DEPLOYMENT GUIDE
Version 1.0

Deploying the BIG-IP LTM System with VMware View

Table of Contents

1

Deploying F5 with VMware View

- Modifying the VMware View Manager configuration
- Configuring the BIG-IP LTM system for VMware View
- SSL Certificates on the BIG-IP system

Deploying F5 with VMware View

Welcome to the F5 Deployment Guide on VMware View (formerly VMware Virtual Desktop Infrastructure - VDI). This document provides guidance and configuration procedures for deploying the BIG-IP Local Traffic Manager (LTM) with the VMware View desktop virtualization solution.

The VMware View portfolio of products lets IT run virtual desktops in the datacenter while giving end users a single view of all their applications and data in a familiar, personalized environment on any device at any location.

The BIG-IP LTM brings advanced application delivery networking performance to VMware View. This can help improve the performance and capacity of VMware View Manager servers, through precise load balancing, traffic management and by offloading processor-intensive functions such as SSL termination and compression.

For more information on VMware View, see ***http://www.vmware.com/products/view/***

For additional resources, see the **VMware forum on DevCentral**.

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

Prerequisites and configuration notes

The following are prerequisites for this solution:

- The BIG-IP LTM system must be running 10.0 or later. We strongly recommend using version 10.0.1 or later.
- Because the BIG-IP LTM system is offloading SSL for the VMware deployment, this guide does not include VMware Security servers.
- This deployment guide is written with the assumption that VMware View is already installed and configured on the network.
- The BIG-IP system uses virtual servers to distribute traffic. Because this term is the same or similar to objects used by VMware, the following definition applies to BIG-IP virtual servers: A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients on an external network can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions. Virtual servers increase the availability of resources for processing client requests. For more information on F5 virtual servers, see the product documentation or the online help.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP Local Traffic Manager (LTM)	v10.0.1 with Hotfix 2, v10.1
VMware View	v3.0.1, v3.2, v3.2.2

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

In our configuration presented in this deployment guide, the client, using the View client or a web browser, connects to the VMware Virtual Desktop Manager (VDM) via the virtual server on the BIG-IP LTM system. The BIG-IP LTM system selects a node from the VDM pool based on health monitor status and load balancing algorithm. At the same time, persistence records are created that the BIG-IP LTM uses to make ensure that clients return to the proper device.

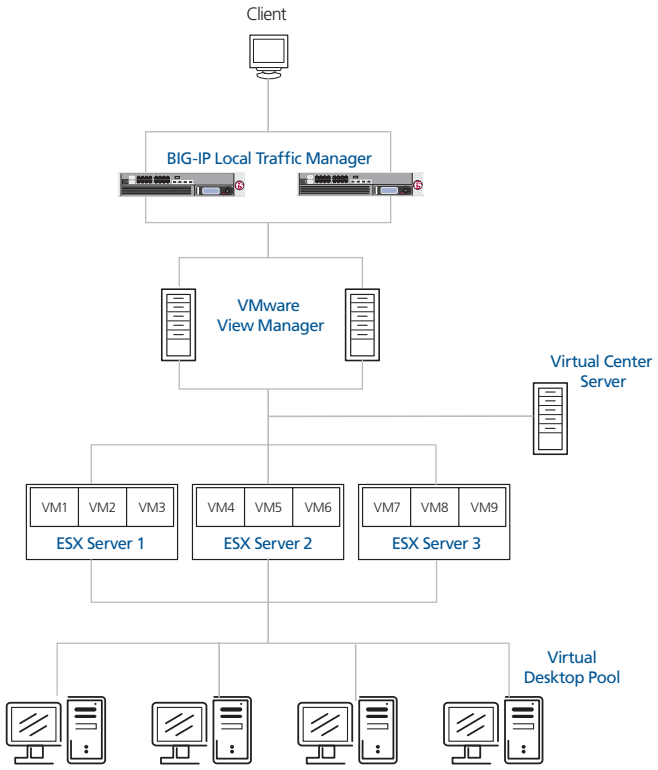

Figure 1.1 *Logical configuration diagram*

Modifying the VMware View Manager configuration

The first task in this guide is to modify the View Manager configuration to allow the BIG-IP LTM system to load balance connections and offload SSL transactions. For more information on modifying any of the VMware settings, see the VMware documentation.

Configuring the Global Settings

In the following procedure, we disable the SSL requirement for client connections in the View Administrator tool.

To modify the VMware configuration

1. Log on to the View Manager Administrator tool.
2. Click the **Configuration** tab.
3. In the Global Settings box, click the **Edit** button.
4. Clear the check from the **Require SSL for client connections** box.
5. Click the **OK** button.

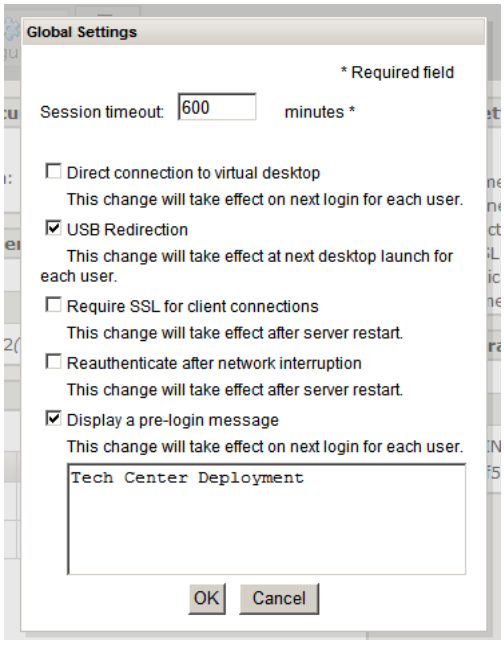

Figure 1.2 *Modifying the View Manager Global Settings*

Note

This setting only applies to View Manager devices - Security servers always require SSL

Configuring the External URL

The final modification to the VMware configuration is to configure the server External URL field with the FQDN of the BIG-IP virtual server. This is the server name that clients use to connect to the View Manager pool. Refer to the VMware View Administrator guide for more information. The following procedure must be performed on each VMware View Manager device.

To configure the External URL

1. Log on to the View Manager Administrator tool.
2. Click the **Configuration** tab.
3. Under **View Servers**, select a View Connection Server entry and click **Edit**.
4. In the **External URL** box, type the DNS name you will associate with the BIG-IP LTM virtual IP address, followed by a colon and the port. In our example, we type **https://broker.f5.com:443**.
5. Clear the **Direct Connection to Desktop** box if it is checked.
6. Click the **Ok** button.

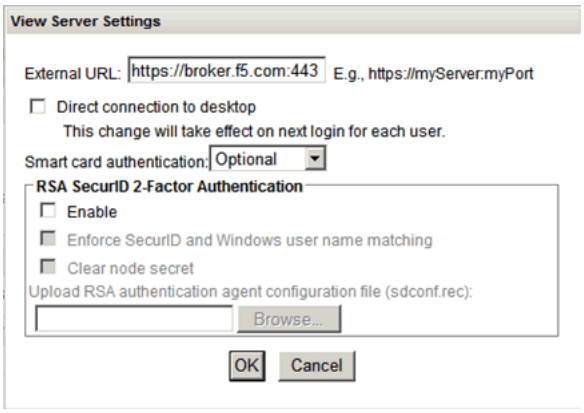

Figure 1.3 *Configuring the External URL*

Configuring the BIG-IP LTM system for VMware View

You can use the application template feature on the BIG-IP system to efficiently configure a set of objects corresponding to VMware View. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

◆ Note

Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.

Running the VMware View application template

To run the VMware View application template, use the following procedure.

To run the View application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **VMware View**. The VMware View application template opens.
4. In the Virtual Server Questions section, complete the following:
   a) You can type a unique prefix for your Microsoft IIS objects that the template will create. In our example, we leave this setting at the default, **my_View_**.
   b) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step a>_virtual_server**. In our example, we type **192.168.14.105**.
   c) If the servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

      If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system uses SNAT automap. See the Online Help for more information. In our example, we leave this at the default setting: **No**.

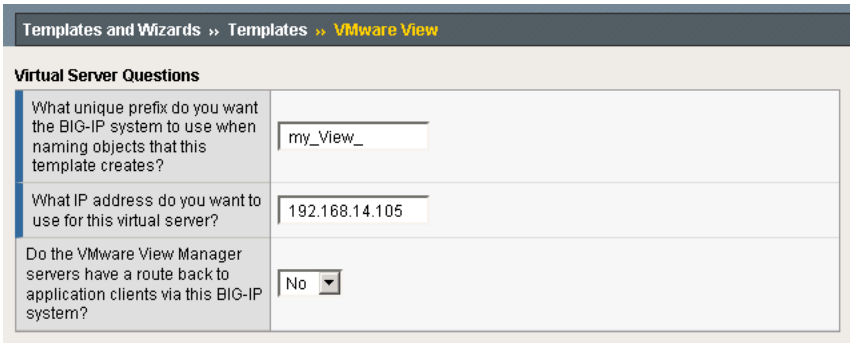

Figure 1.4 *Virtual Server Questions in the VMware View application template*

5. In the SSL Offload section, complete the following

   a) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 9.

   b) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 9.

   For information on generating certificates, or using the BIG-IP LTM 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***.

Figure 1.5 *SSL Encryption questions*

6. In the Load Balancing Questions section, complete the following:

   a) From the new or existing pool list, select the appropriate option. In our example, we select **Create New Pool**.
   If you choose **Use Pool**, select the appropriate pool from the list, and continue with Step 7.

b) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.

c) Next, add each of the View Managers that are a part of this deployment.
In the **Address** box, type the IP address of the first device. In our example, we type **10.132.70.101**.
In the **Service Port** box, type the appropriate port, or select it from the list. In our example, we select **HTTP** from the list.
Click the **Add** button. Repeat this step for each of the View Managers.

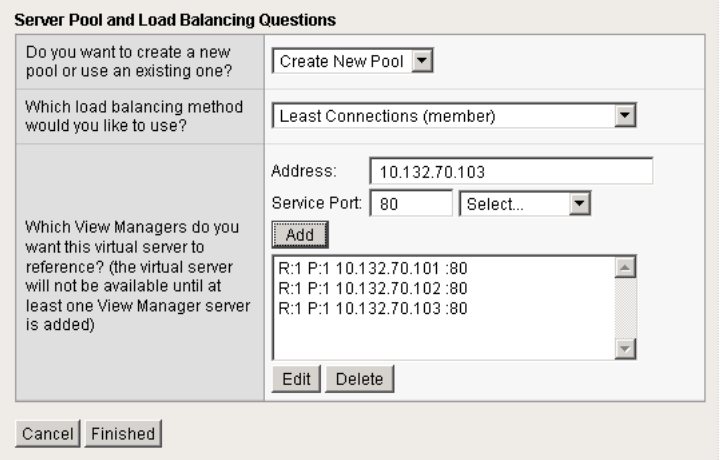

Figure 1.6 *Configuring the Load Balancing options*

7. In the Protocol Optimization Questions section, if most clients are connecting to the virtual server from a WAN, select **WAN** from the list. If most clients are connecting from a LAN, select **LAN** from the list.
This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.
8. Click the **Finished** button.

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created.

SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for VMware View connections on the BIG-IP LTM 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 LTM system. For information on generating certificates, or using the BIG-IP LTM 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 LTM 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**. The list of existing certificates displays.
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**.

If you imported the certificate, repeat this procedure for the key.

2

Manually Configuring the BIG-IP System v10 with VMware View

- Creating the health monitor
- Creating the View Manager server pool
- Creating the Universal Inspection Engine persistence iRule
- Using SSL certificates and keys
- Creating BIG-IP LTM profiles
- Creating the virtual server

Manually configuring the BIG-IP LTM for VMware View

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system, perform the following procedures:

- *Modifying the VMware View Manager configuration*, on page 1-4
- *Creating the health monitor*
- *Creating the View Manager server pool*
- *Creating the Universal Inspection Engine persistence iRule*
- *Using SSL certificates and keys*
- *Creating BIG-IP LTM profiles*
- *Creating the virtual server*

Note

If you are using VMware Security servers with the BIG-IP LTM system, in addition to a Client SSL profile, you have to create a Server SSL profile. See the BIG-IP LTM documentation for details. VMware Security servers were not a part of our deployment scenario.

Modifying the VMware View Manager global settings

You must first follow the procedure *Modifying the VMware View Manager configuration*, on page 1-4 for important changes to the VMware configuration.

Creating the health monitor

The first task is to set up a health monitor for the VMware View Manager devices. This procedure is optional, but very strongly recommended. For this configuration, we create a simple HTTP health monitor. In this example, the advanced fields are not required, and we recommend you use the default values for the send and receive strings.

To configure a HTTP 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 **view-manager-http**.

4. From the **Type** list, select **HTTP**.
   The HTTP 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 (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. Click the **Finished** button.
   The new monitor is added to the Monitor list.

Creating the View Manager server pool

The next step is to create a pool on the BIG-IP LTM system for the View Manager systems. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method.

To create the 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.
3. In the **Name** box, enter a name for your pool.
   In our example, we use **view-manager-pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the health monitor* section, and click the Add (<<) button. In our example, we select **view-manager-http**.
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. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the first server to the pool. In our example, we type **10.133.80.10**
9. In the **Service Port** box, type **80**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each server you want to add to the pool.
12. Click the **Finished** button (see Figure 2.1).

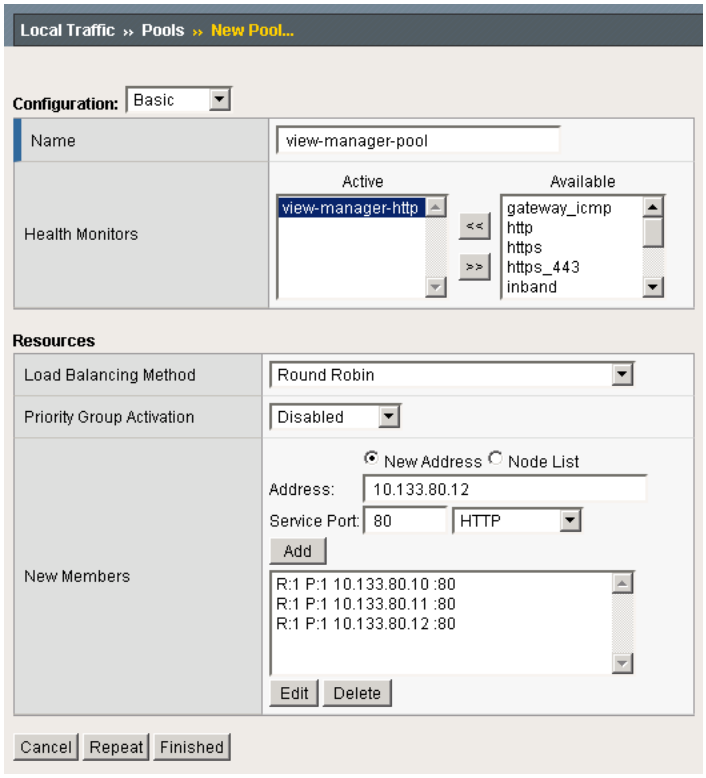

Figure 2.1 *Configuring the BIG-IP LTM pool*

Creating the Universal Inspection Engine persistence iRule

Using the following iRule, the BIG-IP LTM is able to direct traffic with greater precision resulting in a more uniform load distribution on the connection servers. Using the Universal Inspection Engine (UIE), the iRule looks for session information so that the BIG-IP LTM can persist the connections to the proper nodes. The View clients first use the session information in a cookie, and then use it as an URI argument when the tunnel is opened. The first response from the server contains a JSESSIONID cookie. The iRule enters that session ID into the connection table and upon further client requests looks for the information in a cookie or in the URI.

Important

For the following iRule to function correctly, you must be using the BIG-IP LTM system to offload SSL transactions from the View implementation, which is described in this deployment guide.

To create the persistence iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.

2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the Name box, type a name for this rule. In our example, we type **view-jsessionid**.
4. In the Definition box, type the following iRule, omitting the line numbers.
   Important: Line 19 must be entered as a single line.

```
1   when HTTP_REQUEST {
2     if { [HTTP::cookie exists "JSESSIONID"] } {
3       # log local0. "Client [IP::client_addr] sent cookie [HTTP::cookie "JSESSIONID"]"
4       set jsess_id [string range [HTTP::cookie "JSESSIONID"] 0 31]
5       persist uie $jsess_id
6       # log local0. "uie persist $jsess_id"
7     } else {
8       # log local0. "no JSESSIONID cookie, looking for tunnel ID"
9       set jsess [findstr [HTTP::uri] "tunnel?" 7]
10      if { $jsess != "" } {
11        # log local0. "uie persist for tunnel $jsess"
12        persist uie $jsess
13      }
14    }
15  }
16  when HTTP_RESPONSE {
17   if { [HTTP::cookie exists "JSESSIONID"] } {
18     persist add uie [HTTP::cookie "JSESSIONID"]
19     # log local0. "persist add uie [HTTP::cookie "JSESSIONID"] server:
       [IP::server_addr] client: [IP::client_addr]"
20   }
21  }
22  # when LB_SELECTED {
23  # log local0. "Member [LB::server addr]"
24  # }
```

5. Click the **Finished** button.

◆ Tip

The preceding iRule contains logging statements that are commented out. If you want to enable logging, simply remove the comment (#) from the code.

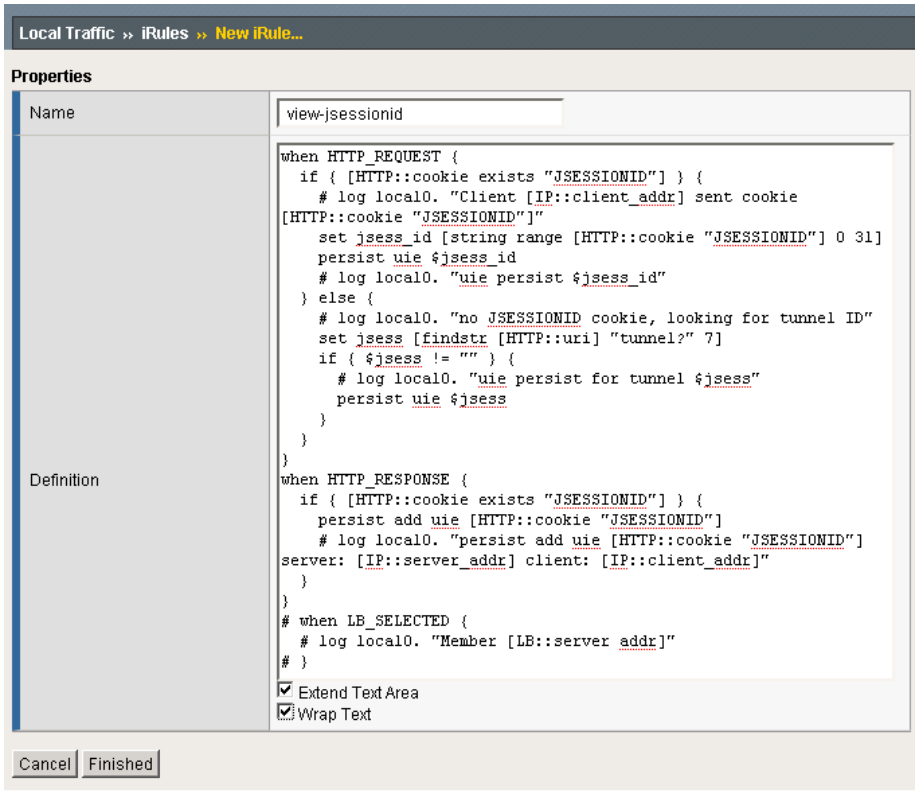

Figure 2.2 *Configuring the persistence iRule on the BIG-IP LTM system*

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for View connections on the BIG-IP LTM 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 LTM system. For information on generating certificates, or using the BIG-IP LTM 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 LTM 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**. The list of existing certificates displays.
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**.

If you imported the certificate, repeat this procedure for the key.

Creating BIG-IP LTM profiles

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

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In this example, we use the **http-lan-optimized-caching** parent profile.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **view-http**.
4. From the **Parent Profile** list, select **http-lan-optimized-caching**. The profile settings appear.

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

Creating the TCP profiles

The next task is to create the TCP profiles. We recommend creating one TCP profile using the **tcp-lan-optimized** parent. If your configuration uses various WAN links and your users are widely distributed, you should also create a second profile that uses **tcp-wan-optimized** as the parent profile. If all of your users are accessing the BIG-IP LTM over a LAN, you only need to create the LAN optimized profile.

Creating the LAN optimized TCP profile

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

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.
4. In the **Name** box, type a name for this profile. In our example, we type **view-lan-opt**.
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 the WAN optimized TCP profile

Now we create is the WAN optimized TCP profile.

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.
4. In the **Name** box, type a name for this profile. In our example, we type **view-wan-opt**.
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 UIE persistence profile

The next profile we create is the persistence profile. This profile references the Universal Inspection Engine iRule you created earlier in this guide.

To create a persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **view-persist**.
5. From the **Persistence Type** list, select **Universal**.
The configuration options for universal persistence appear.
6. In the **iRule** row, check the Custom box. From the iRule list, select the name of the iRule you created in *Creating the Universal Inspection Engine persistence iRule*, on page 2-3. In our example, we select **view-jsessionid**.
7. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

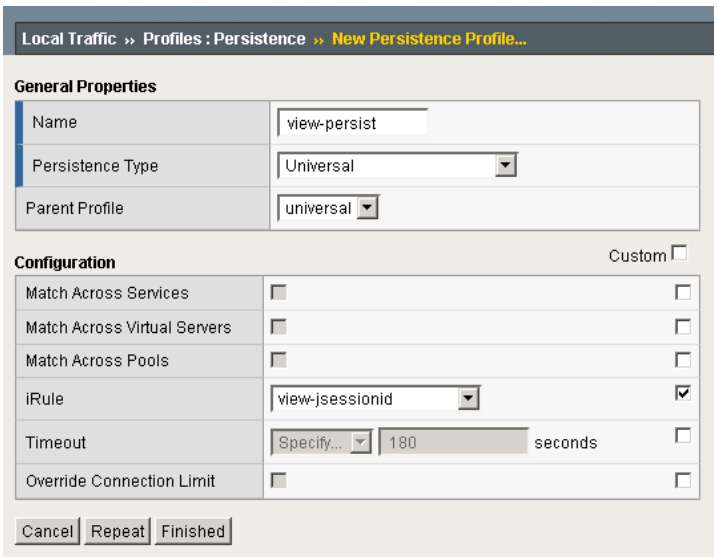

Figure 2.3 *Creating the persistence profile*

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. 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 **view-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 a Client SSL profile

The next step in this configuration is to 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 **view-clientssl**.
6. In the Configuration section, check 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.

Creating the virtual server

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

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 **view-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 **10.133.81.10**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.

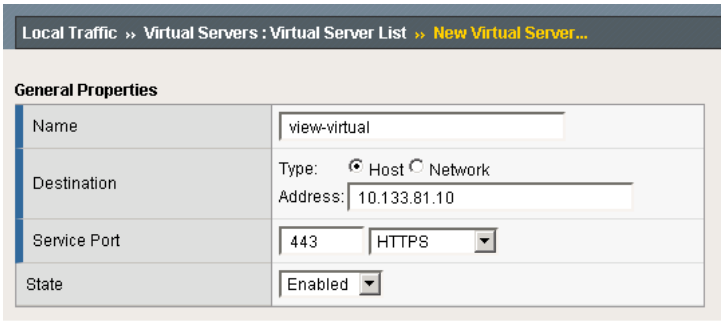

Figure 2.4 *Configuring the virtual server properties*

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 *Creating the WAN optimized TCP profile*, on page 2-7. In our example, we select **view-wan-opt**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in *Creating the UIE persistence profile*, on page 2-8. In our example, we select **view-lan-opt**.

11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*, on page 2-9. In our example, we select **view-oneconnect**.
12. From the **HTTP Profile** list, select the name of the profile you created in *Creating an HTTP profile*, on page 2-6. In our example, we select **view-http**.

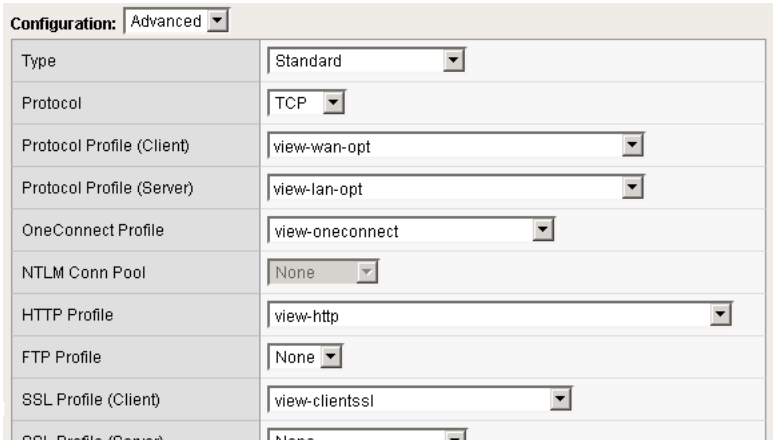

Figure 2.5 *Adding the profiles to the virtual server*

13. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the View Manager server pool*, on page 2-2. In our example, we select **view-manager-pool**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating the UIE persistence profile*, on page 2-8. In our example, we select **view-persist**.

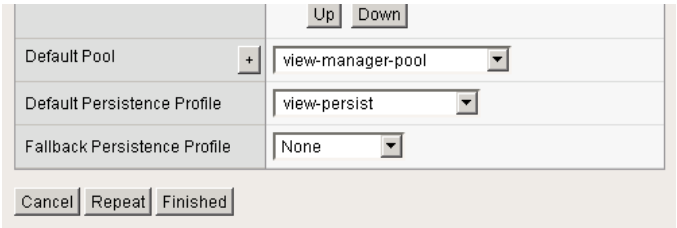

Figure 2.6 *Adding the pool and persistence profile to the virtual server*

15. Click the **Finished** button.

The BIG-IP LTM configuration for VMware View is now complete.