DEPLOYMENT GUIDE

Deploying the BIG-IP System v10 with VMware Virtual Desktop Infrastructure (VDI)

Version 1.0

Table of Contents

1

Deploying the BIG-IP System v10 with VMware Virtual Desktop Infrastructure

- Modifying the VMware Virtual Desktop Manager global settings
- Configuring the BIG-IP system for VMware VDI
- SSL Certificates on the BIG-IP system

Deploying the BIG-IP system v10 with VMware VDI

Welcome to the F5 Deployment Guide on VMware Virtual Desktop Infrastructure (VDI). This document provides guidance and configuration procedures for deploying the BIG-IP Local Traffic Manager (LTM) v10 with VMware VDI.

VMware VDI is an integrated desktop virtualization solution that delivers enterprise-class control and manageability with a familiar user experience. VMware VDI, built on VMware's industry leading and proven virtualization platform, provides new levels of efficiency and reliability for your virtual desktop environment.

One of the unique features of this deployment is the ability of the BIG-IP LTM system to persist VDI client connections on a session by session basis. Other implementations commonly use simple/source address persistence; where all the connections from a single IP address will be sent to one server. With the iRule described later in this document, the BIG-IP LTM is able to direct traffic with greater precision resulting in a more uniform load distribution on the connection servers.

New in version 10.0 of the BIG-IP system are Application Ready Templates. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

For additional resources on F5 and VMware, 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

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- Because the BIG-IP LTM system is offloading SSL for the VMware deployment, this deployment guide does not include VMware Security servers.
- This deployment guide is written with the assumption that VMware server(s), Virtual Center and VDM server(s) are already configured on the network and are in good working order.
- For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.

- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 1-8.
- While we strongly recommend using the application template, you can also manually configure the BIG-IP system. For more information, see *Manually configuring the BIG-IP LTM for VDI*, on page 2-1.

Important

All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0
VMware VDI	2.1.0

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

In our configuration presented in this deployment guide, the client, using the VDI 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 will use to make ensure that clients return to the proper device.

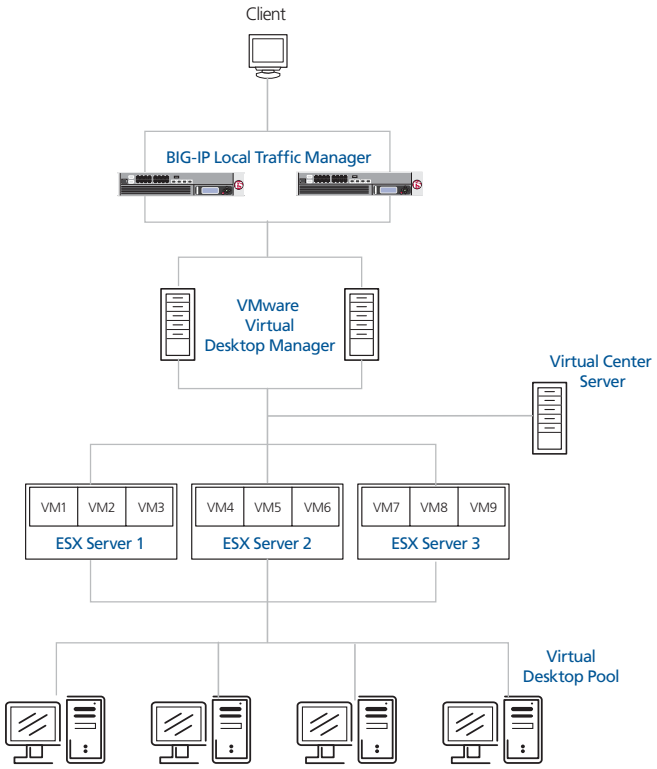

Figure 1.1 *Logical configuration example*

Modifying the VMware Virtual Desktop Manager global settings

Before starting the VDI application template, we modify the VDI configuration to allow the BIG-IP LTM system to load balance VDI connections and offload SSL transactions. In the following procedure, we disable the SSL requirement for client connections in the Virtual Desktop Manager Administrator tool.

To modify the VMware configuration

1. Log on to the VDM Administrator tool.
2. Click the **Configuration** tab.
   The configuration options page opens.
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.

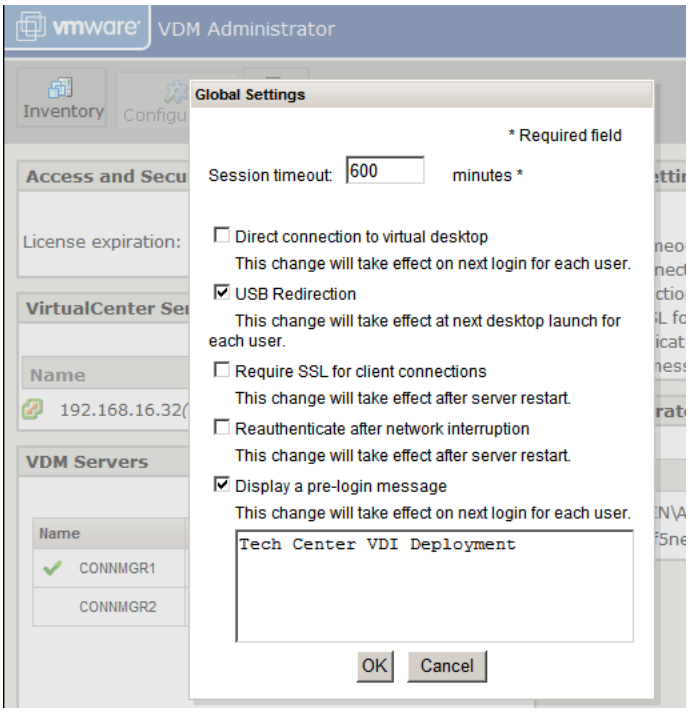

Figure 1.2 *Modifying the VDM Global Settings*

Note

This setting will only apply to Connection Manager servers -- Security servers will always require SSL

Configuring the BIG-IP system for VMware VDI

You can use the new application template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to VMware VDI. 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 VDI application template

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

To run the VDI 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 VDI**. The VMware VDI 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_VDI_**.
   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 **192.168.14.100**.
   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 will use SNAT automap. See the Online Help for more information.
      In our example, we leave this at the default setting: **No**.

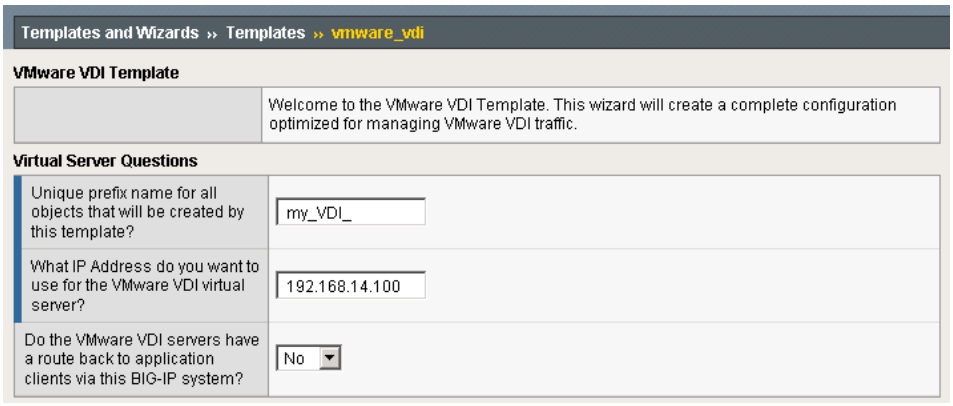

Figure 1.3 *Running the VMware VDI application template*

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 8.

   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 8.

   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***.

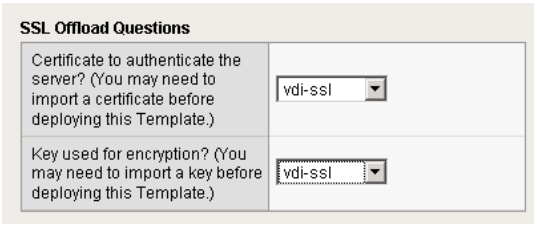

Figure 1.4 *Configuring the BIG-IP system for SSL Offload*

6. In the Protocol Optimization Questions section, if most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be 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.

7. 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 8.

   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 VDI devices that are a part of this deployment.
   In the **Address** box, type the IP address of the first VDI 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 VDI devices.

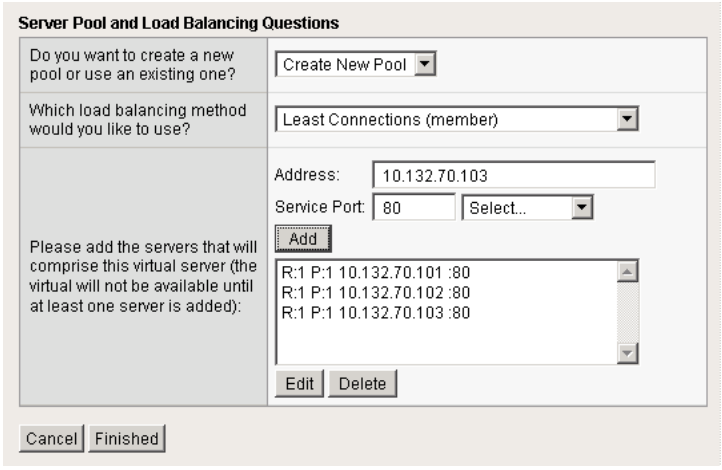

Figure 1.5 *Configuring the Load Balancing options*

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 VDI 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

Deploying the BIG-IP System v10 with VMware Virtual Desktop Infrastructure

- Creating the health monitor
- Creating the Connection server pool
- Creating the persistence iRule
- Using SSL certificates and keys
- Creating BIG-IP LTM profiles
- Creating the virtual server

Manually configuring the BIG-IP LTM for VDI

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 Virtual Desktop Manager global settings*, on page 1-4
- *Creating the health monitor*
- *Creating the Connection server pool*
- *Creating the 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 will 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 Virtual Desktop Manager global settings

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

Creating the health monitor

The next step is to set up a health monitor for the VMware Connection servers. 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 **vdi-connection**.
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 Connection server pool

The next step is to create a pool on the BIG-IP LTM system for the Connection servers. 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. From the **Configuration** list, select **Advanced**.
   The Advanced configuration options appear.
4. In the **Name** box, enter a name for your pool.
   In our example, we use **vdi-connection-pool**.
5. 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 **vdi-connection**.
6. In the **Slow Ramp Time** box, type **300**. We set the Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the Least Connections load balancing algorithm does not send all new connections to that member (a newly available member will always have the least number of connections).
7. 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 (member)**.
8. For this pool, we leave the Priority Group Activation **Disabled**.
9. In the New Members section, make sure the **New Address** option button is selected.
10. In the **Address** box, add the first server to the pool. In our example, we type **10.133.80.10**
11. In the **Service Port** box, type **80**.
12. Click the **Add** button to add the member to the list.

13. Repeat steps 9-12 for each server you want to add to the pool.
14. Click the **Finished** button (see Figure 2.1).

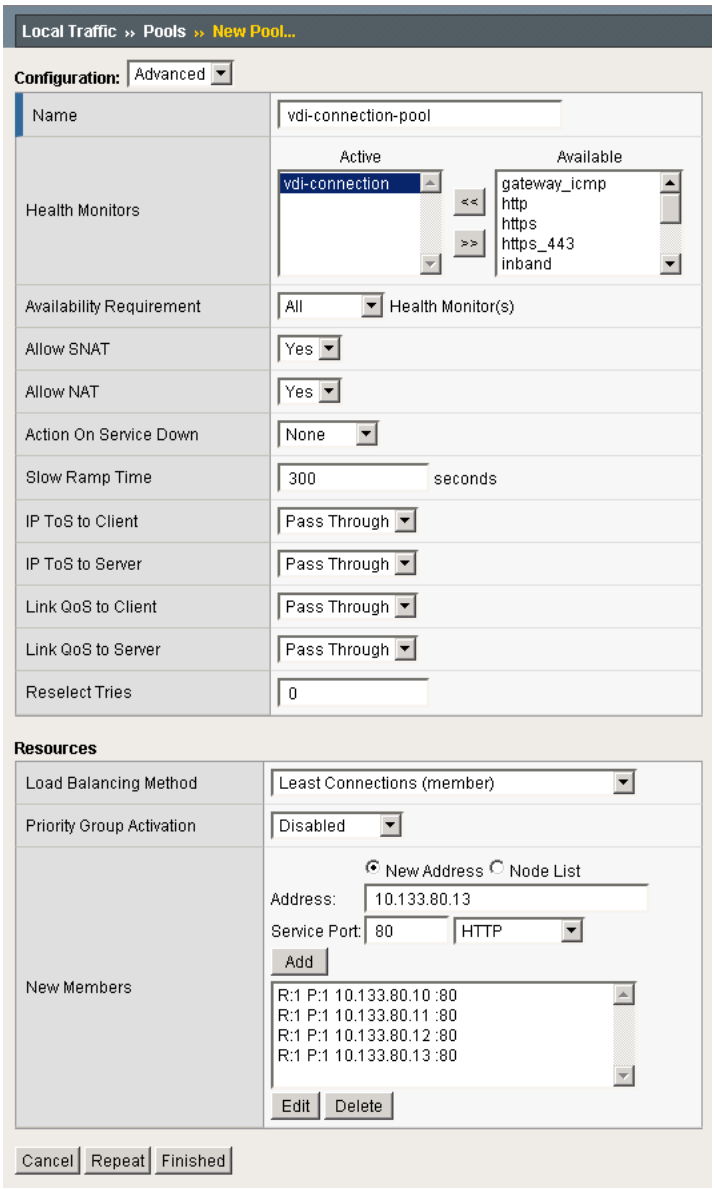

Figure 2.1 *Configuring the BIG-IP LTM pool*

Creating the 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. The iRule looks for session information so that the BIG-IP LTM can persist the connections to the proper nodes. The VDI

clients will first use the session information in a cookie, and then will 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 VDI 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 **vdi-jessionid**.
4. In the Definition box, paste the following rule.

```
 when HTTP_REQUEST {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    # log local0. "Client [IP::client_addr] sent cookie
[HTTP::cookie "JSESSIONID"]"
    set jsess_id [string range [HTTP::cookie
"JSESSIONID"] 0 31]
    persist uie $jsess_id
    # log local0. "uie persist $jsess_id"
  } else {
    # log local0. "no JSESSIONID cookie, looking for
tunnel ID"
    set jsess [findstr [HTTP::uri] "tunnel?" 7]
    if { $jsess != "" } {
      # log local0. "uie persist for tunnel $jsess"
      persist uie $jsess
    }
  }
}
when HTTP_RESPONSE {
  if { [HTTP::cookie exists "JSESSIONID"] } {
    set jsess_cookie [HTTP::cookie "JSESSIONID"]
    persist add uie [HTTP::cookie "JSESSIONID"]
    # log local0. "persist add uie [HTTP::cookie
"JSESSIONID"] server: [IP::server_addr] client:
[IP::client_addr]"
  }
}
```

```
# when LB_SELECTED {
  # log local0. "Member [LB::server addr]"
# }
```

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.

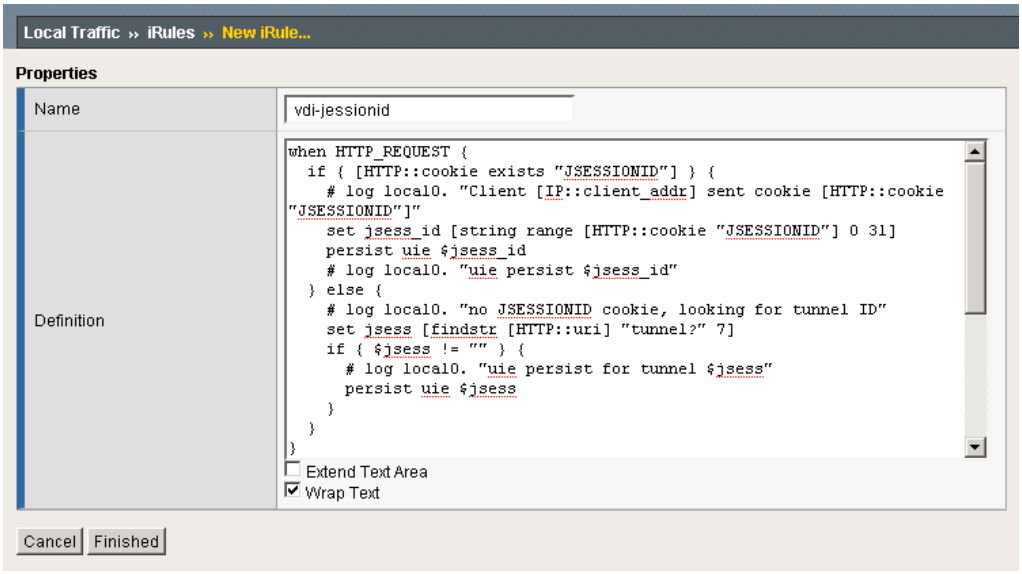

Figure 2.2 *Configuring the persistence iRule on the BIG-IP LTM system*

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 VDI 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

BIG-IP version 9.0 and later use 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.

These profiles use new optimized profiles available in BIG-IP LTM version 9.4 and later. If you are using a BIG-IP LTM version prior to 9.4, the ***Configuration Guide for BIG-IP Local Traffic Management*** for version 9.4 (available on **AskF5**) shows the differences between the base profiles and the optimized profile types. Use this guide to manually configure the optimization settings.

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. Because the default installation of VDM does not compress data sent to the client, we use a parent profile that includes compression. In this example, we use the **http-wan-optimized-compression-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 **vdi-http**.
4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**. The profile settings appear.
5. Check the Custom box for **Redirect Rewrite**, and select **All** from the list.
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 TCP profiles

The next profiles we create are the TCP profiles. If most of the VDI users are connecting via a Local Area Network, we recommend using the **tcp-lan-optimized** parent profile. If the majority of the users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client side TCP connections). 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 LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or do not want to use this optimized profile, you can choose the default TCP parent 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 **vdi-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 the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this 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 **vdi-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 persistence profile

The next profile we create is the persistence profile. This profile references the 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 **vdi-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 persistence iRule*, on page 2-3. In our example, we select **vdi-jessionid**.
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.

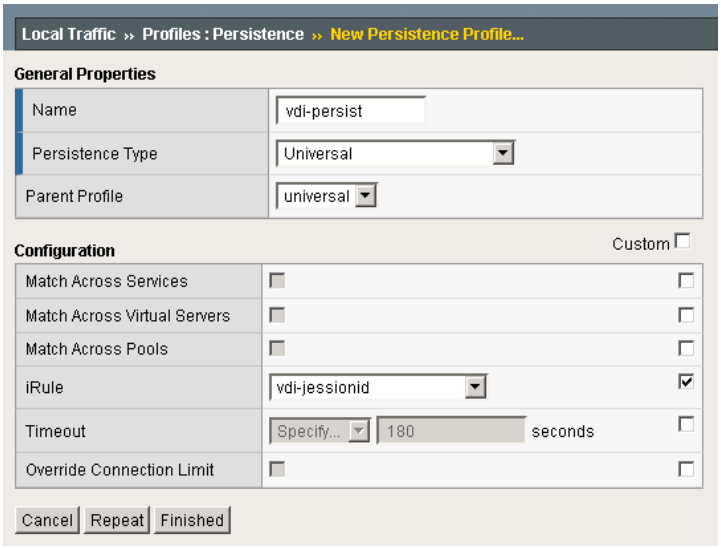

Figure 2.3 *Creating the persistence profile*

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 **vdi-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 **vdi-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 **vdi-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.

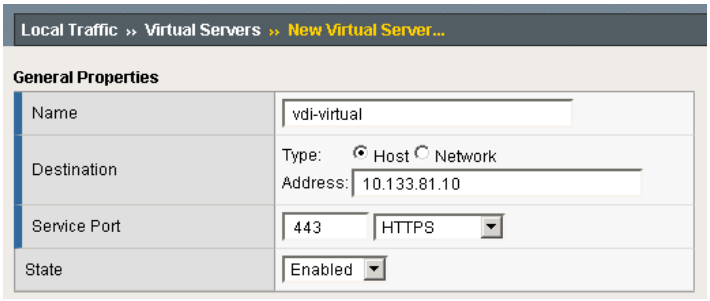

Figure 2.4 *Creating the VDI virtual server*

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. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following step. In our example, we select **vdi-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 **vdi-lan**.
11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*. In our example, we select **vdi-oneconnect**.
12. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **vdi-http**.
13. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*. In our example, we select **vdi-clientssl** (see Figure 2.5).

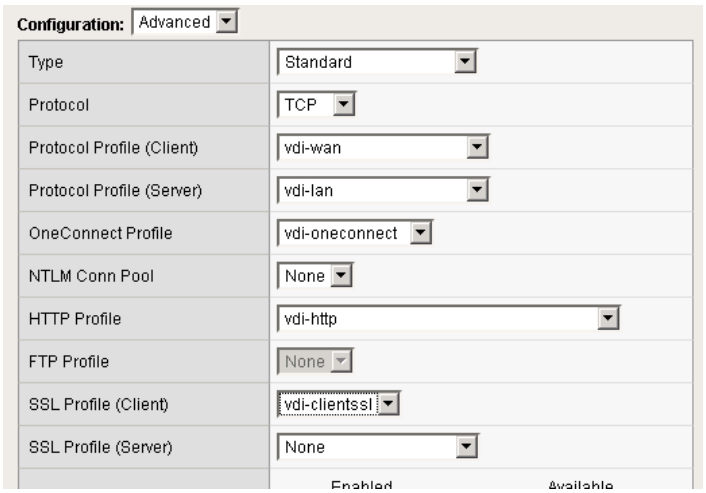

Figure 2.5 *Selecting the VDI profiles for the virtual server*

14. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the Connection server pool* section. In our example, we select **vdi-connection-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profile* section. In our example, we select **vdi-persist**.

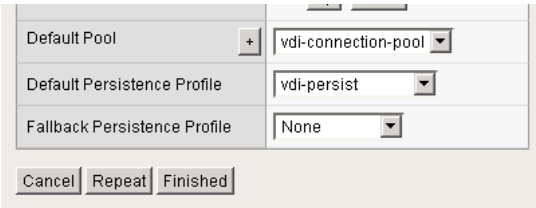

Figure 2.6 *Adding the Pool and Persistence profile to the virtual server*

16. Click the **Finished** button.
    The BIG-IP LTM configuration for the VDI configuration is now complete.