   For example, to change Sara's last name from "Lester" to "Webster," type Webster in the **Last Name** field. Domino processes these name changes periodically (every 60 minutes by default). When the process is complete, the changes are reflected in vpuserinfo.nsf and stnamechange.nsf as follows:
   - In vpuserinfo.nsf, the storageUserId of the renamed user is changed to the new name. For example, "Sara" storageUserId is changed from "CN=Sara Lester" to "CN=Sara Webster".
   - In stnamechange.nsf, a new name change task is created, containing a CSV file that describes the name change.
   An adminp.csv file containing your changes is then attached to the newly created task. For example, the adminp.csv file for changing Sara's last name looks like this:
     ```
     ID,
     "CN=Sara Lester/O=ExampleCorp", "CN=Sara Webster/O=ExampleCorp", "Sara Webster/ExampleCorp"
     ```
7. Run the stnamechange.cmd to complete the name change process.
   For more information, refer to the topic "Running Name Change Tasks on Sametime servers in a community" in this Sametime Information Center. Additional information is available in the Tech Note "NameChange administration tasks in Sametime 8" at the following web address:
   http://www.ibm.com/support/docview.wss?&uid=swg21290627

**Troubleshooting AdminP integration:**

If your AdminP integration does not work properly, use the information below to help resolve issues.

**The AdminP feature is not working**

1. Ensure the AdminP name change add-in is enabled by the following line in the notes.ini:
   ```
   EXTMR_ADDINS=StUpdateAdminP.dll
   ```
2. Turn on the trace files flags, rename in the directory, and analyze the trace files.

**The trace files indicate that the JNI does not find the java class**

1. Ensure the following files are located in the program directory:
   - nadminp.exe
   - StUpdateAdminP.dll
   - AdminpUpdate.jar
• NameChangeUtils.jar
• stnamechange.jar

2. Ensure the following directory flags in sametime.ini have the correct values:
   • ST_JAVA_CLASS_PATH
   • ST_JAVA_JVM_PATH
   • ST_JAVA_LIB_PATH

**Working with trace files:**

Trace files are located in the trace directory.

The Trace flags are located in the [Debug] section of sametime.ini:

```
VP_ADMINP_UPDATE_TRACE=1
ADMINP_ADDIN_DEBUG_LEVEL=5
```

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>StUpdateAdminP_080608_1046_2508_000.txt</td>
<td>C trace files</td>
</tr>
<tr>
<td>stupdateJava_080608_1122.txt.0</td>
<td>Java code trace files for the AdminP name change addin and Name Change API together</td>
</tr>
</tbody>
</table>

**Validation**

Do the following to validate that a name change worked:

1. Rename a user in the Domino directory.
2. On the Domino console, type: tell adminp process all (this will process all the AdminP requests immediately).
3. Verify that a new task with the correct name change was added to stnamechange.nsf.
4. Verify that the user’s “StorageUserId” value was renamed.

**Updated trace information**

Verify that the StUpdateAdminP_080624_1451_3192_000.txt trace file contains a line similar to the following:

```
080624_145626,INF,DEBUG , JNI call completed for name = CN=Sara Lester/O=ExampleCorp
```

Verify that the stupdateJava_080624_1456.txt.0 trace file contains lines similar to the following:

```
Jun 24, 2008 2:56:23 PM
com.ibm.sametime.stupdate.StUpdateDBs updateDb
FINE: from java method old name is CN=Sara Lester/O=ExampleCorp newName = CN=Sara Webster/O=ExampleCorp
```

```
Jun 24, 2008 2:56:23 AM
com.ibm.sametime.namechangeutils.NameChangeUtils createChangeNameTask
INFO: completed.
```
Changing the IP address of an IBM i Sametime Community Server

Your IBM i Sametime Community Server should be set up so that it uses host names and does not refer directly to IP addresses. This allows you to change the IP address for your Sametime Community server by simply updating the host table and DNS.

About this task

To change the IP address for your Sametime Community server, follow these steps:

Procedure

1. Update your host table so that the new IP address is associated with the appropriate host name. Make sure that the fully qualified host name is listed first among the entries for your IBM i Sametime Community Server, before any short names. For more information, see "Updating the host table on IBM i."
2. Likewise, update your DNS entries so that the new IP address is associated with the appropriate host name. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see "Updating the Domain Name Server for IBM i."
3. Stop and restart the Sametime Community Server for the changes to take effect.

Changing the host name of an IBM i Sametime Community Server

The command CHGLSTDOM simplifies the process for changing the host name setting of an IBM i Sametime Community Server.

About this task

The procedure described in this section can also be used to correct problems with the configuration of your Sametime server. For example, if your TCP/IP host table did not correctly list the fully qualified host name first at the time that you setup your Sametime Community Server, many elements of your server configuration may be incorrect. You can correct this problem by following this procedure to change the host name of your Sametime Community Server.

To change the host name, follow these steps:

Procedure

1. Update your host table so that the new host name is associated with the appropriate IP address. Make sure that the fully qualified host name is listed first among the entries for your Sametime server, before any short names. For more information, see "Updating the host table on IBM i."
2. Likewise, update your DNS entries so that the new host name is associated with the appropriate IP address. Check whether your server is configured to search the Domain Name Server (DNS) before the host table. If it is, you must also make sure that the fully qualified host name of your Sametime Community Server is listed first in the DNS. To check the configured search order, see "Updating the Domain Name Server for IBM i."

3. End the IBM i Sametime Community Server.

4. Update the host name for the Domino server using the CHGDOMSVR command. For detailed information on changing the configuration of a Domino server, refer to "Updating the configuration of existing IBM i Domino servers."

5. On any IBM i command line, type the following and press F4:
   CHGLSTDOM

6. On the Change Sametime on Domino display, specify the following and then press Enter:
   - The name of the IBM i Sametime Community Server where you want to make this change (for example, stdom1).
   - The new fully qualified host name for the IBM i Sametime Community Server (for example, stdom1.acme.com).
     - Updates the Ports - Notes Network Ports - Net Address field in the Server document.
     - Adds the host name to the Internet Protocols - HTTP - Host name field in the Server document.
     - Updates Sametime files that reference the host name.

   Note: If your server is enabled for both IPv4 and IPv6 addressing, you must manually update the sametime.ini file so that "VPS HOST=" is set to an explicit IP address, rather than the host name, after running the CHGLSTDOM command. See Configuring the Community Services for IPv6 for detailed instructions.

7. Start the IBM i Sametime Community Server.

8. Open the Domino directory (names.nsf) on your IBM i Sametime Community Server and edit the Server document. Look at the Internet Protocols - HTTP tab in the Server document and locate the Basics - Host name(s) field.

9. The Basics - Host name(s) field may contain more than one name. If any of the names are incorrect or not needed, delete them. Make sure that the correct fully qualified host name is listed first in the field.

   Note: If your server is configured for both IPv4 and IPv6 addressing, there are additional considerations when updating the Host name field. See Configuring Lotus Domino for IPv6 on IBM i for detailed instructions.

10. Save and close the Server document.

11. If you are using HTTP Tunneling with multiple IP addresses, then additional configuration updates are required. See "Updating the host names when using HTTP Tunneling with multiple IP addresses" later in this section.

12. Stop and restart the IBM i Sametime Community Server for the changes to take effect.

What to do next

Updating the IBM i host names when using HTTP Tunneling with multiple IP addresses
If you are using HTTP Tunneling with multiple IP addresses, then you must update your configuration manually after using the CHGLSTDOM command to change the IBM i server host name. If you are not using HTTP Tunneling with multiple IP addresses then this step is not applicable.

The CHGLSTDOM command placed the new host name in the tunneling host name fields, but did not preserve the required prefixes, such as community-, meeting- and broadcast-, in the Sametime configuration. Use the Sametime Administration tool to update the host names in the following fields in the "Connectivity" section:

- **Community Services Network settings -> Address for client connections-Host name** should have prefix of community-
- **Community Services Network settings -> Address for HTTP tunneled client connections-Host name** should have prefix of community-

### Monitoring the Sametime Community Server

The IBM Sametime monitoring charts allow you to monitor Sametime Community server statistics by providing up-to-the-second information about Community Services, web statistics, and free disk space on the server.

#### About this task

All monitoring charts are available from the Monitoring menu in the Sametime Administration Tool. The charts that are available from the Miscellaneous link in the Monitoring menu are part of the Domino web Administration Tool. These charts provide information on web statistics, server memory, and disk space. To view the status of the Sametime Community services since the last server restart, click the Overview link in the Sametime Administration Tool. Also note that the time of day that is listed in the monitoring charts is calculated according to the browser's time zone, not the server's time zone.

#### Procedure

1. Enter the URL for the Sametime Community server:
   ```
   http://hostname/servlet/auth/admin
   ```
   Where **hostname** is the fully qualified Domain Name Service (DNS) name or the IP address of the Sametime Community server you want to administer.

2. Enter the administrator name and password specified during the Sametime Community server installation.

3. Select **Monitoring**.

   **Note:** To view the status of the Sametime services since the last server restart, click **Overview**.

4. Select the appropriate chart for monitoring.

**Monitoring general Sametime Community Server status**

General Server Status monitoring chart allows you to see the status of the IBM Sametime Community Server at a glance.

**Total Community Logins**

The Total Community Logins chart displays current information about:

- **Total Community Logins** - The total number of logins to Community Services on the Sametime Community Server that you are monitoring.
Community Logins chart includes multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

- **Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, the Total Unique Logins chart records only one login for that user. A user logged in from multiple clients is considered a single unique login. Use this chart to determine the current number of Community Services users.

- **Total 2-way Chats** - The total number of 2-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with another user, that chat will be counted in the Total 2-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total n-way Chats** - The total number of multi-person chats taking place on the Sametime Community Server. This chart only includes chats that were started from the Sametime Community Server you are monitoring. For example, if you are monitoring server A and a user who has specified server A as her home server starts a chat with two other users, that chat will be counted in the Total n-way Chats chart. You will not see chats that were started by users who have specified a server other than server A as their home server.

- **Total Number of Active Places** - The Total Number of Active Places chart lists the combined number of n-way Chats and active meetings. Both n-way Chats and online meetings are counted as Active Places; 2-way Chats are not counted in this chart.

**Monitoring Sametime Community Services logins**

A user can be logged in to the IBM Sametime Community Services from more than one client.

To access the Logins chart, open the Sametime Administration Tool and select **Monitoring > Logins**. The Logins chart displays:

- **Community Server Total Logins** - The total number of logins to Community Services, including multiple logins from the same user. For example, if a user is logged in from both the Sametime Connect client and the Participant List component of the Meeting Room, this chart records two logins for that user.

  Internal components of the Community Services also log in to the Community Services. These are intra-server connections between Community Services components that occur as part of the normal operations of the Community Services. These logins are also counted in the total logins chart.

- **Community Server Total Unique Logins** - If a user is simultaneously logged in from multiple Community Services clients, this chart records only one login for that user. A user logged in from multiple clients is considered a single "unique" login. Use this chart to determine the current number of Community Services users.

The Logins chart updates at the time interval specified in the **Polling Interval (seconds)**. Enter a new interval to change the rate at which the chart updates. To update the chart immediately, click **Refresh**.
Monitoring miscellaneous Domino web Administration statistics

The Miscellaneous charts are part of the IBM Lotus Domino Web Administration pages. The IBM Sametime Community Server uses features in the Lotus Domino server and its associated web administration pages.

You can monitor various statistics and events from the Lotus Domino Web Administration pages, including:

- Memory
- Statistics
- Disk Space

To access the Domino Web Administration pages, choose Monitoring > Miscellaneous in the Sametime Administration Tool, and then click the link that appears at the bottom: You can view the Lotus Domino web Administration pages in a new browser window.

Monitoring the Domino log

To access the Domino log, choose Logging - Domino Log in the Sametime Administration Tool, and then click the link that appears on the right. The Domino log launches in a new browser window.

The Domino log is only available from the Sametime Administration Tool. If you record Sametime log information in a text file, the text file does not include information about the Domino log.

A administrator can view additional information about the Sametime server in the Domino log database (log.nsf). The Domino log database records server activity information related to the Domino server and Domino databases, including databases used by the Sametime server (such as the Sametime Meeting Center). During setup, the Domino log database is automatically created and the server is assigned Manager access in the database's Access Control List (ACL). The default access for all other users is Reader.

The Domino log database records information about all server activities, such as database size and usage, server events, calls made to and from the server, and billing for server services. Check the Domino log to monitor:

- Available server disk space
- Available server memory
- Server load
- Server performance
- Databases that need maintenance

Content of the Domino log

The administrator cannot use the Sametime log settings or the Sametime Administration Tool options to determine what appears in the Domino log. The Domino log records information about the activities of the Domino server on which Sametime is installed. Generally, the default settings should provide an adequate record of server activity. However, you can record additional information in this log file by altering settings in the notes.ini file. Recording this additional information might be necessary to troubleshoot a specific system problem.

For more information, see the Maintenance section of the Domino R5 Administration documentation.
**Views in the Domino log**

The Domino log includes many views that do not apply to Sametime. Use the table below to determine which views are relevant for Sametime.

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database-Sizes</td>
<td>Lists the size of the database, the percentage of the database's disk space in use, and the weekly usage for all databases on the server. Use this view to check unused views, database size, and unused space in a database. <strong>Note:</strong> The stconf.nsf database grows in size depending on the number of meetings that have been created. You can archive this database frequently to prevent it from growing too large.</td>
</tr>
<tr>
<td>Database-Usage</td>
<td>Lists the date and time the database was accessed, the type of access, and the name of the user accessing the database for all databases on the server. Use this view to check unused views and unused space in a database.</td>
</tr>
<tr>
<td>Mail Routing Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>Shows Sametime events and error messages not contained in other views. Messages are sorted in order of occurrence. Use this view to check for Sametime error messages, server crashes, and corrupted databases.</td>
</tr>
<tr>
<td>NNTP Events</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Object Store Usage</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Passthru Connections</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By Date</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Phone Calls-By User</td>
<td>Not used by the Sametime server.</td>
</tr>
<tr>
<td>Replication Events</td>
<td>Not used by the Sametime server.</td>
</tr>
</tbody>
</table>
Sample Billing Shows the same information provided in the Usage views, but the information is not categorized. The information in this view can be easily exported to a spreadsheet.

Use this view for billing purposes, such as Meeting Center usage, network usage, and database usage.

Usage-By Date Shows Sametime user transactions sorted by date. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating documents. Each record lists the date and time of the transaction, the user name, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check database use on a specific date and users' transactions with the server.

Usage-By User Shows Sametime user transactions by user name. Transactions are operations such as starting meetings, attending meetings, opening documents, and updating a document. Each record lists the user name, the date and time of the transaction, the minutes of usage, the number of read operations, the number of write operations, the size of the database, and the total number of transactions.

Use this view to check a particular user's transactions on a database.

**General log settings**

The General log settings allow you to specify the format for the Sametime log and to control the information that the log records.

The four types of General log settings are: (Note that meeting server events do not apply to Sametime Limited Use.)

- **Database or text file settings** - Allow you to specify the format for the log and to automatically remove information from the log.
- **Sametime statistics settings** - Allow you to control whether to log statistics related to chats, meetings, and users.
- **Server community events to log settings** - Allow you to control which Community Services events are recorded in the Sametime log.
- **Meeting server events to log settings** - Allow you to control which Meeting Services events are recorded in the Sametime log.

**Log output location:**
To access the "Database or text file" settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The "database or text file" settings allow you to specify the format for the log and to automatically remove old information from the log.

**Enable logging to a Domino database (STLog.nsf)**

Select this setting to record Sametime Meeting Services and Community Services data in the Sametime log database (stlog.nsf). During setup of the Sametime server, the Sametime Log database is automatically created, and the administrator specified during setup is assigned Manager access in the database Access Control List (ACL). The server is also assigned Manager access to the database so that it can write information to the log. The default access for all other users is Reader.

When this option is selected, a Sametime administrator can view all of the information in the Sametime log by opening the Sametime Administration Tool and selecting Logging. The links available from the Logging menu display different views of the Sametime log database.

When this option is selected, you can use the "Remove history after (days)" setting to prevent the Sametime log from growing too large.

If the "Enable logging to a Domino database" option is not selected, Sametime activity is not recorded in the Sametime database, and the links beneath the logging option in the Sametime Administration Tool do not appear.

If you select this option, you cannot select the "Enable logging to a text file" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Remove history after (days)**

Select this setting to automatically remove old information from the Sametime log database (stlog.nsf). In the field provided, specify the age (in days) of information that is automatically removed from the database. The default setting is 60 days.

This setting only applies to the Sametime log database; it does not remove Sametime log information stored in text files. You must manually delete old text files.

After selecting this option, click Update and restart the server for the setting to take effect.

**Logger output location**

Select this setting to record Sametime log information in a text file. When this option is selected, a new Sametime log text file is created every day. By default, the name of each text file contains the date on which the file was created (for example, log_23_Mar_2009.txt). After you select this option, specify a path and file name for the log file in the "Path to log text file" field; for example, in Microsoft Windows: d:\notesdata\chatlogs\txtfiles\log.txt
To view the file, open it in your preferred text editor. You cannot view the text file log from the Sametime Administration Tool.

If you log Sametime activity to a text file:

- Sametime activity is not recorded in the Sametime log database, and the links beneath the logging option in the Sametime Administration Tool do not appear.
- You cannot access the Domino log when you log to a text file.
- You must manually delete the text files from the server hard drive periodically to conserve hard disk space.

If you select this option, you cannot simultaneously select the "Enable logging to a Domino database" option; it is not possible to record Sametime activity in both database and text file format.

After selecting this option, click Update and restart the server for the setting to take effect.

**Sametime Community Server log size and content settings**

To access the log settings, choose Logging - Settings in the Sametime Administration Tool.

The IBM Sametime Community Server uses these log settings:

- General settings - Allow you to specify the format and content of the Sametime Community Server log.
- Capacity Warnings - Allow you to set server usage parameters. When these parameters are exceeded, warning messages are written to the Sametime log. These messages help you monitor server usage and determine the cause of slow server performance.

**Sametime Community Server events log settings:**

To access the IBM Sametime Community Server events log settings, open the Sametime Administration Tool, select Logging - Settings, and click the General tab.

The Community Server events log settings allow you to control which Community Services events are recorded in the Sametime Community Server log. After selecting any of these options, click Update for the settings to take effect.

**Note:** The settings take effect within a reasonable time period. The longest time period you will wait for these settings to take effect is the time interval specified for the "How often to poll for new servers added to the Sametime community" setting in the Configuration - Community Services settings of the Sametime Administration Tool. The default time interval for that setting is 60 minutes.

**Successful logins**

Select this setting to record information about successful Community Services logins and logouts in the Community Logins/Logouts section of the Sametime log. This option is selected by default.

**Failed logins**

Select this setting to record information about failed logins to Community Services in the Place Login Failures, Meeting Login Failures, and Community Logins/Logouts sections of the Sametime log.
Community server events and activities

Select this setting to record information about Community Services events in the Community Events section of the Sametime log. For example, you can view the name and status of each service.

Administering a Sametime Proxy Server

This section describes how to manage an IBM Sametime Proxy Server.

Updating Sametime Proxy Server connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Proxy Server.

Before you begin

If you are configuring the Sametime Proxy Server to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Proxy Server. These settings are only used by the Sametime System Console to connect to the Sametime Proxy Server.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Proxy Server.
3. In the Sametime Proxy Servers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's User name and Password for connecting to the Sametime Proxy Server.
5. By default, the Sametime Proxy Server trusts other Sametime components. If you want to change this, then select Do not auto-accept SSL certificate.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Administering a Sametime Media Manager

The audio/video services are enabled by default following an IBM Sametime Media Manager installation. You can enable and disable the audio/video services from the Sametime System Console. This section describes how to manage the Sametime Media Manager.
About this task

The Sametime Media Manager manages Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between those participants. The Sametime Media Manager supports interactive IP audio and video capabilities and enables clients with the appropriate hardware (sound card, microphone, speakers, and camera) to transmit and receive real-time audio and video in a Sametime meeting room.

Updating Sametime Media Manager connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Media Manager.

Before you begin

If you are configuring the Sametime Media Manager to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Media Manager. These settings are only used by the Sametime System Console to connect to the Sametime Media Manager.

Follow these steps to update connection setting information.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the Edit next to the deployment name of the server with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's User name and Password for connecting to the Sametime Media Manager.
5. By default, the Sametime Media Manager trusts other Sametime components. If you want to change this setting, then select Do not auto-accept SSL certificate.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Managing UDP ports for voice chat and video calls

Change the default UDP ports for computer-to-computer voice chats and video calls in an IBM Sametime deployment.

Before you begin

When the NAT traversal feature is enabled, the Connect client no longer uses the traditional ports (20830+2); instead it uses random ports for ICE negotiation. You should still leave the original ports open so they can be used by older clients that are not supported by the NAT traversal feature.
About this task

IBM Sametime comes with voice chat. With voice chat, users can place and receive audio calls using their computer's and their chat partners' computer audio capabilities. Once a user has a computer-to-computer voice chat started, the user can convert it to a video call so that the user can both see and hear call participants.

Voice chat works with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to speak to other users orally over the computer. The client machines use a single port (UDP port 20830 is the default) for all audio chats, so this port must be opened for both incoming and outgoing UDP traffic.

Video calls also work with user datagram protocol (UDP) packets which flow through UDP ports on the firewall of every client machine to allow users to see video of users with whom they are chatting over the computer. The client machines use a single port (UDP port 20832 is the default) for all video calls, so this port must be opened for both incoming and outgoing UDP traffic.

Note: The client might require ports for the audio and video channels to send RTP and RTCP packets over UDP.

Follow these steps to change the UDP ports:

Procedure
1. Log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. The Sametime Media Manager listens for inbound audio streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for audio calls** field.
6. The Sametime Media Manager listens for inbound video streams from clients on a range of 100 UDP port numbers. Under Participants, enter the starting number of this range of ports in the **Starting UDP port for video calls** field.
7. Click **OK**.
8. Restart the Sametime Media Manager.

Managing multiple audio and video streams

The IBM Sametime Media Manager manages multiple audio and video streams in a meeting.

About this task

The Sametime Media Manager scans the meeting participants and locates the person currently speaking (transmitting audio packets). The Sametime Media Manager performs switching operations as different people speak during a meeting. When a meeting participant speaks, the Sametime Media Manager locks onto that client's audio stream and distributes that stream to all other clients in the meeting.
meeting. When a participant stops speaking, the Sametime Media Manager waits for a brief period of time, and then begins scanning for the other active audio clients.

The video follows the audio. When the Sametime Media Manager switches to a new audio source (speaking person), the Sametime Media Manager through its connections to the clients, ensures that the icon indicating the current speaker is properly updated for all clients. After this update, the Sametime Media Manager sets the video source to the person currently speaking. It is important to ensure that the video does not switch too quickly. Rapid video switching reduces usability. You can control the time interval that must pass before the video switches to the new speaking person.

**Note:** If the current speaker does not have video capabilities or has the video window paused, the Sametime Media Manager send’s the next loudest speaker's video as the active speaker to all participants.

By default, the Sametime Media Manager can lock onto and broadcast a maximum of five audio streams at the same time. In a meeting, if five people speak at the same time, it is possible for all meeting participants to simultaneously hear five people speaking. The Sametime Media Manager designates the audio stream that has been transmitting the longest (generally, the person who started speaking first) as the primary audio stream. The source of the primary audio stream is also the source of the video stream. Audio and video services provided by the Sametime Media Manager have been tested and optimized for sessions with 20 participants. The actual number of participants will vary based on network and environmental conditions. The higher the number of switched audio streams, then the more bandwidth that is required.

In meetings, especially in large meetings, IBM recommends that participants, who are not talking, mute their speakers to reduce noise.

**Procedure**
1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager.**
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.
4. Click the **Configuration** tab.
5. Under Presence, type a number between 2 and 16 in the **Number of switched audio streams** field to change the number of simultaneous audio streams.

   **Note:** The more switched audio streams, the more people are heard simultaneously in a meeting. Meetings could become quite noisy, so use caution when you increase this number.

6. Under **Set the time in milliseconds before switching to the next active speaker**, select a number in **Video switching wait time** to control the time interval that must pass before the video switches to the new speaking person.
7. Click **OK.**
8. Restart the Sametime Media Manager.
Changing the SIP transport protocol in the Sametime Media Manager

You can change the transport protocol that IBM Media Manager uses for the SIP Proxy and Registrar.

About this task

SIP makes use of elements called proxy servers to help route requests to the user’s current location, authenticate and authorize users for media services, and provide Sametime Media features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

The transport protocol determines the network transport mechanism to use for sending SIP messages. The SIP proxy application examines all requests sent by the Sametime Media Manager to determine whether a given request is sent by an appropriate proxy application. All requests are routed according to the transport protocol defined here.

In a multiple machine deployment where Sametime Media Manager components are installed on different machines, you must update the SIP transport protocol on all components: Conference Manager, Packet Switcher, and SIP Proxy and Registrar. Moreover, if you change the SIP transport protocol from TLS to TCP, then the port changes are automatically reflected in the stavconfig.xml file on the Conference Manager. You must manually change the ports in the stavconfig.xml files of the Packet Switcher component.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. Under Server Integration, select a Transport protocol of TLS or TCP. UDP is not supported.
6. Set how frequently in seconds you want SIP to check if a client is still connected. Enter a number between 30 and 300 in the Session expiration field.
7. Click OK.
8. Update SIP Registrar security role settings by following these steps.
   a. Log in to the SIP Proxy and Registrar.
   b. Click Applications > Enterprise Applications.
   c. Click IBM SIP Registrar setting.
   d. Under Detail Properties, click Security role to user/group mapping.
   e. Change security role settings from All Authenticated in Application’s Realm to Everyone if the protocol is updated to TCP. Do this by selecting the checkbox for the AllAuthenticatedUsers role, then select Map Special Subjects and select Everyone. Leave All Authenticated in Application’s Realm if the protocol is selected as TLS.
9. Restart the Sametime Media Manager.
What to do next

If you have deployed the Conference Manager, Packet Switcher, and SIP Proxy and Registrar on separate application servers, and you have changed the SIP transport protocol from TLS to TCP, the Conference Manager stavconfig.xml file automatically reflects this change. You must edit the stavconfig.xml files on the Packet Switcher to reflect this update by changing the secure ports to nonsecure ports. Follow the steps in **** MISSING FILE ****.

Managing media encryption and codecs

You can manage the type of media encryption and codecs used in meetings on the IBM Sametime Media Manager.

About this task

A codec compresses streaming data, such as audio or video, on the transmitting side and decompresses it for playback on the receiving side. Codecs reduce the amount of bandwidth required to send streaming data. Generally, higher compression conserves more bandwidth. Higher compression also results in poorer audio or video quality and requires more resources to compress and decompress the data streams.

You can change the type audio and video codecs.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Media Manager.
3. In the Sametime Media Managers list, click the deployment name of the Sametime Media Manager.
4. Click the Configuration tab.
5. Follow the procedure appropriate for your deployment:
   - Single box deployment with all components on one machine: Under Audio Video Media, keep the default encryption option as Disable or click Enable. Calls made between the Sametime Connect client and any other endpoint supporting SRTP including another Sametime Connect client or a partner conference bridge are encrypted. Audio/video conferences with three or more participants using the Media Manager Packet Switcher or the Sametime Unified Telephony Media Server are not encrypted.
   - Non-clustered distributed and clustered deployments:
     a. Under Audio Video Media change the encryption option to Enable or Disable. This action only automatically updates the stavconfig.xml file of the Conference Manager component.
     b. A manual update is required on Packet Switcher deployments. Update the stavconfig.xml encryption field values to NoEncryption if you have selected Disable, or to SRTP if Enable is selected, into the Deployment Manager server's scope stavconfig.xml files, and run Full-resynchronize on nodes, then restart the Packet Switcher servers.

Note:

NoEncryption and SRTP are the only string literals to update stavconfig.xml with.
The Sametime Community server default refresh interval is one hour. The Sametime Connect client gets the updated server policy attribute after one hour.

6. Prioritize the audio codecs by using the **Up** and **Down** buttons to move the audio codecs in the list.
   
   Sametime Media Manager supports the following audio codecs:
   
   - **ISAC** - Internet Speech Audio Codec (iSAC) is a wideband and adaptive bit rate codec. The bit rate ranges from 10 to 32 kbps (Kilobit per second) depending on the available network bandwidth. This is the default codec.
   - **iLBC** - Internet Low Bit-rate Codec (iLBC) is a narrowband low bit rate speech codec. It requires 15.2 kpbs bandwidth.
   - **G.722.1** - Popular wideband audio codec that operates at one of three selectable bit rates: 32000, 24000, 16000. G7221 is a licensed royalty-free standard audio codec providing high quality, moderate bit rate audio coding.
   - **G.711** - Old and widely supported narrowband codec. It requires 64 kbps bandwidth but consumes less CPU to process.

7. Prioritize the video codecs by using the **Up** and **Down** buttons to move the video codecs in the list.
   
   Sametime Media Manager supports two video codecs:
   
   - **H264** - Also known as AVC and MPEG-4 part 10. It provides high quality, block-oriented, motion-compensation-based video codec for video conferencing. It supports the Baseline Profile without Flexible Macroblock Ordering (FMO).
   - **H263** - A legacy codec and lower quality than H264.

8. Click **OK**.  
9. Restart the Sametime Media Manager.

**Managing video bit-rate**

You can change the video bit-rate that you use in meetings using the IBM Sametime Media Manager.

**About this task**

One of the key factors effecting video quality is the available network bandwidth. The higher the video resolution, the more bandwidth is required and the better quality. The Sametime video codec can automatically adapts to the available bandwidth and reduces the bit-rate to a certain threshold for each chosen video resolution. However, the quality will suffer when the available bandwidth becomes too low, especially during peak utilization when the contention in the network routers causes packet loss. Use the following information as the guideline to set the desire codec resolution.

**Procedure**

1. Log in to the Integrated Solutions Console.  
2. Click **Sametime System Console > Sametime Servers > Sametime Media Manager**.  
3. In the **Sametime Media Managers** list, click the deployment name of the Sametime Media Manager.  
4. Click the **Configuration** tab.  
5. Under Video Bit Rate, select a **Video Resolution**.
   
   - HD-720p 1280x720@60fps 4096kbps
   - HD 960x720@60fps 4096kbps
- XGA 1024x768@35fps 6144kbps
- WIDE FULL HD 1920x1080@30fps 10240kbps
- FULL HD 1440x1080@30fps 8192kbps
- HD-720p 1280x720@30fps 2048kbps
- HD-720p 1280x720@30fps 1472kbps
- HD-720p 1280x720@30fps 1024kbps
- HD-720p 1280x720@30fps 768kbps
- HD 960x720@30fps 2048kbps
- 432P 720x432@30fps 1024kbps
- 432P 720x432@30fps 768kbps
- 432P 720x432@30fps 512kbps
- VGA 640x480@30fps 1024kbps
- VGA 640x480@30fps 896kbps
- VGA 640x480@30fps 512kbps
- VGA 640x480@30fps 384kbps
- W288P 512x288@30fps 384kbps
- CIF 352x288@30fps 768kbps
- CIF 352x288@30fps 512kbps
- QCIF 176x144@30fps 384kbps
- QCIF 176x144@30fps 192kbps
- SQCIF 128x96@30fps 128kbps
- SQCIF 128x96@30fps 64kbps
- 4CIF 704x576@25fps 1536kbps
- 4CIF 704x576@25fps 512kbps
- QVGA 320x240@20fps 384kbps
- VGA 640x480@15fps 896kbps
- CIF 352x288@15fps 384kbps
- QCIF 176x144@15fps 128kbps
- QCIF 176x144@15fps 64kbps
- 4CIF 704x576@12fps 1024kbps
- QVGA 320x240@10fps 192kbps

The video resolution is composed of the following elements:
- **Resolution name** - The video resolution name, for example Common Intermediate Format (CIF).
- **WidthxHeight** - The dimensions of the video in pixels.
- **Framerate** - Frames per second.
- **Bit-rate** - Maximum kilobits per second

6. Click OK.
7. Restart both the Sametime Media Manager and the Sametime Community Server.

**Changing the default number of maximum users**

As demands on video conferencing change, you can update the maximum number of participants to ensure that your network can support this feature.
About this task

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

Note: The maximum number of users can set independently internally (on the Sametime Packet Switcher) and externally (on the MCU that bridges video-conferencing connections).

Procedure
1. On the server hosting IBM Sametime Media Manager, open the ConferenceManager.properties file. In a multiple-machine deployment where Sametime Media Manager components are installed on different machines, go to the server hosting the Conference Manager. If you can adjust the maximum participants setting for each Service Provider Implementation (each adapter); each adapter has its own ConferenceManager.properties file.

   websphere_install_path/AppServer/profiles/profile_name/installedApps/cell_name/ConferenceFocus.ear/ConferenceFocus.war/ConferenceManager.properties

2. Edit the values in the following settings:
   MaximumAudioConferenceUsers=20
   MaximumVideoConferenceUsers=20

   For example, the Radvision TCSPI Adapter ConferenceManager.properties file contains this setting by default:

   #
   # PerConferenceMaximum is the maximum number of users the service provider supports for each conference call.
   # MaximumConferenceUsers=200
   so you will probably want to lower value that to provide better performance within your network.

3. Restart the Sametime Media Manager.

Administering a SIP Proxy and Registrar

This section describes how to manage the properties of a SIP proxy and registrar.

About this task

Session Initiation Protocol (SIP) is a protocol that manages communication in IBM Sametime meeting rooms by maintaining a dialog with each participant, and ensuring that all media flows between meeting participants. SIP makes use of elements called proxy servers to help route information to the user’s current location, authenticate and authorize users for meetings, and provide features to users. SIP also provides a registration function that allows users to send their current locations for use by proxy servers.

Adding a Sametime Media Manager’s SSL certificate to the Sametime System Console

If you need to enable SSL (Secure Socket Layer), make sure you add the certificate from the IBM Sametime server (Sametime Meeting, Proxy, Media Manager, Gateway, or SIP) to the Sametime System Console.
About this task

To enable SSL, you must extract the certificate from the Sametime product server and add it to the trust store of the Sametime System Console. The Sametime product servers include:
- Sametime Meeting Server
- Sametime Proxy Server
- Sametime Media Manager
- Sametime Gateway Server
- SIP Proxy and Registrar

Follow these instructions. See the WebSphere Application Server information center for more information on extracting and adding certificates.

Procedure
1. Log in to the Integrated Solutions Console for the Sametime product server.
2. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
3. Select the alias named root, and click Extract.
4. Enter the name of the .cer file, and select Base64 as the type for storing the process server signer certificate.
5. Log in to the Integrated Solutions Console for the Sametime System Console.
6. Click Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates
7. Click Add.
8. Enter an alias.
9. Enter the file name where you stored the extracted process server signer certificate from the product server.
10. Click Apply.
11. Restart the Sametime System Console deployment manager.

Updating SIP Proxy and Registrar connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the SIP Proxy and Registrar.

Before you begin

If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the SIP Proxy and Registrar. These settings are only used by the Sametime System Console to connect to the SIP Proxy and Registrar.
If you are configuring the SIP Proxy and Registrar to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store using the Integrated Solutions Console (Security > SSL certificate and key management > SSL configurations > CellDefaultSSLSettings > Key stores and certificates > CellDefaultTrustStore > Signer certificates). See the WebSphere Application Server information center for more information on adding certificates.

Follow these steps to update connection setting information.

**Procedure**

1. Log in the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.
3. In the SIP Proxy and Registrar list, click the Edit next to the deployment name of the SIP Proxy and Registrar with the connection information that you want to change.
4. Under Connection Properties, enter the administrator's **User name** and **Password** for connecting to the SIP Proxy and Registrar.
5. By default, the SIP Proxy and Registrar trusts other Lotus Sametime components. If you want to change this, then select **Do not auto-accept SSL certificate**.
6. Click **Save**.
7. Click **Done** to return the SIP Proxy and Registrar list.
8. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

**Managing SIP proxy properties**

You can set properties for the SIP proxy server.

**About this task**

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users to access media services, and provide Sametime media features to users.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.
3. Click the Deployment Name of the SIP Proxy server.
4. In **SIP Proxy and Registrar**, click **Proxy Administration**.
5. Use the following table to set basic SIP proxy properties:
Record route mode

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.

Parallel search mode

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.

Add public IP to outgoing request

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.

6. Specify Handled Domains. These are domains that are managed by the SIP Proxy and Registrar.

7. Routing rules define how SIP messages are routed through the Sametime SIP proxy server. The table shows any existing rules, with the highest priority granted to the first rule in the table. Click a rule to open it for editing or click New to create a new routing rule.

8. Click OK.

9. Restart the SIP Proxy and Registrar.

Creating and editing routing rules for SIP-based messaging

Add or edit routing rules that define how the SIP Proxy server routes SIP-based messages.

About this task

Routing rules tell Sametime where to direct SIP-based messages under certain conditions. The rule consists of one or more conditions, and a destination (SIP endpoint) where call requests that meet the conditions will be routed.

A routing rule uses the same transport protocol as the Sametime Media Manager components. For example, if the Media Manager is configured to use TLS for the SIP signalling, you must use TLS for all routing rules. The supported transport protocols are TCP and TLS over TCP. UDP is not supported.

Procedure

Use the routing rules table in the Proxy Administration page to view, create, or edit rules.

1. On the Sametime System Console, log in to the Integrated Solutions Console as the IBM WebSphere administrator.
2. In the navigation tree, click **Sametime System Console > Sametime Servers > SIP Proxies and Registrars**.

3. On the SIP page, look in the proxies table and click the **Deployment Identifier** of the SIP Proxy and Registrar.

4. On the SIP Proxy and Registrar page, click **Proxy Administration**.

5. In the routing rules table, do one of the following:
   - Click the name of a rule to edit it.
   - Click **New** to create a new rule.

6. Add or modify settings for the routing rule as follows:
   a. Type a name and description of the route in the **Name and Description** fields.
      It is helpful to indicate the route’s direction and endpoint in the name so you can easily distinguish among routes in the routing rules table later.
   b. Use the "Conditions" section to configure the routing rule by defining at least one condition:

   Table 33. Conditions fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>A predefined value indicating the type of request: INVITE, INFO, MESSAGE, or ANY. Select the appropriate value from the field’s list; if you do not select a method, all methods are accepted by this condition.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The originating caller’s IP address, which must match the pattern specified in the regular expression that you provide. You could specify a single IP address: 9,3,186,215 or use an expression to specify a range of IP addresses: 9,3,186,215</td>
</tr>
<tr>
<td>Request URI</td>
<td>The resource, usually the origin server, on which to apply the request. The URI must match the pattern specified in the regular expression that you provide. For example: .<em>example,com,</em> matches both of these incoming initial requests: sip:example,com:5060;transport=tcp SIP/2.0 and sips:subdomain,example,com:5061 SIP/2.0</td>
</tr>
<tr>
<td>Contact Header</td>
<td>The SIP URI of the originating caller. The URI must match the pattern specified in the regular expression that you provide. For example, .<em>20100192,192,0,2\ \ .12:506&lt;01&gt;.,</em> matches incoming initial requests with either of these contact header values: <a href="">sip:20100192\,0\,2\,12:5060;transport=tcp</a> or <a href="">sips:user9920100192\,0\,2\,12:5061;transport=tcp</a></td>
</tr>
</tbody>
</table>
c. In the "Destination" section, select the method to use for storing the address of the destination SIP endpoint:

**Table 34. Destination addressing methods and descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push a Route header field</td>
<td>Insert the destination address into a Route header field of the outgoing SIP request.</td>
</tr>
<tr>
<td>Replace a Request-URI</td>
<td>Replace the original Request-URI with the destination address when creating the outgoing request.</td>
</tr>
</tbody>
</table>

d. Construct the destination address using the method you selected in substep c.

**Push a Route header field**

Supply a value in one or more of the fields described in the table.

**Table 35. SIP URI addressing fields and descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>The scheme can be either SIP or SIPS (the secure version of SIP); the default is SIP. This field is required.</td>
</tr>
<tr>
<td>IP/FQDN</td>
<td>The IP address or fully qualified host name of the destination server (the SIP endpoint). For incoming calls, use the fully qualified domain name of the Sametime Media Manager’s Conference Manager component. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the destination server (the SIP endpoint) is listening on for SIP-based communications. This field is optional; if you do not provide a value, the server uses the correct port. <strong>Note:</strong> Make sure you specify the correct port for the transport protocol. For unsecured TCP communications, the Conference Manager typically uses port 5063; for encrypted TLS communications, the Conference Manager typically uses port 5062.</td>
</tr>
<tr>
<td>Transport</td>
<td>The network transport protocol to use for sending SIP messages: TCP or TLS over TCP (UDP is not supported). Use the same transport protocol throughout the entire route (from the Sametime client to the SIP Proxy/Registrar to the third-party SIP endpoint). For example, if the Media Manager is configured to use TLS for SIP communications, you must use TLS for all routes. This field is optional; if you do not provide a value, the server supplies a transport protocol.</td>
</tr>
</tbody>
</table>

**Replace a Request-URI**

Construct regular expressions to define the original **Request-URI pattern** and its replacement **Output pattern**, which are explained in the table.
Table 36. URI pattern fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request-URI pattern</td>
<td>A regular expression defining the pattern of the original Request URI. Use this field to extract fields or parameters from a Request-URI of a SIP request. A variable stores the part of the Request-URI matched by the part of the regular expression inside the parentheses, indicated by a number. The variables are recalled with the dollar-sign, for example, $1, $2, and so on. These fields or parameters can be used to build the Output pattern. This field is optional.</td>
</tr>
<tr>
<td>Output pattern</td>
<td>A regular expression defining the pattern of the destination's URI (address). This field can contain either a SIP URI or a replacement expression with variables for example, $1, $2, and so on. Variables store the portion of a parenthesized pattern captured from the Request-URI pattern field. After processing any captured variables, the resulting field value must be a valid SIP or SIPS URI. Note: If you do not provide a value in the Request-URI pattern field, this field must contain a valid SIP or SIPS URI.</td>
</tr>
</tbody>
</table>

**Remember:** Regular expressions must follow a strict notation, different from other notation forms you may use. For example, the operating system shell notation for a wildcard (series of 0 or more characters) is the asterisk character: *, The regular expression equivalent for a wildcard is different: it is a combination of a dot followed by an asterisk, as follows: .* Before adding the regular expression to the routing rule, you should test the expressions using any of the testing engines available online. To learn more about creating regular expressions, see the Java Regular Expressions class on the Oracle web site.

e. Click OK to save the rule.
f. Repeat from step 5 until all your routing rules have been defined.
   You must create at least one inbound route and one outbound route between Sametime and each third-party SIP endpoint. You can create different versions of a route using different sets of conditions (all of a route’s conditions must be satisfied for that route to be selected), and you can prioritize routing rules as explained in the next step.

7. Prioritize the routing rules by arranging them in the sequence in which you want them processed:
   It is acceptable to have inbound routes mixed with outbound routes in the sequence because if a message does not satisfy all of the routing conditions, the route will be ignored.
   a. In the routing rules table, select the a route and click the Move Down button or the Move Down button until the route is positioned in the correct sequence.
   b. Repeat as needed until the rules appear in priority sequence.

8. Save the set of routing rules and priorities by clicking Save link in the "Messages" box at the top of the page.
9. Restart the SIP Proxy and Registrar’s server or cluster:
   • For a stand-alone Media Manager or SIP Proxy and Registrar, restart it now as follows:
     a. In the server’s Integrated Solutions Console, click Servers > Server Types > server_type.
     b. In the list of servers, select your server and click the Restart button at the top of the table.
     c. Click the Refresh button and verify that all components are active.
   • For a cluster of SIP Proxy/Registrars, synchronize the nodes before restarting them:
     a. In the Deployment Manager’s Integrated Solutions Console, click System Administration > Nodes.
     b. Select all nodes in the cluster, and then click the Full Resynchronize button at the top of the table.
     c. Back in the navigation tree, click System Administration > Node agents.
     d. Select all nodes in the cluster, and then click the Restart button at the top of the table.

Example

The following examples show different combinations of values for Request-URI pattern and Output pattern that produce specific destination addresses.

• Route all incoming SIP requests to this destination:
  sip:example.com;transport=tcp
  Request-URI pattern: empty
  Output pattern: sip:example.com;transport=tcp
  Because the Request-URI pattern field is empty, the destination is modified on all incoming requests.

• Route incoming SIP requests to a new host, keeping the original user name
  Request-URI pattern: sip:(.+@.*)
  Output pattern: sip:$1@example.com
  The expression in parentheses for Request-URI pattern captures the user name in a variable and the output pattern refers to the variable as $1.
  For example, assume an incoming initial SIP request with a Request-URI of sip:12345@company.com. The Request-URI pattern runs, resulting in the variable $1=12345. The SIP URI for the destination address maintains the same user name, but adds a new host name: sip:12345@example.com.

• Route incoming SIP requests to ”host,” keeping the original user name if the user-name prefix in the Request-URI is ”45”
  Request-URI pattern: sip:(45.+@.*)
  Output pattern: sip:$1@host

• Route incoming SIP requests to ”host,” omitting the prefix if the user-name prefix in the Request-URI is ”45”
  Request-URI pattern: sip:45(.+)@.*
  Output pattern: sip:$1@host

Managing SIP registrar properties

You can set registration expiration properties for the SIP registrar.
About this task
SIP provides a registrar that allows users to send their current locations for use by proxy servers. The SIP registrar accepts user requests and places the information it receives from those requests into the registration table. Registration is how media services learn the current location of a Sametime user. Upon login, and at periodic intervals, the user sends registration messages to the SIP registrar application. These messages associate the user’s SIP URI with the machine into which he is currently logged in. The registrar records this association, also called registration instance or a binding, to the registration table, where it can be used by the SIP proxy.

Follow these steps to set expiration properties for the SIP registrar.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registrar Administration.
5. In the Default Registration Expiration field, type a value in seconds to use as the registration expiration when there is no such parameter set in the user request.
6. In the Minimum Registration Expiration field, type a value in seconds for the minimum expiration interval the SIP Registrar is willing to honor. A request with an expiration interval lower than the minimum expiration will be rejected.
7. In the Maximum contacts for user field, type a value for the maximum number of contacts a user can register, for the same address-of-record.
8. In the Maximum Anonymous users field, type a value for the maximum number of anonymous users that can be registered with the IBM Lotus SIP Registrar.
9. Click OK.
10. Restart the SIP Proxy and Registrar.

Managing SIP registered bindings
Use the SIP Proxy Registration page to monitor SIP registrations.

About this task
The registration of the user occurs during client login and is extended by the client automatically if the client remains logged in. The registration table is a location service used by a SIP to obtain information about a user’s possible location. The registration table specifies the SIP addresses associated with device addresses, as well as the expiration times for currently registered users.

Procedure
1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Registered Bindings. Use this page to find, view, or delete bindings.

5. Use the following table to view binding properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP URI</td>
<td>Identifies a user in IBM Sametime. A SIP URI contains the information to initiate and maintain a communication session with another user. It can have the following formats: sip:user_identifier@host or sips:user_identifier@host.</td>
</tr>
<tr>
<td>Device Address</td>
<td>The location of the machine into which the user is currently logged. The format is sip:host:port;transport=&lt;transport-type&gt;.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>The time when the registration expires, unless it is automatically extended by the Sametime client.</td>
</tr>
</tbody>
</table>

Managing the SIP Proxy and Registrar domains

Use the Handled Domains page to set the domains for which the SIP Proxy and Registrar are responsible.

About this task

If you do not add any domains to the Handled Domains page, then all domains will be managed by the SIP Proxy and Registrar.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > SIP Proxies and Registrars.
3. Click the Deployment Name of the SIP Proxy server.
4. In SIP Proxy and Registrar, click Handled Domains.
5. To add a domain which will be handled by the SIP Proxy and Registrar, enter a domain in the Domain field and click Add.
6. Click OK.

Administering a Sametime Bandwidth Manager

IBM Sametime Bandwidth Manager provides a number of monitoring and management tools. Use these tools to ensure that the bandwidth management component is configured and tuned to best serve your organization's day-to-day needs and support the organization's network policies.

Monitoring the status of bandwidth manager modules

Use the Status tab to monitor the status of the IBM Sametime Bandwidth Manager modules. You can start, stop, or restart server modules as needed.

About this task

The bandwidth manager comprises three components, which can be started and stopped independently:
• **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.

To monitor bandwidth manager 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 **Status** tab.

4. Examine the values in the table. Each row represents a component currently deployed in the environment.

5. Note that the table displays most of the same information as in the Configuration tab, but it adds one more column, **State**. This column indicates the current status of the component instance. It could take four values: Idle, Active, Stopping, and Down. All components go to Idle state after installation or WebSphere Application Server startup. Then all components can be activated or deactivated with "Start" or "Stop" buttons.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component type</td>
<td>The type of the component instance: Bandwidth Pool Manager, Media Session Controller, or SIP Frontend.</td>
</tr>
<tr>
<td>Server name</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, Websphere302Node01Cell\Websphere302Node01\server1).</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.</td>
</tr>
</tbody>
</table>
### Monitoring bandwidth usage for individual links

Use the Links table to monitor bandwidth usage for individual links in the network managed by IBM Sametime Bandwidth Manager.

### About this task

The monitoring interface includes tabs for links, sites, link calls, and site calls. The Links tab provides the following information:

- What is the source site and destination site for each link?
- What city and region are associated with the link?
- How much bandwidth is currently utilized on a link?
- How much un-utilized bandwidth remains for the link?
- What is the percentage of available bandwidth is currently being utilized?
- How many calls are utilizing the bandwidth on that link?

From the link monitoring area, administrators can drill down and see which calls are utilizing the bandwidth on that link.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster SIP URI</td>
<td>The common SIP address for all instances of “SIP Frontend” on the cluster (for single server installation use the same value as for “SIP URI”).</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the current instance. This is an integer value used only for “Bandwidth Pool Manager” 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>

To monitor links, 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 Monitoring tab.
4. Click the Links tab to see a table of links configured for this network.
5. In the Links table, click a link name in the Name column to see the site configuration page for that link.
6. In the **Links** table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the link displayed in that table row.

### Monitoring bandwidth usage for sites

Use the Sites table to monitor bandwidth usage for each site in the network managed by IBM Sametime Bandwidth Manager.

#### About this task

The monitoring interface includes tabs for links, sites, link calls, and site calls. At the top level, the table on the **Sites** tab provides the following information:

- How much bandwidth is currently utilized on a site?
- How much un-utilized bandwidth remains for the site?
- What is the percentage of available bandwidth is currently being utilized?
- How many calls are utilizing the bandwidth on that site?

From the site monitoring area, administrators can drill down and see which calls are utilizing the bandwidth in that site.

To monitor sites, 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 **Monitoring** tab.
4. Click the **Sites** tab to see a table of sites configured for this network.
5. In the **Sites** table, click a site name in the **Name** column to see the site configuration page for that site.
6. In the **Sites** table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the site displayed in that table row.

### Monitoring calls for selected links

Use the Link Calls table to monitor details for calls on a selected link within the network managed by IBM Sametime Bandwidth Manager.

#### About this task

The monitoring interface includes tabs for links, sites, link calls, and site calls. The **Link Calls** tab shows calls that are currently in progress. By choosing a specific
link in the **Link Calls** dropdown list, the administrator can limit the calls shown to those using the selected link. Choosing **Any** will cause all calls in progress to be displayed.

Clicking a call in the **Start Time** column opens the **Call Details** page, which provides the following information:

- Details about the caller: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Details about the callee: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Call route, including the total distance configured for the route taken by the call.
- Call rate policy, including peak utilization policy.

To monitor calls for a link or links, 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 **Monitoring** tab.
4. Click the **Link Calls** tab on the monitoring page.
5. Optionally, click a specific link in the **Link Calls** dropdown list to see calls in progress for that link only. To see all calls currently in progress, choose **Any**.
6. Click the **Link Calls** tab to see a table of calls currently in progress.
7. In the Links table, click a link name in the **Name** column to see the site configuration page for that link.
8. In the Links table, click a number in the **Calls** column to see what calls are currently utilizing bandwidth in the link displayed in that table row.
9. End any call by checking the checkbox next to the start time for that call and then clicking the **End Call** button. To refresh the list of calls at any time click the **Refresh** button.

**Monitoring calls for selected sites**

Use the Site Calls table to monitor calls for each site in the network managed by IBM Sametime Bandwidth Manager.

**About this task**

The monitoring interface includes tabs for links, sites, link calls, and site calls. The **Site Calls** tab shows calls that are currently in progress. By choosing a specific site
in the **Site Calls** dropdown list, the administrator can limit the calls shown to those originating from or terminating at the selected site. Choosing **Any** will cause all calls in progress to be displayed.

Clicking a call in the **Start Time** column opens the **Call Details** page, which provides the following information:

- Details about the caller: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Details about the callee: Details about the caller: name, site, ID, IP address, bandwidth sent, and bandwidth received.
- Call route, including the total distance configured for the route taken by the call.
- Call rate policy, including peak utilization policy.

To monitor calls by site, 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 **Monitoring** tab.
4. Click the **Site Calls** tab on the monitoring page to see a table of calls currently in progress.
5. Optionally, click a specific site in the **Site Calls** dropdown list to restrict the display to calls in progress for that site only. To see all calls currently in progress, choose **Any**.
6. In the **Site Calls** table, click a call link in the **Start Time** column to see the site details for that call.
7. The administrator can end any call by checking the checkbox next to the start time for that call and then clicking the **End Call** button. To refresh the list of calls at any time click the **Refresh** button.

**Bandwidth Manager statistics**

Understanding the Bandwidth Manager monitor statistics can be useful for fine-tuning site and link bandwidth allocations and peak utilization points.

**Links and sites**

- **Bandwidth in Use** shows the static amount of bandwidth allocated for the call, link, or site based on applied Call Rate policies. As such, it is not a reflection of the real-time current bandwidth consumed – rather, it should be considered a maximum allowed for the call.

  The allocated bandwidth does not affect other activities that might be occurring in the monitored element – it affects only audio/video traffic. Chat, call setup,
server communication overhead are all not counted towards the bandwidth allocation. The allocated bandwidth affects only the payload and does not include any transport-related data.

- **Bandwidth Remaining**
  shows the difference between the configured maximum bandwidth for the site or link and the current Bandwidth in Use.

- **Utilization** is the percentage of the maximum bandwidth currently allocated.

- **Calls** is the current number of active calls on the link or site. For conference calls hosted on an MCU or the Sametime Packet Switcher, each individual call leg for each participant is reported as a separate call in the Bandwidth Manager Monitor.

As a general rule-of-thumb for planning purposes, you can assume the actual single-call one-way send bit rate is around 65-75% of the configured maximum call rate as defined in the policy, assuming the client utilizes a codec/resolution that matches the policy. This general rule assumes H264 video is used with ISAC audio, and takes into account transport-independence, normal call activity, and overhead, but it does not take into account other non-audio/video activity that might be taking place concurrently (although unless users are doing lots of big file downloads, this affect should be small relative to the A/V traffic). The receive bit rate will vary depending on the sender’s codec/resolution, and this can also change during a conference call as the active speaker changes. For a large population of users, it should be possible to estimate with a good degree of accuracy the best maximum bandwidths and peak utilization points of any given site or link, but this exercise is beyond the scope of this documentation.

**Call details**

The call details give information about the specific call or call legs on a site or link such as time started, duration, and bandwidth sent or received. Note that the 'Callee sent' statistic makes sense only in the context of point-to-point calls since for conference calls the callee is always the MCU, and the data sent from the MCU differs depending on the other originating call leg.

**Sametime Client auto-tuning feature and its effect on allocated bandwidth**

The Sametime client has an auto-tune feature that potentially reduces either frame-rate or video resolution during a call depending on the current load of the CPU on which the client is running. Overall real bandwidth consumed for a site or link may be further reduced if there are a significant number of overtaxed machines running Sametime on those sites or links. If link and site capacity seems to be consistently insufficient, the auto-tune feature may be the reason.

**Holding calls and pausing videos and their effects on allocated bandwidth**

When the user holds a call (or pauses video), the Bandwidth Manager retains the original bandwidth allocation for the call. Retaining the original bandwidth allocation keeps the bandwidth available when the call resumes. However, this policy results in certain calls being allocated more bandwidth than they are actually using, which is a necessary trade-off for the guarantee of being able to resume calls. When resuming a call from a prior hold, the Bandwidth Manager server gets a new look at the negotiated session, which might or might not match the initial session parameters. As such, Bandwidth Manager might fine-tune the allocated bandwidth to match the new session. The Bandwidth Manager never
Reflector policies and their effects on allocated bandwidth

Reflectors in the topology also affect the amount of bandwidth allocated for each call that flows through reflectors. Defining a reflector on a site effectively doubles the bandwidth allocated for that site for each affected call to account for the extra hop that media traffic must take as it traverses the reflector site.

For example, assume you have the following route:

Caller site → Transit site → Receiver site

Without a reflector, the bandwidth used for a single call on each of the three sites is $n$. When you add a reflector on the Transit site, the allocated bandwidth is still $n$ on the Caller and Receiver sites, but becomes $2n$ on the Transit site.

---

**Administering a Sametime Meeting Server**

This section describes how to manage an IBM Sametime Meeting Server.

**About this task**

The Sametime Meeting Server supports real-time collaboration through screen sharing and a shared whiteboard. The Sametime Meeting Server also provides a variety of other types of support for the meeting activity occurring in Sametime.

**Updating Sametime Meeting Server connection properties on the console**

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Meeting Server.

**Before you begin**

If you are configuring the Sametime Meeting Server to use SSL (Secure Socket Layer), make sure the server’s certificate has been added to the Sametime System Console’s trust store.

**About this task**

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Meeting Server. These settings are only used by the Sametime System Console to connect to the Sametime Meeting Server.

Follow these steps to update connection setting information.

**Procedure**

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Server.
3. In the Sametime Meeting Servers list, click the **Edit** next to the deployment name of the server with the connection information that you want to change.

4. Under Connection Properties, enter the administrator’s **User name** and **Password** for connecting to the Sametime Meeting Server.

5. By default, the Sametime Meeting Server trusts other Sametime components. If you want to change this setting, then select **Do not auto-accept SSL certificate**.

6. Click **Save**.

7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

### Managing file sharing

You can limit the types of files that can be shared in meeting rooms as well as edit file conversion settings for your IBM Sametime Meeting Server configuration.

#### About this task

You can edit but not delete any of the file conversion settings that come installed with IBM Sametime. You can delete any new settings that you have added.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Edit the appropriate configuration value. You can only edit the value; you cannot edit a configuration key name.

#### Table 37. Configuration key values

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.include</td>
<td>pdf, sam, bmp, gif, cgm, htm, html, jpg, jpeg, jpe, 123, wk3, wk4, 123, pre, prz, pic, lwp, xls, xlsx, ppt, pptx, doc, doxx, sdd, sxi, sxw, sdc, sxr, pch, pcd, png, rft, rtf, ods, odp, odt, tiff, tif, eps, txt, bat, ini, vsd, wmf, wpd, wpg, wpg2, xml</td>
<td>List of file type extensions that can be converted by the Sametime Meeting Server for document sharing. Separate extensions by a comma.</td>
</tr>
<tr>
<td>docshare.fileio.codebase</td>
<td>c:\temp\docshare</td>
<td>Location of the temporary directory for document sharing used by the Sametime Meeting Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c:\temp\docshare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or /opt/temp</td>
</tr>
</tbody>
</table>
Table 37. Configuration key values (continued)

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| docshare.native.codebase| c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe                     | Location of the executable file for the Sametime Meeting Server document conversion. Examples:  
c:\Program Files\IBM\Websphere\STMeetingServer\stellent\exporter.exe  
or/opt/IBM/WebSphere/STMeetingServer/stellent/exportsrer.                           |
| docshare.remote.url     | Blank.                                                                                      | URL to a remote Sametime Meeting Server for document conversion. Leave blank for local conversion. Example:  

7. Click **OK**.

**Results**

Configuration changes immediately take effect.

**Requiring meeting passwords**

You can require that all meeting rooms in IBM Sametime have passwords.

**About this task**

Meeting rooms are not required to have passwords by default. You can change this configuration setting so that meeting rooms are required to have passwords.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Scroll down to the **meetingroomcenter.passwords** configuration key. You can only edit the value; you cannot edit a configuration key name.
7. Change the **Configuration Value** to one of the following values:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No password required. This is the default value.</td>
</tr>
<tr>
<td>1</td>
<td>Password required. The password must contain at least five characters.</td>
</tr>
<tr>
<td>2</td>
<td>Strong password required. A strong password must contain eight or more characters, mixed upper and lower case letters, at least one number, and at least one special character (for example: comma, exclamation point, or asterisk).</td>
</tr>
</tbody>
</table>

**Password character restrictions**

In addition to non-English characters, the following characters must not be included in passwords used by Sametime:

: / \ % " & < >

8. Click **OK**.

**Results**

This configuration change immediately takes effect.

**Limiting guest access to the Meeting Room Center**

You can prevent unauthenticated users (guests) from accessing the Meeting Room Center.

**About this task**

Unauthenticated users have limited access to the Meeting Room Center. They can view information in the Meeting Room Center, but they can never create meeting rooms or edit meeting room information. You can change this default value to completely deny them access to the Meeting Room Center. This change does not prevent guest access to an actual meeting; it only prevents access to the Meeting Room Center.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Scroll down to the `meetingroomcenter.allowGuestAccess` configuration key. You can only edit the value; you cannot edit a configuration key name.
7. In the **Configuration Value** field, type `0` to deny unauthenticated user access to the Meeting Room Center.

**Note:** If you change your mind, or if you ever want to grant unauthenticated user access, type `1`.

8. Click **OK**.
Results

This configuration change immediately takes effect.

Defining a Sametime Proxy server for awareness in meeting rooms

You must define the IBM Sametime Proxy server that is used for awareness so that Sametime users can be detected when they are in Sametime meeting rooms.

Before you begin

You must have a Sametime Proxy server installed and configured. You must set up SSO between the Sametime Meeting Server and the Sametime Community Server.

Procedure

1. Log in to the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
3. In the Meeting Servers list, click a server with the configuration that you want to change.
4. Click the Server Configuration tab.
5. Click Edit.
6. Scroll down to the meetingroomcenter.stProxyAddress configuration key. You can only edit the value; you cannot edit a configuration key name.
7. Enter the URL for the Sametime Proxy server used for awareness in the Configuration Value field. For example:
   http://myhostname.mydomain.com:9080
8. Click OK.
9. Restart the Sametime Meeting Server.

Customizing the Sametime Meeting Server configuration

You can customize your IBM Sametime Meeting Server by changing configuration keys. You can also add your own configuration keys.

About this task

The custom configuration keys that you create yourself display after the configuration keys that come pre-configured with the Sametime Meeting Server. Custom configuration keys that you create yourself can be edited and these are the only configuration keys that can be deleted. Do not delete any of the pre-configured custom configuration keys unless directed to do so by IBM.

Table 38. Pre-configured custom configuration keys

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.conversion.timeout.minutes</td>
<td>5</td>
<td>Upload duration (in minutes). Upload a file to the meeting room. If the file cannot be converted in X minutes, then the file cannot be converted any more.</td>
</tr>
</tbody>
</table>
Table 38. Pre-configured custom configuration keys (continued)

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Default Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docshare.jpeg.quality</td>
<td>90</td>
<td>Quality of shared document. The lower the value, the lower the quality.</td>
</tr>
<tr>
<td>meetingroomcenter.maxRoomsPerPage</td>
<td>100</td>
<td>Number of rooms listed on a page in the Meeting Room Center. The configuration key is ignored if the value is less than 100.</td>
</tr>
<tr>
<td>meetingroomcenter.openRoomInNewWindow</td>
<td></td>
<td>Determines if meetings opened from the web browser room manager open in a new window or in the current window.</td>
</tr>
<tr>
<td>meetingroomcenter.stProxySSLAddress</td>
<td></td>
<td>Detects which protocol (SSL or non-SSL) was used to access the meeting server and picks the correct Sametime proxy address to use.</td>
</tr>
<tr>
<td>rtc4web.ejectionTimeout</td>
<td>300</td>
<td>Length of time in seconds that users are locked out of a room when they have been ejected.</td>
</tr>
<tr>
<td>meeting.managedAccess.override</td>
<td>(do not enforce)</td>
<td>Determines whether rooms on the Sametime Meeting Server use managed access, or whether it is optional.</td>
</tr>
<tr>
<td>meetingroom.allowGuestAccess</td>
<td>(allow guest access)</td>
<td>Determines whether guests can access meeting rooms.</td>
</tr>
</tbody>
</table>

Procedure

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Click the **Server Configuration** tab.
5. Click **Edit**.
6. Enter the name of your **Configuration Key**.
7. Enter the **Configuration Value**.
8. Click **OK**.

Turning on full-text indexing in the Meeting Room Center

By default, the Meeting Room Center searches the Meeting Room Center database for rooms without using an index. If the database becomes too big, your deployment might experience performance degradation during searches. You can enable full-text indexing on the room name and owner name fields for enhanced performance on large datasets.
About this task

Full-text indexing takes advantage of the IBM DB2 Text Search service to build, maintain, and search by an enhanced set of indexes on the meeting room name and owner name. This augments search performance.

Full-text indexing is only used when you explicitly search for listed meeting rooms from the meeting room search box. It is not used when you search for hidden rooms, access My Meeting Rooms or access a Selected Contact's Meeting Rooms. Full-text indexes are created for both the room name and owner name.

Full-text indexes are updated every 12 hours. Rooms created in the past 24 hours cannot be found by their full-text index, but can be found by a limited table scan. This action avoids missing a room because the index has not been created, yet. Once a room has been live for more than 24 hours, full-text indexing is available.

Follow these steps to enable full-text indexing:

Procedure
1. Copy enableFullTextIndexing.bat (Windows) or enableFullTextIndexing.sh (Linux, Unix) from the root directory of the Sametime Meeting Server install image to the DB2 bin directory.
   - If you have an extremely large database, this script can be edited to customize the location of the index files.
2. Run the command to start the DB2 Text Search service, which sets up the full-text indexes and enables the database for full-text searches.
   - Windows
     enableFullTextIndexing.bat STMS dbadmin password
   - AIX, Linux, or Solaris
     enableFullTextIndexing.sh STMS dbadmin password
   Replace STMS with the name of the Meeting Server database if you chose a different database name when you created it.
   Replace dbadmin and password with the DB2 Application user ID and password you created when you installed DB2.
3. Follow these instructions to turn on full-text indexing for the Meeting Room Center in the Sametime System Console.
   a. Log in to the Integrated Solutions Console.
   b. Click Sametime System Console > Sametime Servers > Sametime Meeting Servers.
   c. In the Meeting Servers list, click a server with the configuration that you want to change.
   d. Select Server Configuration.
   e. Click Edit.
   f. Change the value of meetingroomcenter.useFullTextIndexing to true. This setting is a custom key. If a search has been previously performed on the server, then the key and the value display in the interface.
   g. Click OK. The changes take effect within one minute.

What to do next

If you restart the server, the service does not restart automatically.
On Windows, you can go into Services and change the DB2TS service to start automatically. From the Start menu, click **Run**, and type `services.msc`, and change the DB2TS services to start automatically.

On Linux, you can edit one of the startup scripts to start `db2ts` when you restart. The command to start `db2ts` is `db2ts start for text`.

For more information on DB2 maintenance, see Best Practices for DB2 maintenance in Sametime.

**Turning off full-text indexing in the Meeting Room Center**

Follow these steps to disable full-text indexing in the Meeting Room Center.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Sametime System Console > Sametime Servers > Sametime Meeting Servers**.
3. In the **Meeting Servers** list, click a server with the configuration that you want to change.
4. Select **Server Configuration**.
5. Click **Edit**.
6. Change the value of `meetingroomcenter.useFullTextIndexing` to `false`.
7. Click **OK**. The changes take effect within one minute.

**What to do next**

These steps are sufficient to turn off full-text indexing; however, the full-text indexes still exist and take up disk space. If you want to permanently delete the full-text indexes, copy `dropFullTextIndexing.bat/sh` to the DB2 bin directory and run `dropFullTextIndex.bat/sh database_name`. For example, `dropFullTextIndexing.bat STMS`. If you remove the database, the `dropFullTextIndexing` script should be run first to properly clean up the indexes.

**Configuring remotely connected Sametime Meeting Servers**

You can configure two different IBM Sametime Meetings deployments to be aware of each other.

**Before you begin**

Determine the routing prefix. The routing prefix is the alias which will be used to route requests to the remote server. This value can be any string value and should make logical sense to the user since it will appear in the meeting URL. For example, if you are setting up routing between the US and Europe, you may want to choose `/eu` for the routing prefix for Europe and `/us` for the United states. This value will be entered into a URI Group and will be used as the key to routing http requests to the remote server.

**About this task**

Configuring remotely connected Sametime Meeting Servers uses routing features built into the WebSphere proxy server to route http requests to other http servers. Connecting remote servers requires setting up generic server clusters and the appropriate URI Groups and routes which define the remote server.
**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Servers > Generic Server Clusters**, and then click **New**.
3. Enter a logical name for the Server cluster, for example **Europe**.
4. Select **http** or **https** as the protocol.
5. Click **Save**.
6. Open the Generic Cluster entry you just saved and click **Ports**.
7. Add the hostname and port number for the remote server.
8. Create a URI Group for your **routingPrefix**.
   a. In the navigator on the left side of the Integrated Solutions Console, click **Environment > URI Groups**, and then click **New**.
   b. Enter a logical name for the URI group, for example **European route**.
   c. Click **Save**.
9. Add the generic server cluster and URI group to the proxy server.
   a. In the navigator on the left side of the Integrated Solutions Console, click **Server > Proxy servers**
   b. Click the proxy server process you would like to add remote routing for.
   c. Click **Http Proxy Server Settings**.
   d. Click **Routing Rules**.
   e. Click **New** and enter a name, for example, **Europe**.
   f. Select **proxy_host** as **Name of the Virtual Host**.
   g. Select the **URI Group** to specify the URI to route /eu/*.
   h. Select the **Generic Server Cluster** to send the messages to, for example, **eu.company.com**.
   i. Click **Save**.
10. Add a special custom property that identifies this as a remote Sametime server connection.
    a. Open the Saved Routing Rule.
    b. Click **Custom Properties** and click **New**.
    c. In the name field add **SametimeRemoteCluster**, and specify **true** in the Value column.
    d. Click **Save**, and then click **Save** again.
11. Save the master configuration.
12. Restart the proxy server process to begin routing to the remote cluster.

**Monitoring meeting room statistics**

You can view usage statistics for IBM Sametime meeting rooms in the Meeting Room Center.

**About this task**

Only administrators can view statistics for meeting rooms. Other Sametime users cannot view meeting room statistics. Deleted meeting rooms are not included in these statistics.

**Procedure**

1. Log in to the Sametime Meeting Room Center.
   
   http://hostname/stmeetings/
2. Click **Meeting Room Statistics**.
3. Click one of the following views:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Displays the total number of rooms and active participants, and the total size of all libraries. An active participant is a participant that is currently in a room.</td>
</tr>
<tr>
<td>Active rooms</td>
<td>Lists all the rooms by meeting room name that currently have participants.</td>
</tr>
<tr>
<td>Usage by room</td>
<td>Lists all active and inactive rooms by meeting room name.</td>
</tr>
<tr>
<td>Usage by owner</td>
<td>Lists all room owners by Sametime ID. Rooms can be active or inactive.</td>
</tr>
</tbody>
</table>

You can click on a column heading in any view to sort the information.

In the Active room or Usage by room views, you can click an owner or room name to get detailed usage statistics on that particular owner or room. In the Usage by owner view, you can click an owner name to get detailed usage statistics.

### Backing up user data for Sametime meeting rooms

All IBM Sametime meeting room user data is stored in an IBM DB2 database, and can be backed up using the DB2 backup commands.

**About this task**

The default Sametime configuration requires that DB2 be shut down for backup. This is because by default, DB2 is configured to reuse the recovery logs. If you want online backup, the database can be configured to archive the recovery logs. In that case, the database is backed up, and all archived recovery logs are backed up. The recovery logs that have been backed up must also be periodically removed. If the database runs out of space to archive the recovery logs, the database will stop accepting changes until space is available.

Database backup and recovery is fully outlined in the DB2 information center. See "Backup overview."

**Example for online backup**

```
db2 update database configuration for STMS using logretain on

db2stop

db2start
```

Perform an offline backup to be kept:
```
db2 backup database STMS
```

Afterwards, you can perform online backups:
```
db2 backup database STMS online include logs
```
Administering a Sametime Gateway Server

Set up and begin using the IBM Sametime Gateway to enable local IBM Sametime users to have real-time collaboration with users of other instant messaging systems. After installing the Sametime Gateway, you can create a local and external community, manage user access, add message handlers if necessary, and set properties such as session time outs and blacklist domains.

Updating Sametime Gateway Server connection properties on the console

You can update connection setting information that the IBM Sametime System Console uses to connect to the Sametime Gateway Server.

Before you begin

If you are configuring the Sametime Gateway Server to use SSL (Secure Socket Layer), make sure the server's certificate has been added to the Sametime System Console's trust store.

About this task

Any changes that you make to the credential and connection information on the Connection Properties page does not change the actual settings on the Sametime Gateway Server. These settings are only used by the Sametime System Console to connect to the Sametime Gateway Server.

Follow these steps to update connection setting information.

Procedure

1. Log in the Integrated Solutions Console.
2. Click Sametime System Console > Sametime Servers > Sametime Gateway Server.
3. In the Sametime Gateway 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 Gateway Server.
5. By default, the Sametime Gateway Server trusts other Sametime components. If you want to change this setting, then select Do not auto-accept SSL certificate.
6. Click Save.
7. If you enabled SSL, then you must restart the Sametime System Console for the changes to take effect.

Assigning users access to external communities

Assign local users access to external or clearinghouse communities so that they can exchange real-time communications with users from external communities. You can assign access only for local users.

About this task

Before you assign users, you must first add an external community or clearinghouse and set its properties. You must also make sure that the IBM Sametime Gateway is configured for use with an LDAP directory that contains person records of users in the local Sametime community.
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 an external community from the table.
3. Click Assign users.
4. Determine if you want to assign equal access to the external community or clearinghouse for everyone or set access for each user.
   - Select Assign access to all users for this route to give everyone the same access.
   - Select Assign access to individual users and groups for this route to set access for each user.
5. In the Search by field, select group, first name, or last name.
6. In the Search for field, type the name, or use an asterisk (*) as a wildcard.
7. From the Search results, select the users to be given access to the external community. Use the Page buttons to see additional names. Search results show names from the local community only because only local users may be assigned to an external or clearinghouse community.
8. Select users and click Add to assign the users. Note that any user assigned to access the external community automatically receives both instant messaging and presence capabilities. These capabilities cannot be changed.
9. Optional. To take names off the assigned users list, select the users and click Remove Selected Names.
10. Click OK.

What to do next
No assignment of external users to the local community is necessary. External community user access to local users is determined when a local community user subscribes to instant messaging and presence with an external user.

Note: 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.

Related reference
“Assign local users and capabilities” on page 153
Assign users and groups from the local community permission to exchange real-time messages with an external community or clearinghouse community. Use this panel to control access to Sametime Gateway and external messaging communities.

Finding users
Determine if a local user is assigned access to an external community. In addition, determine the capabilities assigned to the user.
Before you begin

You must create an external community and assign users to the community first.

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 an external community from the table.
3. Click **Find Users**.
4. Type the user's email address and click **Search** to determine if the user is assigned to access the external or clearinghouse community, and to see the capabilities assigned to the user.

Related reference
“Find user” on page 155
Find a user in LDAP and view the capabilities that the user has permission to use when accessing the selected instant messaging community.

Viewing users
Determine the users and groups that are assigned to access an external community or clearinghouse community.

Before you begin

You must create an external community and assign users and groups to the community first.

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. Click the name of an external or clearing house community to open the details about that community.
3. Click **View Users** to view the users and groups assigned to the external community. To find an individual user, use **Find User** on the community list page.

Related reference
“View users” on page 155
See who has access to exchange real-time messaging with an external community or clearinghouse.

Enabling spam filtering
You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.
About this task

Adding a message handler involves first installing the application as a J2EE application through WebSphere Application Server, starting it, then using the Sametime Gateway administrative console to configure its properties. After the message handler is configured, you must enable it and then restart the application.

The message handler must be a J2EE application that implements the Sametime Gateway plug-in API. See the Sametime Gateway Integration Guide that is included in the Sametime Software Development Kit for information on how to create a message handler plug-in.

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. To add a message handler to Sametime Gateway, log into the Integrated Solutions Console (http://localhost:9060/ibm/console) and click Applications > Enterprise Applications.
2. Click Install and follow the instructions for installing the application.
3. Click Start to start the application. Starting the application causes it to appear in the list of message handlers.
4. Click Sametime Gateway > Message Handlers to view the message handler list.
5. Click the newly installed message handler to edit its properties.
6. Select the type: event logger, access control list, user locator, or other.
7. Optional. Select Run the message handler regardless of whether previous handlers complete their processing of messages. If not selected, the message handler does not run if the preceding message handler failed to complete its handling of a message.
8. Click OK. You should now be back on the message handler list page.
9. Click Sametime Gateway > Message Handlers, select a message handler, and click the Move Up and Move Down buttons to change the order in which the message handler processes messages. Note that User locator message handler must be first and the Event logger message handle must be last.
10. On the Message Handler list page, select the newly installed message handler and click Enable.

Results

To remove a message handler, you must disable the message handler first, and then uninstall the plug-in through WebSphere Application Server.
Related reference
“Troubleshooting message handlers” on page 262
This topic discusses how to troubleshoot message handlers in various stopped and started or enabled and disabled conditions.
“Message handler properties” on page 155
Use this page to configure the properties of a message handler such as the user locator, authorization controller, or event logger.
“Message handler list” on page 157
Use this page to configure message handlers that perform such tasks as finding users in the local community for whom to relay messages, checking the access control for local community members, and logging IBM Sametime Gateway events. Message handlers that are provided by Sametime Gateway, with the exception of the Event logger, do not need configuring.

Maintaining and monitoring Sametime Gateway
The IBM Sametime wiki provides recommended procedures for maintaining and monitoring Sametime Gateway.

About this task
You can find recommendations in the Sametime wiki on the following areas:
- Log files lifecycle and maintenance
- Renewing any SSL certificates
- Monitoring communities
- Periodic maintenance for DB2
- Recycling of Websphere processes
- File system cleanup

See this article in the Sametime wiki :Sametime Gateway - Recommended production maintenance procedures.

Reference
This topic provides property reference help for the administrative user interface, scripting commands, and sample JACL scripts.

Sametime Gateway reference
These topics provide details about IBM Sametime Gateway properties and settings for communities, message handlers, and translation protocols which you can administer through the Integrated Solutions Console.

Sametime Gateway properties:
Use this page to set the maximum chat sessions. You can also specify domains from which to block messages.

Set maximum sessions
This option sets the maximum instant messaging and presence sessions. A limit of 1000 instant messaging and 1000 presence sessions is set by default. Note that maximum sessions set here override the maximum sessions that are set for a route to a community.
<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>no limit</td>
</tr>
<tr>
<td>0</td>
<td>no sessions allowed</td>
</tr>
<tr>
<td>( n )</td>
<td>( n ) sessions allowed, where ( n ) is any integer between 1 and 2147483647</td>
</tr>
</tbody>
</table>

Blacklist domains

Specify the DNS blacklist sites to check when the Sametime Gateway receives a subscription request. The Sametime Gateway rejects messages when either the destination or source domains are in this list. Use Fully qualified domain names or TCP/IP addresses separated by a comma, semicolon, or space. Wild cards using an asterisk in the left-most subdomain position are allowed. For example, \( *\).spamalot.com is allowed.

Related tasks

“Setting a global limit on sessions” on page 201
You should set a global limit for the maximum number of sessions allowed on a server, which helps prevent out-of-memory errors. The value set here will supersede a larger value set in the “Route maximum sessions” property.

Sametime Gateway communities:

View the list of communities and use the list as the starting place to set up communities, assign local users access to external communities, and set properties on communities. The communities list shows the community name, the type of community, and the translation protocol used.

Task buttons

Use the communities list to create a new community or edit the properties of an existing community. Select a community first before using the button actions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Sets up a connection to a local, external, or clearinghouse community. You must supply domain names of the community. The type of community often determines the translation protocol used. External and clearinghouse communities usually use the SIP translation protocol, which relies on the SIP infrastructure in WebSphere Application Server to handle message routing, or the XMPP protocol. The local community is connected to the IBM Sametime Gateway by means of the VP (Virtual Places) protocol.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a community from the Sametime Gateway.</td>
</tr>
<tr>
<td>Find user</td>
<td>Determines if a local user is assigned to the community and determines the capabilities such as instant messaging and presence that are assigned to the user. Enable the Find user button by selecting an external or clearinghouse community. Search by email address only.</td>
</tr>
<tr>
<td>Assign users</td>
<td>Assigns users from the local community permission to access the selected community. You can assign users from the local community only, not from external or clearinghouse communities. Enable the Assign users button by selecting an external or clearinghouse community.</td>
</tr>
</tbody>
</table>
Select and filter buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![select all]</td>
<td>Selects all items.</td>
</tr>
<tr>
<td>![deselect all]</td>
<td>Deselects all items.</td>
</tr>
<tr>
<td>![search]</td>
<td>Searches the custom properties by column. To filter the table, select the column by which to filter, then enter filter criteria. You can use wildcard characters (*)/?, %) and the text is not case-sensitive.</td>
</tr>
<tr>
<td>![filter names]</td>
<td>Hides the filter names from being displayed.</td>
</tr>
</tbody>
</table>

Name

The name is the name given to the community when the community is first created. Click a name to configure properties or assign users to the community.

Type

A community is generally a set of users connected by a common user directory. There are three types of communities: local, external, and clearinghouse communities. You can have an unlimited number of external communities, but you can have only one local community and one clearinghouse community. 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.

The local community is the local Sametime community.

An external community is a set of users in domains connected by a common directory and belonging to a remote company or organization.

A clearinghouse community is a federated group of users linked by an enterprise’s message router. When a message contains destination domains not found elsewhere in a routing configuration, the message may be routed to a clearinghouse community if one exists. A route to a clearinghouse enables Sametime Gateway users to connect to a much wider community.

Translation protocol

A translation protocol is the communication standard used by the Sametime Gateway to code and decode messages from communities into a format understood by Sametime users. The Sametime Gateway provides the following translation protocols:
### Translation Protocol

<table>
<thead>
<tr>
<th>Translation Protocol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for Sametime Gateway</td>
<td>SIP for Sametime Gateway is used to exchange messages with other Sametime communities who use Sametime Gateway versions 7.5 or later.</td>
</tr>
<tr>
<td>SIP for AOL</td>
<td>SIP for AOL is used to connect with AOL Instant Messaging.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>SIP for legacy Sametime Gateway is used to connect with Sametime 6.5.1 and 7.0 servers.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>SIP for OCS is used to connect with Office Communications Server communities.</td>
</tr>
<tr>
<td>VP</td>
<td>VP (Virtual Places) is the proprietary protocol used to connect Sametime Gateway with the local community on the Sametime 7.5 or later server.</td>
</tr>
<tr>
<td>XMPP</td>
<td>XMPP is the Extensible Messaging and Presence Protocol (XMPP) for connecting to Google Talk and XMPP communities.</td>
</tr>
</tbody>
</table>

### Assign users

Click this link to assign users and groups to the route to this community. Note that you must first create the community, and then select the community in the table before you can assign users to the community.

### View users

Click this link to view users assigned to the route for this community. Note that you must first create the community, and then select the community in the table before you can view users in the community.

### Community properties:

Use this page to connect IBM Sametime Gateway to one internal community and multiple external communities, or to edit the connection properties of an existing community. Specify the type of community, the domains to use when accessing the community, the translation protocol that Sametime Gateway uses to communicate with the community, connection details, and any custom properties for the connection or community. After you create a community, use the Assign local users to this community link to give permission to local users to access the external or clearinghouse community.

### Name

Type a descriptive name for the community.
Community type

Select the type of community:

<table>
<thead>
<tr>
<th>Community type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL clearinghouse</td>
<td>The AOL clearinghouse community acts like a message router with links to several communities.</td>
</tr>
<tr>
<td>Local</td>
<td>The local community is the internal IBM Sametime community served by the Sametime Gateway. The Sametime Gateway can connect to only one local community, but the local community can be made up of many domains within the community, as long as those domains are connected by a single user directory.</td>
</tr>
<tr>
<td>External</td>
<td>An external community is any community connected by a common directory and belonging to another company or organization outside the firewall.</td>
</tr>
</tbody>
</table>

Community custom properties

Click this link to add custom properties to the community, or edit existing custom properties. Some external communities may require extending the Sametime Gateway functionality by adding a custom property in order to connect to the community.

Domains

Type at least one unique, Fully qualified domain name or TCP/IP address for the community. List multiple domain names separated by a comma, semicolon, or space. Domain names have two or more parts separated by dots, such as example.com. Each domain name must access the same user directory. For example: example.com, us.example.com, fr.example.com, de.example.com must access the same user directory in the community. The wildcard asterisk (*) is accepted in the first subdomain only.

<table>
<thead>
<tr>
<th>Wildcards</th>
<th>Case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct wildcard use</td>
<td>Asterisk as the first subdomain</td>
<td>*.domain.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.subdomain2.subdomain1.domain.com</td>
</tr>
</tbody>
</table>
Wildcards Case Examples

<table>
<thead>
<tr>
<th>Incorrect wildcard use</th>
<th>Case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single asterisk</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Asterisk as the domain</td>
<td>*.com</td>
<td></td>
</tr>
<tr>
<td>Asterisk as part of a domain or subdomain</td>
<td>*domain.com</td>
<td></td>
</tr>
<tr>
<td>Multiple asterisks in one domain</td>
<td><em>.</em>.domain.com</td>
<td></td>
</tr>
<tr>
<td>Asterisk is any position other than the first</td>
<td>subdomain.*.domain.com</td>
<td></td>
</tr>
<tr>
<td>Asterisk in a TCP/IP address</td>
<td>9.92.128.*</td>
<td></td>
</tr>
<tr>
<td>Domains that are already included when using a wildcard</td>
<td>*.domain.com and subdomain.domain.com. Including the second domain is not needed.</td>
<td></td>
</tr>
</tbody>
</table>

If connecting to any of the following instant messaging communities, include the community domains listed in the following table:

<table>
<thead>
<tr>
<th>Instant messaging communities</th>
<th>Available domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL Instant Messenger</td>
<td>aol.net, corp.aol.com, aol.com</td>
</tr>
<tr>
<td>Google Talk</td>
<td>gmail.com</td>
</tr>
</tbody>
</table>

Translation protocol

A translation protocol translates instant messages from one code standard to another to allow different instant messaging systems that rely on different protocols to talk with each other. Select a protocol that matches the protocol used by the community’s instant messaging application.

<table>
<thead>
<tr>
<th>Translation protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for AOL</td>
<td>Use <strong>SIP for AOL</strong> for all AOL Instant Messenger and AOL clearinghouse community connections.</td>
</tr>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use <strong>SIP for Sametime Gateway</strong> for connections to Sametime Gateway 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 connections to Sametime server versions 7.0 or 6.5.1 only.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>Use <strong>SIP for OCS</strong> for all Office Communication Server connections.</td>
</tr>
<tr>
<td>VP</td>
<td>Use <strong>VP</strong> (Virtual Places) for connecting to the local or internal Sametime community only.</td>
</tr>
<tr>
<td>XMPP</td>
<td>Use <strong>XMPP</strong> to connect with communities that use Google Talk or XMPP.</td>
</tr>
</tbody>
</table>
Translation protocol details

Click this link to view translation protocol properties and custom properties for the protocol.

Connection

Specify the connection properties that the Sametime Gateway uses to connect to the local, external, or clearinghouse community. You are prompted for connection information based on the translation protocol that you select.

<table>
<thead>
<tr>
<th>Community</th>
<th>Translation protocol</th>
<th>Default port</th>
<th>Transport Protocol</th>
<th>Connection details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>VP</td>
<td>1516</td>
<td>TCP</td>
<td>Domain: Fully qualified domain name or TCP/IP address of the Sametime server in the local community. For example: rtcgatewayserv.de.example.com The port number must match the VP port number on the Sametime server.</td>
</tr>
<tr>
<td>External</td>
<td>SIP for AOL</td>
<td>5061</td>
<td>TLS</td>
<td>Domains: aol.net, corp.aol.com, aol.com Requires hostname: sip.oscar.aol.com.</td>
</tr>
<tr>
<td>External</td>
<td>SIP for OCS</td>
<td>5061</td>
<td>TLS</td>
<td>Host name: host name or the IP address of the OCS Edge Server. Domains: domain names of the Office Communications Server community. For example: ocs.example.com</td>
</tr>
<tr>
<td>External</td>
<td>SIP for Sametime Gateway</td>
<td>5060 or 5061</td>
<td>TCP</td>
<td>Host name: domain name of the external Sametime Gateway server or Sametime Server such as ExampleServer1.com, for example. Domains: list of domains used by the external Sametime community.</td>
</tr>
<tr>
<td>External</td>
<td>XMPP (for Google Talk)</td>
<td>5269</td>
<td>TCP</td>
<td>Requires that you set up a domain service (SRV) record and publish it to DNS if connecting to Google Talk. Configure additional connection detail by using the Custom properties link.</td>
</tr>
<tr>
<td>External</td>
<td>XMPP</td>
<td>5269</td>
<td>TCP or TLS</td>
<td>Host name: domain name of the external XMPP server. Domains: list of domains used by the XMPP community.</td>
</tr>
<tr>
<td>AOL</td>
<td>SIP for AOL</td>
<td>5061</td>
<td>TLS</td>
<td>Host name: sip.oscar.aol.com.</td>
</tr>
</tbody>
</table>

Route properties

You must add an internal community before you can view or edit Route properties.
Enable route for this community

Select to enable the route to this community.

Set the maximum sessions for each capability for the route

Select to set the maximum sessions for each capability on the route. Sessions should always be larger than presence. Note that global maximum allowed Sametime Gateway sessions override the maximum sessions for each capability. To increase maximum sessions for each capability, make sure you increase the maximum allowed Sametime Gateway sessions.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>no limit</td>
</tr>
<tr>
<td>0</td>
<td>no sessions allowed</td>
</tr>
<tr>
<td>$n$</td>
<td>$n$ sessions allowed, where $n$ is any integer between 1 and 35000.</td>
</tr>
</tbody>
</table>

Note that community maximum sessions override gateway maximum sessions

Select the capabilities to assign local users for the route

Select the capabilities, instant messaging and presence, to assign to the route. Both capabilities are assigned to the route and are disabled. You must click Assign users to complete the set up of the community by assigning users to use the route.

Translation protocol list:

A translation protocol is a communication standard used by an instant messaging service to initiate interactive, real-time sessions between users. Use this page to view and edit translation protocols installed with the IBM Sametime Gateway

Name

Click the translation protocol to view or edit properties its properties.

Translation protocols

The following protocols are included with Sametime Gateway:

<table>
<thead>
<tr>
<th>Translation protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP for AOL</td>
<td>Use SIP for AOL for all AOL Instant Messenger and AOL clearinghouse community connections.</td>
</tr>
<tr>
<td>SIP for Sametime Gateway</td>
<td>Use SIP for Sametime Gateway for connections to Sametime Gateway versions 7.5 or 7.5.1 communities.</td>
</tr>
<tr>
<td>SIP for legacy Sametime Gateway</td>
<td>Use SIP for legacy Sametime Gateway for connections to Sametime server versions 7.0 or 6.5.1.</td>
</tr>
<tr>
<td>SIP for OCS</td>
<td>Use SIP for OCS to connect to Office Communications Server communities.</td>
</tr>
<tr>
<td>Translation protocol</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VP</td>
<td>Use VP (Virtual Places) to connect with the local, internal Sametime community only.</td>
</tr>
<tr>
<td>XMPP</td>
<td>Use XMPP to connect with communities that use XMPP.</td>
</tr>
</tbody>
</table>

**Translation protocol properties:**

Use this page to view properties for translation protocols. A translation protocol is a communication standard used by a collaborative service provider to initiate interactive, real-time sessions between users. You cannot edit the **Name** or **Java Class**.

**Name**

Sametime Gateway name for the translation protocol.

**Java Class**

Shows the Java class that implements the protocol.

**Custom properties**

Click the custom properties to set name and value pairs for the translation protocol, or to edit the session timeout or subscription timeout properties for SIP-based protocols. This link supports the configuration of custom properties, allowing you to capture third-party software requirements that are not covered by the configuration provided by the Sametime Gateway.

**Assign local users and capabilities:**

Assign users and groups from the local community permission to exchange real-time messages with an external community or clearinghouse community. Use this panel to control access to Sametime Gateway and external messaging communities.

Give users from the local community permission to use instant messaging and presence with the external community. You must map your LDAP directory to the WebSphere Application Server repository before you assign users. The LDAP directory contains members of the local community. You can assign access to internal community users only. It's up to the administrator of an external community to give their users access to the local community through the IBM Sametime Gateway.

**Select capabilities**

- The capabilities of instant messaging and presence are automatically assigned to the route to the community and cannot be changed.
- The "Rich text" capability allows internal and external users to exchange rich text messages, which contain a variety of fonts, colors, and text formatting. This capability is available for the SIP for Sametime Gateway translation protocol only.

**Note:** When federating two Sametime communities, also enable the "rich text" capability for the external Sametime Gateway.
• The "Is typing" capability shows in real time when a chat partner is typing a message. This capability is available for the SIP for Sametime Gateway and SIP for OCS translation protocols only.

Note: When federating two Sametime communities, also enable the "Is typing" capability for the external Sametime Gateway.

Assign access

Select to allow access to the external community to all users, or select to allow access to the external community to individual users and groups in the local directory. When you select the All users option, the user interface hides the Search and assign users and groups field.

Search and assign groups and users

Use the Search by field to select one of the attributes by which you want to search. The default value is Group.

Use the Search for field to type a value that you want to search for, or use the wildcard character (*). The default value is * (all). Whether the search is case-sensitive depends on the user registry that is being used. For example, you might type these values if searching by group:

• To search for all groups, type *.
• To search for groups that begin with the letters luc, type luc*.
• To search for groups that end with the letters cas, type *cas.
• To search for groups that begin with the letters lu and ending with the letter s, type lu*s.

The search field cannot be blank.

In the Maximum results field, type the maximum number of search results that you want to be displayed. Valid values are 1 to 100.

Click Search to find and display a list of one or more existing users that match your search criteria.

In the Search results table, use the Select column to select individual or multiple users or groups. Click the select all icon ( ) to select all users listed. Only those visible on the table are selected if the list of users takes more than one page. If you have more than one page, you must select users from additional pages separately. You can then clear (deselect) only those users that you do not want to select.

Click the deselect all icon ( ) to clear all check boxes on the visible page of the table only.

The Name column lists group names if groups are searched, or short names or user ID if last names or first names are searched.

The E-mail column lists the email address of the user. Nothing appears in this column when you are searching for groups.

In the Selected names field, after you select names, click Add to move the selected groups or names to the Selected names table. The names in the Selected names
table have access to the external community. The Selected names table may potentially be very large, so it displays names over several pages if necessary. Data are thus sorted by data subset only. To use the Remove selected name tool, select a name and click this button to remove users from accessing the external community through the Sametime Gateway.

Related tasks
"Assigning users access to external communities” on page 141
Assign local users access to external or clearinghouse communities so that they can exchange real-time communications with users from external communities. You can assign access only for local users.

Find user:

Find a user in LDAP and view the capabilities that the user has permission to use when accessing the selected instant messaging community.

Purpose

Use this page to determine if a local user is assigned to access the external or clearinghouse community. Also, you can determine the capabilities such as instant messaging and presence that are assigned to the user.

General properties

Type the user’s email address and click Search to return a list of capabilities.

Related tasks
"Finding users” on page 142
Determine if a local user is assigned access to an external community. In addition, determine the capabilities assigned to the user.

View users:

See who has access to exchange real-time messaging with an external community or clearinghouse.

Purpose

Use this page to view a list of users who have access to capabilities on the route between the local IBM Sametime community and an external community.

General Properties

Both instant messaging and presence cannot be edited.

Related tasks
"Viewing users” on page 143
Determine the users and groups that are assigned to access an external community or clearinghouse community.

Message handler properties:

Use this page to configure the properties of a message handler such as the user locator, authorization controller, or event logger.

Message handlers, also known as plug-ins, process instant messages as they pass through IBM Sametime Gateway. They perform such tasks as locating users,
checking the access list to use, checking for spam instant messages, and logging events. Messages are processed by handlers in the order that the message handlers appear in the list. Message handlers that are installed and started but are not yet configured are labeled **Undefined** in the message handler list. The User locator message handler must always be first on the message handler list. The event log handler must run and appear last in the list.

Message handlers are WebSphere Application Server applications that you install through the Integrated Solutions Console by clicking **Applications > Enterprise Applications**.

You add a message handler by first installing it as a WebSphere Application Server application, configuring its properties, and then enabling the message handler.

**Name**

There are three message handlers that are part of Sametime Gateway and cannot be removed:

<table>
<thead>
<tr>
<th>Message handler name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>User locator</td>
<td>The User locator finds the profiles associated with the originator and the target user of the message using the user name and domain from email addresses. The User locator returns an error if an inbound request contains a blacklisted domain name. The handler adds the community identifiers of the originating and target users to the message header.</td>
</tr>
<tr>
<td>Authorization controller</td>
<td>Only messages successfully processed by the User locator are passed to the Authorization controller for further processing. The Authorization controller’s main task is to allow or disallow the initiator of the message in one community to perform the requested operation with the destination user in another community.</td>
</tr>
<tr>
<td>Event logger</td>
<td>The Event logger records instant messaging content and events and publishes them to the SystemOut.log file. Logged events contain the following information:</td>
</tr>
<tr>
<td></td>
<td>• Message request type – subscription or instant messaging request</td>
</tr>
<tr>
<td></td>
<td>• Message initiator’s email address and community name</td>
</tr>
<tr>
<td></td>
<td>• Message receiver’s email address and community name</td>
</tr>
<tr>
<td></td>
<td>• Event status: success or failure</td>
</tr>
<tr>
<td></td>
<td>• Reason for failure</td>
</tr>
<tr>
<td></td>
<td>• Date and time</td>
</tr>
<tr>
<td></td>
<td>• Optional message content</td>
</tr>
<tr>
<td></td>
<td>You must install the Sametime Gateway samples ear file available from the Sametime Software Development Kit before you enable the Event logger.</td>
</tr>
</tbody>
</table>

**Type**

Select the type of message handler. Choices are **User locator**, **Access control**, **Event log**, and **Other**. When a message handler is first installed, the default type is undefined and its status is disabled. To enable the message handler, you must select **Enable the message handler**.
Run this message handler regardless of the status of previous message handlers

Select to make running the message handler mandatory. That is, run the message handler regardless of whether a previously run message handler completed its process or encountered an error. If this setting is not selected, and any preceding message handler raises an error, the message handler will not run. A message handler that is not mandatory is considered conditional.

For example, the table that follows shows that in processing a message the Custom User Locator raises an error. Consequently, the mandatory Virus Checker and System Logger handlers run (in that order), while the conditional handlers, the SPIM Filter and the Custom Logger are skipped.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Mandatory or Conditional</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default User Locator</td>
<td>Access Control List</td>
<td>Conditional</td>
<td>Run</td>
</tr>
<tr>
<td>Custom User Locator</td>
<td>Access Control List</td>
<td>Conditional</td>
<td>Error</td>
</tr>
<tr>
<td>Virus Checker</td>
<td>Virus Checker</td>
<td>Mandatory</td>
<td>Run</td>
</tr>
<tr>
<td>SPIM Filter</td>
<td>Other</td>
<td>Conditional</td>
<td>Skip</td>
</tr>
<tr>
<td>Custom Logger</td>
<td>Event Logger</td>
<td>Conditional</td>
<td>Skip</td>
</tr>
<tr>
<td>System Logger</td>
<td>Event Logger</td>
<td>Mandatory</td>
<td>Run</td>
</tr>
</tbody>
</table>

Custom properties

Click Custom properties to configure additional message handler properties such as name and value pairs.

Related tasks

“Enabling spam filtering” on page 143

You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

Message handler list:

Use this page to configure message handlers that perform such tasks as finding users in the local community for whom to relay messages, checking the access control for local community members, and logging IBM Sametime Gateway events. Message handlers that are provided by Sametime Gateway, with the exception of the Event logger, do not need configuring.

Message handlers are WebSphere Application Server applications that you install using the Integrated Solutions Console by clicking Applications > Enterprise Applications. You can add a custom message handler to the Sametime Gateway by first installing it, configuring its properties, and then enabling the application through the Message handler list.

You can enable and disable message handlers or move message handlers up or down to change the order in which a message handler processes messages.

Note: The Default User Locator must be at the top of the list.
<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the message handler after it has been installed and configured.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the message handler.</td>
</tr>
<tr>
<td>Move Up</td>
<td>Moves the message handler up in the list so that it will process messages before other message handlers. The Default User Locator must remain at the top of the list to function properly. For best results, keep the Event Logger in the last position.</td>
</tr>
<tr>
<td>Move Down</td>
<td>Moves the message handler down in the list so that it processes messages after other message handlers. The Default User Locator must remain at the top of the list to function properly. For best results, keep the Event Logger in the last position.</td>
</tr>
</tbody>
</table>

**Table columns**

Use the Select column to select individual or multiple message handlers. Click the select all icon ( ) to select all message handlers listed, if, for example, you want to enable or disable all message handlers. Only those visible on the table are selected if the list of message handlers takes more than one page. If you have more than one page, you must select handlers from additional pages separately. You can then clear (deselect) only those message handlers that you do not want to select.

Click the deselect all icon ( ) to clear all check boxes on the visible page of the table only.

The Name is the programmatic name of the message handler. Click the name to view or edit the message handler properties.

The Type is one of four types assigned to the message handler. The type provides a general description of the message handler’s purpose but has no effect on how the message handler functions.

The Status shows whether the message handler is enabled or not.

**Related tasks**

“Enabling spam filtering” on page 143
You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

**Custom properties list:**

Use this page to create new properties or to edit existing custom properties for communities, message handlers, connections, or translation protocols. Custom properties provide a way for you to extend the IBM Sametime Gateway by adding, for example, an outbound port number for an additional translation protocol.

**Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new custom property.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected custom properties.</td>
</tr>
</tbody>
</table>
### Custom properties details:

Use this page to edit custom properties for a community, translation protocol, or message handler. You can also specify new properties that are needed to configure third-party elements used by the IBM Sametime Gateway.

You can set arbitrary name-value pairs of data, where the name is a property key and any value that can be used to set internal system configuration properties. Defining a new property enables you to configure a setting beyond that which is available in the Integrated Solutions Console. The Sametime Gateway contains several custom properties pages that work similarly to other property pages in the Integrated Solutions Console.

You can change the value of a translation protocol custom property and add a new name-value pair to an existing translation protocol. You can add new name-value pairs when adding a third party message handler or when changing the properties of an existing message handler.

#### Required

Required properties are those custom properties that are provided by the Sametime Gateway. If you create a new custom property, it cannot be considered required. Required properties cannot be deleted or renamed, but you can edit the Value and Description fields.

#### Name

Specifies the name (or key) for the property. Each property name must be unique. If the same name is used for multiple properties, the value specified for the first property that has that name is used. Do not start your property names with was because this prefix is reserved for properties that are predefined in the application server. Existing custom property names must not be changed if they are required, although you can change the value.

#### Value

Specifies the value paired with the specified name.

#### Description

Provides information about the name-value pair.
**Custom properties provided by Sametime Gateway**

Sametime Gateway provides the following default properties that you can change to fit your environment.

<table>
<thead>
<tr>
<th>Custom Property</th>
<th>Type</th>
<th>Name</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enableContentLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enableImLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Message handler</td>
<td>Event logger</td>
<td>enablePresenceLogging</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>Translation protocol</td>
<td></td>
<td>session_timeout</td>
<td>3600 (seconds)</td>
</tr>
<tr>
<td>Translation protocol</td>
<td></td>
<td>subscription_timeout</td>
<td>3600 (seconds)</td>
</tr>
</tbody>
</table>
| Community       | SIP for Sametime Gateway, legacy Sametime Gateway, AOL, Office Communications Server | servers | 205.188.*.*, 64.12.*.*
| Community       | XMPP (for Google Talk) | servers | talky.l.google.com, talkz.1.google.com
| Community       | Local community | Sametime community exclusion | none (disabled) |
| Community       | Local community | server reconnection timeout  | 60000 (milliseconds or 1 minute) |
| Community       | Local community | server reconnection attempts | -1 (no limit) |
### Script commands

Sametime Gateway provides many `wsadmin` script commands to help you administer and maintain the Sametime Gateway.

The Sametime Gateway accepts a hash table in string format (`$HashString`) from the `wsadmin` script. A hash table, or a hash map, is a data structure that associates keys with values. The primary operation it supports efficiently is a look up. For example, when given a key such as person's email address for example, find the corresponding value for that person's Virtual Member Manager (VMM) ID. The hash table works by transforming the key using a hash function into a hash, a number that the hash table uses to locate the desired value. The script commands handles objects in the Sametime Gateway such as a community, translation protocol, message handler, and so on, in which each entry's key is the name of an attribute in the object, and the entry's value is the associated object value. If there is a nested object in the encoded object, this is represented by a nested hash table.

For example, a community has a corresponding `RTCGWServer` object, so in the hash table that encodes community, the Sametime Gateway server is represented by a hash entry whose key is “RTCGWServer” and whose value is a hash table. The `RTCGWServer` to community is one-to-one mapping. Sametime Gateway converts the incoming hash table into the objects used in the Sametime Gateway administration API and performs the requested function. After process, the Sametime Gateway converts returned objects back into hash tables and returns them as hash table objects to `wsadmin`.

**Related tasks**

“Running sample Jacl scripts” on page 187
Complete these steps to run a sample Jacl script.

**Related reference**

“Sample Jacl scripts” on page 186
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to add communities to Sametime Gateway, give users access to communities, enable logging, and set properties on message handlers.

**Related information**

- Jacl reference
- Wsadmin tool

### Hash string format:

A hash string has the following format (white space ignored except in quotation marks):

```
key=value,...
```

Or:

```
{key=value,...}
```

Where key is:
a string

And, where value is:
a string

Or:
{key=value}

Or:
[[key=value],...]

String A sequence of any characters except quotation mark ("), apostrophe (’),
comma (,), backslash (\), and space ( ). However, you can include the
above characters by enclosing in single or double quotes. But a nested
single or double quote must be escaped by preceding it with a backslash.
The backslash is excluded.

A non-terminal token is an apostrophe (’) or quotation mark (") or backslash (\).

Examples

The following are examples of valid hash table syntax:
name=foo,value=bar

{ name='Mike\' Community', customProperties=[{name=foo,value=bar}, {name=bar, value="foo bar"] } 

{ "some key"="some value", provider={ name='a provider' } }

General Sametime Gateway operations:

This topic describes commands that perform general Sametime Gateway
operations.

getRestrictedDomains:

Returns a list of restricted or blacklisted domains.

Syntax

getRestrictedDomains

Purpose

The getRestrictedDomains command returns a list of blacklisted domains only if
such domains were set in the Sametime Gateway. When the Sametime Gateway
receives a subscription request, the Sametime Gateway checks the DNS blacklist
sites and rejects messages when either the destination or source domains are in this
list.

Data type: String

Sample

This sample returns a list of blacklisted domains in the Sametime Gateway:

set on $AdminControl completeObjectName type=RTCAdminMbean,*
$AdminControl invoke $ons getRestrictedDomains
addRestrictedDomain:

Adds a restricted or blacklisted domain.

Syntax

addRestrictedDomain "domain_name"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>A Fully qualified domain name or IP address.</td>
</tr>
</tbody>
</table>

Purpose

The addRestrictedDomain command adds a blacklisted domain to the Sametime Gateway. When the Sametime Gateway receives a subscription request, the Sametime Gateway checks the blacklist domains and rejects messages when either the destination or source domain is a member of the blacklist.

Data type: String

Sample

This sample adds a blacklisted domain to the Sametime Gateway:

set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons addRestrictedDomain "spamalot.com"

deleteRestrictedDomain:

Deletes a restricted or blacklisted domain.

Syntax

deleteRestrictedDomain "domain_name"

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>A Fully qualified domain name or IP address.</td>
</tr>
</tbody>
</table>

Purpose

The deleteRestrictedDomain command deletes a blacklisted domain from the Sametime Gateway. When the Sametime Gateway receives a subscription request, the Sametime Gateway checks the blacklist domains and rejects messages when either the destination or source domain is a member of the blacklist.

Data type: String

Sample

This sample deletes a blacklisted domain to the Sametime Gateway:

set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons deleteRestrictedDomain "spamalot.com"
setMaxIMSessions:

Sets the maximum instant messaging sessions.

Syntax

setMaxIMSessions session_count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_count</td>
<td>Maximum instant messaging sessions in the Sametime Gateway.</td>
</tr>
<tr>
<td></td>
<td>Set to -1 to allow unlimited sessions.</td>
</tr>
<tr>
<td></td>
<td>Set to 0 to allow no sessions.</td>
</tr>
</tbody>
</table>

Purpose

The `setMaxIMSessions` command sets the maximum instant messaging sessions for the Sametime Gateway. Note that maximum sessions set with this command override community-based settings.

Data type: Integer

Sample

This sample allows unlimited sessions in the Sametime Gateway:

```sh
set ons [adminControl completeObjectName type=RTCAdminMbean,*]
adminControl invoke $ons setMaxIMSessions -1
```

setMaxPresenceSessions:

Sets the maximum presence sessions.

Syntax

setMaxPresenceSessions session_count

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_count</td>
<td>Maximum presence sessions in the Sametime Gateway.</td>
</tr>
<tr>
<td></td>
<td>Set to -1 to allow unlimited sessions.</td>
</tr>
<tr>
<td></td>
<td>Set to 0 to allow no sessions.</td>
</tr>
</tbody>
</table>

Purpose

The `setMaxPresenceSessions` command sets the maximum presence sessions or subscriptions for the Sametime Gateway. Note that maximum sessions set with this command override community-based settings.

Data type: Integer
Sample

This sample allows 1000 presence sessions in the Sametime Gateway:
set ons [$AdminControl completeObjectName type=RTCAgMBean]*
$AdminControl invoke $ons setMaxPresenceSessions 1000

getMaxIMSessions:

Returns the maximum instant messaging sessions.

Syntax

getMaxIMSessions

Purpose

The getMaxIMSessions command returns the maximum instant messaging sessions for the Sametime Gateway.

Data type: Integer

Sample

This sample gets the maximum sessions allowed in the Sametime Gateway:
set ons [$AdminControl completeObjectName type=RTCAgMBean,*]
$AdminControl invoke $ons getMaxIMSessions

getMaxPresenceSessions:

Returns the maximum presence sessions.

Syntax

g getMaxPresenceSessions

Purpose

The getMaxPresenceSessions command returns the maximum presence or subscriptions for the Sametime Gateway.

Data type: Integer

Sample

This sample gets the maximum presence sessions allowed in the Sametime Gateway:
set ons [$AdminControl completeObjectName type=RTCAgMBean,*]
$AdminControl invoke $ons getMaxPresenceSessions

getAuthenticationAliases:

Returns an array containing the valid authentication types for the Sametime Gateway.

Syntax
getAuthenticationAliases

**Purpose**

The `getAuthenticationAliases` command returns the valid authentication aliases used by some non-SIP translation protocols in Sametime Gateway.

**Data type:** String

**Sample**

This sample gets the authentication types in the Sametime Gateway:

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getAuthenticationAliases
```

getUserIDByEmailAddress:

Returns a VMM ID based on a user's email address.

**Syntax**

getUserIDByEmailAddress email address

**Purpose**

The `getUserIDByEmailAddress` command returns a user's Virtual Member Manager (VMM) ID from LDAP using their email address. The command throws an exception if no matches are found.

**Data type:** String

**Sample**

This sample script gets the user id of jsmith@example.com:

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getUserIDByEmailAddress jsmith@example.com
```

getPersonPropertiesByVMMID:

Returns a person's display name and email address based on their VMM ID.

**Syntax**

getPersonPropertiesByVMMID "vmmid"

**Purpose**

The `getPersonPropertiesByVMMID` command gets a person's display name and email address from LDAP using the person's VMM ID. The command returns a hash table that has VMMID as the key, a list of requested properties, and the display name and email address as key-values pairs. There is no need to actually submit the VMM ID to obtain properties. Use the `getPersonPropertiesByVMMID` command with the `getUserIDByEmailAddress` command to get this information.

**Data type:** string
Sample

This sample program first get the user IDs from email addresses, then uses the result to obtain properties of the users based on their VMM ID.

```
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*] \$AdminControl
set m [\$AdminControl invoke \$ons getUserIDByEmailAddress ahermm@us.ibm.com]
set p [\$AdminControl invoke \$ons getUserIDByEmailAddress wangpin@us.ibm.com]
\$AdminControl invoke \$ons getPersonPropertiesByVMMID "$m $p"
```

getListGroupOfUser:

Returns the list of groups a person is member of, including nested groups.

Syntax

getAddressGroupsOfUser(vmmid)

Purpose

The `getListGroupOfUser` command returns a list of groups of which the user is a member, based on the person's VMM ID.

**Data type:** string

Sample

```
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*] \$AdminControl
\$AdminControl invoke \$ons getListGroupOfUser(vmmid)
```

getAddressPropertiesBySearchExp:

Returns properties about a person or group.

Syntax

getAddressPropertiesBySearchExp(searchProp, searchExpr, returnSize)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchProp</td>
<td>integer</td>
<td>The <code>searchProp</code> parameter controls the type of search. Type 0 for group names, 1 for last names, or 2 for first names.</td>
</tr>
<tr>
<td>searchExpr</td>
<td>string</td>
<td>The <code>searchExpr</code> parameter controls what is searched and is not case sensitive. A wildcard asterisk (*) is supported. For example if <code>searchExpr=&quot;mike&quot;</code>, find any user or group named &quot;mike&quot;. If <code>searchExpr=&quot;m*&quot;</code>, then find any user or group beginning with the letter &quot;m&quot;. If <code>searchExpr=&quot;m&quot;</code>, find any user or group ending with the letter &quot;m&quot;. Note that &quot;<strong>m</strong>&quot; is not a valid search expression.</td>
</tr>
<tr>
<td>returnSize</td>
<td>integer</td>
<td>The <code>returnSize</code> parameter is the number of search results to be returned.</td>
</tr>
</tbody>
</table>

Purpose

The `getPersonPropertiesBySearchExp` command allows you return properties such as last name or group name using a search expression. Note that group email addresses are not supported and thus do not appear in search results.
Sample

The example that follows searches for last names beginning with "m".

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getPersonPropertiesBySearchExp "2 m* 3"
```

C2E755D60DDD18968525719A00642F8E
mail15
mail15@us.ibm.com
9DB3D27FF355A6568525719A00643C0C
mail17
mail17@us.ibm.com
04687B65F5492BA58525719A006448A3
mail19
mail19@us.ibm.com

Message handler operations:

This topic describes wsadmin commands that perform message handler operations.

getMHList:

Returns a list of message handlers in the Sametime Gateway.

Syntax

```
getMessageHandlerList
```

Parameter | Data type | Description
--- | --- | ---
handlerName | string | Logical name of the message handler.

Sample

```java
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getMessageHandlerList "*"
```

setMessageHandlerProperties:

Sets the attributes on a message handler.

Syntax

```
setMessageHandlerProperties handlerName, attributes
```

Parameter | Data type | Description
--- | --- | ---
handlerName | string | Logical name of the message handler.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
</table>
| attributes | hash string | Properties of the message handler:  
|  |  | • type: undefined, Event logger, Authorization controller, User locator, and other  
|  |  | • enabled: true or false  
|  |  | • order: 0 being first  
|  |  | • mandatory: true or false |

**Purpose**

The `setMessageHandlerProperties` command sets the properties for the named message handler.

**Sample**

```bash
set ons [{AdminControl completeObjectName type=RTCAdminMbean,*}]
set mhp { enabled=true, type=eventLogger, customProperties=[ {name=A, value=B} ] }
$AdminControl invoke $ons setMessageHandlerProperties "evtlogger {$mhp}"```

**Community operations:**

This topic describes `wsadmin` commands that perform community operations.

**getLocalCommunityName:**

Returns the name of the local community.

**Syntax**

```bash
getLocalCommunityName
```

**Purpose**

The `getLocalCommunityName` command returns the name of the local community as a string result.

**Sample**

```bash
set ons [{AdminControl completeObjectName type=RTCAdminMbean,*}]
set local [{AdminControl invoke $ons getLocalCommunityName}]
$AdminControl invoke $ons getRouteByCommunities "$local company"
```

**getLocalCommunityUid:**

Returns the unique identifier of the local community.

**Syntax**

```bash
getLocalCommunityUid
```

**Purpose**

The `getLocalCommunityUid` command returns the UID of the local community as a string result.

**getCommunityList:**
Returns a list of all local, external, and clearinghouse communities in Sametime Gateway.

**Syntax**

getCommunityList communityName

**Purpose**

The getCommunityList command returns an array of hash tables. If communityName is the name of a community in the system, then the array contains a single hash table populated with key-value pairs. If communityName is ", the hash table contains representations of all the communities in the system.

**Data type:** string

**Sample**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getCommunityList "*"

**newCommunity:**

Adds a new community to the Sametime Gateway.

**Syntax**

newCommunity hashString

**Purpose**

The newCommunity command adds a community based on the attributes that you specify in a hash string.

**Data type:** string

The following samples are taken from the sample Jacl scripts available in stgw_server_root/samples/scripts. Consult the actual scripts for information on properties and parameters.

**Sample: adding the local community**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]

set c {name=InternalCommunityTestName,rTCServers=[[{transport=TCP,hostname=localhost,port=1516}],
internal=true,protocolConnector={name="VP"},domains=[[internal.com,internal2.com]]
puts [$AdminControl invoke $ons newCommunity "{$c}"

**Sample: adding an external community**

set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]

set c {name=externalCommunityTestName,rTCServers=[[{transport=TLS,hostname=localhost,port=5061}],
internal=false,protocolConnector= [{name="SIP for legacy Sametime Gateway"},customProperties=
["session_timeout",value=3600,required=false,description="Optional session timeout for externalCommunityTestName"],
["subscription_timeout",value=3600,required=false,description="Optional subscription timeout for externalCommunityTestName"]},domains=
[test1.com,test2.com]}
puts [$AdminControl invoke $ons newCommunity "{$c}"

setCommunityProperties:
Sets the attribute named by the key to the value in the community named by
communityName.

**Syntax**

setCommunityProperties (communityName, properties)

**Purpose**

The setCommunityProperties command sets the attribute named by the key to the
value in the communityName.

**Data types:** string and hash string

**Sample**

set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
s c {provider = {name=GenericProvider }, customProperties=[(name=f, value="some value")]} AdminControl invoke $ons setCommunityProperties "aol {$c}"

**removeCommunity:**

Removes a community from the Sametime Gateway.

**Syntax**

removeCommunity communityName

**Data type:** string

**Sample**

set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
AdminControl invoke $ons removeCommunity "Company"

**Connection operations:**

This topic describes wsadmin commands that perform connection operations.

**getRTCServerList:**

Returns a list of Sametime Gateway servers.

**Syntax**

getRTCServerList (communityName, primaryProvider, serverName)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>communityName</td>
<td>String</td>
</tr>
<tr>
<td>primaryProvider</td>
<td>boolean</td>
</tr>
<tr>
<td>serverName</td>
<td>String</td>
</tr>
</tbody>
</table>

**Purpose**

The getRTCServerList command returns a list of server hash strings containing a
server with the specified server name. If "*" is specified, a list of all servers is
returned.
**setPrimaryRTCServerProperties:**

Sets the connection properties for a given community.

**Syntax**

```
setPrimaryRTCServerProperties communityName, attributes
```

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Data type</td>
</tr>
<tr>
<td>communityName</td>
<td>string</td>
</tr>
<tr>
<td>attributes</td>
<td>hash string</td>
</tr>
</tbody>
</table>

**Purpose**

The `setPrimaryRTCServerProperties` command sets the connection properties for a given community.

**Sample**

```
set ons [{$AdminControl completeObjectName type=RTCAdminMbean,*}]
set s {hostname=example.com, port=15, transport=TLS, customProperties=([{name=A, value=B}])}
$AdminControl invoke $ons setPrimaryRTCServerProperties "GE {$s}"  
```

**Route operations:**

This topic describes `wsadmin` commands that perform general route or connector operations.

**getRouteByCommunities:**

Returns the attributes for the local and destination communities, including access control information.

**Syntax**

```
getRouteByCommunities sourceName, destName
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external community or clearinghouse community</td>
</tr>
</tbody>
</table>

**Purpose**

The `getRouteByCommunities` command returns the route between the local and external community as a hash string table.

**Sample**

```
set ons [{$AdminControl completeObjectName type=RTCAdminMbean,*}]
set local [{$AdminControl invoke $ons getLocalCommunityName}]
$AdminControl invoke $ons getRouteByCommunities "$local company"
```
setRoutePropertiesByCommunities:

Sets properties for the route between the local and external communities.

Syntax

setRoutePropertiesByCommunities sourceName, destName, attributes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external community or clearinghouse community</td>
</tr>
<tr>
<td>attributes</td>
<td>hash string</td>
<td>Properties for the route.</td>
</tr>
</tbody>
</table>

Purpose

The setRoutePropertiesByCommunities command sets properties for the route.

User and group operations:

This topic describes wsadmin commands that perform Sametime Gateway user and group operations.

getUsers:

Returns a list of users that are granted access to the specified capabilities on this route.

Syntax

getUsers routeUid, capability, index, pageSize

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (return all capabilities) is valid. Do not use 0 or 1.</td>
</tr>
<tr>
<td>index</td>
<td>integer</td>
<td>Page at which to start returning pages specified by pageSize. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19.</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>Number of pages of users to return.</td>
</tr>
</tbody>
</table>

Purpose

The getUsers command returns a list of users associated with the specified capability on the named route for the named community. Capabilities are
numerically indexed but only 2 is valid. Additionally, the command returns \( \text{pageSize} \) entries at a time starting at \( \text{index} \). User operations may only be performed on all capabilities.

**Sample**

```plaintext
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [\$AdminControl invoke \$ons getLocalCommunityName]
\$AdminControl invoke \$ons getUsers \"$somerouteuid2 0 10\"
```

**getUsersByCommunities:**

Returns a list of users by community to which they have access.

**Syntax**

```plaintext
getUsersByCommunities sourceName, destName, capabilities, index, pageSize
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capabilities</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>index</td>
<td>integer</td>
<td>Page at which to start returning pages specified by ( \text{pageSize} ).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if ( \text{index} ) is 0 and ( \text{pageSize} ) is 10, the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>command returns pages 1 to 10. If the ( \text{index} ) is 1 and the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( \text{pageSize} ) is 18, the command returns pages 2 to 19.</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>Number of pages of users to return.</td>
</tr>
</tbody>
</table>

**Purpose**

The getUsersByCommunities command returns a list of users associated with the specified capability on the named route for the named community. Capabilities are numerically indexed. Additionally, the command returns \( \text{pageSize} \) entries at a time starting at \( \text{index} \). User operations may only be performed on all capabilities.

**Sample**

```plaintext
set ons [\$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [\$AdminControl invoke \$ons getLocalCommunityName]
\$AdminControl invoke \$ons getUsersByCommunities \"$local company 2 0 10\"
```

**getGroups:**

Returns a list of groups.

**Syntax**

```plaintext
getGroups routeldid, capability, index, pageSize
```
### Parameter Data type Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>index</td>
<td>integer</td>
<td>Page at which to start returning pages specified by pageSize. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19.</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>Number of pages of groups to return.</td>
</tr>
</tbody>
</table>

### Purpose

The getGroups command returns a list of groups associated with the specified capability on the named route for the named community. Capabilities are numerically indexed. Additionally, the command returns pageSize entries at a time starting at index. Group operations may only be performed on all capabilities.

### Sample

```bash
set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
set local [AdminControl invoke $ons getLocalCommunityName]
AdminControl invoke $ons getGroups "$somerouteuid 2010"
```

`getGroupsByCommunities`:

Returns a list of groups by community.

### Syntax

`getGroupsByCommunities sourceName, destName, capability, index, pageSize`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>index</td>
<td>integer</td>
<td>Page at which to start returning pages specified by pageSize. For example, if index is 0 and pageSize is 10, the command returns pages 1 to 10. If the index is 1 and the pageSize is 18, the command returns pages 2 to 19.</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>Number of pages of groups to return.</td>
</tr>
</tbody>
</table>
Purpose

The `getGroupsByCommunities` command returns a list of groups associated with the specified capability on the named route for the named community. Capabilities are numerically indexed. Additionally, the command returns `pageSize` entries at a time starting at `index`. Group operations may only be performed on all capabilities.

Sample

```
set ons [setControl completeObjectName type=RTCAdminMbean,*]
set local [setControl invoke $ons getLocalCommunityName]
setControl invoke $ons getGroupsByCommunities "$local company2010" 2 0 10
```

`addUser`:

Adds a user with capabilities to a route.

Syntax

```
addUser routeUid, capability, username
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Name of user.</td>
</tr>
</tbody>
</table>

Purpose

The `addUser` command gives a user access to an external community. User operations may only be performed on all capabilities.

Sample

```
set ons [setControl completeObjectName type=RTCAdminMbean,*]
setControl invoke $ons addUser "$somerouteuid 2 jsmith"
```

`addUserByCommunities`:

Adds a user so that the user can access an external community.

Syntax

```
addUserByCommunities sourceName, destName, capability, username
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
</tbody>
</table>
### Parameter Data type Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
</table>
| capability | integer   | Numerical index for capabilities. Only 2 (all capabilities) is supported.  
• 0 returns instant messaging  
• 1 returns presence  
• 2 returns all capabilities |
| username  | string    | User name. |

### Purpose

The `addUserByCommunities` command adds a user with specified capabilities to access the named external community. Capabilities are numerically indexed. User operations may only be performed on all capabilities.

**Sample**

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
set local [$AdminControl invoke $ons getLocalCommunityName]
$AdminControl invoke $ons addUserByCommunities "$local aol 2 jsmith"
```

###addGroup

**Purpose**

The `addGroup` command gives a group access to an external community. Group operations may only be performed on all capabilities.

**Sample**

```
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons addGroup "$somerouteuid 2 sales"
```

### addGroupByCommunities

**Purpose**

The `addGroupByCommunities` command adds a group so that the group can access an external community.

**Syntax**

`addGroupByCommunities routeUid, capability, groupname`
addGroupByCommunities  sourceName, destName, capability, groupName

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 returns all capabilities</td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

**Purpose**

The `addGroupByCommunities` command adds a group with specified capabilities to access the named external community. Capabilities are numerically indexed. Group operations may only be performed on all capabilities.

**Sample**

```plaintext
set ons [AdminControl completeObjectName type=RTCAadminMbean,*]
set local [AdminControl invoke $ons getLocalCommunityName]
AdminControl invoke $ons addGroupByCommunities "$local aol 2 sales"
```

`removeUser`:

Removes a user with capabilities from a route.

**Syntax**

`removeUser routeUid, capability, username`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Name of user.</td>
</tr>
</tbody>
</table>

**Purpose**

The `removeUser` command stops a user's access to an external community. User operations may only be performed on all capabilities.

**Sample**

```plaintext
set ons [AdminControl completeObjectName type=RTCAadminMbean,*]
AdminControl invoke $ons removeUser "$somerouteuid 2 jsmith"
```

`removeUserByCommunities`:
Removes a user so that the user cannot access an external or clearinghouse community.

### Syntax

```cpp
removeUserByCommunities sourceName, destName, capability, username
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 returns all capabilities</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>User name.</td>
</tr>
</tbody>
</table>

### Purpose

The `removeUserByCommunities` command removes a user with specified capabilities and prevents them from accessing the named external community. Capabilities are numerically indexed. User operations may only be performed on all capabilities.

### Sample

```bash
set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
set local [AdminControl invoke $ons getLocalCommunityName]
AdminControl invoke $ons removeUserByCommunities "$local aol 2 jsmith"
```

`removeGroup`:

Removes a group from the specified route.

### Syntax

```cpp
removeGroup routeUid, capability, groupname
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 returns all capabilities</td>
</tr>
<tr>
<td>groupname</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

### Purpose

The `removeGroup` command removes a group’s access to an external community. Group operations may only be performed on all capabilities.
removeGroupByCommunities:

Removes a group so that the group can no longer access the specified external community.

Syntax

removeGroupByCommunities sourceName, destName, capability, groupName

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>Group name.</td>
</tr>
</tbody>
</table>

Purpose

The removeGroupByCommunities command removes a group with specified capabilities and prevents it from accessing the named external community. Capabilities are numerically indexed. Group operations may only be performed on all capabilities.

Sample

set ons [AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons removeGroup "$somerouteuid 2 sales"

getNumOfUsers:

Returns the number of users that are present on a given route and capability.

Syntax

ggetNumOfUsers routeUID, capability

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeuid</td>
<td>string</td>
<td>UID of route between the local and external community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>
Purpose

The `getNumOfUsers` command returns the number of users present on a given route and capability.

Sample

```java
set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getNumOfUsers "$somerouteuid 2"
```

`getNumOfUsersByCommunities`:

Returns the number of users that are present on a given community and capability.

Syntax

```java
getNumOfUsersByCommunities sourceName, destName, capability
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>

Purpose

The `getNumOfUsersByCommunities` command returns the number of users present on a given route and capability.

Sample

```java
set ons [$AdminControl completeObjectName type=RTCAadminMbean,*]
$AdminControl invoke $ons getNumOfUsersByCommunities "$somerouteuid 2"
```

`getNumOfGroups`:

Returns the number of groups that are present on a given route and capability.

Syntax

```java
getNumOfGroups routeUID, capability
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routeUID</td>
<td>string</td>
<td>UID of route between the local and external</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>
Purpose

The `getNumOfGroups` command returns the number of users present on a given route and capability.

Sample

```plaintext
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getNumOfGroups "$somerouteuid 2"
```

`getNumOfGroupsByCommunities`:

Returns the number of groups that are present on a given community and capability.

Syntax

```
getNumOfGroupsByCommunities sourceName, destName, capability
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceName</td>
<td>string</td>
<td>Logical name of the local community.</td>
</tr>
<tr>
<td>destName</td>
<td>string</td>
<td>Logical name of the external or clearinghouse community.</td>
</tr>
<tr>
<td>capability</td>
<td>integer</td>
<td>Numerical index for capabilities. Only 2 (all capabilities) is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 returns instant messaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 returns presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 returns all capabilities</td>
</tr>
</tbody>
</table>

Purpose

The `getNumOfGroupsByCommunities` command returns the number of groups present on a given community and capability.

Sample

```plaintext
set ons [$AdminControl completeObjectName type=RTCAdminMbean,*]
$AdminControl invoke $ons getNumOfGroupsByCommunities "$somerouteuid 2"
```

Script exceptions:

A script command can return two types of exceptions: java.lang.IllegalArgumentException and java.rmi.RemoteException.

`IllegalArgumentException` signal that your request is invalid or incorrectly formatted. In the case of invalid requests, such as removing a community by name for which no matching name can be found or adding a user to a route by community names, the exception wraps the invalid argument data. In the case that the hash-string is incorrectly formatted or cannot be parsed into the desired object, a no-arg `IllegalArgumentException` will be thrown. The exception `java.rmi.RemoteException` is used to wrap administrative run time and database exceptions.

Object attribute reference:
This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

### Community object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>The name of the community</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>domains</td>
<td>List of domains</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>customProperties</td>
<td>Community custom properties</td>
<td>List: custom properties</td>
<td>RW</td>
</tr>
<tr>
<td>internal</td>
<td>Indicates if the community is a local (internal=true) or external (internal=false) community</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>clearingHouse</td>
<td>Indicates if the community is a clearing house community (true)</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>protocolConnector</td>
<td>The translation protocol used by this community</td>
<td>ProtocolConnector</td>
<td>RW</td>
</tr>
<tr>
<td>sSTGWServer</td>
<td>The connections defined for the community.</td>
<td>List: STGWServer</td>
<td>R (W only on community creation)</td>
</tr>
</tbody>
</table>

### STGWServer object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>The name of the connection</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>transport</td>
<td>The transport type for this connection. Accepted values: TCP or TLS</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name for this connection</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>port</td>
<td>The port number for this connection.</td>
<td>Integer</td>
<td>RW</td>
</tr>
</tbody>
</table>

### ProtocolConnector Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Data type</td>
<td>Read (R) or Write (W)</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>name</td>
<td>Name of connector</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>protocol</td>
<td>The translation protocol supported by this connector. Accepted values include SIP for Sametime, SIP for legacy Sametime servers, SIP for AOL, SIP for OCS, VP, and XMPP.</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>customProperties</td>
<td>Custom properties for the translation protocol such as subscription timeout or session timeout.</td>
<td>List: customProperties</td>
<td>RW</td>
</tr>
</tbody>
</table>

**MessageHandler Object**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>Name of the community.</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>customProperties</td>
<td>Custom properties for the message handler.</td>
<td>List: CustomProperties</td>
<td>RW</td>
</tr>
<tr>
<td>mandatory</td>
<td>Run the message handler regardless of whether a previously run message handler completed its process or encountered an error.</td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>order</td>
<td>Specifies the order of precedence of the message handlers.</td>
<td>Integer</td>
<td>RW</td>
</tr>
<tr>
<td>type</td>
<td>The message handler type. Accepted values are: undefined, Event logger, Authorization controller, User locator, and other</td>
<td>String</td>
<td>RW</td>
</tr>
</tbody>
</table>

**Route Object**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>source</td>
<td>The local community.</td>
<td>Hash table</td>
<td>R</td>
</tr>
</tbody>
</table>
### Attribute Description Data type Read (R) or Write (W)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>The destination or external community.</td>
<td>Hash table</td>
<td>R</td>
</tr>
<tr>
<td>enabled</td>
<td>Indicates if the route is enabled or disabled.</td>
<td>Boolean</td>
<td>RW</td>
</tr>
</tbody>
</table>
| capabilities | Capabilities such as instant messaging and presence for the route. Only 2 is valid.  
• 0 = instant messaging  
• 1 = presence  
• 2 = both capabilities | Integer | RW |

### Access Control List (ACL) Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>users</td>
<td>The Virtual Member Manager (VMM) IDs of the users whom are on this access control list.</td>
<td>List : String</td>
<td>RW</td>
</tr>
<tr>
<td>groups</td>
<td>The VMM IDs of the groups whom are on this access control list.</td>
<td>List : String</td>
<td>RW</td>
</tr>
</tbody>
</table>

### CustomProperty Object

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Data type</th>
<th>Read (R) or Write (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique identifier</td>
<td>String</td>
<td>R</td>
</tr>
<tr>
<td>name</td>
<td>Name of the community.</td>
<td>String</td>
<td>R (Write only on creation.)</td>
</tr>
<tr>
<td>value</td>
<td>Value of the property.</td>
<td>String</td>
<td>RW</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td>Boolean</td>
<td>RW</td>
</tr>
<tr>
<td>description</td>
<td>Text description of the custom property</td>
<td>String</td>
<td>RW</td>
</tr>
</tbody>
</table>
Related tasks
“Running sample Jacl scripts” on page 187
Complete these steps to run a sample Jacl script.

Related reference
“Sample Jacl scripts”
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to add communities to Sametime Gateway, give users access to communities, enable logging, and set properties on message handlers.

Related information

Jacl reference
Wsadmin tool

Sample Jacl scripts
Sametime Gateway includes several sample scripts written in Jacl (Java TCL) to add communities to Sametime Gateway, give users access to communities, enable logging, and set properties on message handlers.

Script location
The sample Jacl scripts are located in the following directory:
stgw_server_root/samples/scripts

Jacl scripts
Jacl scripts are a non-graphical alternative that you can use to configure and manage the Sametime Gateway. The WebSphere administrative scripting tool, wsadmin, is a non-graphical command interpreter environment enabling you to run administrative operations on a server in Jacl.

The scripts perform some of the functions available using the Integrated Solutions Console. But in some cases, the scripts offer increased flexibility. For example, when using the graphical interface to add or update an external community that uses a SIP-based protocol, you must use TLS (Transport Layer Security) as the transport protocol. The updateExternalCommunity script commands allows you to use other transport protocols such as TCP or UDP.

The sample scripts include documentation inside each script. See the script and script command reference for command details and syntax.

<table>
<thead>
<tr>
<th>Script</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateExternalCommunity.jacl</td>
<td>Updates the external community by changing its properties such as hostname, domains, port number, and so on.</td>
</tr>
<tr>
<td>GiveAllAcl.jacl</td>
<td>Gives all local Sametime users access to an external community.</td>
</tr>
<tr>
<td>disableAuthz.jacl</td>
<td>Disables the authorization controller message handler. The Authorization controller's main task is to allow or disallow the initiator of the message in one community to perform the requested operation with the destination user in another community.</td>
</tr>
<tr>
<td>EnableEventlogging.jacl</td>
<td>Enables content, instant message, or presence logging in the systemOut.log file.</td>
</tr>
<tr>
<td>getMsghandlerList.jacl</td>
<td>Gets information on message handlers, including message handler names.</td>
</tr>
</tbody>
</table>
### Script Purpose

<table>
<thead>
<tr>
<th>Script</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateMsghandler.jacl</td>
<td>Configures a message handler by setting its properties.</td>
</tr>
</tbody>
</table>

### Related reference

- “Script commands” on page 161
- Sametime Gateway provides many `wsadmin` script commands to help you administer and maintain the Sametime Gateway.
- “Object attribute reference” on page 182

This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

### Related information

- [Jacl reference](#)

### Running sample Jacl scripts:

Complete these steps to run a sample Jacl script.

**Procedure**

1. Log in to the Sametime Gateway server machine as a user with administrative privileges.
2. If the Sametime Gateway server is not started, open a command window. If the server is started, skip to step 5.
3. In the command window, navigate to the Sametime Gateway profile directory that contains binary files: `stgw_profile_root\bin`
4. Type the following command to start Sametime Gateway. Note that `RTCGWServer` is case-sensitive.
   - **AIX, Linux, and Solaris**
     ```bash
     ./startServer.sh RTCGWServer
     ```
   - **Windows**
     ```bash
     startServer.bat RTCGWServer
     ```
   - **IBM i**
     ```bash
     startServer RTCGWServer
     ```
5. Copy the sample scripts from:
   ```bash
   stgw_server_root\samples\scripts
   ```
   to:
   ```bash
   stgw_profile_root\bin
   ```
6. Using a text editor, open the sample script to customize it for your task. The script contains documentation to guide you while editing the script.
7. Open a command window (Q SHELL session on IBM i) and navigate to `stgw_profile_root\bin`.
8. Run the script as follows:
   ```bash
   wsadmin -username username -password password -f script_name.jacl
   ```

Where `username` and `password` are the credentials that you created when you enabled administrative security, and `script_name.jacl` is the name of the sample Jacl script. You must run the `wsadmin` tool with the `-f` option. To see your
changes in the Integrated Solutions Console, you must log out of the console, and then log back into it. Some operations may require stopping and restarting the Sametime Gateway server.

Related reference
“Script commands” on page 161
Sametime Gateway provides many wsadmin script commands to help you administer and maintain the Sametime Gateway.
“Object attribute reference” on page 182
This topic describes the attributes available for each object type and provides the data type and whether the attribute is read, write, or both read and write.

Related information

Wsadmin tool

Back up WebSphere Application Server configurations

As part of a routine maintenance schedule or before upgrading Sametime servers that run on WebSphere Application Server, back up the WebSphere Application Server configurations.

About this task

Run the backupConfig command for each of the configurations that are relevant to Sametime. Note the exact name and location of the backed-up configurations so that you can find them if you need to roll back to an earlier configuration.

1. Back up the Deployment Manager configuration.
2. Back up the application server configuration.
3. Back up the federated node configurations.

For more information, see backupConfig command in the WebSphere Application Server information center.
Chapter 2. Tuning

IBM Sametime administrators can make adjustments to the servers they maintain to provide optimal performance for users as they use instant messaging and web conferencing.

This section contains information about tools provided by WebSphere Application Server and Sametime that help you fine-tune server response time.

Increasing the number of open files on a Sametime server running on Linux

If your IBM Sametime server is hosted on Linux, increase the number of concurrent open files on the server to prevent performance problems.

About this task

Java opens many files and Sametime uses a lot of file descriptors. When a high number of concurrent users (for example, 1,000 or more) connect to the Sametime Community Server, the server may run out of file descriptors.

Prevent this situation by increasing the upper limit on the number of file descriptors in the Linux configuration file.

Procedure

1. Use a text editor and open /etc/security/limits.conf.
2. Add the following lines to the file:
   ```
   * soft nofile 65535
   * hard nofile 65535
   ```
3. Save the file.
4. Restart the Linux server for the operating system change to take effect for all processes.

Tuning a Sametime Community Server

Complete the following tuning procedures to enhance performance.

About this task

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

In addition to the topics in this section, see Optimizing Sametime's Name Lookup solution on the Sametime wiki.

Tuning Sametime LDAP settings

Complete the following procedures to enhance performance
Managing Sametime LDAP internal queues

You can manage advanced configuration settings for the maximum and minimum (MAX/LOW) number of LDAP requests that are pending per connection in the pending queue.

The following settings can be specified in the [Directory] section of the sametime.ini file.

- **ST_DB_LDAP_PENDING_MAX**
  Defines the maximum number of LDAP requests that can be pending per connection in the pending queue. Each connection is for a different type of request; whether search or bind. A Pending Resolve Request is a request that has been sent to the LDAP Server. The request is considered pending until the IBM Sametime Community Server receives a response from the LDAP server for that request. The Sametime Community Server sends, at most, MAX PENDING Requests to the LDAP server. After MAX Pending Requests are sent to the LDAP server on a particular connection, the Sametime Community Server does not send any additional LDAP requests on this connection until the Pending Queue Size drops to the **ST_DB_LDAP_PENDING_LOW** Pending Request queue size.

  For versions prior to Sametime 8.5, the value is set to 10 by default. In Sametime 8.5 and higher, the value is set to 60 by default. Any Sametime service that connects to the LDAP server utilizes the LOW and MAX PENDING queue.

- **ST_DB_LDAP_PENDING_LOW**
  Strongly linked to the **ST_DB_LDAP_PENDING_MAX** setting and to the request queuing feature of Sametime. Once **ST_DB_LDAP_PENDING_MAX** is reached for a certain connection, new LDAP requests are not sent on this connection until the number of pending operations drops to the value set by the **ST_DB_LDAP_PENDING_LOW** setting.

  For versions prior to Sametime 8.5, the value is set to 5 by default. In Sametime 8.5 and higher, the value is set to 30 by default.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sametime 8.5</th>
<th>Sametime pre-8.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST_DB_LDAP_PENDING_MAX</td>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>ST_DB_LDAP_PENDING_LOW</td>
<td>30</td>
<td>5</td>
</tr>
</tbody>
</table>

Special considerations for the PENDING MAX/LOW settings

As the PENDING MAX/LOW settings (**ST_DB_LDAP_PENDING_MAX** and **ST_DB_LDAP_PENDING_LOW**) relate to each LDAP connection, Sametime Community Server might be configured to work with multiple connections per Sametime module, and one connection may stop handling requests while other connections are working well.

The MAX and LOW pending queue sizes are highly dependent upon many factors, such as the resources available to the Sametime Community Server process on the host machine, the resources available to the LDAP process on the LDAP server, the network latency between the Sametime Community Server and LDAP servers, the types of generated searches, and so on. As a result, there is no golden number to guarantee the greatest efficiency for all configurations. By default, MAX and LOW are set to 10 and 5, respectively. However, advanced guidelines for optimizing LDAP configurations generally recommend 60 and 30. IBM typically recommends a size of 120 and 100 for larger corporations with high-powered LDAP servers.
Example of a Pending Low/Max Queue in Sametime.ini:

```
ST_DB_LDAP_PENDING_LOW = 5
ST_DB_LDAP_PENDING_MAX = 10
```

As the Sametime Community Server receives LDAP queries (for example, Sametime Resolve or Authentication requests requiring LDAP look ups), Sametime tries to fulfill those queries by sending corresponding LDAP queries to the LDAP Server. These LDAP queries remain in the “Pending” queue until they are resolved or responded back from the LDAP Server or timed out.

If the PENDING MAX value is 10, the Sametime Community Server does not send more than ten requests to the LDAP Server initially until at least 5 requests are resolved by the LDAP Server so that the low end threshold value specified by PENDING_LOW is reached. Once the number of requests waiting for responses reaches the PENDING_LOW value, the Sametime Community Server once again starts sending more requests to the LDAP Server but repeats the cycle and limits the number of requests in flight to the LDAP Server.

**Note:** If the MAX and LOW sizes for the Pending Queue are not set appropriately, it is possible to overwhelm the LDAP server or artificially reduce the potential high throughput of LDAP requests sent by the Sametime Community Server to the LDAP server.

**Tuning the Sametime LDAP bind operation**

There are different types of bind operations supported by the LDAP protocol. The most common are anonymous and simple bind, also known as authenticated bind.

**About this task**

An anonymous bind is the easiest way to establish a connection with the LDAP server. However, the anonymous client will have limited access to the directory when compared to authenticated clients. Using a simple bind, a client can be authenticated on the LDAP server by providing its DN and password in plain text. The server verifies that such a person exists in the directory and that the supplied password is correct.

The LDAP protocol is asynchronous, so a client can send multiple requests to the LDAP server on the same connection, and does not need to wait for the response of one request before sending the next one. Each request is identified by a request ID, and every response is associated with the original request ID. However, some LDAP servers limit the maximum number of requests that can be pending per single connection.

The following settings are under the [Directory] section of the Sametime.ini file:

- `ST_DB_LDAP_PENDING_BIND_MAX=X`
- `ST_DB_LDAP_PENDING_BIND_LOW=Y`

These settings only affect the bind requests allowing other requests (mainly search requests) to be sent to LDAP in different rates.

To force the IBM Sametime Server to send BIND requests synchronously use the following settings:

- `ST_DB_LDAP_PENDING_BIND_MAX=1`
- `ST_DB_LDAP_PENDING_BIND_LOW=0`
This setting makes sure that no other requests will be sent to LDAP on the same connection before getting the response to the bind request. For more information see the TechNote Adding the ability to send bind requests to LDAP synchronously.

**Tuning multiple connections in Sametime LDAP**

You can edit advanced configuration settings to increase the number of connections per Sametime module.

**About this task**

The **ST_DB_LDAP_CONNECTIONS_NUMBER** setting increases the number of concurrent connections from the IBM Sametime Community Server to the LDAP server(s) specified in the StConfig.nsf per Sametime module. The default setting is set to one connection per module except for StAuthentication.dll, which has two connections.

Before increasing the value to greater than one consider the following points:

- Assume that **ST_DB_LDAP_CONNECTIONS_NUMBER=3**. Note that a value of 3 means that the Sametime Community Server creates $3N$ connections to the LDAP server, where $N$ stands for the number of Sametime components that have an open connection to LDAP. In addition, meeting and Domino components are connected to LDAP so the overall number of connections is greater than $3N$.

- This setting should only be modified if requests are taking an exceptionally long time to process due to long processing queues and there are plenty of resources available on the Sametime Community Server and the LDAP server. Increasing the value of this setting increases the number of LDAP threads available to service the request and multiplies the resource requirements for each one of the Sametime LDAP modules.

**Tuning the Sametime LDAP Keep Alive Interval setting**

You can manage advanced configuration settings to make sure that there is consistent traffic over the LDAP connection.

Specify the **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting in the [Directory] section of the sametime.ini file.

The **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting defines the duration (in minutes) to wait while keeping alive messages that are sent by the IBM Sametime Community Server on idle LDAP connections. Its default value is set to 1 minute. **ST_DB_LDAP_KEEPALIVE_INTERVAL** is an LDAP-based dummy search message whose purpose is to avoid the LDAP server or any network device along the way between the Sametime Community Server and the LDAP server from closing idle connections. This setting is needed in certain LDAP environments where the LDAP server abruptly closes or resets the LDAP connection between Sametime Community Server and LDAP due to no traffic activities on this connection per interval of time set by the LDAP server. To avoid this situation, make sure that there is consistent traffic over the connection by turning on the **ST_DB_LDAP_KEEPALIVE_INTERVAL** setting.

**Tuning the Sametime LDAP Respray Interval setting**

You can manage advanced configuration settings to set how often the connection to the LDAP server should be dropped and re-established.

The **ST_DB_LDAP_RESPRAY_INTERVAL** setting in the [Directory] section of the sametime.ini file defines the frequency, in minutes, that the connection to the LDAP server should be dropped and then re-established. In pre-8.5 versions of
Sametime 8.5, the RESPRAY interval must be higher than the KEEPALIVE interval. By default, the **ST_DB_LDAP_RESPRAY_INTERVAL** setting is disabled.

**Note:** In pre-8.5 versions of Sametime, the RESPRAY interval must be higher than the KEEPALIVE interval. Bear in mind that the RESPRAY operation is an expensive resource task, and might impact performance in an environment where the RESPRAY intervals are set to low values.

**Tuning the Sametime LDAP Maximum Number of Results per Search Query setting**
You can manage advanced configuration settings to define the LDAP maximum number of results per search query.

Specify the **ST_DB_LDAP_MAX_RESULTS** setting in the [Directory] section of the *sametime.ini* file to define the maximum number of entries that can be returned in a single search when searching for people or groups. The default value is **1000**.

**Tuning the Sametime LDAP Minimum Number of Characters to Match setting**
You can manage advanced configuration settings to define the minimum number of characters in the search string required to perform a search.

The **ST_DB_LDAP_MIN_WILDCARD** setting in the [Directory] section of the *sametime.ini* file defines the minimum number of characters to match when searching the LDAP user using wild card characters. When trying to resolve a user or group with a name that is too short than that defined by the **ST_DB_LDAP_MIN_WILDCARD** setting, the IBM Sametime Community Server does not search the LDAP server.

For more information on *sametime.ini* file settings related to the LDAP directory and other techniques for tweaking the Sametime server behavior, refer to these two articles on the IBM Sametime wiki:

* Optimizing Sametime’s Name Lookup solution
* Best Practices for using LDAP with Sametime

These articles provide information about fine-tuning a directory to achieve optimal performance and streamlined connections for Sametime.

**Advanced settings to control contact list size**
You can manage advanced configuration settings for controlling contact list size.

The **MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT** setting in the [Config] section of the *sametime.ini* file limits the number of users that the client can subscribe to, or see awareness on. A public group is counted as one subscription. This limit is published as a server attribute, and the client is responsible for enforcing it. In order to enforce this limit on the server, set the **IGNORE_SUBSCRIBES_ABOVE_MAX** value in the [Config] section of the *sametime.ini* file.

The **ST_GROUPS_MAX_MEMBERS** setting in the [Directory] section of the *sametime.ini* file limits the maximum number of users that the IBM Sametime Community Server will allow in a public group. A public group that is too big will appear empty. Once a group is marked too big, it will remain this way until the server is restarted, even if its contents have changed in the directory to less than
the maximum. Set the value to be a number from 1 - 1000. 1,000 members is the maximum recommended group size. You should not set a value of 0 (zero), which indicates the feature is off.

**Policies and MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT**

The Limit contact list size and Contacts policy settings control the size of the contact list and do not restrain subscriptions. For example, you can set this to 5 and open chat history which has 200 contacts, and the client subscribes to 205 users. If you set this to 5 and the user has 100 contacts on the list already, it does not remove anyone, but it prompts the user to do so. The MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT limits the client so it does not subscribe to users beyond this limit.

**Sametime.ini file**

```
[Config]
MAX_NUMBER_OF_SUBSCRIBES_PER_CLIENT=750
IGNORE_SUBSCRIBES_ABOVE_MAX=751

[Directory]
ST_GROUPS_MAX_MEMBERS=900
```

**Sametime Unified Telephony considerations**

For Sametime Unified Telephony environments the following settings must be applied:

<table>
<thead>
<tr>
<th>Sametime server version</th>
<th>IGNORE_SUBSCRIBES_ABOVE_MAX default Value</th>
<th>IGNORE_SUBSCRIBES_ABOVE_MAX required settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.x</td>
<td>-1 (disabled)</td>
<td>Must be -1. The setting can be omitted from sametime.ini, or explicitly set to -1.</td>
</tr>
<tr>
<td>8.5.x</td>
<td>-1 (disabled)</td>
<td>Must be -1. The setting can be omitted from sametime.ini, or explicitly set to -1.</td>
</tr>
</tbody>
</table>

**Setting a Sametime Polling "Keep Alive" interval for client requests**

You can have the Sametime Polling service keep a client request alive for a certain number of second in cases where a temporary connection loss prevents an immediate response. The setting applies to clients who connect through HTTP and use the Sametime Polling service.

**About this task**

The VP_MAX_PENDING_TIME setting in the [Polling] of the sametime.ini file defines the interval (in seconds) to keep messages pending that are sent by the client. Its default value is set to 0 seconds, which keeps a request pending indefinitely. When the VP_MAX_PENDING_TIME is set to a value larger than 0, the Sametime Polling service sends a response to the client after the specified number of seconds.
Tuning Sametime Media Manager

Complete the following tuning procedures to enhance performance.

Before you begin

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.

Limiting participants in a video conference

The default maximum number of participants in a single audio-only or video conferences is set to 20. You can adjust this number up or down to accommodate specific network consumption requirements.

About this task

Network factors affecting audio and video services include bandwidth and latency. The more bandwidth available to the server and the shorter latency will allow more participants per call. The bandwidth to the server is recommended at least 1Gbps (Gigabit per second), and latency from client to server should be less than 150ms.

Environmental conditions affecting audio and video services include server capacity, total number of simultaneous users, selected audio codec and video resolution, expected number of interactive participants, expected number of video participants, and expected number of simultaneous calls. These conditions will effect the limit of the number of participants per call.

Edit the ConferenceManager.properties for every Conference Manager and change the MaximumVideoConferenceUsers value to a number participants appropriate for your network and the environmental conditions at your site.

Procedure

1. On the server hosting the Sametime Media Manager Conference Manager component, navigate to the following directory:

   WAS_INSTALL_ROOT/profiles/STMSAppProfile/installer/installedApps/cell_name/ConferenceFocus.ear/ConferenceFocus.war

2. Open the ConferenceManager.properties file for editing.

3. Locate the section shown here:

   #
   # MaximumAudioConferenceUsers is the maximum number of users the service provider supports for each audio conference call.
   #
   MaximumAudioConferenceUsers=20

   #
   # MaximumVideoConferenceUsers is the maximum number of users the service provider supports for each video conference call.
   #
   MaximumVideoConferenceUsers=20

5. Save and close the file.
6. Restart the server so the change can take effect.
7. Repeat this process on every Conference Manager component. if you have a clustered deployment, apply to every cluster member.

Modifying the dynamic port range to improve Packet Switcher performance

Make sure that the port range is available for the IBM Sametime Media Manager Packet Switcher

About this task

The default range of audio and video ports on the Packet Switcher might fall in the range of dynamic port for the system. If the port is already allocated by a system process when the Packet Switcher tries to allocate it for a conference, the packet switcher marks this as a bad port and will not use this port again, until after restart. If too many ports in the range get marked as bad ports, this could lead to performance degradation. You can change the default port range by using the Sametime System Console (Sametime System Console > Sametime Servers > Sametime Media Manager > deployment_name) or in the stavconfig.xml.

Procedure

To determine UDP dynamic port range, type the following command from the command line:
Windows 2008:

```
netsh int ipv4 show dynamicport udp
```

For Windows 2003, use 1025 as your start port and use 3975 as your end port for both TCP and UDP.

Linux:

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

Setting log files size and rotation for the Sametime Media Manager

You can specify the maximum size and number of log files to be stored on the IBM Sametime Media Manager.

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the Sametime Media Manager retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file “Maximum Size” (shown in the table below) to more than 20MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Media Manager where the logs will be stored. If you installed Sametime Media Manager components on separate machines or as separate cell profiles, you must adjust the log file information on all Conference Manager and Packet Switcher servers.
Procedure

1. In the Integrated Solutions Console for the Sametime Media Manager component, click **Servers > Server Types > WebSphere application servers > STMediaServer.**
2. Under “Server Infrastructure,” click **Java and Process management > Process Definition.**
3. Under “Additional Properties,” click **Logging and Tracing > JVM Logs.**
4. Under “General Properties,” update the following fields both for **System.out** and **System.err** sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click **OK.**
6. Return to Additional Properties.
7. Under “Additional Properties,” click **Logging and Tracing > Diagnostic Trace.**
8. Click **File** and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click **OK.**
10. Click **Save** to save these changes to the master configuration.
11. If the Sametime Media Manager is clustered, repeat these steps for each node within the cluster.

Setting log files size and rotation for the SIP Proxy and Registrar

You can specify the maximum size and number of log files to be stored on the server.

**Before you begin**

Before performing this procedure, make sure you have the required disk space. IBM recommends that the SIP Proxy and Registrar retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file "Maximum Size" (shown in the table below) to more than 20MB.

**About this task**

Complete these steps using the Integrated Solutions Console on the SIP Proxy and Registrar where the logs will be stored.
Procedure

1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere application servers > STMediaServer.
4. Under "General Properties," update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.

Tuning Sametime Bandwidth Manager

Complete the following tuning procedures to enhance performance.

Tuning the SIP Session timeout on the Sametime Bandwidth Manager

You can set the amount of time the IBM Sametime Bandwidth Manager leaves inactive calls connected by setting a timeout value in the Bandwidth Manager Configuration page.

About this task

Sametime uses SIP heartbeats to detect if a user has been disconnected and these heartbeats keep a session active. Because of these SIP heartbeats, an inactive session timeout does not occur under normal circumstances on an active call even if the parties are not actively speaking for longer than the timeout interval. Nonetheless, in order to prevent stale sessions from remaining in the system in the event of heartbeat failure, set this value to a reasonably short timeframe of 1 hour (which is the default).
Procedure
1. In the Integrated Solutions Console for the Sametime Bandwidth Manager component, click **Sametime Servers > Bandwidth Manager**.
2. Navigate to the “Configuration” tab.
3. Change the “Inactive Session Timeout” to a specific number of minutes, such as 60. “0” means no timeout.

Setting log files size and rotation for the Sametime Bandwidth Manager

You can specify the maximum size and number of log files to be stored on the IBM Sametime Bandwidth Manager

**Before you begin**

Before performing this procedure, make sure you have the required disk space. IBM recommends that the Sametime Bandwidth Manager retain a history at least 2GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file “Maximum Size” (shown in the table below) to more than 20MB.

**About this task**

Complete these steps using the Integrated Solutions Console on the Sametime Bandwidth Manager where the logs will be stored.

**Procedure**

1. In the Integrated Solutions Console for the Sametime Bandwidth Manager, click **Servers > Server Types > WebSphere application servers > Bandwidth_manager_name**.
2. Under “Server Infrastructure,” click **Java and Process management > Process Definition**.
3. Under “Additional Properties,” click **Logging and Tracing > JVM Logs**.
4. Under “General Properties,” update the following fields both for **System.out** and **System.err** sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
6. Return to Additional Properties.
7. Under “Additional Properties,” click **Logging and Tracing > Diagnostic Trace**.
8. Click **File** and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
</tbody>
</table>
9. Click OK.
10. Click Save to save these changes to the master configuration.
11. If the Sametime Bandwidth Manager is clustered, repeat these steps for each node within the cluster.

### Configuring automatic thread dumps for hung threads for the Sametime Bandwidth Manager

To help troubleshoot hung processes and performance slowdowns, configure your IBM Sametime Bandwidth Manager to generate a thread dump automatically when the servers detect hung threads.

#### About this task

Follow these steps to create a custom property to automatically generate a thread dump when a hung thread is detected. Repeat these steps for each server. In the case of a clustered environment, repeat these steps on all Sametime Bandwidth Manager servers in the cluster.

#### Procedure

1. Log in to the Integrated Solutions Console.
2. Click Servers > Server Types > WebSphere application servers.
3. In the table listing the WebSphere application servers, click the link representing the server you want to modify.
5. Supply the name of the custom property:
   com.ibm.websphere.threadmonitor.dump.java
6. Set the value to true.
7. Click OK, and then click Save to save changes to the master configuration.

### Tuning a Sametime Gateway Server

Complete the following tuning procedures to enhance performance. Set the thread pool and the Java virtual machine (JVM) garbage collection policy. Fine tune the SIP proxy service settings and modify the Data Replication Services on a cluster. Some procedures must be repeated on each server in a cluster.

#### Before you begin

Tuning your deployment is important to maintain optimum performance, and should not be considered optional.
Limiting Sametime Gateway global and community-level sessions

You can limit the number of sessions that a particular server supports, or choose to leave the sessions unrestricted.

Whenever a user subscribes to be notified of another user's status changes; a presence session object is created. Whenever two users start a new chat, an instance messaging session object is created. These session objects take up considerable space in memory. To avoid a scenario in which a very high level of user activity might cause an out-of-memory error to occur, set the maximum session property to a predefined limit that you know is supported. In the event of these limits being reached, the server will not create any new sessions, but will continue to serve existing sessions.

IBM Sametime Gateway global limits and Community limits

There are two configuration levels regarding the maximum sessions limit in Sametime Gateway: global limits and community limits. The global limit will be enforced on all communities in your Sametime Gateway deployment as a whole (that is, the sum of all the external communities' sessions cannot exceed the global limit). The community limit is applied to a specific Sametime Gateway community and helps ensure that a single community doesn't use up all of the available memory for its own sessions while blocking others from creating new sessions. If you have only one community, then there is no need to specify community limits; specifying global limits is enough.

In a cluster, the maximum number of sessions is applied to each node, so the true maximum is the number of nodes multiplied by the maximum sessions value; for example, if your cluster has two nodes and your maximum sessions is set to 5000, then your cluster actually supports a maximum of $2 \times 5000 = 10,000$ sessions.

Note: If you set a community's session limits to a value higher than the overall global limit, the global limit will still be enforced.

Setting a global limit on sessions

You should set a global limit for the maximum number of sessions allowed on a server, which helps prevent out-of-memory errors. The value set here will supersede a larger value set in the “Route maximum sessions” property.

About this task

The procedure that follows sets a global limit for the maximum number of sessions allowed at one time on a particular server. The global limit that you specify here will be enforced on all communities in your IBM Sametime Gateway deployment as a whole (that is, the sum of all the external communities sessions cannot exceed the global limit).

Expected state:

- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.
Procedure
1. In the Integrated Solutions Console, click Sametime Gateway > Gateway Properties.
2. Select Set maximum sessions.
   Deselect the box if you do not want to limit instant messaging and presence sessions.
3. Set the maximum sessions for instant messaging by typing an integer.
   Assuming max JVM heap was set to 1.5GB, the recommended value is 8,000 for a single server deployment.
4. Set the maximum sessions for presence by typing an integer.
   Assuming max JVM heap was set to 1.5GB, these are the recommended values:
   - For a single server, or a cluster instance without SIP session replication enabled, the recommended value is 100,000.
   - For a cluster instance with SIP session replication enabled, the recommended value is 100,000.
5. Click Apply.
6. Restart the Sametime Gateway server; if you have a cluster of Sametime Gateway servers, restart the cluster.

Related reference
“Sametime Gateway properties” on page 145
Use this page to set the maximum chat sessions. You can also specify domains from which to block messages.

Setting a community-level limit on sessions in Sametime Gateway
You can limit the maximum number of sessions allowed on a server by each community in IBM Sametime Gateway, which helps prevent out-of-memory errors. The total sessions for individual communities on a particular server contribute to that server's "global" total number of sessions.

Before you begin
If you have more than one external community, there are a number of factors to consider when deciding on community-level maximum session limits. The following table shows different strategies for choosing community limits:

<table>
<thead>
<tr>
<th>Scenario 1</th>
<th>Settings</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1</td>
<td>global max=10 community A max=5 community B max=5</td>
<td>Because G=10, there cannot be more than 10 sessions in a community. Pros: An overloaded community (A=5) will not interfere with community B reaching its own specified maximum (B=5), The server resources are not fully utilized: even if community A uses less than 5 sessions, community B cannot use more than its own limit of 5 sessions.</td>
</tr>
<tr>
<td>Scenario</td>
<td>Settings</td>
<td>Comments</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>global max=10</td>
<td>Because G=10, there cannot be more than 10 sessions in a community.</td>
</tr>
<tr>
<td></td>
<td>community A max=10</td>
<td>Pros: The server resources are fully used; if community A uses less than 5 sessions then community B could use more than 5 sessions.</td>
</tr>
<tr>
<td></td>
<td>community B max=10</td>
<td>Cons: Communities are not insulated and protected from each other. If community A has 8 sessions, then community B can only have 2 sessions (since G=10).</td>
</tr>
</tbody>
</table>

**Attention:** In a cluster, the maximum number of sessions is applied to each node, so the true maximum is the number of nodes multiplied by the maximum sessions value; for example, if your cluster has two nodes and your maximum sessions is set to 5000, then your cluster actually supports a maximum of $2 \times 5000 = 10,000$ sessions.

**About this task**

The procedure that follows sets community-level limits for the maximum number of sessions allowed at one time on a particular server.

Expected state:
- Single server: the Sametime Gateway server is started.
- Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

**Procedure**

1. In the Integrated Solutions Console, click **Sametime Gateway > Communities**.
2. In the "Communities" table, select a community for which you want add or change session limits.
3. Select **Set maximum sessions for the route**.
   - Deselect this option if you do not want to limit the number of instant messaging and presence sessions.
4. Set the maximum sessions for instant messaging by typing an integer.
   - The recommended value is the matching global value divided by the number of external communities, though you may choose a different limits strategy.
5. Set the maximum sessions for presence by typing an integer.
   - The recommended value is the matching global value divided by the number of external communities, though you may choose a different limits strategy.
6. Click **Apply**.
7. Restart the Sametime Gateway server; if you have a cluster of Sametime Gateway servers, restart the cluster.

**What to do next**

**Note:** If you set either (or both) of the community’s session limits to a value higher than the overall global limit, the global limit will still be enforced.
Specifying connection attempts and a time out when connecting with the local Sametime server

You can optionally set properties for when the IBM Sametime Gateway server becomes disconnected from the local Sametime community server. You can set how many times Sametime Gateway should try to connect to the local Sametime community server. Also, you can set the time to wait between attempts to connect.

About this task

When the Sametime Gateway server is disconnected from the Sametime server, by default Sametime Gateway tries to connect for one minute, then stops, then tries again to connect. This process goes on indefinitely unless you change these defaults by creating two custom properties, one for connection attempts and the other for the connection time out.

Procedure

1. In the Integrated Solutions Console, click Sametime Gateway > Communities.
2. In the table that lists communities, click the Local community.
3. On the local community panel, click Custom properties, and then click New.
4. To set the number of connection attempts, in the name field, type Server connection attempts.
5. In the value field, type -1 (to try infinitely), or some other number.
6. Click OK.
7. To set the connection time out, in the name field, type Server connection time out.
8. In the value field, type a number in milliseconds. For example, type 30000 to set the time out to 30 seconds.
9. Click OK.
10. Restart the Sametime Gateway server, or, if you have a cluster of Sametime Gateway servers, restart the cluster.

Related reference

“Custom properties details” on page 159
Use this page to edit custom properties for a community, translation protocol, or message handler. You can also specify new properties that are needed to configure third-party elements used by the IBM Sametime Gateway.

Setting thread pool values

Set the thread pool values for an IBM Sametime Gateway server and the SIP container to improve performance between the SIP container and the Sametime Gateway application server layer. By using a thread pool, server components can reuse existing threads, which helps improve performance by reducing the overhead of creating new threads at run time.

Procedure

1. From Integrated Solutions Console, click Servers > Server Types > WebSphere application servers > RTCGWServer, and then under Additional Properties, click Thread Pools.
2. Click New, and then type a name of your choice, such as STGWPooll, in the Name field.
3. Type 30 in the Minimum Size field.
4. Type 30 in the Maximum Size field.
5. Keep the default value of 5000 for thread inactivity.
6. Click OK, and click Save to save changes to the master configuration.
7. Click Servers > Server Types > WebSphere application servers > RTCGWServer, and under Container Settings, select SIP Container Settings > SIP Container.
8. From the dropdown list of Thread pool, select the thread pool that you just created.
9. Set Maximum dispatch queue size to 5000.
10. Keep the default values of 120000 for Maximum application sessions, and 5000 for Maximum messages per averaging period.
11. Click OK, and click Save to save changes to the master configuration.
12. If Sametime Gateway is clustered, repeat the preceding steps for each node of the cluster.

**Configuring automatic thread dumps for hung processes**

To help troubleshoot hung processes and performance slowdowns, configure your IBM Sametime Gateway servers and XMPP/SIP Proxy servers to generate a thread dump automatically when the servers detect hung threads.

**About this task**

Follow these steps to create a custom property to automatically generate a thread dump when a hung thread is detected. Repeat these steps for each Sametime Gateway and XMPP/SIP Proxy servers. In the case of a clustered environment, repeat these steps on all Gateway servers and XMPP/SIP Proxy servers in the cluster.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click Servers > Server Types > WebSphere application/proxy servers.
3. In the table listing the WebSphere application and proxy servers, click the link representing the proxy server you want to modify.
5. Supply the name of the custom property:
   com.ibm.websphere.threadmonitor.dump.
6. Set the value to true.
7. Click OK, and then click Save to save changes to the master configuration.

**Setting the JVM garbage collection policy**

Set the following required JVM arguments and memory settings for all of your IBM Sametime Gateway server instances. The instructions in this topic are not applicable to any of the SIP Proxy instances you might have.

**About this task**

**Attention:** Do not set the following JVM garbage collection policy on SUN Solaris machines, otherwise you will not be able to start Sametime Gateway.
Procedure

1. From Integrated Solutions Console, click Servers > Application Servers > RTCGWServer.
4. In the Generic JVM arguments field, enter the following value as one continuous line. (It has been formatted with line breaks to fit into this page format.)
   -Xgcpolicy:gencon -Xgc:scvNoAdaptiveTenure,scvTenureAge=8,stdGlobalCompactToSatisfyAllocate
   -Xmn256m -Xverbosegclog:${SERVER_LOG_ROOT}/gc.log,1,14000

   The Generic JVM arguments must be entered as a single continuous line, despite the fact that it might have been broken into several lines due to documentation formatting limitations. If the user this is split into multiple lines, the server will not start up.
5. In the Initial Heap Size field, enter 1500.
6. In the Maximum Heap Size field, enter 1500.
7. Click OK, and click Save to save changes to the master configuration.
8. If IBM Sametime Gateway is clustered, repeat the preceding steps for each node of the cluster.

Setting log files size and rotation

You can specify the maximum size and number of log files to be stored on the server.

Before you begin

Before performing this procedure, make sure you have the required disk space. IBM recommends that the IBM Sametime Gateway server retain a history at least 2 GB in size, to assist with troubleshooting. If you can spare more disk space than that, feel free to set the file ”Maximum Size” (shown in the table below) to more than 20 MB.

About this task

Complete these steps using the Integrated Solutions Console on the Sametime Gateway server where the logs will be stored.

Procedure

1. In the Integrated Solutions Console, click Servers > Server Types > WebSphere application servers > RTCGWServer.
4. Under ”General Properties,” update the following fields both for System.out and System.err sections:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20 MB.</td>
</tr>
</tbody>
</table>
Option Description
Maximum Number of Historical Log Files A value of 2 is the recommended maximum.

5. Click OK.
6. Return to Additional Properties.
8. Click File and update the following fields in the Trace section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20 MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>A value of 15 is the recommended maximum.</td>
</tr>
</tbody>
</table>

9. Click OK.
10. Click Save to save these changes to the master configuration.
11. If Sametime Gateway is clustered, repeat these steps for each node within the cluster.

Related tasks
“Setting a diagnostic trace on Sametime Gateway” on page 251
You can specify how the server handles Sametime Gateway log records. You can select a Sametime Gateway server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Setting threshold warnings for monitoring server load
Set up a warning so that a message appears when the maximum number of subscriptions or instant messaging sessions is approached. This is useful for monitoring server load due to instant messaging and subscriptions.

About this task
Create custom properties that define two threshold values: one for instant messaging sessions, and one for subscriptions. Whenever either of these values is reached, the warning message will appear in the log.

Expected state:
• Single server: the Sametime Gateway server is started.
• Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

Procedure
1. In the Integrated Solutions Console, open the Custom properties page for the server.
   • On a single server: Click Servers > Server Types > WebSphere application servers > server_name > Server Infrastructure > Administration > Custom Properties.
   • On a clustered server: Click System administration > Cell > Command Properties
2. Click New and enter the following information for the subscriptions threshold warning:
3. Click OK to save the new custom property.
4. Click New again, and enter the following information for the instant messaging threshold warning:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>com.ibm.sametime.gateway.max.im.warning.threshold</td>
</tr>
<tr>
<td>Value</td>
<td>A number representing the threshold value (the maximum number of instant messages allowed before the warning message is generated in the log).</td>
</tr>
<tr>
<td>Description</td>
<td>Threshold warning message for maximum instant messaging sessions</td>
</tr>
</tbody>
</table>

5. Click OK to save this new custom property.
6. Restart the Sametime Gateway server; if you have a cluster of Sametime Gateway servers, restart the cluster.

**Tuning the SIP proxy**

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.
   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 -Xgc:con -Xg:noneAdaptiveTenure,tenureAge=8, stdGlobalCompactToSatisfyAllocate -Xgc:parallel`
   g. Click OK, and click Save to save changes to the master configuration.
Resolving email addresses as Sametime IDs more efficiently

You can configure a custom Java class filter to ensure the efficient resolving of email address as IBM Sametime IDs (STId).

About this task

When you process an external user request to interact with an internal user, the Sametime Gateway requests that the Sametime Community Server interpret (resolve) the internal user's email address as the internal user's Sametime ID (STId). The Sametime Community Server resolves the STId, by searching LDAP with the user's email as the search filter. Multiple simultaneous queries could lead to a performance issue. Sametime Gateway is expected to report slow resolve behavior with messages like the following one:

```CLFRC0268W
Performance warning: The resolve operation: Email --> STId {0} --> {1}
took {2} seconds to complete. Review your community server and/or LDAP configuration, and consult the Sametime Gateway Infocenter. Awaiting {3} more resolve requests to complete.
```

Procedure

To ensure an effective LDAP search, verify that you have a configured a custom Java class that can generate an efficient email to STId LDAP search. Using the Sametime Community Server default LDAP search leads to degraded performance caused by a full scan of the LDAP tree. The example `StLdapCustomized` class described in Creating custom Java classes for searching the LDAP provides an efficient way to resolve email to STId. You might also consider limiting the base DN in which to search. See one of the steps in Sametime prerequisite: Connecting to an LDAP server on configuring a base DN.

What to do next

As an additional step for optimizing the LDAP searches on the Community server, you can also include or exclude certain domains from user and group directory lookups.

Tuning a WebSphere proxy server

This section contains procedures for tuning a WebSphere proxy server that is used by a cluster of IBM Sametime servers running on WebSphere Application Server.

About this task

Note that this section is not referring to the SIP Proxy, but rather to a WebSphere proxy server.

Disabling the proxy read-ahead mechanism on the WebSphere proxy server

You can disable the read-ahead mechanism on the IBM WebSphere proxy server to resolves a HIGH CPU issue that occurs when terminating connections with read-ahead enabled.

Procedure

1. Log in to the Integrated Services Console.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
4. Under **Proxy Settings**, expand **HTTP Proxy Server Settings**.
5. Click **Proxy settings**.
6. Under **Additional Properties**, click **Custom properties**.
7. Click **New** to create a custom property.
8. Specify the **Name** of the new property as `http.connectionPoolReadAheadEnabled`.
9. Set the **Value** of the new property to `false`.
10. Click **New** to create another custom property.
11. Specify the **Name** of the new property as `dynacache.extension.lookup_timeout_property`.
12. Set the **Value** of the new property to `20000`.
13. Click **Apply**, and then click **Save**.

**Adjusting the WebSphere proxy server thread pool settings**

Increase the WebContainer thread pool settings of the IBM WebSphere proxy server to match the same settings as the IBM Sametime Meeting Server.

**About this task**

A thread pool lets servers reuse threads instead of creating new threads at runtime.

**Procedure**

1. Log in to the Integrated Services Console.
2. Click **Servers** > **Server Types** > **WebSphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
4. Under **Additional Properties**, click **Thread pools**.
5. Click **Proxy**.
6. Under **General Properties**, make sure the **Minimum Size** and **Maximum Size** are both set to `50` threads.
7. Click **Apply**, and then click **Save**.

**Setting JVM verbose garbage collection and heap sizes on the Websphere proxy server**

In order to monitor IBM WebSphere Application Server JVM heap for specific applications, enable the JVM verbose garbage collection logging for the WebSphere Application Servers.

**Procedure**

1. Log in to the Integrated Solutions Console.
2. Click **Servers** > **Server Types** > **WebSphere proxy servers**.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
5. Click **Process definition**.
6. Under **Additional properties**, click **Java Virtual Machine**.
7. Under General Properties, make sure the Verbose garbage collection check box is cleared.
8. Under General Properties, make sure the Initial heap size is set to 512MB.
9. Under General Properties, make sure the Maximum heap size is set to 1024MB.
10. Click Apply, and then click Save.

Extending the HTTP persistent timeout on the WebSphere proxy server

You can extend the HTTP persistent timeout on the IBM WebSphere proxy server to stay connected longer.

Before you begin

About this task

The default rtc4web timeout value is 30 seconds. This is the default timeout for the WebSphere proxy server persistent timeout setting, too. This can causes a rare condition to occur where both sides of the connection can let go at the same time. In order to minimize this conflict, extend the WebSphere proxy server HTTP Persistent timeout to stay connected longer.

Procedure

1. Log into Integrated Solutions Console on the server where the WebSphere proxy server is configured.
2. Click Servers > Server Types > WebSphere proxy servers.
3. In the table listing the WebSphere proxy servers, click the link representing the proxy server you want to modify.
4. Under Proxy Settings, expand the HTTP Proxy Server Settings tree.
5. Click Proxy server transports.
6. Click HTTP_PROXY_CHAIN. It should be associated with port 80.
7. Click HTTP inbound channel (HTTP 3).
8. Under General Properties, set the Persistent timeout to 60 seconds.
9. Click Apply, and then click Save.
10. Click Servers > Server Types > WebSphere proxy servers.
11. Click the name of the proxy server.
12. Under Proxy Settings, expand the HTTP Proxy Server Settings tree.
13. Click Proxy server transports.
14. Click HTTPS_PROXY_CHAIN. It should be associated with port 443.
15. Click HTTP inbound channel (HTTP 4).
16. Under General Properties, set the Persistent timeout to 60 seconds.
17. Click Apply, and then click Save.
18. Repeat for every WebSphere proxy server that you configured for the cluster.
Chapter 3. Troubleshooting

When users or servers are having problems with IBM Sametime, administrators take steps to find and solve problems as quickly as possible.

This section contains information about troubleshooting and logging tools that can help you debug and fix problems affecting servers or users.

Other sources of information

Use the following links to find other hints and tips when troubleshooting Sametime servers:

- Sametime wiki:
  www.lotus.com/idd/stwiki.nsf/
- Support Portal for Sametime:
  http://www.ibm.com/software/lotus/support/sametime/support.html
- Tech Notes for Sametime Gateway:
  www.ibm.com/support/search.wss?q=Sametime%20Gateway&rs=477&tc=SSKTXQ&dc=DB520&dtm

Troubleshooting Sametime clients

Use the following information to troubleshoot problems with IBM Sametime Connect and browser-based clients.

Logging and tracing on Sametime Connect

IBM Sametime Connect users can enable tracing on their clients.

1. On the machine where you use the Sametime Connect client, open the .config/rcpinstall.properties file in a text editor.
   To locate your Sametime workspace, see the topic Locating the Sametime Connect workspace
2. Add the following lines to the end of the file, depending on what kind of issue you're diagnosing.
   General client issues:
   com.ibm.collaboration.realtime.level=FINE
   Telephony and audio/video issues, including Sametime Unified Telephony and Meetings:
   General issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.tcspi.level=FINEST
   com.ibm.collaboration.realtime.multimedia.level=FINE
   Audio/video quality issues:
   com.ibm.collaboration.realtime.internal.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.level=FINE
   com.ibm.collaboration.realtime.telephony.softphone.level=FINER
   com.ibm.collaboration.realtime.multimedia.level=FINER

   Note: In Sametime 8.5.1, the last line above will generate a substantial number of large audio/video trace files in your Sametime logs directory. During audio/video or Sametime Unified Telephony softphone calls, you might get 10
MB of tracing or more for each minute of the call. Do not use that level unless you have been instructed to do so and have ample free space on your hard drive.

**Instant messaging issues:**
- `com.lotus.sametime.community.kernel.level=FINER`
- `com.lotus.sametime.im.level=FINEST`
- `com.lotus.sametime.places.level=FINEST`
- `com.ibm.collaboration.realtime.rtcadapter.level=FINEST`
- `com.ibm.collaboration.realtime.people.internal.level=FINE`
- `com.ibm.collaboration.realtime.internal.sametime.level=FINER`
- `com.ibm.collaboration.realtime.login.level=FINEST`
- `com.ibm.collaboration.realtime.community.internal.level=FINEST`

**Login issues:**
**General login failures:**
- `com.ibm.collaboration.realtime.community.internal.level=FINEST`
- `com.ibm.collaboration.realtime.im.community.level=FINEST`
- `org.apache.commons.httpclient.level=FINE`
- `com.ibm.rcp.internal.security.auth.module.level=FINEST`
- `com.ibm.collaboration.realtime.login.level=FINEST`
- `com.ibm.rcp.internal.security.level=FINEST`
- `com.ibm.rcp.security.level=FINEST`

**SSO failures:**
- `com.ibm.collaboration.realtime.community.internal.level=FINEST`
- `com.ibm.collaboration.realtime.im.community.level=FINEST`
- `org.apache.commons.httpclient.level=FINE`
- `com.ibm.rcp.internal.security.auth.module.level=FINEST`
- `com.ibm.collaboration.realtime.login.level=FINEST`
- `com.ibm.rcp.internal.security.level=FINEST`
- `com.ibm.rcp.security.level=FINEST`

**Managed settings:**
- `com.ibm.collaboration.realtime.policy.sametime.managedsettings.level=FINEST`

**Meetings:**
**General issues:**
- `com.ibm.rtc.meetings.level=FINER`
- `com.ibm.rtc.spaces.level=FINEST`
- `com.ibm.collaboration.realtime.appshare.level=FINEST`
- `com.ibm.rtc.core.level=FINER`
- `com.ibm.sharedmaps.level=FINER`

**Calendar integration issues:**
- `com.ibm.rtc.meetings.servers.level=FINEST`
- `com.ibm.rtc.meetings.shelf.level=FINEST`
- `com.ibm.rtc.meetings.shelf.ui.level=FINEST`
- `com.ibm.rtc.meetings.util.level=FINEST`
- `com.ibm.collaboration.realtime.calendar.level=FINEST`
- `com.ibm.collaboration.realtime.calendar.notes.level=FINEST`

**Connectivity issues:**
- `com.ibm.rtc.core.level=FINEST`
- `com.ibm.rtc.spaces.level=FINEST`

**Screen sharing issues:**
- `com.ibm.rtc.meetings.appshare.level=FINER`
- `com.ibm.collaboration.realtime.appshare.level=FINER`

**Document sharing/conversion issues:**
- `com.ibm.rtc.meetings.documents.level=FINER`
- `com.ibm.rtc.meetings.appkit.image.level=FINER`
- `com.ibm.workplace.converter.level=FINER`

3. Save and close the file.
4. Restart your Sametime Connect client.
5. View the error log and trace files in Sametime Connect, by clicking Help > Support > View Log and View Trace.
   In most cases, View Trace provides the most useful information.

6. (Optional) If you need to provide logs to someone else for diagnostics, you can use IBM Support Assistant to collect logs and other data.
   For the Sametime 8.5.2 Connect standalone client and Lotus Notes 8.5.2:
   a. Click Help > Support > Collect Support Data.
      After a few moments, the Collect Support Data dialog opens.
   b. Click Next to start the collection. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   c. Send the zip file to the person diagnosing the problem.
   For Lotus Notes 8.5.x:
   a. Click Help > Support > IBM Support Assistant.
   b. Select the Collect Data tab.
   c. Under Lotus Notes 8.5.x, select Notes General Problem Data Collection and click Add.
   d. Click Collect All to start the collection.
   e. When you are prompted for a reason, enter a descriptive response, and click OK.
   f. When you are prompted about collecting the .metadata directory, click OK.
   g. When the collection completes, a link to the collection zip file appears in the Collect Support Data dialog.
   h. Send the zip file to the person diagnosing the problem.

Alternate logging and tracing (standalone client only)

If you are using the standalone IBM Sametime Connect client for Release 8.5.1 or later, you can use IBM Support Assistant to enable or disable logging for certain client components. You can also do this with the Sametime Connect 8.5 Connect client, but the procedure is different. This procedure gives you the opportunity to reproduce the issue during the collection process, optionally restarting the client if that’s required to reproduce the problem. Although this procedure method doesn’t provide as much control over logging as the procedure above, it does not require restarting your client in order to enable/disable logging. The Lotus Notes embedded client does not provide the ability to enable or disable logging for individual Sametime components.

1. Click Help > Support > Collect Support Data. After a few moments, the Collect Support Data dialog opens.
2. Click the Customize link. The Collect Data - Sametime dialog displays.
3. Expand the Sametime Connect node in Collector Selection and select Sametime Connect Custom Tracing, then click Add to add custom tracing to the Collector Queue.
4. Click Collect All. After a few moments, the User Input dialog opens.
5. Select up to three components to collect tracing data.
6. Click OK and follow the instructions on the screen to complete the data collection.
7. When the collection completes, a link to the collection zip file appears on the dialog. You might have to scroll down in the dialog to see the link.
Locating the Sametime Connect workspace

Both IBM Sametime Connect and IBM Lotus Notes store user-specific data, including configuration data, preferences, and trace logs, in a workspace folder on your local hard drive or a network drive. In order to diagnose Sametime Connect issues, you might be asked to update or collect files in your workspace.

About this task

The workspace location varies depending on whether you are using the standalone Sametime Connect client or Lotus Notes, the operating system, and the product release. This topic helps you locate your workspace.

Sametime Connect standalone client

This release of Sametime Connect uses the following default workspace locations:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 and Vista</td>
<td>C:\Users\user_name\AppData\Roaming\Lotus\Sametime</td>
</tr>
<tr>
<td>Microsoft Windows XP</td>
<td>C:\Documents and Settings\user_name\Application Data\Lotus\Sametime</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/Sametime</td>
</tr>
<tr>
<td>Linux (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Sametime Data</td>
</tr>
<tr>
<td>Mac OS (upgrade older client)</td>
<td>~/Lotus/Sametime</td>
</tr>
</tbody>
</table>

Note: If you upgrade an older Sametime Connect 8.x client to this release, the existing workspace location is used, rather than the default workspace location.

Lotus Notes

Lotus Notes stores the workspace in the Notes data directory. For Notes 8.5.1 and later releases, the default workspace locations are:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows (single-user client)</td>
<td>C:\Program Files\IBM\Lotus Notes\Data\workspace</td>
</tr>
<tr>
<td>Linux</td>
<td>~/lotus/notes/data/workspace</td>
</tr>
<tr>
<td>Mac OS</td>
<td>~/Library/Application Support/Lotus Notes Data/Expeditor/Applications</td>
</tr>
</tbody>
</table>

For Microsoft Windows, the location of the Notes data directory varies depending on whether the client is single user or multi user, whether you're upgrading an existing client or installing a new one, and which version of Windows you're using. For more information, see Notes installation directories for Windows in the Lotus Notes information center.
Troubleshooting audio and video in the Sametime Connect client

Enable diagnostics for audio and video in the IBM Sametime Connect client to assist with troubleshooting issues.

About this task

The following properties can be appended to the rcpinstall.properties file to enable audio and video diagnostic information. Find the file in the following location:

Microsoft Windows

In Microsoft Windows, this file is stored in the following directory: C:\Documents and Settings\user\Application Data\Lotus\Sametime\config\rcpinstall.properties.

Linux

home_dir/Lotus/Sametime/.config/rcpinstall.properties

Mac OS X

$HOME/Library/Application Support/Lotus Sametime Data/.config/rcpinstall.properties

The properties are listed by priority; they should not all be enabled at the same time.

# use for basic audio/video session troubleshooting
com.ibm.collaboration.realtime.multimedia.phonegrid.internal.client.level=FINE
# only use for ICE troubleshooting
com.ibm.ice.level=FINE
# only use for SIP troubleshooting
com.ibm.collaboration.realtime.telephony.softphone.level=FINE

The following notes about audio and video in the IBM Sametime Connect client can help you with issues raised by users.

Audio video call incompatibility

Sametime 8.5 and later releases require the Sametime Media Manager for computer audio and video calls. In order to participate in audio or video calls, all parties must be using Sametime 8.5 or later clients, and must be logged in to a Sametime 8.5 or later server configured with the Sametime Media Manager.

Troubleshooting the Sametime web audio-visual plugin

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

Enabling diagnostics for audio and video in the Sametime web audio-visual plugin

Enable diagnostics for audio and video for the IBM Sametime web audio-visual plugin to assist with troubleshooting.
About this task

The following logs help you and IBM Support troubleshoot and debug issues with the Sametime Web audio-visual plugin:

- UI traces
- Client logs
- Server logs

UI traces

To enable the UI traces for JavaScript processing, append the following parameters to the meeting or meeting room URL in the browser’s address bar:

?stmeetingsDebugLevel=debug&stmeetingsDebugScope=all

Client logs

Logs for the Sametime web audio-visual plugin are stored in the following locations:
- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

The logging level is set with the LogFileLevel parameter in the WebPlayer.ini file. Logging level options are:
- 0 (default - no log information)
- 2 (errors only)
- 8 (errors and traces)
- 16 (maximum level of errors, traces, and notifications)

Find the WebPlayer.ini file in the following location:
- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/

ICE diagnostics

Enable diagnostics on the use of ICE with the log_level setting in the ice.properties file. The trace level fine is sufficient. Trace options are:
- fine
- finer
- finest

Find the ice.properties file in the following location:
- Microsoft Windows XP: %PROGRAMFILES%\IBM\Lotus\Sametime WebPlayer\
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/
GIPS Debug Trace

Set the GIPSDebugTraceEnable variable to true in the preferences.ini file.

Find the preferences.ini file in the following location:

- Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone
- Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Plugins\stwebsoftphone
- Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Plugins/stwebsoftphone

Additional troubleshooting tools

Macintosh client running Firefox

Install XCode on the client machine, then install gdb, the GNU Project Debugger.
1. In a command window, type gdb and press Enter.
2. Type attach Firefox and press Enter.
3. Type c to continue.
4. When the browser crashes, type bt or backtrace and press Enter.
5. Copy all the traces into a file and include it in a Support request.
6. Type detach and q to exit.

Windows client

For Windows clients, running Internet Explorer 6 or 7, first try installing and using WinDBG, the Windows debugging tool available from Microsoft.
1. Start Internet Explorer.
2. Start WinDBG and use the File - Attach to a Process menu command to attach to the Internet Explorer process.
3. When a crash occurs, use View - Stack Trace to see the stack trace. Save the file as a .dmp file and include it in a Support request.

If WinDBG is changing the timing and not reproducing the crash, install and run the usercoredump.exe instead. Instructions are in this Microsoft Support article: How to use the Userdump.exe tool to create a dump file.

Install the program as described here: http://www.microsoft.com/downloads/details.aspx?FamilyID=E089CA41-6A87-40C8-BF69-28AC08570B7E&displaylang=en

Unless you have a specific need, disable the "dump on process termination" feature when you run the Setup.exe program.

Capture debugging information with one of these two methods:

- Set up user dump rules in advance.
  1. Go to the Control Panel and double-click Process Dump.
  2. Click New.
  3. Add Firefox.exe.
  4. Select Firefox and click Rules.
  5. Add a custom rule with the following selections:
Select c:\crashdump as the Dump file folder. Leave the default Exception Codes and select **Ignore exceptions that occur inside Kernel32.dll**. Set the MinDump Type as **Complete** and Save Mode as **Overwrite**. Do not select anything else.

6. Repeat the previous steps to add a custom rule for Iexplorer.exe.

- Capture process information after a crash.
- When the program stops responding, move to the version of Userdump.exe for your processor at the command prompt, and then type the following command:
  
  `userdump PID`

  where *PID* is the process ID (PID) of the program that has stopped responding. To obtain the PID of the program, open Task Manager, and then click the **Process** tab.

The user dump file is generated in the c:\crashdump folder and can be included in a Support request.

**Related concepts**

“Log file locations” on page 283

Use this reference to locate log files for IBM Sametime components.

**Related tasks**

“Enabling logging and tracing for a Sametime Proxy Server” on page 238

The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.

“Setting a diagnostic trace on a Sametime Media Manager server” on page 239

You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Troubleshooting issues with the Sametime web audio-visual plugin**

Consider these guidelines to help users troubleshoot the IBM Sametime web audio-visual plugin.

**Installing the plugin**

- The plugin works only with Internet browser (32-bit) on supported 32-bit or 64-bit operating systems (32-bit certifications only).
- The plugin can be installed on the client by any user. If the plugin is installed under the Administrator account, verify that the plugin installed into %WINDIR%\Downloaded Program Files folder, then uninstall the plugin and install the plugin again without using the administrator account.
- If a new profile is created for Firefox on a Mac client at a non-default location, the plugin installation will not succeed. Modify the path to an absolute path for newly created profiles in the Firefox profiles.ini file.

**Issues with using the plugin**

The meeting moderator sees the “Waiting for moderator” message in the Conferencing Panel upon entering his or her own meeting room.

  Clear the browser’s cache, restart the browser, and then join the meeting again.
The message “Video Starting” appears, but the call does not start.

Take the following steps to ensure the connection can be completed:

1. Make sure that only one browser instance (tab or window) is opened for the Sametime Meeting Room client (a Sametime client cannot attend multiple meetings at the same time).
2. Exit the client.
3. On the client workstation, check the sip.log file to determine whether the client was able to register with the SIP Proxy and Registrar.
   - Find the log in the Logs directory:
     - Microsoft Windows XP: %APPDATA%\IBM\Lotus\Sametime WebPlayer\Logs
     - Windows Vista and Windows 7: %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\Logs
     - Mac OS X: $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer/Logs
       a. Look for a “200 OK” message from the SIP Proxy and Registrar.
       b. Search for “Message In -> SIP/2.0 200 OK” and “CSeq: 1 REGISTER”:
          - If the “200 OK” message was received from the SIP Proxy and Registrar, then check the Sametime Proxy Server log for an indication of why the client registration failed.
          - If there was no “200 OK” message received from the SIP Proxy and Registrar, then verify that the client can telnet to the server as described in the next step.
4. Test the telnet connection to the SIP Proxy and Registrar server by opening a command prompt on the client workstation and running the following command:
   - telnet SIP_hostname_or_IPaddress port
     for example:
     - telnet 10.10.10.10 5080
     - If the client can telnet to the server, check whether the SIP Proxy server received the REGISTER request (using a network sniffer or WebSphere traces).
     - If the client cannot telnet to the server, check your network connections.

The user's status disappears in the meeting room.

Refresh the page or exit and then re-enter the meeting.

If remote video is not rendering and a user pauses the video, “Hide My Video” does not hide the local video.

Refresh the page or exit and then re-enter the meeting.

The audio-video plugin may experience problems if Gmail, Skype, or Net Meeting applications are running.

For best results, exit those applications before entering the Sametime meeting room.

IE6 and IE7 performance deteriorates if a user leaves and rejoins an audio-visual call multiple times in multiple-window mode.

Run the meeting room client in single-window mode.

If a user attempts to join the same meeting from two types of clients, the attempt from the second client will be unsuccessful.

Leave the Meeting room from one client before joining the other.
Audio and video are not working as expected.
Make sure that the appropriate latest sound and video device drivers are installed on the client machine.

The user sees a Conferencing Panel disabled in an A/V-enabled Meeting room or does not see live names.
Refresh the browser page. If that does not correct the problem, contact the administrator to make sure all Sametime servers are running and configured properly.

Troubleshooting meeting invitations
If users at your site are having difficulty inviting other users to meetings, verify the host name for the meeting room in their client preferences.

About this task
If a user enters a value for a server preference that is not a fully qualified host name, then the users that he or she invites into meetings might not be able to attend.

Procedure
1. In the IBM Lotus Sametime Connect client, click File > Preferences...
2. In Preferences, click Server Communities.
3. Click the host name for the server community that hosts the meeting room.
4. Click the Server tab.
5. Verify that the host name is fully qualified.
   For example, it should be messaging.yourcompanya.com and not messaging.
6. If it is not a fully qualified host name, click Server Communities and remove the server community and re-add with the correct host name.
7. Click OK.

Resolving problems with business cards
If Business Cards are not displaying user information as expected, check the server configuration, then the client, and finally, the business cards themselves.

Checking the server configuration
Check and validate the configuration on the storage repository you use with the Sametime Community Server. A configuration problem is the most likely cause of problems with Business Cards. For more information, see the appropriate section in Managing business cards.

Checking the UserInfo servlet on the client
The UserInfo servlet on the client receives and responds to client requests. The servlet must be working correctly to provide the requested details for Business Cards. Follow these steps to verify that the UserInfo servlet is responding correctly.
1. Determine the distinguished name (DN) of the user whose Business Card you want to view. Here are sample DNs of the various directory types:
   - Domino directory: cn=sametime User/O=IBM
   - Active directory: cn=Sametime User, cn=users,dc=austin,dc=ibm,dc=com
   - TDS directory: uid=Sametime user,ou=Austin,o=IBM
2. Compose a URL to simulate the HTTP request that the client makes to retrieve details for a Business Card:

- [protocol]://[hostname]/servlet/UserInfoServlet?operation=3&setid=1&UserId=[User DN]
- [protocol] = {http, https}
- [hostname] = {Fully qualified hostname of the Sametime server}
- [User DN] = {The full distinguished name of the user for whose information you are seeking}

Examples:
- Domino Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/O=IBM
- Active Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User, cn=users, dc=austin, dc=ibm, dc=com
- TDS Directory:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=uid=Sametime user, ou=Austin, o=IBM

Note:
- Do not use spaces in the URL for the UserInfo servlet operation. A space is translated into %20 in the URL, and the servlet will not produce a result; for example:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime User/O=IBM

  is translated to:
  http://sametime.ibm.com/servlet/UserInfoServlet?operation=3&setid=1&userId=cn=Sametime%20User/O=IBM

  . The characters "%20" are inserted before the word "User" to represent the space.
- The name "UserInfoServlet" is case sensitive.
- Do not use apostrophes or quotation marks in the URL.

3. Enter the URL you’ve composed into a web browser’s address field, and view the result.

You should see the details you are expecting to see. If you do not, enable tracing for the UserInfo servlet as described in UserInfoConfig Debug tracing.

An UNKNOWN error for the "user id" means the user ID specified could not be located. The most common reasons for this error are:
- An incorrect user distinguished name has been specified
- The directory in which the user is located is not reachable/searchable

Checking the client

If the UserInfo servlet on the client is responding correctly, enable client-side tracing to determine what is happening on the client. Follow the instructions in Logging and tracing on Sametime Connect.
Checking that Business Cards meet requirements

Finally, verify that the business cards follow these requirements.
- Photos must be less than 45 kilobytes (recommended: 10 kb).
- Business Card photo requires .jpg or .gif.
- Using the jpegPhoto LDAP attribute to store photos requires the inetOrgPerson objectClass.

Note: Active Directory 2000 native/mixed mode does not provide inetOrgPerson objectClass by default.
- When you are using more than one storage type to store user information, the secondary storage repository cannot be of the same TYPE as the primary storage (the directory used by Sametime for authentication). For example, if Sametime is configured to use the Domino directory, then the secondary storage cannot also be a Domino directory.

Troubleshooting a Sametime System Console

Use the following topics to troubleshoot problems in an IBM Sametime System Console.

Sametime System Console log locations

The following table shows you where to find IBM Sametime System Console logs.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Solutions Console administration logs</td>
<td>was_install_root\profiles\STSCDMgrProfile\logs</td>
</tr>
<tr>
<td>Find WebSphere Application Server-specific logs. The majority of messages that administrators are interested in are here.</td>
<td></td>
</tr>
<tr>
<td>Sametime System Console server logs</td>
<td>was_install_root\profiles\STSCAppProfile\logs</td>
</tr>
<tr>
<td>Find logs for the application server of the cell profile of the console.</td>
<td></td>
</tr>
<tr>
<td>Sametime System Console client registration utility</td>
<td>system_console_install_location\console\logs</td>
</tr>
<tr>
<td>Find logs for the product server registration into the console. This post-registration utility refers to product servers as being clients of the console.</td>
<td>For example: c:\WebSphere\STSeringCell\Console\logs</td>
</tr>
<tr>
<td>Product installation log for installer</td>
<td>temp\SSClogs</td>
</tr>
</tbody>
</table>

Determining Sametime server status using the Integrated Solutions Console

You can use the Integrated Solutions Console to determine if an IBM Sametime Meeting Server, Proxy Server, or Media Manager is running.

About this task

You should verify the node agent, the server, and installed applications are running.
Procedure
1. Log in to the Integrated Solutions Console.
2. Click System Administration > Node agents.
3. Locate the node for your server and verify that the Started indicator is displaying in the Status column.
4. Click Servers > Server Types > WebSphere application servers.
5. Locate your server and verify that the Started indicator is displaying in the Status column.
6. Click Applications > Application Types > WebSphere enterprise applications.
7. Locate your resource and verify that the Started indicator is displaying in the Application Status column.

What to do next
To start a server or node, see Starting and stopping servers from the Sametime System Console.

The console.properties file
The console.properties file contains settings used to register an IBM Sametime server with the Sametime System Console. This file is used with both IBM WebSphere-based servers and IBM Lotus Domino-based servers.

Sample settings for registering a Sametime server with the Sametime System Console:

#Specify the fully qualified host name for Sametime System Console
SSCHostName=ssc.in.ibm.com

#SSC WAS credentials
SSCUserName=wsadmin
SSCPassword=password

#Specify true if you want to connect to Sametime System Console server using Secure Connection, else false.
SSCSSLEnabled=true

#Specify the HTTP port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.
SSCHTTPPort=9080

#Specify the Secure Https port to Connect, can be found in <WAS_installRoot>/profiles/<profileName>/logs AboutThisProfile.txt.
SSCHTTPSPort=9446

#The log level for the Sametime System Console Client logs
# INFO - Information logs
# FINE - Information logs as well as severe messages
# FINEST - ALL logs (recommended)
LogLevel=FINEST

The productConfig.properties file for WebSphere-based servers
The productConfig.properties file contains settings used to register an IBM Sametime server running on IBM WebSphere with the Sametime System Console.
Sample settings for registering a WebSphere-based Sametime server with the Sametime System Console; settings will vary depending on the server and your own environment.

#ProductType - It specifies the type of product Installed
#Community Server - com.ibm.lotus.sametime.communityserver
#Proxy Server - com.ibm.lotus.sametime.proxyserver
#Media Server - com.ibm.lotus.sametime.mediaserver
#Gateway Server - com.ibm.lotus.sametime.gatewayserver
#Meeting Server - com.ibm.lotus.sametime.meetingserver
ProductType=com.ibm.lotus.sametime.meetingserver

# OfferingVersion = Version of the Installed Server
OfferingVersion=8.5.0.0

#InstallType- Installation Type - PN, SN, DM or Cell (WAS based Product) . For Domino Based STNODE.
InstallType=Cell

#DepName = Specify a unique Deployment Name with which you want to register the server.
DepName=Meeting Server 85

#MeetingInstallLocation - The location where the Product Specific files are copied.
#ProxyInstallLocation=C:\Program Files\IBM\Websphere\STPServerCell
#MediaInstallLocation=C:\Program Files\IBM\Websphere\MediaServerCell
#SSCInstallLocation=C:\Program Files\IBM\Websphere\STSCServerCell
#GatewayInstallLocation=C:\Program Files\IBM\Websphere\STGWServerCell
MeetingInstallLocation=C:\Program Files\IBM\Websphere\STMServerCell

#NodeIP- The IP of the machine on which the product server is installed
NodeIP=9.126.186.45

#NodeHostName- The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com

###WAS##
# Was Credentials - User Name and Password of Product Was server
WASUserID=wsadmin
WASPassword=wsadmin

#WASInstall - The root location where WAS is installed.
WASInstall=C:\ibm\WebSphere\AppServer

#WASSoapPort - The Soap Connector address for product WAS
WASSoapPort=8503

#WASHost - The hostname of the machine on which WAS is installed.
WASHost=myserver.abc.com

#WasCell - The Cell name of the Was Default profile
WASCell=myServerCell

#WASDMNode - The Node name of the Deployment Manager profile
WASDMNode=myServerDMNode

#WASNode - The Node name of the Secondary Node profile
WASNode=myServerNode

#WASAppProfile - The Appserver Profile name (Primary Node/Secondary profile)
WASAppProfile=STMAppProfile

#WASAppServerName - The servername for the AppServer profile.
WASAppServerName=STMeetingServer

#WASDMProfile - The Dmgr Profile name (DM profile)
WASDMProfile=STMDMgrProfile

#WASDMServerName - The servername for the DM profile
WASDMServerName=dmgr

#WASSNProfile - The SN profile name
WASSNProfile=STMSNProfile

#WASDMSoapPort - The Soap Connector address for DM Profile
WASDMSoapPort=8503

#WASDMHost - The Deployment Manger host name
WASDMHost=hare.abc.com

#PreRequisite Database Details
#DBHost - The hostname of the DB used by product.
DBHost=9.122.64.26

#DBPort - The port on which the database server listens
DBPort=50000

#DBAppID - The application username for Database server
DBAppID=db2inst1

#DBAppPassword - The application password for Database server
DBAppPassword=passw0rd

#DBName - The database Name used by the product
DBName=testDB

#PreRequisite Ldap Details
#LDAPHost - The hostname of ldap registered with the product.
LDAPHost=bluepages.ibm.com

#LDAPPort - The port of ldap registered with the product.
LDAPPort=389

#LDAPBindAnonymous - Is anonymous access allowed for ldap registered with the product.
LDAPBindAnonymous=true

#LDAPBindDN - The Bind Distinguished name for ldap registered with the product.
LDAPBindDN=cn=root

#LDAPBindPwd - The Bind password for ldap registered with the product.
LDAPBindPwd=password

#LDAPType - The Type of ldap registered with the product.
LDAPType=IDS6

#LDAPLoginField - The LoginField of ldap registered with the product.
LDAPLoginField=mail;cn;uid

#LDAPBaseDN - The search base of ldap registered with the product.
LDAPBaseDN=o=abc.com

#LDAPDisplayName - The display name of ldap registered with the product.
LDAPDisplayName=cn
# LDAPPersonObjectClass - The object class of ldap registered with the product.
LDAPPersonObjectClass=Person
# LDAPSSLEnabled - Specifies if configured LDAP is SSL enabled.
LDAPSSLEnabled=false
# PreRequisite Community Server Details
# STCommunityServerHost - The hostname of the community server registered with the product.
STCommunityServerHost=xyz.abc.com
# STCommunityServerPort - The Community server port which registered with the product.
STCommunityServerPort=1516
# ConferenceFocusHost - The Conference Focus server hostname used by media server
ConferenceFocusHost=stdev3.abc.com
# ConferenceFocusPort - The WAS SIP port for Conference Focus
ConferenceFocusPort=5063
# AVPacketSwitcherHost - The Packet Switcher server hostname used by media server
AVPacketSwitcherHost=stdev3.abc.com
# AVPacketSwitcherPort - The port for Packet Switcher.
AVPacketSwitcherPort=5063
# ProxyRegistrarHost - The Proxy Registrar server hostname used by media server
ProxyRegistrarHost=stdev3.abc.com
# ProxyRegistrarPort - The port for Proxy Registrar
ProxyRegistrarPort=5080
# ComponentName - The component installed on the Media Server
ComponentName=Complete
# AVPacketSwitcherServerName - The WAS server name for media server.
AVPacketSwitcherServerName=STMediaServer
# AVPacketSwitcherSwitchId - It's a combination of "AVPacketSwitch" + NodeName.
AVPacketSwitcherSwitchId=PacketSwitchamalvadkMediaNode
# STReflectorHost - The SameTime reflector host
STReflectorHost=
# STReflectorPort - The SameTime reflector port
STReflectorPort=
# STMeetingServerHost - The Meeting server host name
STMeetingServerHost=
# ConsoleDBHost - The hostname of the DB used by System Console Server
ConsoleDBHost=amalvadk.in.ibm.com
# ConsoleDBPort - The port on which the System Console database server listens
ConsoleDBPort=50000
#ConsoleDBAppID - The application username for System Console Database server
ConsoleDBAppID=db2inst1

#ConsoleDBAppPassword - The application password for System Console Database server
ConsoleDBAppPassword=passw0rd

#ConsoleDBName - The database Name used by the product
ConsoleDBName=SSCDB

SSCEnabled - Specifies if the product is installed via SSC or not.
SSCEnabled=FALSE

#DBType=Specifies the type of DB2 or DB2_iseries.
DBType=DB2

The productConfig file for the Sametime Community server

The productConfig.properties file contains settings used to register an IBM Sametime Community Server with the Sametime System Console. This file is used only with the Sametime Community Server; a different copy of the file is used for IBM WebSphere-based servers.

Purpose

Example settings for registering a Sametime Community server with the Sametime System Console:

#ProductType - It specifies the type of product Installed
#Community Server - com.ibm.lotus.sametime.communityserver
#Proxy Server - com.ibm.lotus.sametime.proxyserver
#Media Server - com.ibm.lotus.sametime.mediaserver
#Gateway Server - com.ibm.lotus.sametime.gatewayserver
#Meeting Server - com.ibm.lotus.sametime.meetingserver
ProductType=com.ibm.lotus.sametime.communityserver

# OfferingVersion = Version of the Installed Server
OfferingVersion=8.5.0.0

#InstallType-Installation Type -PN,SN,DM or Cell (WAS based Product) . For Domino Based STNODE.
InstallType=STNODE

#DepName = Specify a unique Deployment Name with which you want to register the server.
DepName=Comm Server

#NodeHostName- The fully qualified Hostname of the machine on which the product is installed
NodeHostName=myserver.abc.com

Troubleshooting clustering

This section describes how to troubleshoot problems with clustering servers in IBM Sametime.

Each of the WebSphere-based Sametime products is installed with an SSCConnetcer servlet, which starts an mbean that allows the Sametime System Console to initiate a limited number of remote configuration commands before the Sametime product is federated into the WebSphere cell of the Sametime System Console. During the clustering process, this mbean is contacted, and the application initiates the addNode command, which starts the federation process. During this process, the Primary Node's server where the mbean is running stops. This is required in order to federate properly. As a result, the Sametime System Console actually has no communication with the Primary Node during the federation process.
The Sametime System Console tests as many factors as possible to ensure that the federation succeeds prior to actually running the `addNode` command, and gives the user a warning if one of these conditions is found. Once the `addNode` command is initiated, the Sametime System Console begins polling the Deployment Manager configuration at intervals until it detects that the Primary Node's configuration has been added successfully. Once it determines it has been successfully added, it alerts the administrator that the federation was successful. If after 5 minutes it does not detect the node in the Deployment Manager's configuration, it gives an error stating that federation did not succeed.

Occasionally, federation actually takes longer than 5 minutes. In this case, simply waiting a few minutes and clicking **Federate Node** again results in a success message. Other times, the Deployment Manager has to be restarted, and then clicking **Federate Node** results in a success message. Very rarely, there is another condition that cannot be anticipated by the Sametime System Console that leads to the failure. In these cases, the administrator needs to look at the Primary Node's `AddNode.log` for additional information to help resolve the issue, and if necessary, contact IBM Support for assistance.

In other extremely rare cases, running the federation from the Sametime System Console results in an error in the `AddNode.log`, but running the `addNode` command directly successfully federates the node into the Deployment Manager. This is an acceptable workaround if the administrator cannot figure out why the clustering guided activity is failing. Run one of the following commands to federate the node:

```
addNode.bat dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses
./addNode.sh dmgrhost dmgrsoapport -username username -password password -includeapps -includebuses
```

After manually running `addNode`, the administrator can use the clustering guided activity for the remainder of the clustering process without any issues. The application recognizes the federated status of the node and proceeds accordingly.

After running the clustering guided activity, the administrator should make sure that all nodes are synchronized before restarting any node agents. In the Integrated System Console, click **System Administration > Nodes**, and select the nodes you want to synchronize, and then click the **Synchronize**.

---

**Troubleshooting a Sametime Community Server**

Use the following information to troubleshoot problems with an IBM Sametime Community server.

**Troubleshooting general issues in the Sametime Community Server**

The topics in this section describe how to debug general issues with the IBM Sametime Community server that can be easily reproduced.

**Gathering Sametime Community Server general diagnostic data**

Collect information for IBM Support to investigate Sametime awareness problems and related issues.

**About this task**

The recommended trace level for gathering general diagnostic information, `VP_TRACE_ALL=1`, is very verbose, and therefore should only be used in on
servers which have available disk space and CPU utilization to spare. If you are enabling trace on a production server which is running near capacity, please contact IBM Support to get more specific diagnostic settings which do not have as high of an impact on system resource.

Follow these instructions to set the trace level, and then reproduce the problem to gather information.

**Procedure**

1. Stop the Lotus Domino and Sametime Community Server.
2. Remove old log files from the Sametime trace directory.
3. Use a text editor to edit the *sametime.ini* file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`). Add the following line to the *Debug* section to set the trace level:
   
   ```
   VP_TRACE_ALL=1
   UCM_SNIFF=0
   VP_SNIFF=0
   UCM_DELAY_SNIFF=0
   VP_DELAY_SNIFF=0
   ```

4. Restart the Lotus Domino and Sametime Community Server.
5. Reproduce the problem that you want to troubleshoot, so you can collect diagnostic information.
6. Collect diagnostic information:
   a. Run the following collector utility: `stddiagzip.bat` located in the Sametime binary folder. For Windows, this is `C:\Lotus\Domino` by default. The output file is in the following format:

   ```
   \Trace\stdiags_hostname_MM_DD@hh_mm.zip
   ```

   b. Collect the following data:
      - The sametime.log file - Preserve as much history as possible. Do not remove data from this log.
      - The sametime.ini file
      - The communityConfig.txt file
      - The Stlog.nsf file - Keep this file small, not more than 1M.
      - STConfig.nsf
      - Details of user IDs that were used to reproduce the problem.
      - The exact time and date of the reproduced failure.
      - Client Application type and version that was used to reproduce the problem.
      - If you are troubleshooting a server crash, send all the core dump files which were created at the time of the crash.
      - Any additional details about the deployment, configuration, abnormal behavior, or any other general details that might help IBM Support with the problem investigation.

**What to do next**

After collecting the diagnostic information, any trace which was enabled on the Sametime Community Server should be disabled or reverted back to the default level. Use the STRuntimeDebug tool to enable and disable traces without having to restart the server.
Controlling the size and content of diagnostic data

You can set the maximum size file of each trace file and the maximum number of trace files used until the files are recycled. The setting is applicable to the IBM Sametime C++-based Community Service Application.

Procedure

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).
2. Add the following lines to the `Debug` section:
   
   - `ST_TRACEFILE_SIZE=file_size` - Sets the maximum file size of each trace file.
   - `ST_TRACEFILE_CNT =number_of_files` - Set the number of trace files generated per Sametime service application.

   `ST_TRACEFILE_SIZE` multiplied by `ST_TRACEFILE_CNT` equals the maximum size of the trace files on the Operating System hard disk per Sametime Community Service Application.

3. And finally, this.

Example

If the `sametime.ini` contains the following settings:

```
ST_TRACEFILE_SIZE=10
ST_TRACEFILE_CNT=25
```

Then 10 X 25 equals 250, so 250 MB is the maximum disk space each Sametime Service application consumes for the trace files.

Sametime Community Server log and trace file formats

The IBM Sametime Community Server log and trace files follow a specific naming format.

Log files

For Sametime 8.5 and later, log files are named `Sametime_YYYYMMDD.log`, where `YYYYMMDD` is the date. The log files are located in the `.../Domino/Trace` folder.

Note: For older versions of Sametime, the log file is named `samtime.log` and is located in the main application directory (data directory on Unix).

When the Sametime Community Server starts, a script runs that purge old logs. The script purges `sametime_YYYYMMDD.log` files that were created `X` number (`X` is 30 by default) of days ago or more. You can change the number of days by editing the `T_PURGE_LOGSOLDER_THAN` setting in the `sametime.ini` file.

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory (for example: `C:\Program Files\lotus\domino`).
2. Add or edit the following line in the `Control` section:

   `T_PURGE_LOGSOLDER_THAN=number_of_days`

Trace files

Trace files are logged in the `.../Domino/Trace` folder. Once a process starts, most of the components in the name of the trace file remain unchanged until the process is...
restarted. Only the counter part changes. The pattern for generating file names follows this format. The name of the process always displays in the log file. The other components of the format are optional:

<The name of the process>_<date of process startup>_<time of process startup>_<the process id number in the OS>_<trace file counter>

For example, if the trace file is named StResolve_090720_1922_5544_088.txt, then the name has the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Always displays/Optionally displays</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the process</td>
<td>Always</td>
<td>StResolve</td>
</tr>
<tr>
<td>Date of process startup</td>
<td>Optional</td>
<td>090720</td>
</tr>
<tr>
<td>Time of process startup</td>
<td>Optional</td>
<td>1922</td>
</tr>
<tr>
<td>Process id number in the OS</td>
<td>Optional</td>
<td>5544</td>
</tr>
<tr>
<td>Trace file counter</td>
<td>Optional</td>
<td>088</td>
</tr>
</tbody>
</table>

**Sametime Community Server trace files location**

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  From the Domino program directory, run the stdiagzip.bat file.
  For example:
  C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat

- **AIX/Linux/Solaris**
  `/local/notesdata> sh stdiagzip.sh`
  A zip file generated by the stdiagzip script is created in the `data_dir/Trace` directory

- **IBM i**
  `call QSAMETIME/STDIAGZIP servername`
  A zip file generated by the stdiagzip program is created in the `data_dir/trace` directory

**Gathering Sametime Community Server name change utility diagnostic data**

Collect information for IBM Support to investigate the IBM Sametime name change utility.

**About this task**

Since the trace files require large amounts of disk space, you should leave these settings turned off by default, and only enable them when you need to run the name change utility for special overall organization migrations.

Before you start the name change utility task, follow these instructions to set the trace level for gathering diagnostic information.

**Procedure**

1. Use a text editor to edit the `sametime.ini` file, which is located in the Sametime Community Server installation directory. For example:
   C:\Program Files\lotus\domino.
2. Add the following line to the Debug section to set the trace level:
   
   ```
   VP_NCSA_TRACE=1
   VP_LDAP TRACE=1
   ```

3. Restart the Sametime Community Server.

4. After the name change task finishes, you can collect the diagnostic information:
   - A `namechange_*.txt` debug log file
   - If you ran a name change task in RESOLVE mode, then a `StResolve_*.txt` is produced, too.

5. Disable the `sametime.ini` file settings after the utility successfully finishes by setting the values to 0.

**NSD Log and core dump file location**

When an IBM Sametime Community Services process crashes, an NSD log or core dump file is created with the relevant information about the crash.

The NSD log contains information about the tasks that were running when the process crashed, as well as general system information that may help determine the cause of the crash. The log is stored in the server’s `.\data\trace` directory. On Windows, the log is stored in the server’s `.\trace` directory. Part of the Sametime Community Components, using Notes API libraries, creates an NSD log in an alternate directory: `.\data\IBM_TECHNICAL_SUPPORT`.

**Important:** The date in the NSD log file’s name is not its creation date, but rather the date when the crashing process was first executed. To find the date when the NSD log was produced, look inside the log or use the file creation date based on the operating system information.

**Troubleshooting LDAP in Sametime**

See the following article to troubleshoot LDAP problems in IBM Sametime.

**About this task**

The "Best Practices for using LDAP with Sametime" article in the Sametime wiki contains a table with common problems and resolutions:

```
```

**Troubleshooting network issues on the Sametime Community Server**

The topics in this section describe how to diagnose networking problems that affect performance with the IBM Sametime Community server.

**About this task**

Some environments are sensitive to network behavior, or use a configuration that is insufficient for the expected Sametime capacity, which may result in the following symptoms:

- **Delayed messages**: are caused by slow network performance. The messages may be one-to-one chats, group chats, and status updates of users.
- **Lost messages**: can occur when network slowdowns delay the delivery of messages and they are sent after the intended recipient logs out.
- **Failure to start a chat**: can occur when the request to start a chat times out on the recipient’s end. The timeout is typically set to 30 seconds.
Best practices for performance of the Sametime Community Server

Delays can be caused by insufficient throughput of server-to-server connections. Follow these best practices to improve the throughput between servers.

About this task

Occasional delays, especially when data centers from different continents or remote geographies are online and active together, can be caused by large individual messages. If a large message is sent out and the throughput is insufficient, the message can take an unusually long time to be transferred. While one message is being transferred, no other message can be transferred on the same server-to-server connection.

Frequent or sustained delays indicate that the throughput is not high enough between two servers or given servers on remote geographies. In this situation, the delays get progressively longer, until it appears that no messages are being transferred.

Although network bandwidth can be a factor in low throughput, in most production environments, bandwidth is more than sufficient for Sametime. However, high network latency combined with a small TCP send buffer can often result in network delays. In particular, sites with servers in remote geographies may encounter this problem.

Use these best practices to improve throughput.

- All Sametime Community servers and multiplexers (if used) should be located in the same data center. Maintaining a short distance between servers is much more important than the distance between servers and clients.
- If the policy is to deploy servers on remote sites for site redundancy, try to set up sites with very low latency between them. High latency (for example, 250 ms) lowers throughput significantly. Low throughput causes congestion, which in turn causes long delays of 30 seconds or more.
- Here is a simple formula for calculating the throughput of a server-to-server connection:
  \[
  \text{throughput} = \frac{\text{buffersize}}{\text{roundtrip\_latency}}
  \]
  - Buffer size is 8 KB by default on Windows. Sametime. Server-to-server connections default to 64 KB, which is the largest useful size on standard TCP.
  - Estimate the round trip latency by using the ping command.

Improving throughput on Sametime 8.5 servers

Sametime 8.5 Community Server, as well as hotfixes on top of earlier select releases, allows you to change the default server-to-server buffer size to improve performance. In the sametime.ini file, use the following buffer size settings, which match the default settings of Sametime 8.5.1 and later servers.

[Connectivity]

VPS_SERVER_SOCK_SO_SNDBUF=65536

VPS_SERVER_SOCK_SO_RCVBUF=65536
For older servers, contact IBM support to see if a fix is available for SPR #ICAE7QLJJP for your release and operating system that supports the changes.

**Collecting data about network congestion problems that affect the Sametime Community server**

To diagnose network problems that affect performance and stability of the IBM Sametime Community Server, add specific flags related to network traffic to the `sametime.ini` file. Running the server with these flags allows you to collect data that you can then send to IBM Support for evaluation.

**About this task**

Follow these steps to add specific data collection flags to the `sametime.ini` file.

**Procedure**

1. Open a text editor on the Sametime Community Server.
2. Open the `sametime.ini` file located in the Sametime Community Server installation directory. For example, the default directory in Windows is `C:\program files\lotus\domino`.
3. Navigate to the Sametime Community Server's config section. The name is specific to the operating system you're running on.
   - **Windows**
     ```
     [Debug-STCommunity]
     ```
   - **AIX, Linux, and Solaris**
     ```
     [Debug-stserver]
     ```

   **Note:** If you are troubleshooting a Sametime server running a release earlier than Sametime 8.5, contact IBM Support for the "per-component debug" feature, which is based on SPR#ICAE7QLJJP. This feature provides the Debug-STCommunity or Debug-stserver sections described above.

4. Add one or more of the following flags.

   **Table 41. Sametime.ini flags related to network diagnostics**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCM_TRANSFER_RATE_SAMPLE_INTERVAL</td>
<td>The interval, in seconds, of sampling transfer rates of all Sametime TCP connections. A value of 0 indicates no sampling.</td>
<td>Recommended value for investigating delays and slow traffic: 5</td>
</tr>
<tr>
<td>UCM_TRANSFER_RATE_TRACE_ALL_SAMPLES</td>
<td>All transfer rate samples should be printed to debug trace files. A value of 1 indicates samples should be printed.</td>
<td>Recommended value for investigating delays and slow traffic: 1</td>
</tr>
</tbody>
</table>
Table 41. Sametime.ini flags related to network diagnostics (continued)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPS_SERVER_TRANSFER_RATE_REPORT_FREQ</td>
<td>Setting this flag to a number greater than 0 sends reports of the transfer rates of server-to-server TCP connections to the sametime.log file. The flag is not useful for investigating delays or slow traffic, but rather to get an idea of the transfer rates. A value of 0 indicates no reports. Any other number represents how many times a day you want to generate reports.</td>
<td>In order to get a report once every 3 hours (8 times a day), set it to 8.</td>
</tr>
<tr>
<td>UCM_DELAY_THRESHOLD</td>
<td>The threshold, in seconds, above which data queued for sending and not yet sent is reported as &quot;delayed&quot; in the socket layer. A value of 0 indicates no delay detection in the socket layer.</td>
<td>Recommended value for investigating delays: 10</td>
</tr>
</tbody>
</table>
| UCM_DELAY_SNIFF             | When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by UCM_DELAY_THRESHOLD.                                                                                     | This flag is only useful in a few special cases.  
Recommended value: 0                                                              |
| VP_DELAY_THRESHOLD          | The threshold, in seconds, above which encrypted data queued for sending and not yet sent would be reported as "delayed" in the encryption layer. A value of 0 indicates no delay detection in the encryption layer.                 | Recommended value for investigating delays: 10                                      |
| VP_DELAY_SNIFF              | When set to 1, this flag dumps buffer contents to the debug trace files when a delay is detected by VP_DELAY_THRESHOLD.                                                                                      | This flag is only useful in a few special cases.  
Recommended value: 0                                                              |

5. Save the sametime.ini file.  
6. Restart the Sametime Community Server.  

**What to do next**  
When you no longer need to collect the data, set the flags back to 0 and restart the server.  

**Troubleshooting network problems on Domino**  
Learn about the tools and utilities that you can use when troubleshooting problems on a Sametime Community Server.  

**Basic networking knowledge and skills**
Sametime relies on networking to "work" as does Domino.

Use Ping, Telnet, Netstat and IPConfig to verify that tunneling is set up correctly on the network and in DNS.

Use Ipconfig (at the DOS or command prompt) to:
- gather pertinent information for troubleshooting general TCP/IP network problems
- troubleshoot IP issues on DHCP clients.

Use Netstat to determine:
- if an application other than a Domino server task is bound to a specific port
- if there is a network connectivity problem at the network interface or with the physical media of the network
- if the local network segment might be overloaded.

Use Traceroute to determine the physical layout of a network or internetwork.

Use the Ping utility to:
- test connectivity to a host
- gather information for troubleshooting connectivity problems.

Use the Telnet utility to connect to a Domino server and check the status of an application on a well-known port.

Use the NotesConnect utility to determine:
- services running on a machine
- network configuration problems
- if the target host name can be resolved to its IP address

The link below is provided as a reference:
Networking Basics - Key Concepts in Computer Networking

---

Troubleshooting a Sametime Proxy Server

Use the following topics to troubleshoot problems in an IBM Sametime Proxy Server.

Enabling logging and tracing for a Sametime Proxy Server

The IBM Sametime Proxy Server utilizes the JSR-47 logging to record various events for troubleshooting. Using the IBM Websphere Integrated Solutions Console, you can fine tune the amount of captured trace content.

Before you begin

Ensure that the Sametime Proxy Server is running.

About this task

Follow these steps to enable tracing on the Sametime Proxy Server.
**Procedure**

1. Login to the WebSphere Integrated Solutions Console with administrator privileges on port 8601. For example: `https://yourserver.com:8601/ibm/console`
2. Select **Troubleshooting > Logs and Trace**.
3. Select **STProxyServer**.
4. Select **Diagnostic Trace**.
5. Select the **Runtime** tab.
6. Select **Change log level details**.
7. Type in the desired log setting, or select the components and levels by expanding the *All Components* twistie.
8. Enable the "**Save runtime changes to configuration as well**" checkbox.

Trace.log will be created in `...\profiles\STPAppProfile\logs\STProxyServer` for Windows or `/opt/IBM/WebSphere/AppServer/profiles/xxxxSTPPNProfilex/logs/STProxyServer` for Linux.

<table>
<thead>
<tr>
<th>Log levels</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>*=info</td>
<td>Enabled by default. All SEVERE, WARNING, and INFO messages will be logged to Systemout.log and Systemerr.log.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.stproxy.</em>=all:com.ibm.collaboration.realtime.*=all</td>
<td>Sometimes it is necessary to turn on rtc4web long-poll logging. Use this level to trace the long-poll traffic during the Proxy run and use states.</td>
</tr>
<tr>
<td><em>=info: com.ibm.rtc.</em>=all:com.ibm.collaboration.realtime.*=all</td>
<td>Turns on all rtc4web logging to the FINEST level. In most cases, com.ibm.rtc.servlet.RTCServlet=fine should be sufficient.</td>
</tr>
</tbody>
</table>

**Troubleshooting a Sametime Media Manager**

Use the following topics to troubleshoot problems in an IBM Sametime Media Manager.

**Setting a diagnostic trace on a Sametime Media Manager server**

You can specify how the server handles IBM Sametime Media Manager log records. You can select a Sametime Media Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Procedure**

1. In the Integrated Solutions Console, click **Troubleshooting --> Logs and Trace**.
2. Click the **STMediaServer** if components are stored on different servers, the server component you want to change.
3. Under General Properties, click **Change Log Detail Levels**.

4. In the text box, append the following settings.

   For a single server:
   ```
   :com.lotus.sametime.telephony.*=all:
   com.ibm.mediaserver.*=all:
   com.ibm.telephony.conferencing.spi.*=all:
   com.ibm.ws.sip.*=all:
   com.ibm.sametime.telephony.sipfocus.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.packetswitch.*=all:
   com.lotus.sametime.telephonymanager.*=all:
   com.ibm.ice.*=all
   ```

   For the conference manager only:
   ```
   :com.lotus.sametime.telephony.*=all:
   com.ibm.mediaserver.*=all:
   com.ibm.telephony.conferencing.spi.*=all:
   com.ibm.ws.sip.*=all:
   com.ibm.sametime.telephony.sipfocus.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.telephonymanager.*=all
   ```

   For the packet switcher only:
   ```
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all:
   com.ibm.sametime.packetswitch.*=all:
   com.ibm.ice.*=all
   ```

   For the SIP Proxy and Registrar only:
   ```
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all
   ```

5. Check the box to reflect the log settings in the Configuration tab as well.

6. Click **OK**, and then **Save**.

7. Restart the Sametime Media Manager.

8. Monitor the log files in the following locations.

   **Windows**:
   ```
   WAS_Install_Root\WebSphere\AppServer\profiles\HostName_Media_deploymentType_Profile_Number\logs
   ```

   **Linux**:
   ```
   /opt/IBM/WebSphere/AppServer/profiles/HostName_Media_deploymentType_Profile_Number/logs
   ```

**Logging and tracing on Sametime Media Manager**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.

2. If you cannot solve the problems using these files, try using a trace.

3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.
For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

**Gathering Sametime Media Manager logs and traces for IBM Support**

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

**About this task**

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

**Procedure**

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   
   For more information, see the following topic in the WebSphere Application Server information center:
   
   Gathering information with the collector tool (deprecated).

2. Run the collector on the IBM Sametime Media Manager server.
   
   - Run collector on the WebSphere Application Server profiles.
     
     The profiles are stored in the `\profiles` directory; for example on Microsoft Windows:
     
     ```
     C:\Program Files\ibm\WebSphere\AppServer\profiles
     ```
     
     The profile name follows this format:
     
     `HostName_Media_deploymentType_Profile_Number`
     
   - The collector resides in the `\bin` directory below the profile; for example:
     
     ```
     C:\Program Files\ibm\WebSphere\AppServer\profiles\wp1ccdilvm053MediaAPNProfile1\bin\collector.bat
     ```
     
     The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
     
     `HostName_Media_deploymentType_Profile_Number-WASenv.jar`
     
     **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. Submit the collector generated log files to IBM support.

**Troubleshooting a Sametime Media Manager using JVM logs**

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.
About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of a IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it's better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting > Logs and Trace.
2. Click STMediaServer.

   Note: Any configuration changes to the JVM logs that are made to a running IBM Sametime Media Manager do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting video quality

To ensure good quality video in your video-enabled IBM Sametime meeting rooms and Sametime Connect video calls, check your video driver.

Sametime Connect video calls and video-enabled Sametime meeting rooms take advantage of the hardware acceleration available in modern video cards and their associated drivers. If you are experiencing difficulty in establishing video call connections, or experience poor video quality in video in meeting rooms, ensure that you are using a video driver that takes full advantage of your video card’s acceleration hardware.

Refer to the A/V Client Support & Requirements section in the system requirements:
http://www.ibm.com/support/docview.wss?rs=477&uid=swg27016451

Troubleshooting Sametime Media Manager component clusters

This section explains how to troubleshoot clusters of IBM Sametime Media Manager components.

Enabling logging and tracing for a Conference Manager cluster

Enable traces and logs for the members in a Conference Manager cluster.
Procedure

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.lotus.sametime.telephony.**=all:
   com.ibm.telephony.conferencing.spi.**=all:
   com.ibm.ws.sip.**=all:
   com.lotus.sametime.telephony.sipfocus.**=all:
   com.ibm.sip.*=all:
   com.lotus.sametime.telephonymanager.**=all
7. Click Apply.
8. Save your changes by clicking the Save link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

Enabling logging and tracing for a SIP Proxy and Registrar cluster

Enable traces and logs for the members in a SIP Proxy and Registrar cluster.

Procedure

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   :com.ibm.ws.sip.*=all:
   com.ibm.sip.*=all
7. Click Apply.
8. Save your changes by clicking the Save link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

Configuring a Sametime Community Server to allow connections from Conference Manager nodes

Add Conference Manager nodes to the list of Trusted IPs for an IBM Sametime Community Server.

About this task

This task is only necessary if you see the ST_CONNECT_HOST_UNREACHABLE error in the Conference Manager logs, which means that the Community Server is not allowing connections from the Conference Manager nodes. Enable the connection by adding
each Conference Manager node’s IP address to the list of Trusted IPs for the Sametime Community Server.

**Procedure**

1. Log into the Sametime System Console’s Integrated Solutions Console as the WebSphere administrator.
2. Click **Sametime System Console > Sametime Servers > Sametime Community Servers**.
3. In the "Sametime Community Servers" table, click the name of a Community Server.
4. Click the **Connectivity** tab.
5. Add the Conference Manager nodes to the list of trusted servers:
   a. Under "Trusted Servers" enter the IP address (or host name) of the server where a Conferencing Manager node is hosted.
   b. Click **Add**.
   c. Repeat for each node in the Conference Manager cluster.
   d. Click **OK**.
6. Restart the Sametime Community Server.

**Enabling traces and logs for the WebSphere proxy server used by a Media Manager cluster**

Enable traces and logs for an IBM WebSphere proxy server that is used with an IBM Sametime Media Manager cluster.

**About this task**

Both Conference Manager clusters and SIP Proxy and Registrar clusters can use a WebSphere proxy server; this task applies to both clusters.

**Procedure**

1. Log into the Deployment Manager’s (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Troubleshooting > Logs and trace**.
3. In the "Logging and Tracing" table, click the name of a WebSphere proxy server to open its "Logging and Tracing" page.
4. Under "General Properties" click **Diagnostic Trace**.
5. Under "Additional Properties" click **Change Log Detail Levels**.
6. In the text box, append the following settings:
   :com.ibm.ws.sip.*=all
   :com.ibm.ws.proxy.*=all
7. Click **Apply** and then save the changes by clicking the Save link the "Messages" box at the top of the page.

---

**Troubleshooting Sametime Bandwidth Manager**

Use the following topics to troubleshoot problems in an IBM Sametime Bandwidth Manager.

**Setting a diagnostic trace on a Sametime Bandwidth Manager**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs
such as the JVM logs and the IBM service log. You can specify how the server handles IBM Sametime Bandwidth Manager log records. You can select a Bandwidth Manager server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

**Procedure**

1. In the Integrated Solutions Console, click **Troubleshooting --> Logs and Trace**.
2. Click the server name of the Bandwidth Manager.
3. Under General Properties, click **Change Log Detail Levels**.
4. In the text box, append the following settings.
   - For a single server:
     :com.avistar.*=all
   - If you suspect a problem with the SIP messaging, append:
     com.ibm.ws.sip.*=all:
     com.ibm.sip.*=all:
   - If you suspect a problem with federated repository or LDAP access, append:
     :com.ibm.websphere.wim.*=all:
     com.ibm.wsspi.wim.*=all:
     com.ibm.ws.wim.*=all
5. Click **Apply**, and then **Save**.
6. Restart the Sametime Bandwidth Manager.
7. Monitor the log files in the following locations.
   - Windows:
     WAS_Install_Root\WebSphere\AppServer\profiles\Bandwidth_Manager_profile\logs\Bandwidth_Manager_server_name
   - Linux:
     /opt/IBM/WebSphere/AppServer/profiles/Bandwidth_Manager_profile/logs/Bandwidth_Manager_server_name

**Troubleshooting a Sametime Bandwidth Manager using JVM logs**

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

**About this task**

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of an IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it is better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.
The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

**Procedure**

1. In the Integrated Solutions Console, click **Troubleshooting > Logs and Trace**.
2. Click the server name of the Bandwidth Manager.
3. Under General Properties, click **JVM Logs**.

   **Note:** Any configuration changes to the JVM logs that are made to a running IBM Sametime Bandwidth Manager do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the **Runtime** tab, then click **View**.

**Troubleshooting using the Bandwidth Manager Monitor and Policy Testing tools**

IBM Sametime Bandwidth Manager provides tools in the administrative interface that can help troubleshoot problems in network topology setup.

**About this task**

The administrative tools you can use to troubleshoot problems are the Monitor and the route, call policy, and bandwidth test pages.

- **Monitor**
  The Monitor is accessed from the “Monitoring” tab in the user interface. It provides views into the currently active calls in the system. This activity can be organized in views by the Links and Sites that are configured, and also by individual calls. The Bandwidth Manager statistics topic explains the different statistics you can view.

- **Testing Routes, Call Rate Policies, Reflector Policies, and Bandwidth**
  The administrative interface allows you to test out call rate policies, routes, and bandwidth allocation before actually deploying them. There are buttons to access the Test Bandwidth Manager Policies page from the Call Rate Policies tab, the Monitoring tab, the Sites tab, and the Reflector Policies tab. The test page allows you to enter the caller and callee endpoint addresses, site names or groups, and user and group names to see which sites are used, which routes are used, how much bandwidth is allocated, and which reflector policies (if any) are used.

**Related reference**

“Bandwidth Manager statistics” on page 129
Understanding the Bandwidth Manager monitor statistics can be useful for fine-tuning site and link bandwidth allocations and peak utilization points.

**Troubleshooting Sametime Bandwidth Manager clusters**

This section explains how to troubleshoot clusters of IBM Sametime Bandwidth Manager servers.

**Enabling logging and tracing for a Bandwidth Manager cluster**

Enable traces and logs for the members of an IBM Sametime Bandwidth Manager cluster.
**Procedure**
1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click **Troubleshooting > Logs and trace**.
3. In the "Logging and Tracing" table, click the name of a cluster member to open its "Logging and Tracing" page.
4. Under "General Properties" click **Diagnostic Trace**.
5. Under "Additional Properties" click **Change Log Detail Levels**.
6. In the text box, append the following settings.
   - For a single server:
     ```
     :com.avistar.*=all
     ```
   - If you suspect a problem with the SIP messaging, append:
     ```
     com.ibm.ws.sip.*=all:
     com.ibm.sip.*=all:
     ```
   - If you suspect a problem with federated repository or LDAP access, append:
     ```
     :com.ibmwebsphere.wim.*=all:
     com.ibm.wsspi.wim.*=all:
     com.ibm.ws.wim.*=all
     ```
7. Click **Apply**.
8. Save your changes by clicking the **Save** link in the "Messages" box at the top of the page.
9. Repeat for every cluster member.

---

**Troubleshooting a Sametime TURN Server**

If your IBM Sametime deployment experiences problems with NAT traversal, begin by troubleshooting the Sametime TURN Server.

**About this task**

**Attention:** Diagnostics should only be enabled under the advice of IBM Technical Support. IBM Technical Support will be able to determine whether extended diagnostics are required.

**Procedure**
1. On the TURN Server, navigate to the directory where the TURN Server files were installed (for example, C:\TURN).
2. Open the **logging.properties** file for editing.
3. Change the following settings as shown:
   ```
   com.ibm.stun.level=INFO
   com.ibm.turn.server.level=INFO
   ```
4. Save and close the file.
5. Restart the TURN Server.

**What to do next**

If you cannot isolate a problem on the TURN Server, you may need to troubleshoot other Sametime components that are involved in NAT traversal:
- Sametime Connect client
- Sametime web audio-visual plugin
- Sametime Proxy Server
Troubleshooting a Sametime Meeting Server

Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server.

Setting a diagnostic trace on a Sametime Meeting Server

You can specify how the server handles IBM Sametime Meeting Server log records. You can select a Sametime Meeting Server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and trace.
2. Click the Sametime Meeting Server that you want to trace.
3. Under General Properties click Diagnostic Trace
4. Under Additional Properties, click Change Log Detail Levels.
5. In the text box, append the following settings:
   
   
   To get even more detailed traces, use this setting instead:
   
   **=info: com.ibm.rtc.*=all
   
6. Click Apply, and then Save.
7. Monitor the log file in IBM\WebSphere\AppServer\profiles\HostName_Meeting_deploymentType_Profile_Number\logs

Logging and tracing on Sametime Meeting Server

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.
1. The first source of information for configuration and administration problems are the general-purpose logs.

2. If you cannot solve the problems using these files, try using a trace.

3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

Gathering Sametime Meeting Server logs and traces for support

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting problems.

About this task

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem.

Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite.

Procedure

1. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.

   For more information, see the following topic in the WebSphere Application Server information center:

   Gathering information with the collector tool (deprecated)

2. Run the collector on the IBM Sametime Meeting Server.
   - Run collector on the WebSphere Application Server profiles.
     The profiles are stored in the \profiles directory; for example on Microsoft Windows:
     `C:\Program Files\ibm\WebSphere\AppServer\profiles`
   - The collector resides in the \bin directory below the profile; for example:
     `C:\Program Files\ibm\WebSphere\AppServer\profiles\HostName_Meeting_deploymentType_Profile_Number\bin\collector.bat`

   The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:

   `HostName_Meeting_deploymentType_Profile_Number-WASenv.jar`

   **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

3. Submit the collector generated log files to IBM support.
Troubleshooting a Sametime Meeting Server using JVM logs

To start troubleshooting a problem on an IBM Sametime meeting server, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

About this task

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of an IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful for monitoring the health of the running application server but can help in determining a problem, although it’s better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived, files to keep and which of the log files to rollover or archive based by time or size or both.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the IBM Sametime Meeting Server.

   Note: Any configuration changes to the JVM logs that are made to a running Sametime Meeting Server do not take effect until you restart the server.

4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the Runtime tab, then click View.

Troubleshooting a Sametime Meeting Server cluster

Use the following topics to troubleshoot problems in an IBM Sametime Meeting Server cluster.

Troubleshooting WebSphere proxy issues with the Sametime Meeting Server cluster

You can troubleshoot issues with the IBM WebSphere proxy server used with the IBM Sametime Meeting Server cluster by setting traces and logs.

Procedure

1. Log into the Deployment Manager's (the Sametime System Console) Integrated Solutions Console as the WebSphere administrator.
2. Click Troubleshooting > Logs and trace.
3. In the "Logging and Tracing" table, click the name of a WebSphere proxy server to open its "Logging and Tracing" page.
4. Under "General Properties" click Diagnostic Trace.
5. Under "Additional Properties" click Change Log Detail Levels.
6. In the text box, append the following settings:
   
   ```
   com.ibm.rtc.proxy.filter.*=all
   ```
   Based on this output, IBM might recommend other settings.

7. Click Apply and then save the changes by clicking the Save link the "Messages" box at the top of the page.
8. Repeat for every WebSphere proxy server used by the cluster.

---

Troubleshooting a Lotus Sametime Gateway Server

Use the following topics to troubleshoot problems in an IBM Lotus Sametime Gateway Server.

Other sources of information

Use the following links to find other hints and tips when troubleshooting Lotus Sametime Gateway:

- Lotus Sametime wiki:
  ```
  www.lotus.com/ldd/stwiki.nsf/
  ```

- Technotes for Lotus Sametime Gateway:
  ```
  www.ibm.com/support/search.wss?q=Sametime%20Gateway&rs=477&tc=SSKTXQ&dc=DB520&dtm
  ```

- WebSphere Application Server diagnostic tools to help troubleshoot database connection problems:
  ```
  Troubleshooting data access problems
  ```

Setting a diagnostic trace on Sametime Gateway

You can specify how the server handles Sametime Gateway log records. You can select a Sametime Gateway server to enable or disable a system log for the server, specify where log data is stored, and choose a format for log content. You can also specify a log detail level for components and groups of components.

Procedure

1. In the Integrated Solutions Console, click Troubleshooting --> Logs and Trace.
2. Click the RTCGWServer that you want to trace.
3. Under General Properties, click Change Log Detail Levels.
4. Select the Runtime tab.
5. Under com.ibm.rtc.*, click com.ibm.rtc.gateway.*.
6. From the context menu, select All Messages and Traces. You should now see the following text in the log detail level field: **info:
   ```
   com.ibm.rtc.gateway.*=all
   ```
   The result looks like this:
   ```
   ```
7. If SIP traces are required, add the following string to the detail level field, using a colon (:) as a delimiter.
   ```
   com.ibm.ws.sip.stack.transaction.transport.TransportCommLayerMgr=all
   ```
   7. The result looks like this:
   ```
   ```
8. Select Save runtime changes to configuration as well.
9. Click OK, and then Save. Restarting server1 is not necessary.
10. Monitor the log file in `stgw_profile_root\logs\server_name\trace.log`
11. If Sametime Gateway is clustered, repeat Steps 1 through 9 for each node in the cluster.

**What to do next**

Set a diagnostic trace on the SIP Proxy server, as described in Tracing a Session Initiation Protocol proxy server in the WebSphere Application Server information center.

**Related tasks**

“Setting log files size and rotation” on page 206
You can specify the maximum size and number of log files to be stored on the server.

**Logging and tracing**

The Integrated Solutions Console provides a variety of logs to collect logging messages. System messages from the server are written to general-purpose logs such as the JVM logs and the IBM service log.

Other logs are very specific in nature and focused on a component or activity. The general purpose logs such as the JVM logs and the IBM service log can be helpful in monitoring the health of the application server, however, the problem determination procedure for a specific component might instruct you to examine the contents of a component- or product-specific log. This section describes the log files available for IBM WebSphere Application Server, the logs that the server and services make use of, and how you can configure and view the files.

1. The first source of information for configuration and administration problems are the general-purpose logs.
2. If you cannot solve the problems using these files, try using a trace.
3. For runtime code problems, again look at the general-purpose logs first. Then running a trace with component-specific flags as required.

For more information about logging and tracing, go to the Monitoring and Troubleshooting documentation for distributed operating systems in the WebSphere Application Server Library at http://www-01.ibm.com/software/webservers/appserv/was/library/.

**Setting a diagnostic trace for specific user names and domains**

In IBM Sametime Gateway, you have the option to turn on diagnostics traces only for those transactions that are in the context of specific user names and domains. This feature is also known as selective tracing.

**About this task**

If Sametime Gateway is a production system at your site that handles a high number of transactions per second, you might not be able to safely turn on server-wide diagnostic without exhausting the system's CPU resources. Another factor to consider when using server-wide diagnostic traces is that the volume of the produced traces can get quite large. To avoid these unwanted effects, you have the option to turn on diagnostics traces only for those transactions that are in the context of specific user names and domains. For example, you might want to trace only those transactions that are executed in context of the user joe@example.com, or for all of the users of the domain im.com, or even both. The user names and domains specific diagnostic is designed to work in parallel with the normal
WebSphere server-wide diagnostic trace. One method does not contradict the other. The user names and domains pattern by which the diagnostic trace is produced is given as a regular expression. You have the option to engage this selective tracing without having to restart your Sametime Gateway servers.

Follow these steps to set the user names and domains specific diagnostic trace:

**Procedure**

1. Turn on WebSphere Application Server tracing.
   a. In the Integrated Solutions Console, click **Troubleshooting > Logs and Trace**.
   b. Click the **RTCGWServer** that you want to trace – typically, all of the servers in the cluster.
   c. Under **General Properties**, click **Change Log Detail Levels**.
   d. The screen initially shows the Configuration tab. If the server is **not** running, the Configuration tab is the only tab on screen. If the server is running, an additional Runtime tab is available. If it is available, switch to the Runtime tab, and also select **Save runtime changes to configuration as well**.
   e. In the text area you should see the following text:
      ```
      *=info:
      ```
      Replace it with:
      ```
      *=info: com.ibm.rtc.gateway.tracing.StgwLogger=all:
      ```
   f. Click **OK**, and then click **Save**.
2. Define a trace pattern as a custom property
   Create a custom property that defines the user names and domains pattern to trace by. Whenever a transaction is executing in the a user name and domain context that matches the pattern, the transaction produces the required diagnostic traces. If the transaction’s context does not match the set pattern, no diagnostic trace is produced.

   **How to compose a pattern**

   Suppose we want to trace all of those transactions which involve:
   `user1@domain10.com`, or `user2@domain2.com`, or `user20@domain2.com`, or `user212@domain2.com`
   We could use the following pattern:
   `(OE )?user1@domain10.com|(OE )?user2.*@domain2.com`

   **Regular expression breakdown**
   - `(OE )?` - a required prefix that should always appear before the user name.
   - `user1@domain10.com` - the user’s email address.
   - `|` - the pipe character denotes an OR logical condition.
   - `user2.*@domain2.com` - matches any user name that begins with user2, then contain any number of characters, and ends with @domain2.com.

   IBM recommends that you test your regex pattern, before applying it. You can find an online web tester by entering `java online regular expression testing` in a search engine. For additional help on regular expressions, see the Java Regular Expression tutorial: [http://java.sun.com/docs/books/tutorial/essential/regex/index.html](http://java.sun.com/docs/books/tutorial/essential/regex/index.html)

   **Expected state**
   - Single server: the Sametime Gateway server is started.
• Cluster: the Deployment Manager is started, and the node agent and the Sametime Gateway server are started on at least one node.

a. In the Integrated Solutions Console, open the Custom properties page for the server.
   - On a single server, click **Servers > Server Types > WebSphere application servers > server_name > Server Infrastructure > Administration > Custom Properties**.
   - On a clustered server, click **System administration > Cell > Custom Properties**.

b. Click **New** and enter the following information for trace pattern filter custom property:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>tracing.filter.pattern</code></td>
</tr>
<tr>
<td>Value</td>
<td>Regular expression</td>
</tr>
</tbody>
</table>
| Description | A regular expression to serve as a user names and domains pattern For example: 
                `(\@\s{1})?user1@domain10.com|\@\s{1})?user2.*@domain2.com` |

c. Click **OK** to save the new custom property.

d. Restart the Sametime Gateway server. If you have a cluster of Sametime Gateway servers, restart the cluster. Traces are printed to the log file: `stgw_profile_root/logs/trace.log`. See the following additional procedure if you do not wish to restart the environment for these settings to take effect.

3. Optional: Additional steps to apply the pattern in runtime without restarting the server.

   If you are not able to restart your Sametime Gateway environment, then the following procedure can be used to apply the new pattern during runtime without a server restart. You are still required to enter the described custom property in order to persist the trace across server restarts. If in a cluster, the following steps need to be executed once on the Sametime Gateway deployment manager only (there’s no need to execute on each cluster member directly), or on the standalone server (if not in a cluster):

a. Copy the following script from `stgw_server_root/config/adminscripts/setTracePattern.py` to the Deployment Manager node: `app_server_root/bin`.
b. Open a command window and navigate to `app_server_root/bin`
c. Run the following command:

```
wadmin -lang jython -username username -password password -f setTracePattern.py "pattern"
```

Where **username** is the administrative user ID that you use to log in to the Integrated Solutions Console. You created this user ID when you installed Sametime Gateway. Where **pattern** is a regular expression, surrounded by quotation marks, by which to trace individual users or domains. For example:

```
wadmin -lang jython -username wasadmin -password gateway4u -f setTracePattern.py "(\@\s{1})?user1@domain10.com|(\@\s{1})?user2.*@domain2.com"
```

Note that when you enter the pattern using the shell command line, due to character escaping requirements, use \s{1} instead of the space character. Other than this difference, the custom property pattern and the command
line pattern should be identical. In order to stop tracing and remove the pattern use "remove" as the pattern. For example:
wsadmin -username wasadmin -password gateway4u -f setTracePattern.py "remove"

Note: Any pattern will be lower case, because the tracing filter is not case sensitive.

d. Make sure that the last line that the script prints is the following message:
OK: successfully set pattern on all servers.
e. Make sure have performed the previous steps of starting WebSphere traces and creating the required custom property, in order to preserve the trace settings for server restarts.

Gathering logs and traces for IBM support

Use the IBM Websphere Collector tool to gather logs and traces that IBM Customer Support can use when troubleshooting your problem.

About this task

The collector tool gathers information about your WebSphere Application Server installation and packages it in a Java archive (JAR) file that you can send to IBM Customer Support to assist in determining and analyzing your problem. Information in the JAR file includes logs, property files, configuration files, operating system and Java data, and the presence and level of each software prerequisite. Be sure you set the log file size and rotation before you collect the information. The default log file rotation leaves the user only one file, which fills up and gets overwritten rather quickly.

Procedure

1. Follow these steps to configure the log file size and rotation settings.
   a. Log in to the Integrated Solutions Console.
   b. Click Servers Server Types WebSphere Application Server.
   c. In the Application Servers list, click the server name.
   d. Under Troubleshooting, click Diagnostic trace service.
   e. Under General Properties, update the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Rotation</td>
<td>Make sure this is managed by file size rather than file age.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Set this value to at least 20MB.</td>
</tr>
<tr>
<td>Maximum Number of Historical Log Files</td>
<td>Set this to a value that, when multiplied by the file size, gives you at least 2GB of history in your logs; in this example, you would use 50 files as the maximum.</td>
</tr>
</tbody>
</table>

   f. Click OK, and then click Save.

2. Use the IBM Websphere Collector tool to gather logs and traces from all of the environment machines.
   For information on using the Websphere Collector tool, see the WebSphere information center at the following web address:
   Gathering information with the collector tool (deprecated)
3. Run the collector on each of the computers in the Sametime Gateway deployment.

**Notes**
- On each machine, run collector once for each of the WebSphere Application Server profiles.
  - The profiles are stored in the \profiles directory; for example on Microsoft Windows:
    - C:\Program Files\ibm\WebSphere\AppServer\profiles
  - The collector resides in the \bin directory below the profile; for example:
    - C:\Program Files\ibm\WebSphere\AppServer\profiles\RTCGW_Profile\bin\collector.bat
  - The output from each execution of the collector is placed in your current working directory, and includes the name of the profile on which it was run using the format:
    - myHostName-MyCellName-MyNodeName-RTCGW_Profile-WASenv.jar

  **Note:** The generated files will include all log files located in the "logs" directory under the profile directory. To reduce the log size, you might choose to delete all of the existing log files, recreate the problem, and only then gather the logs.

4. Submit the collector generated log files to IBM support.

**Gathering performance data**

IBM Sametime Gateway tracks the number of subscriptions and instant messaging requests, requests for each community, and the response time of subscriptions. You can view these statistics to help tune or troubleshoot Sametime Gateway problems.

**About this task**

You can enable and view the following statistics about Sametime Gateway:

<table>
<thead>
<tr>
<th><strong>STGWStats Group</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IMRequestCount</td>
<td>Count of the instant messaging requests that are sent from all communities</td>
</tr>
<tr>
<td>SubscribeRequestCount</td>
<td>Count of subscription requests that are sent from all communities</td>
</tr>
<tr>
<td>IMResponseTime</td>
<td>Average instant messaging response time based on the last response time of all communities</td>
</tr>
<tr>
<td>SubscribeResponseTime</td>
<td>Average subscription response time based on the last response time of all communities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Individual community example</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IMRequestCount</td>
<td>Count of the instant messaging requests that are sent from this community</td>
</tr>
<tr>
<td>SubscribeRequestCount</td>
<td>Count of subscription requests that are sent from this community</td>
</tr>
<tr>
<td>IMResponseTime</td>
<td>The last instant messaging response time sent from this community</td>
</tr>
<tr>
<td>SubscribeResponseTime</td>
<td>The last subscribe response time sent from this community</td>
</tr>
</tbody>
</table>

256 IBM Sametime: Administration Guide
Procedure

1. To enable statistics gathering:
   a. In the Integrated Solutions Console, click Monitoring and Tuning > Performance Monitoring Infrastructure (PMI)
   b. Click RTCGWServer.
   c. On the Runtime tab, select Custom.
   d. Click Apply and Save.
   e. Click RTCGWServer.
   f. On the Runtime tab, click (not select) Custom.
   g. Select the STGWStats Group. The right panel shows the four counters that belong to Sametime Gateway.
   h. Select STGWCounters and click Enable. If you can’t find the STGWStats Group in the tree view, it means the object is not being called or initialized. This may be the result of no successful subscribes between communities.

2. To view statistics:
   a. In the Integrated Solutions Console, click Monitoring and Tuning > Performance Viewer.
   b. Click RTCGWServer.
   c. Expand Performance Modules.
   d. Select Communities under the STGWStats Group, or select STGWStats Group, or select both to see group and individual community data.
   e. Click View Module.

What to do next

In the sample below, STGWStats Group is selected to show community averages, and community ping62 and community pingwang are also selected to show individual community performance data.
Troubleshooting installation

These steps help you troubleshoot installation problems by describing how you can use a different tablespace name for the database and how you can clean your system of previous installations.

About this task

Many installation problems are caused when the installer cannot locate the database or when installing a new instance of Sametime Gateway and a previous installation has not been completely removed from the system. The following steps describe how to use a different tablespace in the database or clean your system of previous installations.

Procedure

1. Open the installation log file at \stgw_server_root\logs\installlog.txt
2. If log reports an error in finding the DB2 database, check to make sure you are using the tablespace name USERSPACE1. Sametime Gateway expects USERSPACE1 by default. To install using a different tablespace name, use the following command when you run the installer:
   
   `install.bat -VTableSpaceName="tableSpaceName"

   Where `tableSpaceName` is the name of the tablespace that you want the installer to use.
3. To clean your system of previous installations, use the log to find the location of the Install Shield Multiplatform (ISMP) database called the Vital Product Database (VPD). For example, examine this log entry from Windows (formatted to fit on the page):

   `(Nov 24, 2007 2:22:22 PM), stGwInstall, com.ibm.rtc.gateway.install.CheckVPDRegistry, msg1, using VPD registry at C:\Program Files\Common Files\InstallShield\Universal\common\Gen2\vpd\vpd`

   The location of this registry varies from system to system. On Windows, VPD is usually found in the `\Program Files\Common Files\InstallShield\Universal\common\Gen2` folder. If a Sametime Gateway server is uninstalled, but an error occurs and the product is not unregistered, the VPD shows that Sametime Gateway is installed on the system. When a new installation is initiated, and a previously installed Sametime Gateway server is detected, the installer prompts you to upgrade or install a new version, or the installer forces you to install a Deployment Manager server or a Primary Server on the same system. None of these scenarios are desired because there are no Sametime Gateway servers installed on the system.
4. Back up the `Gen2` folder. Note that the VPD registry may be used by other programs that are installed with InstallShield, so removing this registry may interfere with other programs. It’s recommended that you do not remove the `Gen2` folder unless absolutely necessary.
5. Remove the original `Gen2` folder.
6. If installing on Windows, delete the following left over files:
   
   - `C:\Windows\nifregistry`
   - `C:\Windows\vpd.properties`
7. Start the installation again.
Troubleshooting WebSphere Application Server

Transaction files may become locked and WebSphere Application Server may be in a state where nodes need to manually synchronized. If WebSphere Application Server is not responding in a logical manner, try carrying out these steps.

**Procedure**

1. Backup all configuration files on each node by running the backupConfig command.
2. Stop the node agents on each node.
3. Stop all servers.
4. Stop the Deployment Manager.
5. Manually synchronize the configurations, even if it says the nodes are fully synchronized, by copying the file system $stgw_profile_root/config$ directory from the Deployment Manager to the config directory on each cluster member, including the proxy server node.
6. Delete all tranlog lock files from the file system. On each node, delete the contents of $stgw_profile_root/tranlog$.
7. Delete files in the temp and wstemp directories. On each node, delete the contents of: $stgw_profile_root/temp$, $stgw_profile_root/wstemp$, and $stgw_profile_root/config/temp$.
8. Reboot each node.
9. Start the cluster.

**Related information**

- [WebSphere Application Server backupConfig command](wsadminbackupcommandreference)

Troubleshooting the Sametime Gateway using JVM logs

To start troubleshooting a problem, check the JVM log files first. These log files collect output for the System.out and System.err output streams for the application server process. One log file is specified for the SystemOut.log output stream and one file specified for the SystemErr.log output stream.

**About this task**

An application can write print data to the JVM logs either directly in the form of System.out.print() or System.err.print() method calls or by calling a JVM function, such as Exception.printStackTrace(). In addition, the System.out JVM log contains system message events written by the WebSphere Application Server. In the case of an IBM WebSphere Application Server Network Deployment configuration, JVM logs are also created for the deployment manager and each node manager, since they also represent JVMs.

- SystemOut.log is more useful monitoring the health of the running application server but can help in determining a problem, although it’s better to use the IBM Service log and the advanced capabilities of the Log Analyzer to determine a problem.
- SystemErr.log contains exception stack trace information that is useful when performing problem analysis.

The JVM log files are self-managing to the extent that they can be configured not to grow beyond a certain size. Also, you can set how many historical, or archived,
files to keep and which of the log files to rollover or archive based by time or size or both.

**Procedure**
1. In the Integrated Solutions Console, click **Troubleshooting --&gt; Logs and Trace**.
2. Click the **RTCGWServer**.
3. Under General Properties, click **JVM Logs**.

**Note:** Any configuration changes to the JVM logs that are made to a running RTCGWServer do not take effect until you restart the server.
4. To configure or change a log setting, use the settings on the Configuration tab.
5. To view the output of the logs, click the **Runtime** tab, then click **View**.

**Troubleshooting a failed WebSphere Application Startup**

In the event that a change is made to a WebSphere Application Server component of Sametime Gateway, WebSphere Application Server could fail to start.

**Procedure**
1. Use a text editor to open the WebSphere Application Server file here:
   `stgw_profile_root\config\cells\<CellName>\nodes\<NodeName>\servers\RTCGWServer\server.xml`.
2. In the server.xml file, search for `jvmEntries`. For example:
   ```xml
   <jvmEntries xmi:id="JavaVirtualMachine_1190064977109" verboseModeClass="false" verboseModeGarbageCollection="false" verboseModeJNI="false" initialHeapSize="1024" maximumHeapSize="1280" runHProf="false" debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
genericJvmArguments="-Xgcpolicy:gencon -Xgc:scvNoAdaptiveTenure, scvTenureAge=8, stdGlobalCompactToSatisfyAllocate -Xmm256m" disableJIT="false"/>
   ```

   If the JVM arguments are incorrect, you must modify the `genericJvmArguments` attribute of the `jvmEntries` element of server.xml. You could leave it blank, to eliminate all errors, or try modifying the value of the attribute until it is correct. Two value here are the heap sizes. These values are set when you set the JVM garbage collection policy. But you can set them set them in the server.xml as well. These values are the `initialHeapSize` with a recommended value of 1024, and `maximumHeapSize`, set to a recommended value of 1280.
3. Save the file and restart the server.

**Troubleshooting starting a cluster**

Complete these steps to troubleshoot starting a cluster of Sametime Gateway servers.

**Procedure**
1. View the log file `stgw_profile_root\logs\SystemOut.log` for errors such as these:
   ```
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWIS1538I: The messaging engine, ME_UUID=35D47B7F8071E6CC,
   INC_UUID=7F6C7FC371ED5F7, is attempting to obtain an exclusive lock on the data
   [CommonEventInfrastructure_Bus:STGW_Cluster.000-CommonEventInfrastructure_Bus]
   CWIS1545I: A single previous owner was found in the messaging engine's data store,
   ME_UUID=DEE28FEE74BF8BCE, INC_UUID=62266226371260A2
   ```
2. Use the Integrated Solutions Console to stop the Sametime Gateway servers, but do not stop the node agents.
3. Open a command window and navigate to: \stgw_profile_root\translog
4. Delete all the files in this directory.
5. Start the DB2 Control Center.
6. Click All Systems > <nodename> > Instances > DB2 > Databases > STGW > Tables.
7. Find the table named IBMWSSIB.SIBOWNER.
8. Select all rows that appear in this table and click Delete.
9. Click Commit and then close the DB2 Control Center.
10. Click Servers > Clusters.
11. Select the Sametime Gateway servers and click Start to start the cluster.
12. To ensure that the CommonEventInfrastructure_Bus has started properly, click Service Integration > Buses.
13. Click CommonEventInfrastructure_Bus.
14. Click Messaging engines.
15. Look for a status green arrow next to the @ClusterName@.000-CommonEventInfrastructure_Bus which indicates that the bus started correctly. If it is not started, check the SystemOut.log for details.

Troubleshooting secondary node problems

In a cluster configuration, when a primary node is stopped, and awareness or instant messaging is not working when relying on a secondary node, check to make sure there are virtual host definitions created for each cluster member for the configured ports.

About this task

View the log file \stgw_profile_root\logs\SystemOut.log for this error:

If you find this error, the virtual hosts definitions must be updated to have host aliases defined for the SIP ports configured on each cluster member.

Procedure

1. In the Integrated Solutions Console, gather the port configurations for each defined cluster member by selecting Servers > Application Servers.
2. Select a cluster member.
3. Under Communications, click **Ports**.
4. Record both the SIP_DEFAULTHOST and SIP_DEFAULTHOST_SECURE port numbers.
5. Repeat the preceding steps for each cluster member.
6. Select **Environment > Virtual Hosts**.
7. Select **default_host**
8. Under Additional Properties, click **Host Aliases**.
9. For each of the defined cluster members, ensure the ports that you recorded are present in the definitions.
   
   For example, if the secondary node is defined on server1.example.com at ports 5062 and 5063, ensure the host aliases are defined as *:5062 and *:5063.
10. To create a new virtual host definition:
    
    a. Click **New**.
    b. Type the Fully qualified domain name of the host.
    c. Type the port number.
    d. Click **OK** and **Save**.
    e. Repeat for each port that requires a virtual host.

**Troubleshooting connections to external communities**

Consult the SIP return codes when you are troubleshooting a failed connection to an external community.

**About this task**

While attempting to connect to external communities, various undocumented return codes are received in the event of error or configuration mismatches. Specifically, if a user has an issue while connecting to the SIP proxy, return codes 408 and 503 are returned. Use these return codes to determine what the Sametime Gateway error messages mean.

<table>
<thead>
<tr>
<th>SIP Return Code Range</th>
<th>Link to Table</th>
</tr>
</thead>
</table>

**Troubleshooting message handlers**

This topic discusses how to troubleshoot message handlers in various stopped and started or enabled and disabled conditions.

**Log messages**

If you see "Not all the message handlers are up" in the SystemOut.log:

- Use the Integrated Solutions Console to check if all default message handler plugins are up and running. Click **Applications > Enterprise Applications** to view the state of the message handler applications.
- Also check if any message handler is disabled. Click **Sametime Gateway > Message Handlers** to view the message handler list.
If an application is enabled and you stop an application without first disabling it, the plugin manager considers this as a fatal condition and starts failing the requests. To disable a plugin, disable the application from the message handler page first, then stop the application from Integrated Solutions Console. This will alert the core plugin manager to omit the message handler from the execution sequence without failing the requests.

**Message handler is disabled first and then stopped**

Always disable the message handler first, and then stop it before removing the message handler. If you are debugging the core functionality, and wishes to disable the plugin, this is the sequence to follow. When a message handler plugin stops after being disabled, the configuration service removes the message handler object from the database. The configuration service alerts the core plugin manager of the change, and the core plugin manager subsequently omits this message handler from the execution sequence without adversely affecting the requests. You do not need to restart the server in order to disable or delete the message handler.

**Message handler is stopped without being disabled first**

Stopping the message handler before disabling it creates an error condition. The core plugin manager fails all the requests until the message handler plugin is disabled.

**Message handler is disabled while it is running**

The core plugin manager takes the message handler plugin out of the execution sequence. Requests continue to be processed and the plugin application is not invoked. If the message handler plugin is enabled, the core plugin manager puts the plugin back in the execution sequence, and starts forwarding requests to the newly enabled plugin.

**Message handler is stopped, and then uninstalled without being disabled first**

Stopping the message handler before disabling it creates an error condition. Disabling the message handler does not remove the message handler from the configuration. The disabled message handler remains in the configuration until the next time Sametime Gateway starts.

**Related tasks**

“Enabling spam filtering” on page 143

You can extend the IBM Sametime Gateway by adding a message handler to perform SPIM (instant message spam) filtering, virus checking, additional logging, and so on. Use this page to add a message handler to the Sametime Gateway.

**Troubleshooting slow or missing awareness changes**

The IBM Sametime Gateway server uses the Sametime community server resolve mechanism for resolving emails of internal community users to Sametime Ids - the unique representation of a Sametime user - and resolving Sametime Ids to user details - email and home cluster.

**About this task**

For each resolve request, the Sametime community server consults the directory server. Receiving the response from the Sametime community server is time...
To provide a warning on unreasonable response times, the Sametime Gateway collects resolve statistics. By default, the Sametime Gateway provides a warning only if the response time of the resolve request is greater than 25 seconds. The warning time is configurable, and it is possible to change it by adding a custom property to the local community.

Custom property name: **resolver.stat**

Valid values:
- **All** - prints the response time of all resolve requests.
- **Number of seconds** - prints the response time of the resolve requests which are greater than the defined value.

To avoid a heavy load of messages on the Sametime Gateway server, for each 1000 identical messages only the first 5 are printed to the **SystemOut.log** file. If there are more than 5 identical messages, the first five are printed individually, followed by a summary of the rest of the identical messages. See below:


[6/9/09 15:39:58:948 IDT] 00000021 ResolverStat W com.ibm.rtc.gateway.vp.util.resolve. ResolverStat printToTrace The previous log message printed by this thread has been printed 5 times. The next 995 messages of this message code would not be printed to the log.

**Troubleshooting XMPP and Google community connections and awareness**

This section describes how to troubleshoot XMPP/Google community connection and awareness problems. You can find missing SRV records, and fix firewall wrong settings and "Google Apps" registration.

**About this task**

Follow these steps for troubleshooting XMPP/Google community connections and awareness

**Procedure**

1. If the XMPP/Google community cannot connect, check the following areas:
• The firewall is open for all possible incoming and outgoing connections from the other domain. For Google, see the following topic. Google sometimes changes their IPs, so the firewall should be updated: Opening ports in the firewalls.

• SRV records are well defined for ALL domains defined in the internal domains community page. Use the following command:

```
nslookup -type=SRV -class=all _xmpp-server._tcp.DOMAIN_NAME.com
```

Where `DOMAIN_NAME` is your domain name.

For example:

```
C:\>nslookup -type=SRV -class=all _xmpp-server._tcp.gvarim.com
unknown query class: all
Server: dhcpsrv3.haifa.ibm.com
Address: 9.148.45.11

_xmpp-server._tcp.gvarim.com SRV service location:
priority = 5
weight = 0
port = 5269
svr hostname = vmgwteam1.haifa.ibm.com
gvarim.com nameserver = dhcpsrv3.haifa.ibm.com
vmgwteam1.haifa.ibm.com internet address = 9.148.45.161
dhcpsrv3.haifa.ibm.com internet address = 9.148.45.11
```

- Your SRV record can be resolved by a public DNS. You can use the `nslookup` command from a computer outside the organization or by using public DNS resolution websites. You can use SRV verification instructions from this document: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21316296

- Your partner domain SRV record can be resolved by your DNS. Can be checked by this command:

```
nslookup -type=SRV -class=all _xmpp-server._tcp.DOMAIN_NAME.com
```

Where `DOMAIN_NAME` is your partner domain name.

For example:

```
C:\>nslookup -type=SRV -class=all _xmpp-server._tcp.google.com
unknown query class: all
Server: dhcpsrv3.haifa.ibm.com
Address: 9.148.45.11

Non-authoritative answer:
_xmpp-server._tcp.google.com SRV service location:
priority = 20
weight = 0
port = 5269
svr hostname = xmpp-server1.1.google.com
_xmpp-server._tcp.google.com SRV service location:
priority = 20
weight = 0
port = 5269
svr hostname = xmpp-server2.1.google.com
```

- For Google, make sure there is no domain from your defined internal domains, which is registered with “Google Apps.” See this Technote: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21295505

2. If an XMPP proxy is installed, check the following:

• Your proxy should listen to the correct port and not conflict with another port definition on this machine. See the following topic: Configuring the XMPP proxy server.
Custom properties well defined with the correct cluster node and proxy name. See the following topic: Configuring the XMPP proxy server.

3. If there is no awareness after the community is already connected:
   - For Google, make sure there is no domain from your defined internal domains, which is registered with “Google Apps.” See this technote:
   - For the Assign Users definitions, see the following topic: Assigning users access to external communities
   - For presence and chat limitations, see the following topic: Limiting Sametime Gateway global and community-level sessions.

4. If there are still connection and awareness issues, see the following Technote on collecting data: http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg21316296

**Error message severity levels and situations**

This topic describes error message severity levels and the situations in which you are likely to encounter them.

In addition to the following information, see "Monitoring Sametime Gateway system events by tailing the SystemOut.log file" in the IBM Sametime wiki.

There are three message severity levels:
- Informational: the event only contains general information and is not reporting an error.
- Warning: a harmless error event that won't interfere with normal operation or a significant event that might require an action on the administrator's part.
- Error: Minor, Critical, and Fatal events.

The following situations will prompt log messages:
- Any message written to the server console.
- Any operation or action that affects the operation of the system such as starting and stopping a server or reconfiguration.
- Any changes to connected systems or environment (network connectivity, database availability) that can affect the components' continued operation.
- Failures or errors of any related component and any recovery or restart operations performed.
- Any response to operator commands for statistics, status, or other information that might need to be correlated to other events or information.

The following types of messages might be issued:

**Start messages**

indicate when a component begins the startup process, finishes the startup process, or aborts the startup process. Start messages could include words like: starting, started, initializing, and initialized.

**Stop messages**

indicate when a component begins to stop, has stopped, or has failed to stop. Stop messages could include words like: stop, stopping, stopped, completed, and exiting.
Feature messages
announce when a component feature is ready (or not ready) for service requests. Messages could include words like: now available, currently available, and transport is listening on port 123.

Dependency messages
Are produced by a component that cannot find another component or feature that it needs, such as messages about not finding the expected version of the component or that say a resource was not found, or that an application or subsystem that was unavailable. Dependency messages could include words like: could not find, and no such component.

Request messages
Identify the completion status of a request. Typically these requests are complex management tasks or transactions that a component undertakes on behalf of a requester and not the mainline simple requests or transactions. Request messages could include words like: configuration synchronization started, and backup procedure completed.

Configure messages
Identify any changes that a component makes to its configuration or messages that describe current configuration state. Configure messages could include words like: port number is, address is, and process id.

Connect messages
Identify aspects about a connection to another component, for example, that say a connection failed, was created, or has ended. Connect messages could include words like: connection reset, connection failed, and failed to get a connection.

Create messages
Register when a component creates an entity, for example, indicating that a document or file was created or that an EJB was created. Create messages could include words like: was created, about to create, and now exists.

Report messages
Collect heartbeat or performance data reported from a component, such as current CPU utilization or current memory heap size. Report messages could include words like: utilization value is, buffer size is, and number of threads is.

Availability messages
Report data about a component’s operational state and availability. This situation provides a context for operations that can be performed on the component by distinguishing whether a product is installed, operational and ready to process functional requests, or operational but ready or not ready to process management requests. This type of message is different from Dependency messages, which pertain to services. Availability messages could include words like: now ready to take requests, online, and offline.

Troubleshooting installation or uninstallation
Use the following topics to troubleshoot problems that occur after installing and uninstalling IBM Sametime servers.

Troubleshooting a Sametime System Console installation
To install the IBM Sametime System Console server, the DB2 application user ID must have administrator rights to be able to create and update tables in the
database. If the user does not have administrator rights and installation was not successful, follow these steps to create the tables required by the installation program.

**About this task**

Connect to the system console database (for example, STSC). Then enter the `createSchedTable.ddl` command to create additional tables in the database.

**AIX, Linux, or Solaris**

```
db2 connect to STSC

db2 -tf createSchedTable.ddl
```

**Windows**

```
db2cmd

db2 connect to STSC

db2 -tf createSchedTable.ddl
```

**Troubleshooting a Sametime Gateway installation**

These steps help you troubleshoot installation problems by describing how you can use a different tablespace name for the database and how you can clean your system of previous installations.

**About this task**

Many installation problems are caused when the installer cannot locate the database or when installing a new instance of Sametime Gateway and a previous installation has not been completely removed from the system. The following steps describe how to use a different tablespace in the database or clean your system of previous installations.

**Procedure**

1. Open the installation log file at `stgw_server_root\logs\installlog.txt`

2. If the log reports an error in finding the DB2 database, check to make sure you are using the tablespace name `USERSPACE1`. Sametime Gateway expects `USERSPACE1` by default. To install using a different tablespace name, use the following command when you run the installer:

   ```
   install.bat -VTableSpaceName="tableSpaceName"
   ```

   Where `tableSpaceName` is the name of the tablespace that you want the installer to use.

3. To clean your system of previous installations, use the log to find the location of the Install Shield Multipanother (ISMP) database called the Vital Product Database (VPD). For example, examine this log entry from Windows (formatted to fit on the page):

   ```
   (Dec 24, 2009 2:22:22 PM), stGwInstall,
   com.ibm.rtc.gateway.install.CheckVPDRegistry, msg1,
   using VPD registry at C:\Program Files\Common Files\InstallShield\Universal\common\Gen2\vpddb\vpd
   ```
The location of this registry varies from system to system. On windows, VPD is usually found in the \Program Files\Common Files\InstallShield\Universal\common\Gen2 folder. If a Sametime Gateway server is uninstalled, but an error occurs and the product is not unregistered, the VPD shows that Sametime Gateway is installed on the system. When a new installation is initiated, and a previously installed Sametime Gateway server is detected, the installer prompts you to upgrade or install a new version, or the installer forces you to install a Deployment Manager server or a Primary Server on the same system. None of these scenarios are desired because there are no Sametime Gateway servers installed on the system.

4. Back up the Gen2 folder. Note that the VPD registry may be used by other programs that are installed with InstallShield, so removing this registry may interfere with other programs. Do not remove the Gen2 folder unless it is absolutely necessary.

5. Remove the original Gen2 folder.

6. If installing on Windows, delete the following left over files:
   - C:\Windows\.nifregistry
   - C:\Windows\vpd.properties

7. Start the installation again.

Registering a Sametime server manually on AIX, Linux, Solaris, and Windows

On IBM AIX, Linux, Sun Solaris, and Microsoft Windows, you can manually register an IBM Sametime server from the console if a problem occurs during the installation process and results in a failure to register the server.

About this task

A successful registration on AIX, Linux, Solaris, or Windows automatically registers the following servers from the Sametime System Console:
- Sametime Community Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server

If a problem arises during installation and the server is not successfully registered, follow the instructions in the appropriate topic below to complete the registration:

Registering a Community Server manually on AIX, Linux, Solaris, and Windows

If automatic registration fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime Community server with the Sametime System Console.

Before you begin

The Sametime System Console must be started.

About this task

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

Procedure
1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's Sametime console directory:
      • **AIX, Linux, Solaris**: The console directory is under the Community Server data directory; for example: /opt/IBM/domino85/notesdata/console
      • **Windows**: The console directory is under the Domino directory; for example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and productConfig.properties files.

2. Update the following values in the console.properties file and save the file.
   **Table 44. 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. |
   |            | For example, on Windows the file is stored at: C:/IBM/WebSphere/AppServer/profiles/AppServerProfile/logs/AboutThisProfile.txt |
   | SSCUserName | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin. |
   | SCCPassword | Enter the WebSphere Application Server password associated with the SCCUserName. |
   | SSCSSLEnabled | Change this value to "true" to connect to the Sametime System Console using a secure connection. |
   | SSCHTTPSPort | Specify the HTTPS port used by the Sametime System Console server if SSCSSLEnabled is set to "true." |

3. Verify that the settings in the productConfig.properties file are correct, modifying them as needed before saving and closing the file.
   Only the required values in this file are listed here:
   **Table 45. productConfig.properties settings**
   | DepName | Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console. |
   | NodeHostName | Provide the fully qualified host name for the Community Server that is being registered. |

4. Start the Sametime Community Server.
5. Now register the server:
a. Run the registerSTServerNode registration utility from the /console directory.
   - AIX, Linux, Solaris: registerSTServerNode.sh
   - Windows: registerSTServerNode.bat

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

Registering and federating a Sametime Proxy Server, Media Manager, Meeting Server, or Sametime Advanced manually on AIX, Linux, Solaris, and Windows

If automatic registration and federation fails after installing from a deployment plan on AIX, Linux, Solaris, or Windows, you can manually register an IBM Sametime server with the Sametime System Console. This process also federates the node if it was not federated after installation.

Before you begin

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

About this task

This procedure works for the following Sametime servers:

- Sametime Proxy Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Advanced

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

- console.properties
- productConfig.properties

Procedure

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

| SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
**Table 46. 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 SSCSSEnabled 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>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>

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 47. Sametime Proxy Server**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

**Table 48. Sametime Media Manager**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WAS UserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

**Note:** Remove any values for STCommunityServerHost or STCommunityServerPort in the productConfig.properties file when you are preparing to register a Media Manager with the Packet Switcher component. The Community server is not a prerequisite for Packet Switcher and these values cause registration to fail.

**Table 49. Sametime Meeting Server**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBAppPassword</td>
<td>Specify the password associated with the database ID.</td>
</tr>
</tbody>
</table>
Table 49. Sametime Meeting Server (continued)

<table>
<thead>
<tr>
<th>WASPassword</th>
<th>Specify the password associated with the WASUserID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

Table 50. Sametime Advanced

<table>
<thead>
<tr>
<th>DBAppPassword</th>
<th>Specify the password associated with the database ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>Provide a descriptive name for your deployment. It must be a unique deployment name on the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

4. If you are registering a Sametime Meeting Server, start the server. Otherwise, proceed to the next step.

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

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

Manually removing WebSphere Application Server

You may need to remove WebSphere Application Server manually if it remains on the system after Sametime fails to install or uninstall completely. WebSphere Application Server is installed when you install the following Lotus Sametime servers: Sametime System Console, Sametime Proxy Server, Sametime Media Manager, Sametime Meeting Server, and Sametime Gateway.

Manually removing WebSphere Application Server on AIX, Linux, Solaris, and Windows

Remove WebSphere Application Server on AIX, Linux, Solaris, and Windows manually if it remains on the system after Sametime fails to install or uninstall completely.

Before you begin

Stop all servers associated with the Sametime server in the order shown below. For more information, see Command reference for starting and stopping servers.

1. Log in to the Integrated Solutions Console on the Deployment Manager and stop the node agent for the server (or servers if you are working in a cluster).
2. Stop the Sametime server.
3. Stop WebSphere Application Server.
4. Stop the Deployment Manager.
5. Close all browsers and command windows that are accessing the server you plan to uninstall.

**About this task**

If after an attempted Sametime install or uninstall, you have many files and folders left in `was_install_root/profiles/profile_name` or `was_install_root/bin`, run the WebSphere Application Server uninstall program to remove the rest of the files. Remove WebSphere Application Server only if it is not in use by any other server on the system.

**Windows**

1. From the Microsoft Windows Start menu, select **Settings > Control Panel > Add/Remove Programs**.
2. Select **IBM WebSphere Application Server** from the list and click **Add/Remove**. Click **Yes** when prompted to remove the server.
3. When the Windows uninstall program completes, click **OK** to exit the uninstall program.
4. Delete the WebSphere Application Server installation directory (for example, `C:\Program Files\IBM\WebSphere`).

**AIX, Linux, Solaris**

1. Go to the WebSphere Application Server installation root folder (for example, `/opt/IBM/WebSphere/Appserver`).
2. Navigate to the uninstall folder.
3. Run the uninstall command:
   ```
   ./uninstall
   ```
4. After uninstallation completes, delete the WebSphere Application Server installation directory (for example, `/opt/IBM/WebSphere/AppServer`).

For more information, see Uninstalling the WebSphere Application Server product in the WebSphere Application Server information center.

**Manually removing WebSphere Application Server on IBM i**

Remove WebSphere Application Server on IBM i manually if you have removed all Sametime servers from the system, and no longer want the program installed.

**Before you begin**

Stop all servers running on the WebSphere Application Server system. If the server belongs to a cluster, you will also need to stop all node agents in the cluster, and then stop the Deployment Manager. Finally, close all browsers and command windows that may have been accessing the WebSphere Application Server.

**About this task**

After uninstalling a Sametime server from IBM i, WebSphere Application Server will still be installed on the system. You may choose to uninstall WebSphere Application Server only if it is not in use by any other server on the system.
Stop all java processes. Then follow the steps in the WebSphere Application Server 7 Information Center to remove unneeded WebSphere Application Server software from the system:

Uninstalling the product on IBM i

**Manually removing DB2 data on AIX, Linux, Solaris, and Windows**

If DB2 installation or uninstallation was unsuccessful, you can follow these steps to manually remove DB2 and other files.

**About this task**

Remove the DB2 software, then remove the rest of the DB2 files and data left on the system.

**Procedure**

1. Remove the DB2 from your operating system. For example, if you are running DB2 on Windows, use the Control Panel, Add/Remove Programs panel and remove the programs.
2. Remove all files in the local /tmp or temp directory.
3. Manually remove user and group information.
   - **Linux**
     - Remove user home directories under /home.
     - DB2 Instance user account: db2admin (or the administrator account specified during installation)
     - DB2 Administration Server (DAS) user account: dasuser1
     - DB2 users group: db2admin (or the same as the DB2 Instance user account name defined by user)
     - DB2 Administration users group: dasadm1
   - **Windows**
     - Remove DB2 users and groups:
     - DB2 Instance user account: db2admin (or the administrator account specified during installation)
     - DB2 Administration Server (DAS) user account: db2admin
     - DB2 users group: DB2USERS
     - DB2 Administration users group: DB2ADMNS
4. Remove these directories for DB2.
   - The directories below show the Windows path. They will differ on Linux.
   - c:\documents and settings\all users\application data\ibm\db2
   - c:\documents and settings\all users\application data\ibm\db2history
   - c:\documents and settings\db2admin
   - c:\documents and settings\install user\application data\ibm\vshet
   - c:\documents and settings\install user\application data\ibm\db2
5. Delete the remaining DB2 directories.
Unregistering a Sametime server on AIX, Linux, Solaris, or Windows

On IBM AIX, Linux, Sun Solaris, and Microsoft Windows, you can manually unregister an IBM Sametime server from the console if a problem occurs during the uninstallation process and results in a failure to unregister the server.

About this task

A successful unregistration on AIX, Linux, Solaris, or Windows automatically unregisters the following servers from the Lotus Sametime System Console:

- Sametime Community Server
- Sametime Media Manager
- Sametime Meeting Server
- Sametime Proxy Server

If a problem arises during uninstallation and the server is not successfully unregistered, follow the instructions in the appropriate topic below to complete the unregistration:

Unregistering a Sametime Community Server

To remove an IBM Sametime Community Server from the list of the Sametime System Console's managed servers, run the unregister utility on the server. This step is required before uninstalling a Community Server that you installed without a deployment plan and then registered with the Sametime System Console later using the registration utility. If you installed the server with a deployment plan, unregistering is only needed if you are performing some other activity that requires removal of the product from the console.

Before you begin

The Sametime System Console must be started.

About this task

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

- console.properties
- productConfig.properties

Procedure

1. Back up the console.properties and productConfig.properties files:
   a. Navigate to the Community Server's Sametime console directory:
      - AIX, Linux, Solaris: The console directory is under the Community Server data directory; for example: /opt/IBM/domino85/notesdata/console
      - Windows: The console directory is under the Domino directory; for example: C:\Lotus\Domino\console
   b. Make back-up copies (using different names) of the console.properties and productConfig.properties files.
2. Update the following values in the console.properties file and save the file.
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 52. productConfig.properties settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DepName</td>
<td>The Dep Name must be the name that was used when you installed: the unique name for this deployment as known by the Sametime System Console.</td>
</tr>
<tr>
<td>NodeHostName</td>
<td>Provide the fully qualified host name for the Community Server that is being unregistered.</td>
</tr>
</tbody>
</table>

4. Start the Sametime Community Server.

5. Now unregister the server:

   a. Run the unregister utility with the following command:
      - **AIX, Linux, Solaris:** `unregisterProductNode.sh`
      - **Windows:** `unregisterProductNode.bat`

   b. As the unregister utility runs, you will be prompted to enter the Location of the notes.ini file. You are only prompted for the notes.ini file location when unregistering the server. Type the full path to the directory containing the notes.ini file (for example, `/stserver/data`), and press Enter.

   The utility unregisters the server, generating a log file called `ConsoleUtility.log` and storing it in the `console/logs` directory. If the unregistration is successful, the `console.pid` will be removed.
Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when
server unregistration fails” on page 281
If you attempted to unregister an IBM Sametime server from the console using
either the uninstallation program or the manual unregistration utility and it failed,
you can update the console itself to complete the unregistration task. You can also
use this method if the installed server has failed and cannot be uninstalled or
unregistered.

Unregistering a Sametime Proxy Server, Media Manager, Meeting
Server, or Sametime Advanced
To unregister an IBM Sametime server from the list of the Sametime System
Console's managed servers, run the unregister utility on the server. You do not
normally need to unregister a Sametime server. This step is needed only if there
was a problem with the uninstallation or you are performing some other activity
that requires removal of the product from the console.

About this task
This procedure works for the following Sametime servers:
• Sametime Proxy Server
• Sametime Media Manager
• Sametime Meeting Server
• Sametime Advanced

Skip this task if you are uninstalling the Sametime System Console.

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

Procedure
1. Back up the console.properties and productConfig.properties files:
   a. On the server to be unregistered, navigate to the InstallLocation/console
directory.
   b. Make backup copies (using different names) of the console.properties and
      productConfig.properties files.
2. Update the following values in the console.properties file and save the file.
   
   Table 53. 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>
</table>

278  IBM Sametime: Administration Guide
Table 53. `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 <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 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 54. 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 55. Sametime Media Manager

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>DepName</td>
<td>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 56. 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>
</tbody>
</table>
Table 56. Sametime Meeting Server (continued)

<table>
<thead>
<tr>
<th>DepName</th>
<th>The unique descriptive name of the deployment as it was registered with the Sametime System Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeHostName</td>
<td>The fully qualified host name of the server.</td>
</tr>
</tbody>
</table>

Table 57. Sametime Advanced

<table>
<thead>
<tr>
<th>DBAppPassword</th>
<th>Specify the password associated with the database ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WASPassword</td>
<td>Specify the password associated with the WASUserID.</td>
</tr>
<tr>
<td>LDAPBindPwd</td>
<td>Specify the password associated with the LDAPBindDN.</td>
</tr>
<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. Now unregister the server:
   a. Run the `unregisterWASProduct.sh` unregistration utility from the `/console` directory.
      - **AIX, Linux, Solaris**: `./unregisterWASProduct.sh`
      - **Windows**: `unregisterWASProduct.bat`
      The utility unregisters the server, generating a log file called `ConsoleUtility.log` and storing it in the `console/logs` directory. If the unregistration is successful, the `console.pid` will be removed.

Related tasks
“Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails” on page 281
If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**Updating the Sametime System Console when server unregistration fails**

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**About this task**

The steps for removing the server's entry from the Sametime System Console's database vary with the operating system on which the console runs:
Updating the Sametime System Console on AIX, Linux, Solaris, or Windows when server unregistration fails

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

Before you begin

Make a note of the product type, host name, install type, and deployment name for the Sametime server you want to remove.

About this task

This utility removes information about a Sametime server from the IBM DB2 database used by the Sametime System Console, effectively unregistering the server. This method is useful when you are unable to complete the unregistration task from the server itself; for example:

- If you have run an uninstall, and received an error message stating that the Sametime System Console could not be contacted to remove the server from the configuration.
- If you experienced a catastrophic server failure and cannot run the uninstallation program or the unregistration utility on that server.
- If you want to force the removal of a server from the Sametime System Console's topology for some reason and the unregistration utility failed.

Procedure

1. Working on the Sametime System Console server, navigate to the InstallLocation/console directory.
2. Update the following values in the console.properties file before saving and closing the file:

   | SSCHostName | Provide the fully qualified host name of the Sametime System Console server. |
   | SSCHTTPPort | Specify the HTTP port used for the Sametime System Console server if SSL is not enabled and the value for SSCSSLEnabled is "false." |
   | SSCUserPassword | Enter the IBM WebSphere Application Server User ID that you created when you installed Sametime System Console. The default is wasadmin. |
   | SSCPassword | Enter the WebSphere Application Server password associated with the SSCUserName. |

3. Run the updateStaleEntry utility:
   a. Open a command window and run the following command:
      - AIX, Linux, Solaris: ./updateStaleEntry.sh -uninstall
• **Windows:** updateStaleEntry.bat -uninstall

b. When prompted, provide the product type, host name, install type, and deployment name for the Sametime server that you are removing from the console's database.

The utility removes the server from the database and generates the ConsoleUtility.log file, storing it in the console/logs directory.

4. Restart the Sametime System Console.

**Updating the Sametime System Console on IBM i when server unregistration fails**

If you attempted to unregister an IBM Sametime server from the console using either the uninstallation program or the manual unregistration utility and it failed, you can update the console itself to complete the unregistration task. You can also use this method if the installed server has failed and cannot be uninstalled or unregistered.

**Before you begin**

Make a note of the product type, host name, install type, and deployment name for the Sametime server you want to remove.

**About this task**

This utility removes information about a Sametime server from the IBM DB2 database used by the Sametime System Console, effectively unregistering the server. This method is useful when you are unable to complete the unregistration task from the server itself; for example:

• If you have run an uninstall, and received an error message stating that the Sametime System Console could not be contacted to remove the server from the configuration.

• If you experienced a catastrophic server failure and cannot run the uninstallation program or the unregistration utility on that server.

• If you want to force the removal of a server from the Sametime System Console's topology for some reason and the unregistration utility failed.

**Procedure**

1. Working on the Sametime System Console server, navigate to the /QIBM/UserData/Lotus/stii_ssc/console directory.

2. Update the following values in the console.properties file before saving and closing the file:

<table>
<thead>
<tr>
<th>SSCHostName</th>
<th>Provide the fully qualified host name of the Sametime System Console server.</th>
</tr>
</thead>
</table>

*Table 59. console.properties settings*
Table 59. console.properties settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSCHTTPPort</strong></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><strong>SSCUserName</strong></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><strong>SSCPassword</strong></td>
<td>Enter the WebSphere Application Server password associated with the SSCUserName.</td>
</tr>
</tbody>
</table>

3. Run the updateStaleEntry utility:
   a. From an IBM i command line, run the following command to start the QShell Interpreter: QSH
   b. Navigate to the server's console directory; for example: cd /stserver/data/console.
   c. Run the shell script to unregister the cluster: updateStaleEntry.sh.
   d. When prompted, provide the product type, host name, install type, and deployment name for the Sametime server that you are removing from the console's database.
   e. When the utility finishes, press F3 to exit QSH.
      The utility removes the server from the database and generates the ConsoleUtility.log file, storing it in the console/logs directory.

4. Restart the Sametime System Console.

Log file locations

Use this reference to locate log files for IBM Sametime components.

Collecting the proper files and information helps to expedite problem determination and resolution for IBM Sametime when you are working with IBM Support. Provide the following information:

* A precise description of the issue, error message, and steps to reproduce
* Applicable screen shots of the problem or error message
* Log files pertaining to your problem

Installation Files

Installation log files can be found in the following locations:

- **Windows**
  C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs
  C:\ProgramData\IBM\Installation Manager\logs
- **AIX/Linux/Solaris**
  `/var.ibm/InstallationManager/logs`
- **Websphere-based application log files** are created on the server's file system for each server's instance.
  `WebSphere_install_directory/profiles/program-profile/logs/*`
- **IBM i**
  `/QIBM/UserData/LOTUS/stii/logs`

### Sametime System Console

Sametime System Console log files can be found in the following locations:

- **Windows**
  - C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCDMgrProfile\logs
  - C:\Program Files\ibm\WebSphere\AppServer\profiles\STSCAppProfile\logs
- **AIX/Linux/Solaris**
  - `/opt/IBM/WebSphere/AppServer/profiles/STSCDMgrProfile/logs`
  - `/opt/IBM/WebSphere/AppServer/profiles/STSCAppProfile/logs`
- **IBM i**
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCDMgrProfile/logs`
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STSCAppProfile/logs`

### Sametime Proxy Server

Sametime Proxy Server log files can be found in the following locations:

- **Windows**
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STPAppProfile\logs
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STPDMgrProfile\logs
- **AIX/Linux/Solaris**
  - `/opt/IBM/WebSphere/AppServer/profiles/STPDMgrProfile/logs`
  - `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile/logs`
- **IBM i**
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPDMgrProfile/logs`
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STPAppProfile/logs`

### Sametime Meeting Server

Sametime Meeting Server log files can be found in the following locations:

- **Windows**
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STMDMgrProfile\logs
  - C:\Program Files\IBM\WebSphere\AppServer\profiles\STMAppProfile\logs
- **AIX/Linux/Solaris**
  - `/opt/IBM/WebSphere/AppServer/profiles/STMDMgrProfile/logs`
  - `/opt/IBM/WebSphere/AppServer/profiles/STMAppProfile/logs`
- **IBM i**
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMDMgrProfile/logs`
  - `/QIBM/UserData/Websphere/AppServer/V7/SametimeWAS/profiles/STMAppProfile/logs`
Sametime Media Manager

Sametime Media Manager log files can be found in the following locations:

- **Windows**
  
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSMgrProfile\logs
  C:\Program Files\IBM\WebSphere\AppServer\profiles\STMSAppProfile\logs

- **Linux**
  
  /opt/IBM/WebSphere/AppServer/profiles/STMSMgrProfile/logs
  /opt/IBM/WebSphere/AppServer/profiles/STMSAppProfile/logs

Sametime Community Server

The Sametime Community Server has a series of configuration and log files for problem determination. You can run a script that automatically collects these logs.

- **Windows**
  
  From the Domino program directory, run the stdiagzip.bat file.
  For example:
  
  C:\Program Files\ibm\Lotus\Domino\stdiagzip.bat

- **AIX/Linux/Solaris**
  
  /local/notesdata> sh stdiagzip.sh
  
  A zip file generated by the stdiagzip script is created in the data_dir/Trace directory

- **IBM i**
  
  call QSAMETIME/STDIAGZIP servername
  
  A zip file generated by the stdiagzip program is created in the data_dir/trace directory

Sametime clients

The Sametime Connect log files are in the logs directory, which is located under the client workspace directory. For example, logs are located in the following directory on Windows XP:

C:\Documents and Settings\user_name\Application Data\Lotus\Sametime\logs

Logs for the Sametime web audio-visual plugin are stored in the following locations:

- **Microsoft Windows XP:** %APPDATA%\IBM\Lotus\Sametime WebPlayer\n- **Windows Vista and Windows 7:** %USERPROFILE%\AppData\LocalLow\IBM\Lotus\Sametime WebPlayer\n- **Mac OS X:** $HOME/Library/Application Support/IBM/Lotus/Sametime WebPlayer\n
Related concepts
“Logging and tracing on Sametime Connect” on page 213
IBM Sametime Connect users can enable tracing on their clients.

Related tasks
“Locating the Sametime Connect workspace” on page 216
Both IBM Sametime Connect and IBM Lotus Notes store user-specific data, including configuration data, preferences, and trace logs, in a workspace folder on your local hard drive or a network drive. In order to diagnose Sametime Connect issues, you might be asked to update or collect files in your workspace.

Directory conventions
Directory variables are abbreviations for the default installation paths for IBM AIX, Linux, Solaris, IBM i, and Microsoft Windows. This topic defines the directory variable and its matching default installation directory for each supported operating system.

<table>
<thead>
<tr>
<th>Directory variable</th>
<th>Operating system</th>
<th>Default installation root</th>
</tr>
</thead>
<tbody>
<tr>
<td>was_install_root</td>
<td>AIX</td>
<td>/usr/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/usr/IBM/WebSphere/AppServer7</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt/IBM/WebSphere/AppServer7</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/ProdData/WebSphere/AppServer/V7/ND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/QIBM/ProdData/WebSphere/AppServer7/V61/ND</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[drive]:\Program Files\IBM\WebSphere\AppServer7</td>
</tr>
<tr>
<td>Directory variable</td>
<td>Operating system</td>
<td>Default installation root</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><code>app_server_root</code></td>
<td>AIX</td>
<td><code>/usr/IBM/WebSphere/AppServer</code></td>
</tr>
<tr>
<td>Root directory for the creation of WebSphere Application Server profile directories.</td>
<td>For Sametime Gateway upgrade: If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: <code>/usr/IBM/WebSphere/AppServer7</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td><code>/opt/IBM/WebSphere/AppServer</code></td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td><code>/QIBM/UserData/WebSphere/AppServer/V7/ND</code></td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td><code>[drive]:\Program Files\IBM\WebSphere\AppServer</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade: If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: <code>[drive]:\Program Files\IBM\WebSphere\AppServer7</code></td>
</tr>
<tr>
<td><code>stSSC_profile_root</code></td>
<td>All platforms Primary node</td>
<td><code>app_server_root/profiles/STSCAppProfile</code></td>
</tr>
<tr>
<td>The Sametime System Console profile directory</td>
<td>Secondary node</td>
<td><code>app_server_root/profiles/STSCAppProfile</code></td>
</tr>
<tr>
<td><code>stM_profile_root</code></td>
<td>All platforms Primary node</td>
<td><code>app_server_root/profiles/STMAppProfile</code></td>
</tr>
<tr>
<td>The Sametime Meeting Server profile directory</td>
<td>Secondary node</td>
<td><code>app_server_root/profiles/STMSAppProfile</code></td>
</tr>
<tr>
<td><code>stP_profile_root</code></td>
<td>All platforms Primary node</td>
<td><code>app_server_root/profiles/STPAppProfile</code></td>
</tr>
<tr>
<td>The Sametime Proxy Server profile directory</td>
<td>Secondary node</td>
<td><code>app_server_root/profiles/STPSAppProfile</code></td>
</tr>
<tr>
<td><code>stMS_profile_root</code></td>
<td>All platforms Primary node</td>
<td><code>app_server_root/profiles/STMSAppProfile</code></td>
</tr>
<tr>
<td>The Sametime Media Manager profile directory</td>
<td>Secondary node</td>
<td><code>app_server_root/profiles/STMSSAppProfile</code></td>
</tr>
<tr>
<td><code>stgw_profile_root</code></td>
<td>AIX</td>
<td><code>/opt/IBM/WebSphere/AppServer/profiles/RTCGW_Profile[1,2,...]</code></td>
</tr>
<tr>
<td>Sametime Gateway profile directory</td>
<td>For Sametime Gateway upgrade: If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: <code>/opt/IBM/WebSphere/AppServer7/profiles/RTCGW_Profile[1,2,...]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td><code>/opt/IBM/WebSphere/AppServer/profiles/RTCGW_Profile[1,2,...]</code></td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td><code>/QIBM/UserData/WebSphere/AppServer/V7/ND/RTCGW_profile</code></td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td><code>[drive]:\Program Files\IBM\WebSphere\AppServer7/profiles/RTCGW_Profile[1,2,...]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sametime Gateway upgrade: If you upgraded from 8.0.x (WebSphere 6) to 8.5.x (WebSphere 7), the default installation root is: <code>[drive]:\Program Files\IBM\WebSphere\AppServer7/profiles/RTCGW_Profile[1,2,...]</code></td>
</tr>
<tr>
<td>Directory variable</td>
<td>Operating system</td>
<td>Default installation root</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>stgw_server_root</td>
<td>AIX</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td></td>
<td>Linux and Solaris</td>
<td>/opt/IBM/WebSphere/STgateway</td>
</tr>
<tr>
<td></td>
<td>IBM i</td>
<td>/QIBM/UserData/STgateway/[profile name]</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>[drive]\Program Files\IBM\WebSphere\STgateway</td>
</tr>
<tr>
<td>stADV_profile_root</td>
<td>All platforms</td>
<td><strong>Primary node</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STADVVPNProfile</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Secondary node</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>app_server_root/profiles/STADVSNProfile</td>
</tr>
</tbody>
</table>
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
5 Technology Park Drive
Westford Technology Park
Westford, MA 01886
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy,
modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

These terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM  
AIX  
DB2  
DB2 Universal Database Domino  
Domino  
Domino Designer  
Domino Directory  
i5/OS  
Lotus  
Lotus Notes  
Notes  
OS/400  
Sametime  
WebSphere

AOL is a registered trademark of AOL LLC in the United States, other countries, or both.

AOL Instant Messenger is a trademark of AOL LLC in the United States, other countries, or both.

Google Talk is a trademark of Google, Inc, in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.