



Deploying the BIG-IP LTM with SAP NetWeaver and Usage Type Process Integration

Version 1.0

Introducing the SAP NetWeaver with Usage Type PI deployment guide

Welcome to the F5 - SAP Usage Type Process Integration (PI) Deployment Guide. By taking advantage of this Application Ready infrastructure for SAP Usage Type PI (formerly known as Usage Type XI) deployments, organization can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI. This guide gives you step-by-step procedures on how to configure the BIG-IP LTM system for SAP Usage Type PI deployments.

With SAP Usage Type PI customers can connect systems and applications together to achieve common business-to-business tasks. Both internal company and cross-company application integration is possible with PI. During the configuration phase of designing the collaboration process and setting up the system landscape it's helpful to create Web Application servers that are redundant for high availability.

Unlike software load balancers, BIG-IP LTM deployed in a high-availability pair will not itself be a single point of failure and therefore no additional configuration is required on BIG-IP itself. To configure SAP NetWeaver Usage Type PI for a high availability, configuration changes may need to be made to the Local System Landscape Directory, the Exchange Profile, the User Management Engine, the Integration Server, the Central Adapter Engine, the Central Monitoring Server and the Dialog Instance, depending on your particular setup of SAP. This guide covers the configuration of all of these steps, although several of them may be optional in your landscape.

During the configuration of your SAP Landscape, primarily the local host name and port are replaced with virtual host name and port. For further instructions, please consult *SAP Note 951910*. This guide is intended to show all of the locations within SAP where changes may be necessary, however it is up to each individual administrator to analyze and decide whether the change applies to their SAP landscape.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Prerequisites

The following are prerequisites and configuration notes about this deployment:

- ◆ The BIG-IP LTM should be running version 9.4.x or later.
- ◆ SAP should be using NetWeaver 2004s (7.0) or later with Usage Type PI (Process Integration), with update to NW2004s Service Pack 08 or higher completed.
- ◆ We assume you are very familiar with SAP installation and configuration procedures. Consult your SAP administrator/consultant or the SAP documentation for specific SAP information.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	9.4.5 and 9.4.6. Although not specifically tested at this time, this configuration also applies to v10.0 and later.
SAP Usage Type PI	NetWeaver 2004s (7.0) with Usage Type PI, including update to NW2004s Service pack 08.

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

For SAP Usage Type PI high availability, BIG-IP local traffic managers are configured in front of PI Dialog instances with round robin load balancing. BIG-IP LTM monitors the health of servers and appropriately distributes load between servers insuring uptime for critical SAP PI services.

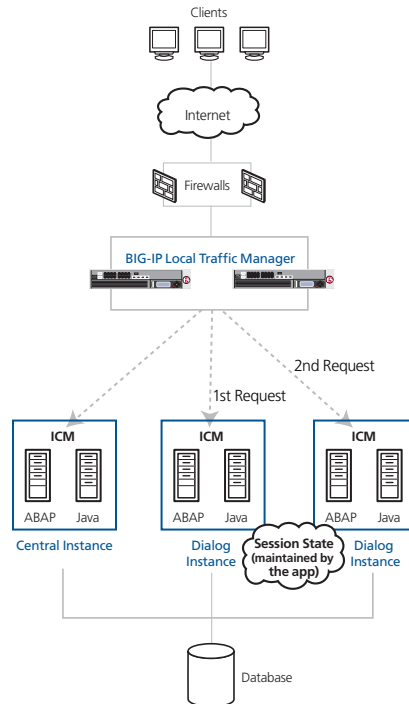


Figure 1 Logical configuration example

Configuring the SAP NetWeaver platform for load balancing Usage Type PI

◆ Important

*The following information covers the most important parts of the SAP NetWeaver configuration for Usage Type PI. Not all of these configuration details will apply to every SAP installation, however we do cover all of the places where changes may be necessary. For more detailed instructions on configuring your SAP solution see the SAP documentation, contact SAP or your consultant, or refer to SAP notes such as **SAP Note 951910**.*

The first step in configuring your SAP Landscape for high availability is to choose a new IP address, host name and port that will be used as the IP, name and port for your incoming connections. Register this information with your company's DNS and network administration groups before proceeding.

For example, let's assume there is an SAP environment currently with four dialog instances that will be used in the high availability landscape. In our examples, we use the name

MyCompanyVirtualHostname.companyname.com, and choose port number **80** and assign **MyCompanyVirtualHostname** an IP Address of **10.100.100.50**. These settings go both on the BIG-IP system, and into the SAP Configuration.

In the following section, we provide guidance for the SAP configuration based on the information from our example above. Configure the following SAP values anywhere you see these settings in the SAP PI configuration:

- ◆ **<Virtual Host>**
This is the host name (MyCompanyVirtualHostname in our example). Type your host name here, or what SAP may refer to in some circumstances as SAP Web Dispatcher Hostname. This is also the host name that resolves to the BIG-IP LTM virtual server.
- ◆ **<httpport>**
This is the port (80 in our example). Type the appropriate port here. SAP may refer to this in some circumstances as SAP Web Dispatcher Port. This should match the BIG-IP LTM virtual server port number.
- ◆ **<cihost>**
This is the existing Central Instance host name. This should not change, but you need it as a reference if this is the very first time you are setting up your SAP landscape.
- ◆ **<dihost>**
This is your existing Dialog Instance Hostname. This should not change, but you need it as a reference if this is the very first time you are setting up your SAP landscape.
- ◆ **<SID>** is your System ID.
- ◆ **<instno>** is your PI Instance ID.

Configuring the Exchange Profile

The first procedure is to configure the Exchange Profile. Before starting this procedure, refer to *SAP Note 951910*. This note has a file attachment which provides additional configuration fields that you need in your SAP PI configuration. This file is used in the following procedure.

To configure the Exchange Profile

1. From a web browser, call the Exchange Profile URL, using the following syntax:
http://<hostname:portnumber>/webdynpro/dispatcher/sap.com/tc~xi~exprofui/XIProfileApp

Note: The host name and port number you use here is the direct host name and port number of your SAP Instance, not the Virtual Host Name. If you are using SSL security, the protocol would be HTTPS, not HTTP.

2. From the **Export** menu, export the current profile by selecting **Export Data**, and then **Save**.
3. Import the delta exchange profile that you downloaded from SAP Note 951910. From the **Import** menu, select **Browser for zip file** and then **Import Data**.
Do **NOT** overwrite your current profile information. This merge adds the new parameters for you.
4. Follow the instructions found in SAP Note 951910 for configuring the Exchange Profile. Change the settings to match the Virtual Hostname on your BIG-IP LTM.
5. Change the database connection of the exchange profile using the following steps:
 - a) Click **Connection**.
 - b) Select **Load Balancing**, and then set the following values:
Message Server: <virtual host>
SID: <SID>
Logon Group: **SPACE**
(where SPACE is the Default RFC Group)
 - c) Click **Save**.

Configuring the Local System Landscape Directory

If you are using a stand alone SAP Gateway as an additional component in a SAP Cluster Group, you should configure the Local System Landscape Directory (SLD). This is optional, and may not be necessary for a typical SAP Usage Type PI deployment.

See *SAP Note 1064290* for further instructions.

To configure the local system landscape directory

1. Using a text editor, go to the following directory:
/usr/sap/<SID>/SYS/profile
Where <SID> is your system ID.
2. Add an entry to the start profile **START_SCS<instno>_<virtual host>**, for example:

```
#-----  
# Start SAP gateway service  
#-----  
_GW = $(DIR_EXECUTABLE)\gwrds$(FT_EXE)  
Start_Program_05 = local $(_GW) pf=$(_PF)
```

3. Save and close the file.
4. Change to the directory **/usr/sap/<SID>/SYS/exe/uc/<os>/** and edit the **sapcpe** file **scs.lst** to add **gwmon** and **gwrds**. You see a long list similar to the truncated version below. Add the new entries:

```
...  
librfc32u.dll  
librfc32u.pdb  
libsapu16vc71.dll  
libsapu16vc71.pdb  
icuuc30.dll  
icuin30.dll  
icudt30.dll
```

```
gwmon  
gwrds
```

Note: If you are using Microsoft Windows, you must add the file extension to the last two entries:

```
gwmon.exe  
gwrds.exe
```

5. Save and close the file.
6. Change the enqueue replication port in Java SCS and in the enqueue replication instance profile (default port is **sapgw<instno>**).

Set **enque/encni/repl_port** to a different, unused value.
For specific instructions, refer to **SAP Note 1064290** and consult the SAP documentation.

Changing the Local SLD configuration

The next step is to change the Local SLD configuration. If you are not using the Local SLD, this procedure is optional.

To change the Local SLD configuration

1. Open the SAP GUI, and login to your instance as a PI super user.
2. Call the ABAP transaction **SLDAPICUST** and set the HTTP connect data to **<virtual host>:<httpport>**. In our example, we use **MyCompanyVirtualHostname** and port **80** (see Figure 2).

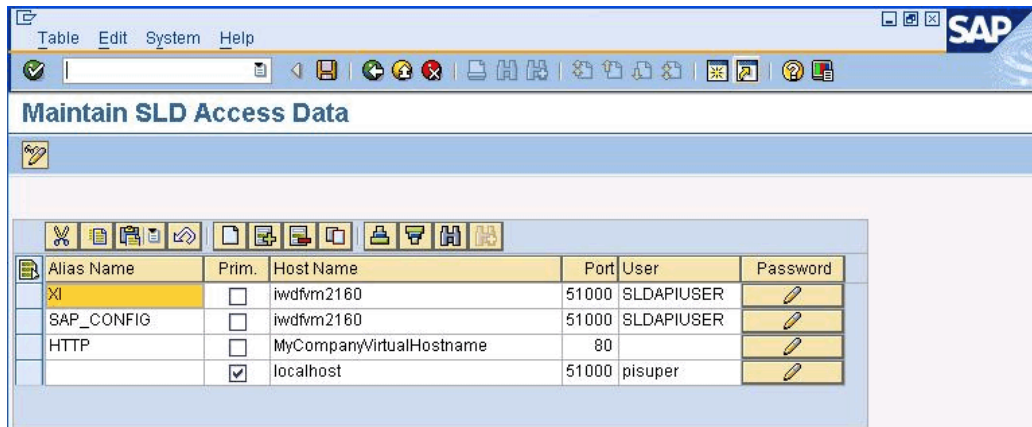


Figure 2 Changing the Local SLD configuration

3. Next, call the ABAP transaction **RZ70** and change the gateway setting to **<virtual host>** and **sapgw<instno>**. In our example, we use **MyCompanyVirtualHostName** and **sapqw10** (see Figure 3).
4. Click the **Save** icon/button.

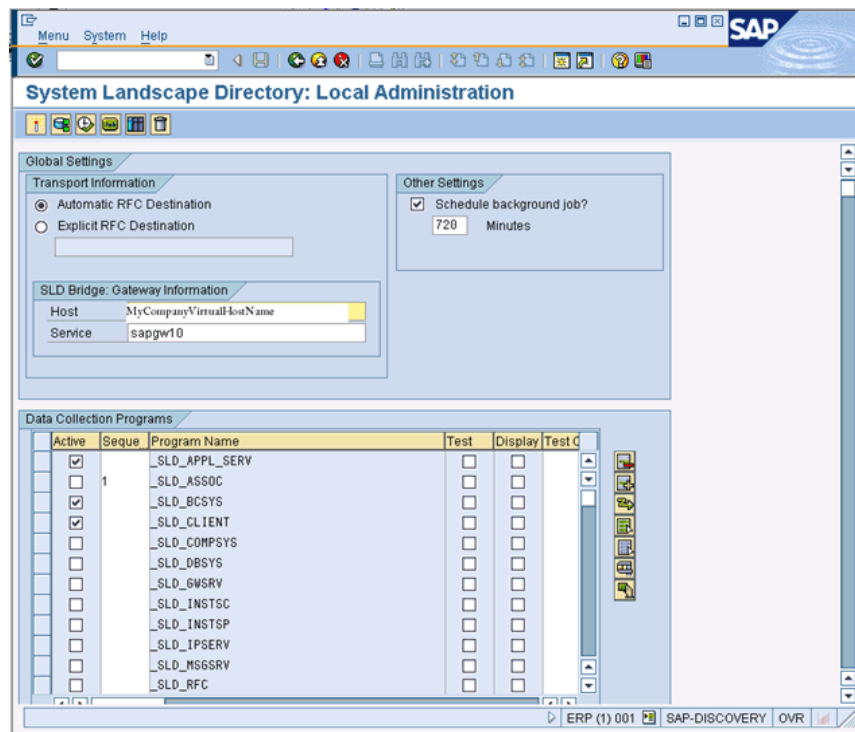


Figure 3 Configuring SLD Bridge gateway information

You perform the next part of this procedure from a web browser.

5. From a web browser, open Java SLD Administration.
6. Go to Java SLD Administration, choose **Profile-->Dataprovider**, and change the gateway settings to **<virtual host>** and **sapgw<instno>**. In our example, we use **MyCompanyVirtualHostName** and **sapgw10**
7. Submit the changes to save them.

The final part of this procedure in this section uses the J2EE Visual Administrator.

8. Start the J2EE Visual Administrator client.
9. Select the Data Supplier service, and set the HTTP connection data to **<virtual host>:<httpport>**. In our example, we use **MyCompanyVirtualHostName** and port **80** (see Figure 4).
10. Click the **Save** button.

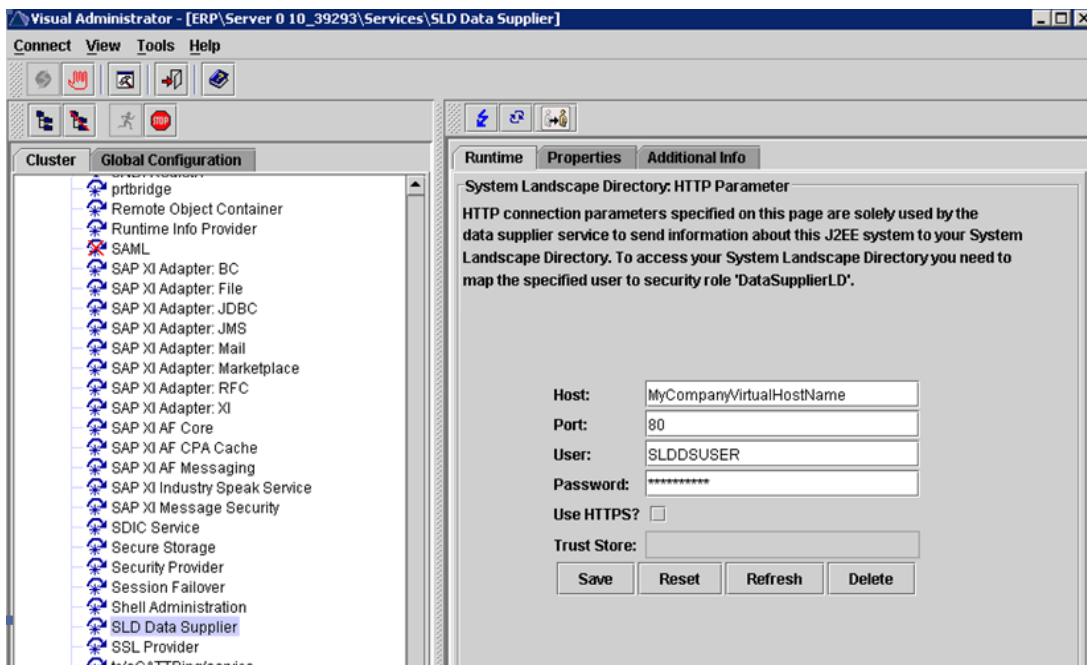


Figure 4 Configuring the HTTP connection parameters from the Visual Administrator

Configuring the User Management Engine

To enable local RFC connections between the user management engine (Java) and the ABAP stack, the variable \$\$ is used for addressing.

To configure the user management engine

1. Start the J2EE Visual Administrator.
2. From the **Global Configuration** menu, select **Server**, then **Services** and then **UME Provider**.
3. Specify the following values:


```
ume.r3.connection.master.ashost=localhost
ume.r3.connection.master.sysnr=$$
```
4. Click **Save**.

Configuring the Integration Server

To enable load balancing for SAP applications that retrieve the URL of the Integration Server from the SLD (for example, Adapter Engines) the pipeline URL registered in SLD needs to be adapted.

To change this, go to Business System Maintenance in SLD and select the Integration Server's business system. Enter the virtual hostname and the port of the SAP Web Dispatcher in the field Pipeline URL.

For specific instructions on how to Maintain a Business System for the Integration system, go to the following SAP document:

http://help.sap.com/saphelp_nw70/helpdata/en/43/39c7b227b91bcb0000000a1553f7/frameset.htm From the list in the third bullet, click **Integration Server**. In the Maintaining the Pipeline URL of the Integration Server section, click **Maintaining a Business System for Integration Server**.

Configuring the Central Adapter Engine

To enable load balancing between the Integration Server and the central Adapter Engine, you must adapt the host name property used for the SLD registration of a J2EE server node.

To adapt the host name property of the J2EE server node

1. Open the J2EE Visual Administrator.
2. Expand Cluster Global Settings, and then select the service **SAP XI AF CPA Cache**.
3. Type the virtual hostname and the ports of the SAP Web Dispatcher for the properties:
`SLD.selfregistration.hostName`
`SLD.selfregistration.httpPort`
`SLD.selfregistration.httpsPort`
4. Restart the J2EE Engine cluster.

Configuring the Central Monitoring Server

To enable load balancing to the central monitoring server, you must adapt the corresponding RFC destination.

To configure the Central Monitoring Server

1. Open the SAP GUI, and login to your instance as a PI super user.
2. Call transaction **SM59** (see Figure 5).
3. Expand **ABAP connections**.
4. Choose the RFC destination **CentralMonitoringServer-XIAlerts**.
5. Select **Load Balancing**.
6. Specify the following values:
`Target System: <SID>`
`Message Server: <virtual host>`
`Group: SPACE`

7. Select the RFC destination **PMI<SID><client>**.

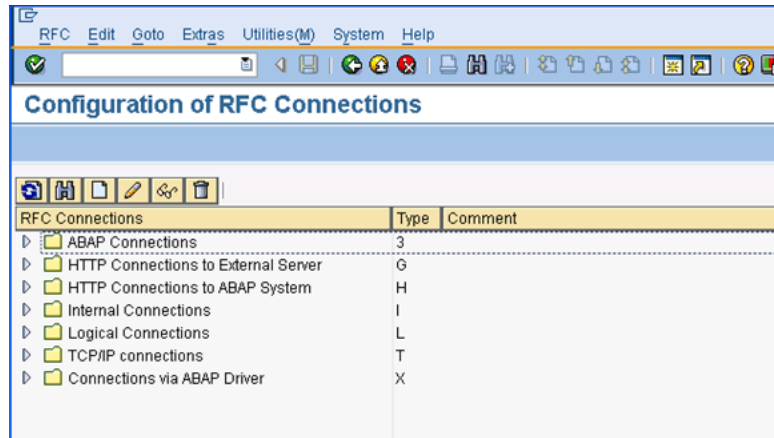


Figure 5 Calling transaction SM59

8. Select **Load Balancing**.
9. Specify the following values:
 - Target System:** <SID>
 - Message Server:** <virtual host>
 - Group:** SPACE
10. Click the Save button/icon.

Configuring the Dialog Instance

To ensure that update and spool processing is always possible, you should configure at least one separate UPD work process and one separate SPO work process.

Check the dialog instance profile. If required, configure a UPD work process and an SPO work process.

For information on how to configure these objects, consult your SAP documentation.

Configuring the BIG-IP LTM system for SAP Usage Type PI

In this section, we configure the BIG-IP LTM system. If you are using the BIG-IP LTM to offload SSL transactions, be sure to see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 18.

Creating the TCP health monitor

For SAP PI, we create a simple TCP health monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific.

To configure a TCP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
The Monitors screen opens.
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 **sap_tcp**.
4. From the **Type** list, select **TCP**.
The TCP Monitor configuration options appear.
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. In our example, we use an **Interval** of **30** and a **Timeout** of **91** (see Figure 6).
6. In the Send String and Receive Rule sections, you can add an optional Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Local Traffic >> Monitors >> New Monitor...

General Properties

Name: sap_tcp

Type: TCP

Import Settings: tcp

Configuration: Basic

Interval: 30 seconds

Timeout: 91 seconds

Send String:

Receive String:

Reverse: Yes No

Transparent: Yes No

Cancel Repeat Finished

Figure 6 Configuring the health monitor

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the SAP PI devices. You associate the monitor you just created with this pool.

To create the Internet Connection Manager pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.
Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.
3. In the **Name** box, enter a name for your pool. In our example, we use **sap_pi**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP health monitor* section, and click the Add (<<) button. In our example, we select **sap_tcp**.
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 **Round Robin**.

6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first server to the pool. In our example, we type **10.133.20.15**.
8. In the **Service Port** box, the appropriate port for SAP PI. In our example, we type **52000**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 7-9 for each server you want to add to the pool. In our example, we repeat these steps once for **10.133.20.16** and **10.133.20.17**.
11. Click the **Finished** button.

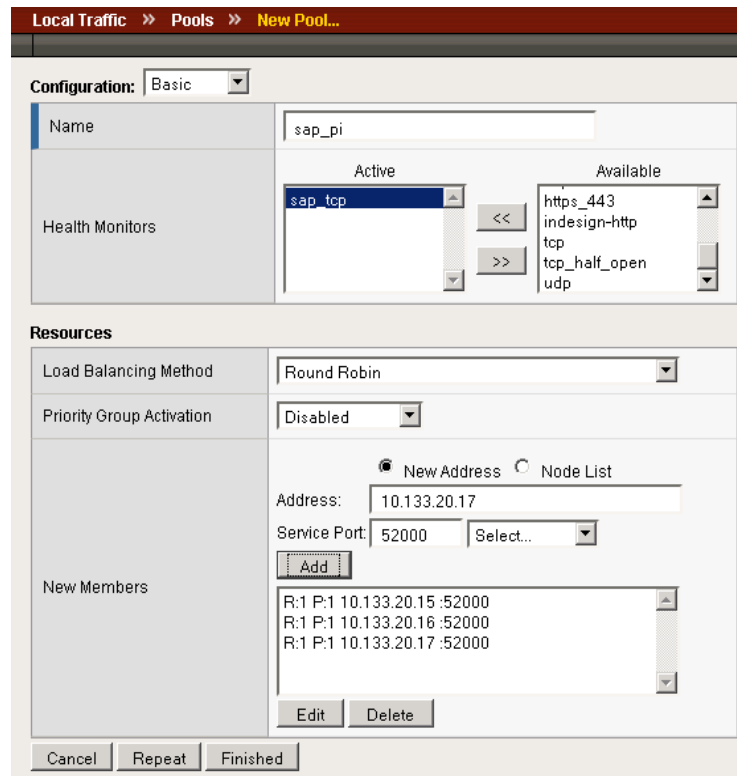


Figure 7 Creating the pool for the PI devices

Creating the profiles

A *profile* is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Creating the TCP profiles

First, we create the TCP profiles. If the majority of the users are accessing the system from remote or home offices, we recommend using the **tcp-wan-optimized** (for client side TCP connections) and **tcp-lan-optimized** (for server-side TCP connections) parent profiles. If most users are accessing deployment via the LAN, use the base TCP profile instead of this WAN optimized profile. In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile. Remember, if most users are accessing the installation via the LAN, use the base TCP profile instead of this WAN optimized profile.

To create a new TCP WAN optimized 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 **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap-pi-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the LAN optimized TCP profile

Now we configure the LAN optimized profile. If you have already created a simple TCP profile, based off the default TCP profile (and not the WAN optimized profile above), you do not need to create another TCP profile, continue with the next procedure.

To create a new TCP 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 **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap-pi-lan**.

-
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
 6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
 7. Click the **Finished** button.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. Testing has demonstrated that this can provide significant performance improvements for SAP implementations. 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. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap-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.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the virtual server

Next, we configure a virtual server that reference the profiles and pool you created in the preceding procedures.

◆ Note

*If you are using the BIG-IP LTM to offload SSL from the PI installation, you should not create the following virtual server. Continue with **Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment**, on page 18.*

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **sap-pi-virtual**.
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 **10.133.21.35**.
6. In the **Service Port** box, type a port or select a service from the list.
In our example, we type **80**.

General Properties	
Name	sap-pi-virtual
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network
	Address: 10.133.21.35
Service Port	80 HTTP
State	Enabled

Figure 8 Creating the SAP PI 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 name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **sap-pi-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap-pi-lan**.

-
- From the **OneConnect Profile** list, select **sap-oneconnect**.

Configuration:	Advanced
Type	Standard
Protocol	TCP
Protocol Profile (Client)	sap-pi-wan
Protocol Profile (Server)	sap-pi-lan
OneConnect Profile	sap-oneconnect
HTTP Profile	None

Figure 9 Selecting the profiles for the virtual server

- In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **sap_pi**.

Default Pool	+	sap_pi
Default Persistence Profile		None
Fallback Persistence Profile		None
Cancel Repeat Finished		

Figure 10 Adding the pool to the virtual server

- Click the **Finished** button.

The configuration for the SAP PI is now complete. If you are offloading SSL from the PI deployment, continue with the following section.

Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

The BIG-IP LTM device can be configured as an SSL proxy, offloading the SSL duties from the servers.

◆ Important

This section is optional, and only necessary if you are using the BIG-IP LTM system for offloading SSL.

Using SSL certificates and keys

Before you can enable the BIG-IP system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SAP connections on the BIG-IP device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP system. For information on generating certificates, or using the BIG-IP system to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

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** list, select the type of import (**Key** or **Certificate**).
5. Select the import method (text or file).
6. Type the name of the key or certificate.
7. Click **Import**.

If you imported the certificate in the preceding procedure, repeat the entire procedure for the key.

Creating a Client SSL profile

For offloading SSL, you must create a Client SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**.
The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button.
The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **sap-clientssl**.
6. In the Configuration section, click a check in the **Certificate** and **Key Custom** boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
9. Click the **Finished** button.

For more information on creating or modifying profiles, or SSL Certificates, see the BIG-IP documentation.

Creating an HTTPS virtual server

The next step is to create a virtual server for the SSL offload that uses the Client SSL profile you just created.

To create a new HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **sap-pi-ssl**.
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 **10.133.21.50**.

6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. From the Configuration list, select **Advanced**.
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*. In our example, we select **sap-tcp-wan** from the list
10. From the **Protocol Profile (Server)** select the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap-tcp-lan** from the list.
11. From the **OneConnect Profile** list, select **sap-oneconnect**.
12. From **SSL Profile (Client)** list, select the name of the profile you created in the *Creating a Client SSL profile* section. In our example we select **sap-clientssl**.
13. In the Resources section, from the **Default Pool** list, select the pool you created for your SAP PI nodes in the *Creating the pool* section. In our example, we select **sap_pi**.
14. Click the **Finished** button.

This concludes the steps necessary to use the BIG-IP LTM system to offload SSL traffic.