Introducing the *reliability* *failover* *clustering* Sametime Enterprise Meeting Server

Level: Beginner
Works with: Sametime 3.0
Updated: 03-Sep-2002

by
Kay
Saffari

The Sametime Enterprise Meeting Server (EMS) is an important addition to the Sametime world. What is EMS, and what does it offer to you, the administrator? EMS is a new application in the Sametime family that works in conjunction with the core Sametime 3.0 server to better handle Sametime environments with large user populations. EMS allows you to create and manage a Sametime Meeting Services server cluster.

You can use EMS to:
- Cluster Meeting Services and Community Services to provide failover for online meetings and for presence and chat functions
- Make changes to all servers managed by EMS, or to change individual servers within the Meeting Services cluster
- Find meetings from one central location
- Load-balance among servers in a cluster so that no one server is more heavily taxed than another

More improvements with EMS include better scalability and better use of system resources through load-balancing across the clustered servers. This article provides an overview of EMS, including its features and administrative capabilities. It assumes that you are familiar with Sametime server administration.

EMS architecture
EMS is a new application in the Sametime family that is used with the Sametime 3.0 server. EMS is a Java 2 Enterprise Edition (J2EE) application that uses Java servlets, JavaServer Pages (JSP), Java Database Connectivity (JDBC), Java Message Service (JMS), Java applications, tag libraries, and a relational database. Before installing EMS, you must set up a J2EE environment that includes the following components:
- IBM Universal Database v7.2
- IBM MQSeries v5.2.1
- IBM WebSphere Application Server v4.0

Because EMS relies on standard Java APIs, it should work with any platform. To date, it has been tested in the Win32 environment. EMS was built and tested on WebSphere 4.0.2 and 4.0.3. However, EMS is not limited to use with WebSphere; you can install EMS on other J2EE application servers. EMS uses the DB2 relational database, which has proven to be a reliable and scalable database. DB2 can be used with other databases.

EMS, Sametime, WebSphere, and Domino
You install EMS on a dedicated machine, then use EMS to cluster your Sametime 3.0 servers. While EMS requires a J2EE server to run, the Sametime 3.0 servers require Domino. In fact, you must install Sametime 3.0 on top of a Domino 5.0.10 server. To connect the Sametime servers to EMS, you apply a Sametime service pack to the server and then add the server to the cluster using the administration tool available from EMS.

The servers in the cluster are managed by EMS and are referred to as "room servers." The room servers have Meeting Services and Community Services. As managed servers, the room servers have centralized configurations and centralized logging and monitoring. You can check on all managed room servers from a central location—EMS.
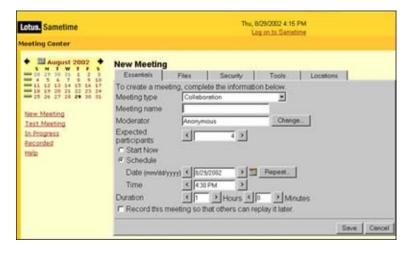
When necessary, you can remove a server from a cluster so that it is no longer a room server managed by EMS. Because a server can include many active meetings, it is best not to intentionally cause a failover condition to remove the server. Instead, change the appropriate parameters so that the number of meetings on the server is set to zero; this change prevents new activity on the server. Current active meetings are allowed to complete before the server is removed from the cluster.

The EMS user interface

EMS provides the user interface (UI) for scheduling and attending meetings, downloading Sametime clients, and administering all Sametime servers in the cluster. If your company is one of the many IBM customers with more than 20,000 seats, you, no doubt, have experienced the challenge of locating a meeting in such a large environment. EMS provides better tools for both locating and attending meetings. For example, the calendar search tool lets you select a specific date, week, or month to search for meetings in the specified time range. You can also search for a meeting by the meeting name.

Also, with EMS, the user always attends meetings in the same way—by browsing to the EMS machine. Users do not have to know or keep track of different Sametime server names. Once located, meetings can be sorted by date, name, or moderator. The following screen shows the options for creating a new meeting in EMS:

EMS security

Because EMS is a J2EE application, security for EMS is based on WebSphere settings rather than Domino settings. None of the Domino security information in the **Sametime Administrator's Guide** (such as Access Control List settings) apply to EMS.

EMS security includes the following:
- The ability to assign security roles to users to allow or prohibit access to features
- Authentication of users accessing EMS
- Use of the Secure Sockets Layer (SSL) protocol to encrypt meeting materials sent between EMS and the clustered servers

Assigning security roles
WebSphere security roles are used to provide authenticated or unauthenticated access to EMS. If the security roles are configured to require authentication, the security roles determine the access level that individual users have to EMS. The default EMS security role setting allows anonymous (or unauthenticated) users to access all features of EMS, except the EMS Sametime Administration Tool. An anonymous user can create and attend meetings and modify or delete meetings, including meetings created by other users.

Use the security roles if you do not want unauthenticated users to access EMS. The security roles restrict access and require users or groups of users to authenticate when accessing EMS, creating a meeting on EMS, or attending a meeting on EMS.

On a Sametime server that is not part of a server cluster, the security features discussed above are provided by the ACL settings of Domino databases. With EMS, the WebSphere security roles essentially replace Domino ACL settings when restricting user access to meeting activity. A WebSphere security role is also used to provide access to the administration tool on EMS.

Use the WebSphere Advanced Administration Console to assign security roles to the users in the LDAP directory for your Sametime community.

Authentication of users
Because EMS is a WebSphere application, LDAP is required for authentication. Only a single directory is supported, but the directory can contain multiple partitions if necessary. For example, the directory can be partitioned to contain separate directories for different companies; the users from one company cannot access the directory for the other company.

The single sign-on (SSO) feature of EMS allows the user to log on once, regardless of the number of authentications required. This feature is carried out by use of Lightweight Third-Party Authentication (LTPA) tokens. Users receive a LTPA token when authenticating with EMS.

Secure Sockets Layer (SSL) encryption
EMS installs on a WebSphere server. To access a WebSphere application, Web browser users must connect to the IBM HTTP server that is installed with WebSphere. You can encrypt Web browser connections to EMS by configuring the IBM HTTP server to support SSL. For more information, see the IBM Redbook, **IBM WebSphere V4.0 Advanced Edition Handbook**.

SSL can be used to encrypt the following:
- HTTP traffic between Web browsers and EMS
- HTTP traffic between EMS and Sametime servers

You must follow one procedure to set up SSL encryption for Web browsers and another procedure to set up SSL between the Sametime servers and EMS. Each procedure provides security for different kinds of information.

If you want to encrypt user names and passwords and other information transmitted between Web browser users and EMS, you must configure the IBM HTTP server to support SSL. The IBM HTTP server is installed as part of the WebSphere server installation described in the WebSphere manual. To configure the IBM HTTP server to support SSL, you must:
- Manage the SSL certificates
  This task requires the creation of an SSL key database to store the certificates. You must then obtain the certificates and add them to the key database. Refer to the **Sametime Administrator's Guide** for more information.
- Configure the IBM HTTP server to support SSL
  An SSL link must be established for the Web browser and the HTTP server to exchange the SSL certificates.

To establish this link, you must configure the IBM HTTP server to support SSL. This task involves several steps: accessing the IBM HTTP Administration Server; setting up the security module; setting up the secure IP host and the additional port for the secure server; and setting up the virtual host structure for the secure server.

Refer to the **Sametime Administrator's Guide** for detailed information about each of these steps.

Administration of EMS

EMS provides a central point for administration of all servers within the cluster. To make an administrative setting, browse to the EMS Sametime Administration Tool on the EMS machine. This tool provides an interface to each of the servers in the cluster and allows you to add or remove servers as necessary.
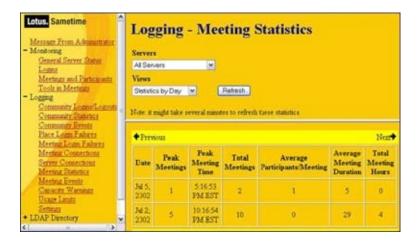
EMS is deployed as a J2EE Web application archive (WAR) on one or more WebSphere Application Server (WAS) nodes and accessed via a Web browser. The room servers contact EMS to obtain configuration information. Also, the DB2 schema is available if you want to build custom triggers or monitors, or if you want to generate your own billing or usage reports.

Monitoring and logging

The Sametime monitoring and logging functionality is greatly improved with EMS. Monitoring refers to the ability to oversee meetings currently in progress in the cluster. With EMS, you can monitor a specific server or all servers in a cluster for such information as total number of logins, meetings and participants, tools in meetings, and general server status. The following screen shows a monitoring screen containing general server status information:

Logging refers to historical information about meetings that have already terminated. EMS provides numerous reporting options for viewing logged information, including community statistics, login failures, meeting statistics, capacity warnings, and much more. You can use the historical logging information to determine peak usage of any server in the server cluster and the average number of participants per meeting. With this knowledge, you might choose to add a server to the cluster to better handle the load. The following screen shows a logging screen containing meeting statistics:

The EMS Sametime Administration Tool
If you cluster Meeting Services, you must install EMS and use the EMS Sametime Administration Tool to administer the servers in the cluster. You create the Meeting Services cluster before using the EMS Sametime Administration Tool. You can also use the EMS Sametime Administration Tool to administer the servers in a Community Services cluster. However, when you make a change that affects the functioning of the Community Services, the change applies to all servers in the Community Services cluster.

When you deploy EMS, you must maintain your EMS user community in a single LDAP directory. The LDAP directory should exist on a dedicated server, separate from both the EMS machine and the Sametime servers in the Meeting Services cluster. EMS administrators should be listed in a group named "stadmins" within this LDAP directory.

Use the EMS Sametime Administration Tool to:
- Send a message to all users logged in to the Sametime community
- Monitor a cluster
- View log information for a cluster
- Configure connectivity (networks and ports) for a cluster
- Configure Community Services for a cluster
- Configure Meeting Services for a cluster
- Configure audio/video services for a cluster

Although similar to the Sametime 3.0 Administration Tool, the EMS Sametime Administration Tool does not offer the same features. The following features are not available with the EMS Sametime Administration Tool:
- The Server Overview feature
- The Miscellaneous monitoring feature
- The Domino log feature
- Sametime Discussion and TeamRoom databases
- The ability to schedule a Latitude MeetingPlace telephone conference calls

Automatic failover
The EMS prevents single points of failure in the server cluster by seamlessly redirecting users on a failed server to a functioning server. Rather than having to reconnect or endure downtime, the user simply refreshes the screen and is transferred to a new server.

The automatic failover procedure is initiated when EMS determines that a server in the cluster has failed. Servers managed by EMS report usage and resource information to EMS at regular intervals. EMS performs load-balancing of scheduled meetings based on this information. If a managed server fails to send a status message to EMS, EMS assumes server failure and initiates the automatic failover procedure.

The automatic failover procedure differs for clustered Meeting Services and Community Services. With Meeting Services, all active meetings on a failed server are moved to a different server in the cluster. If a server fails, the users attending the meeting on that server press refresh, and the meeting restarts on a different server.

With clustered Community Services, the Sametime Connect client attempts to reconnect when a server fails. The

rotating DNS System or WebSphere Edge Server ensures that the client connects to a different server. A "disconnected" message displays in the Connect client status bar, and then the user sees a message indicating that the client is connecting again. Users can also manually reconnect by selecting the People - Reconnect to Sametime menu option within the Connect client.

The automatic failover feature also applies to recorded meetings. Recorded meetings are stored on the specific server where the meeting is initiated. If that server fails, the recording of the meeting continues on a functioning server. To view the entire recorded meeting, both segments of the recording—from two different servers—must be played back. However, the user only needs to play the recording from EMS; the fact that the recording is located on two servers is transparent to the user.

Load-balancing
The EMS load-balancing feature ensures that each meeting is started on the Sametime server in the cluster that is best able to bear the load of the meeting. With the Meeting Services, EMS monitors the load on each server in the cluster. When a new meeting is scheduled to begin, EMS selects the least-loaded server in the cluster as the meeting host. The servers in the cluster communicate with EMS using JMS (Java Message Service) messages and HTTP.

The load-handling capability of each server in the cluster is determined by parameters that you enter when you add the server to the cluster. Examples of these parameters include "maximum number of active meetings" and "maximum number of users in each meeting." EMS considers these load-handling parameters and the current load on each server in the cluster when selecting the best server to host a meeting.

The load-balancing feature ensures that each server in the cluster does not exceed load restrictions imposed by you and that the meeting load is distributed equally among servers in the cluster. Load-balancing is accomplished a bit differently with the Community Services. When creating a Community Services cluster, you must deploy a rotating DNS system or IBM WebSphere Edge Server in front of the cluster. The rotating DNS system or IBM WebSphere Edge Server distributes the client connections evenly to the servers in the Community Services cluster.

Meeting Services and Community Services
Every Sametime 3.0 server includes both Community Services (instant messaging and presence capabilities) and Meeting Services (screen sharing, whiteboard, interactive audio/video, send Web page, and polling). You can use EMS to cluster the Meeting Services. When you cluster the Meeting Services, EMS provides load-balancing and failover for all Sametime online meetings, including screen-sharing and whiteboard meetings, interactive audio/video meetings, and broadcast meetings.

You can also cluster Community Services, which does not require EMS. The ability to cluster one or both types of services provides the flexibility to manage the two services differently to best meet the needs of your organization. For example, if your company uses Sametime Connect frequently but has few online meetings, you might cluster Community Services only. If your company uses Sametime to conduct many online meetings and broadcast presentations but uses Sametime Connect infrequently, you might use EMS to cluster Meeting Services only. You can choose to have some servers in your community function independently and others included in a cluster managed by EMS.

If you choose to cluster both the Community Services and the Meeting Services, you must perform the procedures in this order:
1. Create the Community Services cluster.
2. Deploy EMS.
3. Create the Meeting Services cluster.

All servers that have both the Meeting Services and Community Services clustered must be Sametime 3.0 servers. You can create a Community Services cluster that includes both Sametime 3.0 servers and previous releases. However, you cannot cluster the Meeting Services of servers with different Sametime releases.

Community Services
Previous versions of Sametime used a single server (or *home* server) to provide Community Services to users. If the home server failed, Community Services were no longer available to the users. If you cluster Community Services, users can receive these services from any server within the server cluster, ensuring continuous access to instant messaging and presence capabilities if a server fails.

To create a Community Services cluster, you perform several steps, including the creation of a Domino server

cluster to support the Community Services cluster. You also deploy a rotating DNS system or IBM WebSphere Edge Server (Network Dispatcher) to direct client connections to the Community Services multiplexers on the Sametime servers. The rotating DNS system or WebSphere Edge Server provides load-balancing among the clustered servers.

To cluster Community Services, you need the following:
- A separate machine for each Sametime server installation
- One machine for use as an LDAP Directory server if you cluster both the Community Services and the Meeting Services
- One machine for the EMS installation if you cluster both Community Services and Meeting Services
- A rotating DNS system or WebSphere Edge Server for load-balancing

The Sametime servers must have TCP/IP connectivity on these ports:

Port	Description
1516	The default port for server-to-server Community Services connections
1503	The default port for Sametime server-to-server Meeting Services connections
1352	The default port for server-to-server connections between the Domino servers on which the Sametime servers are installed
389	The default LDAP port for Sametime (if you deployed LDAP on a separate server)

Meeting Services and EMS

To create a Meeting Services cluster, deploy EMS and use the EMS Administration Tool to add Sametime servers to the Meeting Services cluster. When Meeting Services are clustered with EMS, end users enter the URL of the EMS machine to access EMS when scheduling and attending meetings. End users are unaware that the meetings are actually taking place on different servers in the cluster.

When scheduling a meeting on EMS, the user is required to identify the expected number of participants and duration of the meeting. This information (referred to as "resource booking") allows for capacity planning for the servers in the Meeting Services cluster. If necessary, you can configure each managed server in the cluster differently to meet the expected meeting loads.

When a scheduled meeting begins, the meeting is assigned to the server with the lightest load. If that server fails, the meeting is immediately redirected to the server with the next lightest load. Alerts are displayed when meeting capacity is exceeded for a server, but the meeting limits are not strictly enforced. In other words, a meeting that is in progress is not stopped because it has surpassed the defined meeting capacity.

Instant meetings are handled differently than scheduled meetings. Because instant meetings are not planned, resource booking and capacity planning are not possible before the meeting occurs. Instead, you can decide how each managed server will handle instant meetings by setting an administrative setting. The following table identifies the settings.

Setting	Server behavior for instant meetings
0	The server will allow scheduled meetings and chat, but no instant meetings.
n	The server will allow instant meetings up to the indicated number. When that limit is reached, the server will divert instant meetings to other servers in the cluster.
Unlimited	The server will allow an unlimited number of instant meetings. The instant meetings will be load-balanced among all servers that support them.

Conclusion

The Enterprise Meeting Server promises advantages for administrators and for end-users. As an add-on to the core Sametime 3.0 server, EMS provides load-balancing and failover capabilities for Meeting Services through the

clustering of servers. It also takes advantage of standards-based technologies like J2EE and JMS. Plans for future enhancements to EMS are already in the works, including the ability for EMS to communicate outside corporate firewalls. With the benefits it offers today and the enhancements planned for the future, EMS provides many advantages for online meetings and communication.

ABOUT THE AUTHOR
Kay Saffari is a freelance writer in Lexington, Kentucky, where she lives with her husband and two children. She was previously employed by Lotus as a technical writer/editor, by AT&T as a technical writer, and by Electronic Data Systems as a computer programmer.