DEPLOYMENT GUIDE
Version 1.1

Deploying the BIG-IP LTM with IBM Lotus Sametime

Table of Contents

Deploying the BIG-IP LTM with IBM Lotus Sametime

Deploying the BIG-IP LTM with IBM Lotus Sametime

Welcome to the F5 deployment guide for the BIG-IP Local Traffic Manager (LTM) and IBM Lotus® Sametime® unified communications platform. This guide provides a highly effective way to direct traffic for Sametime servers with the BIG-IP LTM. The BIG-IP LTM also provides the top-level distribution that allows for simple and effective scalability of Sametime servers and ensures that customers maximize their return on investment.

IBM Lotus Sametime software provides integrated real-time communications services—voice, data and video—that make it easy for people to find, reach and collaborate effectively with others.

For more information on IBM Lotus Sametime, see ***http://www-01.ibm.com/software/lotus/sametime/***.

For more information about the BIG-IP system, visit ***http://www.f5.com/products/big-ip/***.

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this deployment:

- The servers must be preinstalled first with IBM Domino and Domino must be replicating across all the servers. Then IBM Lotus Sametime must be installed on the servers. For more information on installing Domino and Sametime, refer to the IBM documentation.
- If you are using the BIG-IP LTM to offload SSL transactions from the Sametime Community service (optional), we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. See *Appendix A: Configuring the BIG-IP LTM to offload SSL from the Community service*, on page 10 for more information about SSL offload.
- Sametime uses the following TCP ports, ensure any firewalls between the BIG-IP LTM and your IBM servers allow these ports:
  - Community: TCP port 1533
  - Meetings: TCP port 8081
  - Web: TCP port 80
- The BIG-IP LTM procedures for the Sametime Meeting and Web/HTTP Data components are based on the classic Meeting server and not the WAS based Meeting server available with 8.5.
- We recommend backing up your BIG-IP system configuration prior to beginning this deployment guide. See *Appendix B: Backing up and restoring the BIG-IP system configuration*, on page 13.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.2, 10.2.1 (applicable to 10.0 and later)
IBM Domino Sametime	8.5.1

Document Version	Description
1.0	New guide
1.1	Added clarification that the BIG-IP procedures for the Sametime Meeting and Web/HTTP Data components are based on the classic Meeting server and not the WAS based Meeting server available with 8.5.

Configuration example

Using the configuration in this guide, the BIG-IP system is optimally configured to load balance traffic to IBM Lotus Sametime servers. Figure 1 shows a simple, logical BIG-IP Sametime configuration.

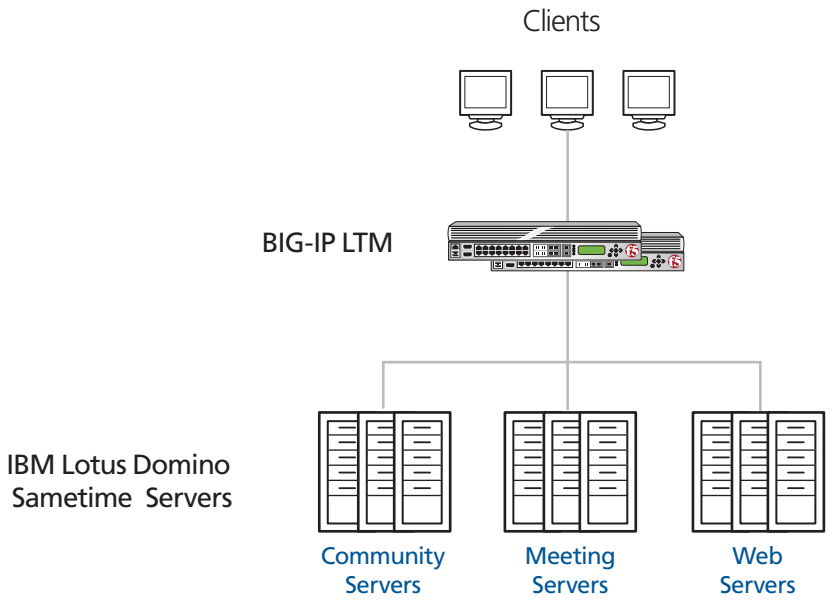

Figure 1 *Example Configuration*

Configuring the BIG-IP LTM for Sametime servers

To configure the BIG-IP product to direct traffic to the Sametime servers, you need to complete the following procedures. *Appendix A: Configuring the BIG-IP LTM to offload SSL from the Community service*, on page 10 contains optional procedures for offloading SSL from the Community service onto the BIG-IP system.

Configuring health monitors

The first task is to create the health monitors. Monitors are optional, but we highly recommend using the monitors below to verify that the nodes and services are available. For this configuration, we configure HTTP and TCP monitors.

Creating the HTTP monitor

The first health monitor we create is for HTTP traffic. This monitor defines Send and Receive Strings in an attempt to retrieve explicit content from nodes. In this case, the monitor sends a request for the Sametime server Login page, and is successful when that page is returned.

To create the HTTP monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **Sametime-HTTP**.
4. From the **Type** list, select **HTTP**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a (1:3) +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. In the **Send String** box, type the following

   ```
   GET /names.nsf?login HTTP/1.0\r\n\r\n
   ```

7. In the **Receive String** box, type:

   ```
   Log In
   ```

8. Click the **Finished** button.
   The new monitor is added to the Monitor list (see Figure 2, on page 4).

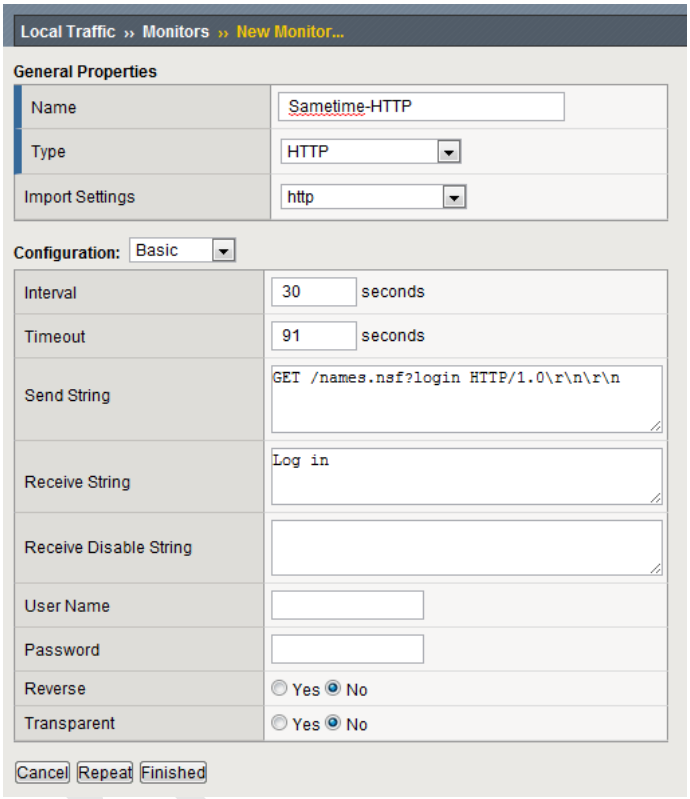

Figure 2 *Sametime HTTP monitor*

Creating the TCP monitor

The next monitor we create is a TCP monitor for the Meeting service.

To create the TCP monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **Sametime-TCP**.
4. From the **Type** list, select **TCP**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a (1:3) +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. The rest of the settings are optional. Configure as applicable for your implementation.
7. Click the **Finished** button.

Creating the pools

The next task is to define load balancing pools for the Sametime servers. We create three Sametime pools on the BIG-IP LTM: one for Community (which uses port **1533**), one for Meetings (which uses port **8081**), and one for HTTP data on port **80**.

Note

Remember, the BIG-IP LTM procedures in this guide for the Sametime Meeting and Web/HTTP Data components are based on the classic Meeting server and not the WAS based Meeting server available with 8.5.

To create the Sametime pools

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, type a name for your pool. We recommend you use a name that includes the Sametime service, such as **Sametime-Community**.
4. In the **Health Monitors** section, select the appropriate health monitor for the Sametime service and then click the Add (<<) button:
   - For HTTP data and the Community service, use the HTTP monitor you created in *Creating the HTTP monitor*, on page 3.
   - For the Meeting service, use the TCP monitor you created in *Creating the TCP monitor*, on page 4.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Least Connections (node)**.
6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first Sametime server to the pool. In our example, we type **10.132.81.100**.
8. In the **Service Port** box, type the appropriate Service Port for the Sametime service:
   - For HTTP data, type **80** or select HTTP from the list.
   - For the Meeting service, type **8081**.
   - For the Community service, type **1533**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 8-10 for each server you want to add to the pool.
    In our example, we repeat these steps five times for the remaining servers, **10.132.81.101 - .105**.

11. Click the **Repeat** button.
12. Repeat this procedure for each of the other Sametime services until you have created all three pools, and then click the **Finished** button.

Creating the profiles

The next step is to create the profiles. Although you may use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. By creating new profiles, you may easily modify the profile settings specific to your deployment without altering default global behaviors.

Creating TCP profiles

In this section, we create the TCP profiles. We recommend creating **tcp-lan-optimized** and **tcp-wan-optimized** profiles.

Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile.

To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens by default.
2. On the Menu bar, from the **Protocol** menu, select **TCP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **Sametime_tcp_lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

The next task is to create the WAN optimized profile.

To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **Protocol** menu, select **TCP**.
2. Click the **Create** button. The New TCP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **Sametime_tcp_wan**.

4. From the **Parent Profile** list, select **tcp-wan-optimized**.
5. Modify any of the other settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating a persistence profile

Next, we create a persistence profile. For this deployment, we use Source Address Affinity (src_addr) persistence.

To create a persistence profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, click **Persistence**.
2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **Sametime-persist**.
4. From the **Persistence Type** list, select **Source Address Affinity**.
5. Configure any of the options as applicable. In our example, we leave the defaults.
6. Click **Finished**.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can use existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **Sametime-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.

6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the virtual servers

The next task is to define virtual servers that reference the pool and profiles you created in the preceding procedures.

For Sametime, we create three virtual servers, one for each service (Community, Meetings, and Web/HTTP data).

To create the virtual servers

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type an appropriate name for this virtual server. We recommend using a name that includes the service, such as **Sametime-Community-vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.10.120.**
6. In the **Service Port** box, type the appropriate Service Port for the Sametime service:
   - For HTTP data, type **80** or select HTTP from the list.
   - For the Meeting service, type **8081**.
   - For the Community service, type **1533**.

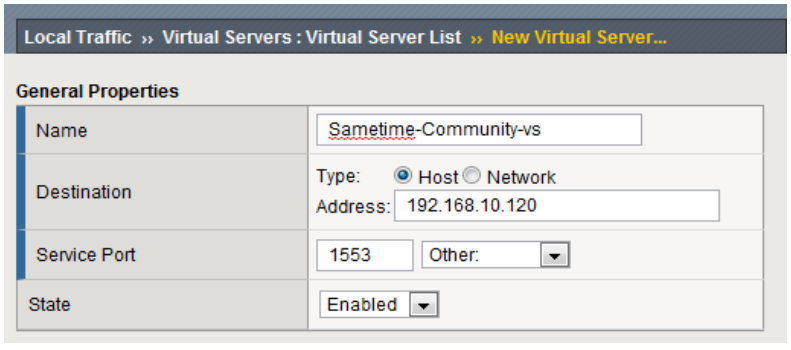

Figure 3 *General properties of the Community virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list, select the profile you created in *Creating the WAN optimized TCP profile*, on page 6. In our example, we type **Sametime_tcp_wan**.
10. From the **Protocol Profile (Server)** list, select the profile you created in *Creating the LAN optimized TCP profile*, on page 6. In our example, we type **Sametime_tcp_lan**.
11. *For the HTTP Data virtual server **only***:
    From the **HTTP profile** list, select **HTTP.**
12. From the **OneConnect Profile** list, select the profile you created in *Creating a OneConnect profile*, on page 7. In our example, we type **Sametime_oneconnect.**
13. From the **SNAT Pool** list, select **Automap**.
14. In the Resources section, from the **Default Pool** list, select the appropriate pool you created for the Sametime service in *Creating the pools*, on page 5:
    - HTTP data
    - Meeting service
    - Community service
15. From the **Default Persistence Profile** list, select the profile you created in *Creating a persistence profile*, on page 7. In our example, we select **Sametime_persis**t.
16. Click the **Repeat** button.
17. Repeat this procedure for each of the Sametime services. When you have completed all three virtual servers, click the **Finished** button.

This completes the base configuration. If you are using the BIG-IP system to offload SSL for the Community service, see *Appendix A: Configuring the BIG-IP LTM to offload SSL from the Community service*, on page 10.

Appendix A: Configuring the BIG-IP LTM to offload SSL from the Community service

In this appendix, we show you how to configure the BIG-IP LTM system to offload SSL processing from the Community service. Although this is an optional part of the configuration, by offloading SSL transactions onto the BIG-IP LTM, you free processing power on the Sametime servers, allowing them to be more efficient.

SSL offload requires one change to the Sametime configuration, and adding a SSL profile to the BIG-IP LTM virtual server you already created.

Modifying the Sametime configuration to allow SSL offload

The first task in this section is to modify your Lotus Domino Sametime clients. This can be done administratively via global settings in the client or via specific settings for each client.

In the following procedure, we document changing the specific connection, but the deployment of this setting across your infrastructure will depend on your global management capabilities.

To modify the Sametime configuration

1. Open the Lotus Domino Sametime client
2. In the **Host Server** box, type the appropriate Sametime host name or IP address.
3. Click the **Connectivity** button.
4. Click the *Connection* tab.
5. Clear the **Use global connection settings (defined in main server communities preference page)** box, if it is checked.
6. In the Connection section, click the **Direct connection using TLS** option button.
7. Click the **OK** button (see Figure 4, on page 11).

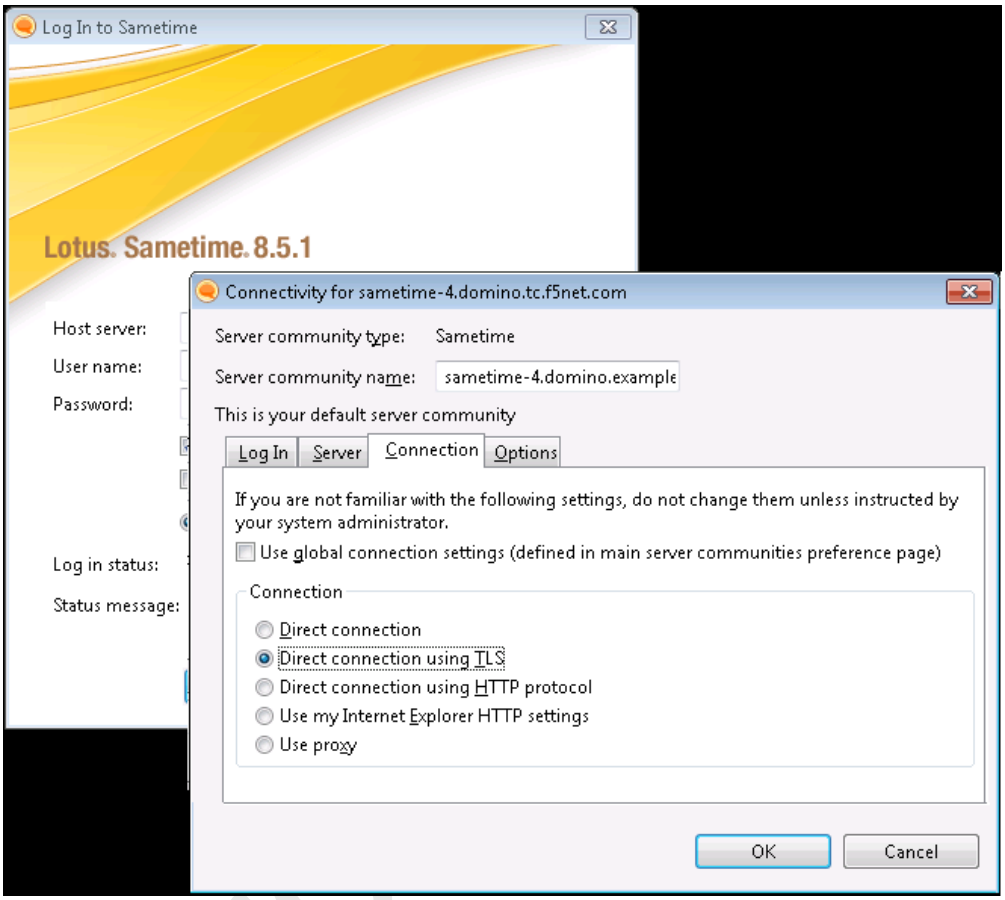

Figure 4 *Connectivity settings for Sametime*

Creating a Client SSL profile

The next task in this section is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).

5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.
8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Sametime-ssl**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Modifying the virtual server

The next task is to modify the virtual server you created for the Connectivity service to use the SSL profile. you just created.

To modify the existing virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, click the virtual server you created for Community in *Creating the virtual servers*, on page 8. In our example, we click **Sametime-Community-vs**.
3. From the **SSL Profile (Client)** list, select the name of the profile you created in *Creating a Client SSL profile*, on page 11. In our example, we select **Sametime-ssl**.
4. Click the **Update** button.

This completes the SSL offload configuration.

Appendix B: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before and after you finish this configuration. When you save the BIG-IP configuration, it collects the following critical data and compresses it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving and restoring the BIG-IP configuration

The Configuration utility allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS).

To save the BIG-IP configuration

1. On the **Main** tab, expand **System**, and then click **Archive**.
2. Click the **Create** button.
3. In the **File Name** box, type a name for this archive file.
   The other settings are optional.
4. Click the **Finished** button. The archive is created.

To restore a BIG-IP configuration

1. On the **Main** tab, expand **System**, and then click **Archive**.
2. Click the **Upload** button.
3. In the **File Name** box, type the file name, or click **Browse** to find it.
4. Click **Upload**.