



Deploying the BIG-IP System v11 with VMware View 4.5

What's Inside:

- 2 What is F5 iApp™?
- 2 Prerequisites and configuration notes
- 3 Configuration flow
- 3 Modifying the VMware Virtual Desktop Manager global settings
- 6 Preparation Worksheet
- 7 Getting Started with the iApp for VMware View
- 10 Next steps
- 11 Troubleshooting??
- 12 Appendix: Manual configuration table

Welcome to the F5 and VMware® View® Deployment Guide. This document contains guidance on configuring the BIG-IP system version 11 for VMware View 4.5, resulting in a secure, fast, and available deployment.

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

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy and accurate way to configure the BIG-IP system for VMware View.

Why F5?

F5 and VMware have a long-standing relationship that centers on technology integration and solution development. As a result, customers can benefit from leveraging the experience gained by peers from deploying proven, real-world solutions.

F5's products and solutions bring an improved level of reliability, scalability, and security to VMware View deployments. For large VMware View deployments requiring multiple pods or several data centers, F5's products provide the load balancing and traffic management needed to satisfy the requirements of customers around the world.

F5 and VMware continue to work together on providing customers best-of-breed solutions that allow for better and faster deployments as well as being ready for future needs, requirements, and growth of your organization.

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

Products and versions tested

Product	Version
BIG-IP LTM	v11
VMware View	2.1, 3.0.1, 4.0, and 4.5

Document Version

1.0

Important: Make sure you are using the most recent version of this deployment guide at <http://www.f5.com/pdf/deployment-guides/vmware-view-45-iapp-dg.pdf>.

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for VMware View acts as the single-point interface for building, managing, and monitoring VMware View deployments.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network*: <http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf>.

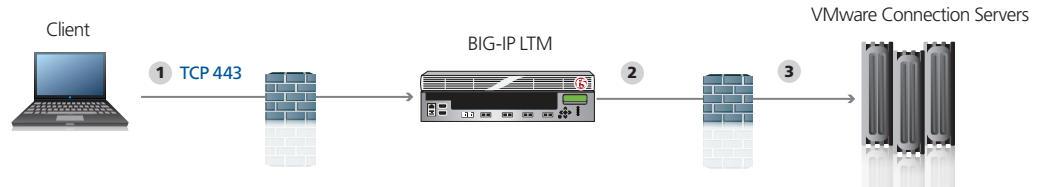
Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- This document is written with the assumption that you are familiar with both F5 devices and VMware View. For more information on configuring these devices, consult the appropriate documentation.
- For this deployment guide, the BIG-IP LTM system **must** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- This deployment guide provides guidance for using the iApp for VMware View found in version 11.0 and later. For advanced users extremely familiar with the BIG-IP, there is a manual configuration table at the end of this guide. However, we strongly recommend using the iApp template.
- Because the BIG-IP system will be offloading SSL for the VMware View deployment, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system.
- This deployment guide contains guidance on Application Visibility Reporting. Note that AVR is licensed on all systems, but if you wish to use it, AVR must be provisioned before beginning the iApp template.
- If you are using or plan to use PC over IP (PCoIP), see *Special note about PC over IP on page 3*
- This deployment guide is written with the assumption that VMware server(s), Virtual Center and connection brokers are already configured on the network and are in good working order.

Configuration flow

The following traffic flow diagram shows the BIG-IP LTM with a VMware View deployment using Connection Servers only.



Traffic Flow:

1. The client machine makes a connection to the BIG-IP virtual IP address for the VMware Connection Servers. The SSL connection terminates on the BIG-IP device.
2. BIG-IP offloads SSL and establishes a connection to the VMware Connection Servers.
3. After authentication, desktop entitlement, and selection are complete, desktop connections proceed through the BIG-IP to the appropriate View Desktop.

Special note about PC over IP

Beginning with VMware View 4, VMware supports PC over IP (PCoIP) as a display protocol. PCoIP is an application encrypted UDP protocol, so the BIG-IP system cannot offload encryption for it.

If you want to use PCoIP, we recommend you enable direct connections to the desktop using PCoIP. This means the View client connects to the View Manager server for authentication, authorization and obtaining desktop information. Then, when the users choose a desktop to connect to, the view client opens a new connection directly to the desktop, bypassing the BIG-IP and connection manager. If you are deploying an environment with mixed display protocols, we recommend enabling direct access for all protocols. Refer to the VMware View administrators guide for details.

This does not apply if you are using VMware Security Server.

Modifying the VMware Virtual Desktop Manager Global Settings

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

Modifying the VMware View global settings

The first task is to modify the View configuration Global Settings.

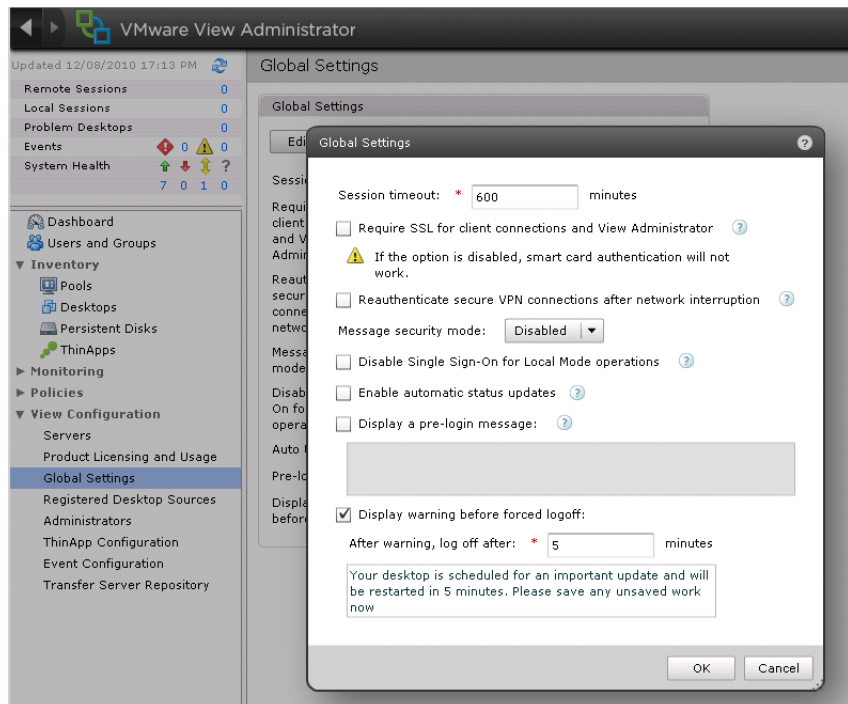
Note



The following SSL setting applies only to Connection Manager servers, Security servers always require SSL.

To modify the VMware configuration for View 4.5

1. Log on to the View Manager Administrator tool.
2. From the left Navigation pane, click to expand **View Configuration**, and then click **Global Settings**.
Global Settings page opens in the main pane.
3. Click the **Edit** button.
4. Clear the check from the **Require SSL for client connections and View Administrator** box.
5. Click the **OK** button.
6. You must reboot or restart the server after making this change. We strongly recommend rebooting.

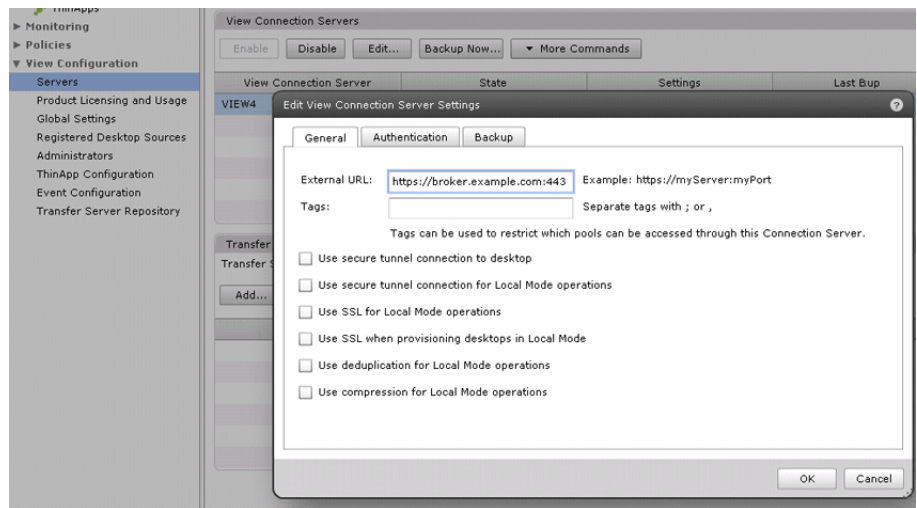


Configuring the External URL

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 modify the VMware configuration for View 4.5 without Security Server

1. Log on to the View Manager Administrator tool.
2. From the navigation pane, click to expand **View Configuration** and then click **Servers**. The Servers Settings opens in the main pane.
3. In the *View Connection Servers* box, select a View Connection Server and then click the **Edit** button.
4. On the General tab, in the **External URL** box, type the DNS name or IP address you will associate with the BIG-IP LTM virtual IP address for the Connection servers, followed by a colon and the port. In our example we type: **https://broker.example.com:443**
5. Click to clear the **Use Secure tunnel connection to desktop** box, if checked.
6. Click **OK** to close the window
7. Repeat these steps for each Connection Server.



This completes the modifications to VMware View.

Preparation Worksheet

In order to use the iApp for VMware View, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➔ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	SSL Offload	Pool Members	Sync/Failover Groups*	TCP request queuing*	WAN or LAN clients
IP address you will use for the LTM virtual server:	You must have imported a certificate and key into the BIG-IP LTM before running the template.	View server IP addresses: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to View are coming over a: LAN WAN
Optional Modules (you must have provisioned modules before running the template)					
<i>Application Visibility Reporting (AVR) - optional</i>					
If using AVR, we strongly recommend you first create an custom Analytics profile before running the template.					
Analytics profile name:					

Configuring the BIG-IP iApp for VMware View 4.5

Use the following guidance to help configure the BIG-IP system for VMware View using the BIG-IP iApp template.

Getting Started with the iApp for VMware View

To begin the VMware View iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **VMware-View_**.
5. From the **Template** list, select **f5.vmware_view**.
The VMware View iApp template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**

If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

- a. **Device Group**

If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

- b. **Traffic Group**

If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Analytics

This section of the template asks questions about Analytics. The Application Visibility Reporting (AVR) module allows you to view statistics specific to your VMware View implementation. AVR is available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. Note that these are only for application visibility reporting, you can view object-level statistics from the BIG-IP without provisioning AVR.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile before beginning the template. To create a new profile, from the Main tab, select **Profiles** and then click **Analytics**. Click **New** and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions.

1. **Enable Analytics**

Choose whether you want to enable AVR for Analytics.

Tip

If using AVR, create a new Analytics profile before beginning the iApp for more specific reporting

2. **Analytics Profile**

You must decide whether to use the default Analytics profile, or create a new one. As mentioned previously, we recommend creating a new profile to get the most flexibility and functionality out of AVR. If you choose to create a new profile after starting the template, you must exit the template, create the profile, and then restart the template.

To use the default Analytics profile, choose Use **Default Profile** from the list.

To choose a custom profile, leave the list set to **Select a Custom Profile**, and then from the Analytics profile list, select the custom profile you created.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients can send traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**

This is the address clients use to access VMware View (or a FQDN will resolve to this address). You need an available IP address to use here.

2. **Routes or secure network address translation**

If the View servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #3) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new address as the destination address when responding to traffic originating through the BIG-IP.

If you indicate the View servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the View servers.

We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

If you are configuring your BIG-IP LTM in a "one-armed" configuration with your View servers -- where the BIG-IP virtual server(s) and the View servers have IP addresses on the same subnet -- you must choose **No**.

3. **More than 64,000 simultaneous connections**

If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with #4.

If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.

4. **NTLM**

If you have configured the View servers to use NTLM authentication, select **Yes** from the list. If the View servers do not use NTLM, leave the list set to **No**.

SSL Encryption questions

Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the **Configuration Guide for BIG-IP Local Traffic Manager** available at <http://support.f5.com/kb/en-us.html>.

To configure the BIG-IP to offload SSL, select **Yes** from the list.

1. **Certificate**
Select the certificate for you imported for View from the certificate list.
2. **Key**
Select the associated key from the list.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the View servers and configure the pool.

1. **New Pool**
Choose **Create New Pool** unless you have already made a pool on the LTM for the View devices.
2. **Load balancing method**
You can choose any of the load balancing methods from the list. In our example, we use the default, **Round Robin**.
3. **Address/Port**
Type the IP Address and Port for each View Connection Server. You can optionally add a Connection Limit (see note on the left). Click **Add** to include additional servers to the pool.
4. **TCP Request Queuing**
TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *New Features Guide for BIG-IP Version 11*, available on Ask F5.

If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.
 - a. Type a queue length in the box. Leave the default of 0 for unlimited.
 - b. Type a number of milliseconds for the timeout value.

🔗 Important

If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port

Protocol Optimization Questions

In this section, you configure security and protocol optimizations.

1. **WAN or LAN**
Specify whether most clients are connecting over a WAN or LAN.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the VMware View service you just created. To see the list of all the configuration objects created to support View, on the Menu bar, click **Components**. The complete list of all View related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the VMware View implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your VMware View Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the View configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, you can always get object-level statistics.

AVR statistics

If you have provisioned AVR, you can get application-level statistics for your View application service.

To view AVR statistics

1. On the Main tab, expand **iApp** and then click **Application Services**.

2. From the Application Service List, click the VMware View service you just created.
3. On the Menu bar, click **Analytics**.
4. Use the tabs and the Menu bar to view different statistics for your View iApp.

Object-level statistics

If you haven't provisioned AVR, or want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Troubleshooting

Q: What do I use as the "External URL" in my View Connection Server Settings?

A: The External URL is the IP or DNS address that the View Client uses to connect back to the network. In this deployment guide, we give the example of the External URL `https://broker.example.com:443`. In this example we are suggesting that the IP addresses mapped to this Virtual Server is configured on the BIG-IP LTM. Connections from the View Client therefore map back to this IP address. If there is an upstream device, such as a firewall or router, in front of the BIG-IP LTM that is providing NAT to the BIG-IP, the External URL should be the IP or DNS address that maps to that NAT device. The NAT device would then deliver the traffic to the BIG-IP.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for VMware View. Advanced users extremely familiar with the BIG-IP can use following table to configure the BIG-IP LTM manually. This table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (Main tab-->Local Traffic -->Monitors)	Name	Type a unique name	
	Type	HTTP	
	Interval	30 (recommended)	
	Timeout	91 (recommended)	
Pool (Main tab-->Local Traffic -->Pools)	Name	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Load Balancing Method	Choose your preferred load balancing method	
	Address	Type the IP Address of the Connection Server nodes	
	Service Port	80 (repeat Address and Service Port for all nodes)	
iRule (Main tab-->Local Traffic -->iRules)	Name	Type a unique name.	
	Definition	See <i>Creating the iRule on page 13</i>	
Profiles (Main tab-->Local Traffic -->Profiles)	HTTP (Profiles-->Services)	Name Parent Profile	Type a unique name http-lan-optimized-caching
	TCP WAN (Profiles-->Protocol)	Name Parent Profile	Type a unique name tcp-wan-optimized
	TCP LAN (Profiles-->Protocol)	Name Parent Profile	Type a unique name tcp-lan-optimized
	Persistence (Profiles-->Persistence)	Name Persistence Type iRule	Type a unique name Universal Select the iRule you created above
	OneConnect (Profiles-->Other)	Name Parent Profile	Type a unique name oneconnect
	Client SSL (Profiles-->SSL)	Name Parent Profile Certificate Key	Type a unique name clientssl Select the Certificate you imported Select the associated Key you imported
	Virtual Server (Main tab-->Local Traffic -->Virtual Servers)	Name	Type a unique name.
	Address	Type the IP Address for the virtual server	
	Service Port	443	
	Protocol Profile (client)¹	Select the WAN optimized TCP profile you created above	
	Protocol Profile (server)¹	Select the LAN optimized TCP profile you created above	
	OneConnect Profile	Select the OneConnect profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	SSL Profile (client)	Select the Client SSL profile you created above	
	SNAT Pool	Automap (optional; see <i>SNAT Pools on page 13</i>)	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Universal Persistence profile you created above	

¹ You must select **Advanced** from the **Configuration** list for these options to appear

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, as described in this deployment guide.

To create the persistence iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this rule. In our example, we type **view-jsessionid**.
4. In the **Definition** box, copy and paste the following iRule, omitting the line numbers.

```

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.

SNAT Pools

If your Connection Servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, enable SNAT Automap to translate the client's source address to an address. The Connection Servers use this new source address as the destination address for client traffic originating through the BIG-IP.

If your View deployment is exceptionally large, specifically more than 64,000 simultaneous connections, a SNAT Pool must be configured, with a SNAT address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

This completes the Connection Server LTM configuration.

Document Revision History

Version	Description
1.0	New Version

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

**F5 Networks,
Corporate Headquarters**
info@f5.com

**F5 Networks
Asia-Pacific**
apacinfo@f5.com

**F5 Networks Ltd.
Europe/Middle-East/Africa**
emeainfo@f5.com

**F5 Networks
Japan K.K.**
f5j-info@f5.com

