DEPLOYMENT GUIDE
Version 1.0

Deploying the BIG-IP LTM System with Oracle Beehive Collaboration Suite

Introducing the F5 and Oracle Beehive deployment guide

Welcome to the F5 and Oracle® Beehive Collaboration suite deployment guide. This guide contains step-by-step procedures for configuring F5 devices for Beehive deployments in a secure, fast and highly available deployment. This document was produced as a joint effort between F5 and Oracle and describes the configuration and operational best practices for using F5 BIG-IP as the application delivery controller with an Oracle Beehive Maximum Availability Architecture (MAA) deployment.

Oracle Beehive provides an integrated set of collaboration services built on a single scalable, secure, enterprise-class collaboration platform. Beehive allows users to access their collaborative information through familiar tools while enabling IT to consolidate infrastructure and implement a centrally managed, secure, and compliant collaboration environment built on Oracle technology.

For more information on Oracle Beehive, see ***http://www.oracle.com/technology/products/beehive/index.html***

For more information on the F5 devices included in this guide, see ***http://www.f5.com/products/***.

Prerequisites and configuration notes

The following are general prerequisites for this deployment.

- While this deployment guide includes some Oracle Beehive configuration procedures, most of the procedures in this document are performed on the BIG-IP Local Traffic Manager (LTM) system. For more information on how to deploy or configure Oracle Beehive, consult the appropriate Oracle documentation.
- This document is written with the assumption that you are familiar with both the F5 devices and Oracle Beehive Collaboration software. For more information on configuring these products, consult the appropriate documentation.
- For Beehive, you should configure the first application node before cloning other application nodes to save configuration steps. When you have finished the configuration in this guide, you can clone the Beehive application node. For more information, consult the Oracle documentation.
- We recommend you create a Beehive generic user for BIG-IP LTM health monitors to use for more granular service level monitoring.
- The BIG-IP LTM system should be running version 9.4.7. We strongly recommend using version 10.0.1 or later.
- The following BIG-IP LTM configuration instructions assume you are connected to the web-based configuration utility using a web browser.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.0.1 (applicable to v9.4.7 and later)
Oracle Beehive	v1.5

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

The architecture presented in Figure 1 is one example of an MAA implementation for Oracle Beehive. The rich set of Oracle high availability features provide the flexibility to implement an MAA architecture that is optimized for your specific business requirements.

The Application Tier is the core of the system and includes all Oracle Beehive server components, including interoperable, function-specific services that provide the system's enterprise collaboration features.

The Application Tier supports multiple Oracle Beehive server instances. Each Oracle Beehive server instance includes the necessary components to host the Oracle Beehive services, including:

- Oracle HTTP Server: The Web server component which enables connections between supported clients over Hypertext Transport Protocol (HTTP) and Secure Hypertext Transport Protocol (HTTPS).
- Oracle Application Server Containers for J2EE (OC4J): J2EE v1.4 -compliant containers that provides an infrastructure for deploying, undeploying, and redeploying J2EE-compliant applications and modules. Oracle Beehive services are deployed in OC4J containers.

This deployment guide focuses on the F5 BIG-IP LTM providing traffic management for the following Beehive Application Tier services/components:

- Calendaring Extensions for WebDAV (CalDAV)
- Extensible Messaging and Presence Protocol (XMPP)
- File Transfer Protocol (FTP)
- Internet Message Access Protocol (IMAP)
- Simple Mail Transfer Protocol (SMTP)
- Web-based Distributed Authoring and Versioning (WebDAV)

- Oracle Beehive Integration for Outlook (OBIO)
- Push Internet Message Access Protocol (P-IMAP)
- Open Mobile Alliance Data Synchronization (OMA-DS)

The following is an architectural overview of the F5 and Beehive deployment, based on the Oracle Maximum Available Architecture.

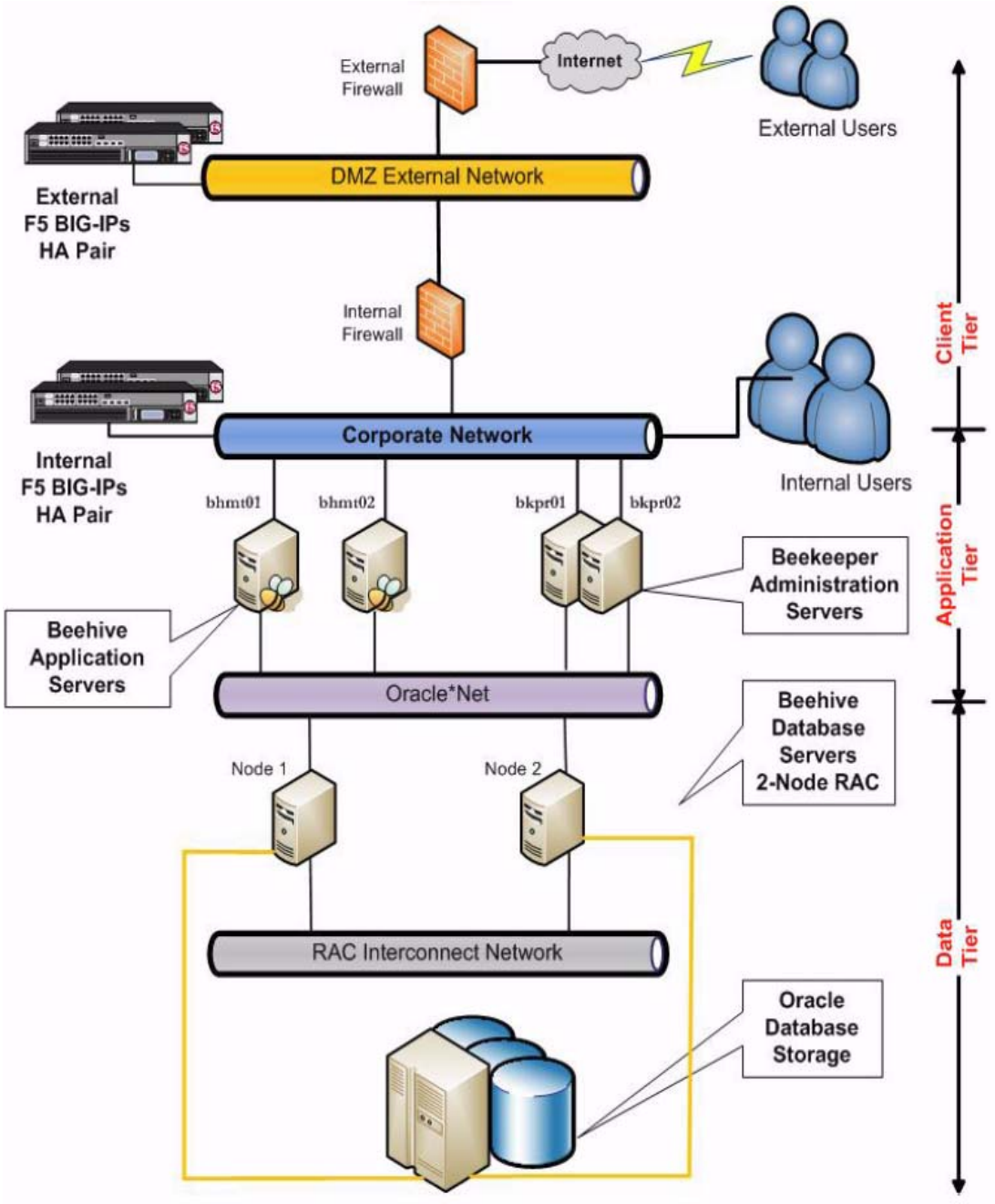

Figure 1 *BIG-IP LTM and Oracle Beehive logical configuration example*

Deploying the BIG-IP LTM with Oracle Beehive

This deployment guide is divided into the following sections:

- *Configuring the BIG-IP LTM*, on page 4
- *Configuring Oracle Beehive for the BIG-IP LTM*, on page 14
- *Configuring the BIG-IP LTM to offload SSL (optional)*, on page 18

We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. For information on backing up or restoring a BIG-IP LTM configuration, refer to the appropriate BIG-IP LTM manual, available on *Ask F5*.

Configuring the BIG-IP LTM

In this section we configure the BIG-IP LTM for multiple Oracle Beehive services. Because the LTM configuration for each Beehive service is nearly identical, rather than repeat the set of instructions for each service, we provide a detailed example for one set of BIG-IP LTM configuration objects (health monitor, load balancing pool, profile, and virtual server).

Table 1, on page 5 contains a list of Beehive services, and the associated information (such as monitor type and ports) to use when configuring the BIG-IP LTM. Review each table, and for the services and protocols applicable to your configuration, repeat the procedures in *Configuring the BIG-IP LTM for the Beehive services*, using the information from the table as appropriate.

How to use the following table

For each of the line items in the following tables, you must create a health monitor, pool, profile(s), and virtual server on the BIG-IP LTM. You may want to print the table for reference.

- **Beehive Service**
  This describes the Beehive service.
- **Monitor Type**
  This is the type of health monitor. When configuring the BIG-IP LTM monitor, you select this monitor from the **Type** list.
- **TCP Port**
  This is the TCP port used by the service. You use this port when configuring the BIG-IP LTM pool in the **Service Port** field.
- **Virtual Server Port**
  This is the Service Port you enter when configuring the BIG-IP LTM virtual server in the **Service Port** field.
- **F5 Profiles**
  This column contains the TCP profiles you must create while configuring the BIG-IP LTM system. All objects have a TCP profile. Some of the objects have additional profiles.

Beehive Service	Monitor type	TCP Port	Virtual Server Port	Profiles
Beehive HTTP	HTTP	7777	80	TCP
IMAP	IMAP	5143	143	TCP
SMTP	SMTP	2225	25	TCP
Beehive Transport Protocol (BTP)	TCP	21401	21401	TCP
Beehive Transport Protocol Secure (BTPS)	TCP	5224	5224	TCP
XMPP Presence	TCP	5122	5222	TCP
XMPPS Presence	TCP	5123	5223	TCP
FTP	FTP	2121	2121	TCP
Beekeeper HTTP	HTTP	7779	80	TCP, persistence

Table 1 *Table of Beehive services and associated BIG-IP configuration objects*

Important

If you are using the BIG-IP LTM system to offload SSL for services such as ***Beehive HTTPS****,* ***IMAPS****,* ***SMTPS****,* ***FTPS****, and* ***Beekeeper HTTPS****, there are additional BIG-IP LTM configuration objects you must configure. After completing the following non-SSL objects, see* ***Configuring the BIG-IP LTM to offload SSL (optional)****, on page 18.* *We have documented both secure and unsecure connections for completeness. As a best practice, we recommend using only secure connections.*

Configuring the BIG-IP LTM for the Beehive services

Use the following procedures as a template for configuring the Beehive services applicable to your configuration, as described in Table 1.

Creating the health monitors

The first step is to configure the health monitor. This procedure uses entries from the **Monitor Type** and **CP Port** columns in the table above.

Note

There are three services that have additional fields specific to the health monitor type (IMAP, SMTP, and FTP). They are clearly marked in the following procedure.

To configure a 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 unique name for this monitor. We recommend prefacing the monitor name with *mon_* and then including the Beehive Service and TCP port number from Table 1. For example, **mon_http7777**.
4. From the **Type** list, select the monitor type found in the **Monitor Type** column in Table 1. For example, if the column contains **HTTP**, select **HTTP** from the list.
5. From the **Configuration** list, select **Advanced**.
6. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a Interval of **30** and a Timeout of **91**.
7. For the **IMAP** monitor only:
   a) In the **User Name** box, type the name of a dedicated monitor account. In our example, we type **F5monitor**.
   b) In the **Password** box, type the password associated with the user name in step a (see Figure 12, on page 25).
8. For the **SMTP** monitor only:
   a) In the **Domain** box, type the name of your SMTP domain. In our example, we type **siterequest.com** (see Figure 13, on page 26).
9. For the **FTP** monitor only:
   a) In the **User Name** box, type the name of a dedicated monitor account. In our example, we type **F5monitor**.
   b) In the **Password** box, type the password associated with the user name in step a.
   c) In the **Path/Filename** box, type the full path and filename of the file the system attempts to download. In our example, we type
   `/Oracle/F5monitorsPersonalWorkspace/Documents/monitor.txt`
   See Figure 14, on page 27.
10. In the **Alias Service Port** box, type the appropriate port found in the **TCP Port** column. For example, if the column contains **7777**, type **7777** in the **Alias Service Port** box (see Figure 2 for this example).
11. All other configuration settings are optional, configure as applicable for your deployment.
12. Click the **Finished** button.

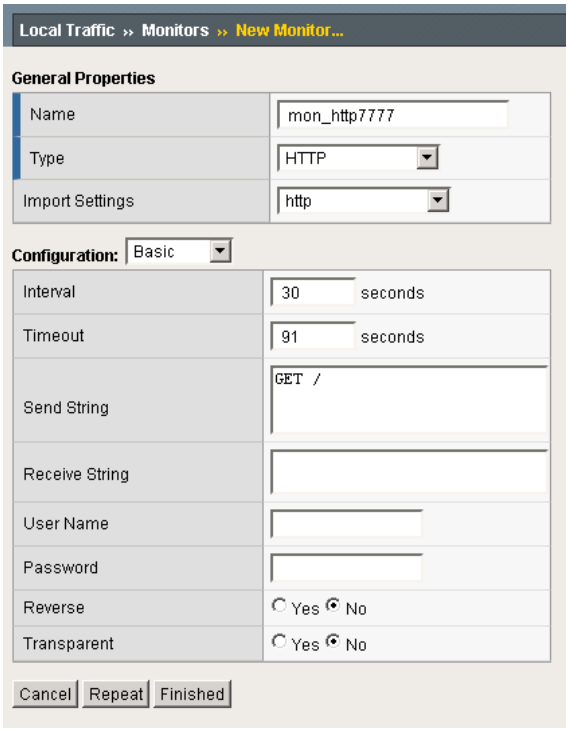

Figure 2 *Creating the health monitor*

Creating the Beehive pools

The next step is to create the pools on the BIG-IP LTM system. This procedure uses entries from the **TCP Port** column in the table above.

To create the pools

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, type a unique name for this Pool.
We recommend prefacing the pool name with *pool_* and then including the Beehive Service and TCP port number from Table 1. For example, **pool_http7777**.
4. In the Health Monitors section, from the **Available** list, select the name of the monitor you created in *Creating the health monitors*, on page 5, and click the Add (**<<**) button. Be sure to use the monitor that is associated with the same service or protocol as this pool. For example, if you are configuring the pool **pool_http7777**, you would select **mon_http7777**.

5. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). We recommend selecting **Least Connections (member)** for all pools in this configuration.
6. In the New Members section, you add the Beehive servers to the pool.
   a) In the **Address** box, type the IP address of the Beehive Server.
   b) In the **Service Port** box, type the service number from the **TCP Port** column in the table above. For example, if you are configuring the Beehive HTTP pool, use port **7777**.
   c) Click the **Add** button to add the member to the list.
   d) Repeat steps a-c for each server you want to add to the pool.
7. Click the **Finished** button.

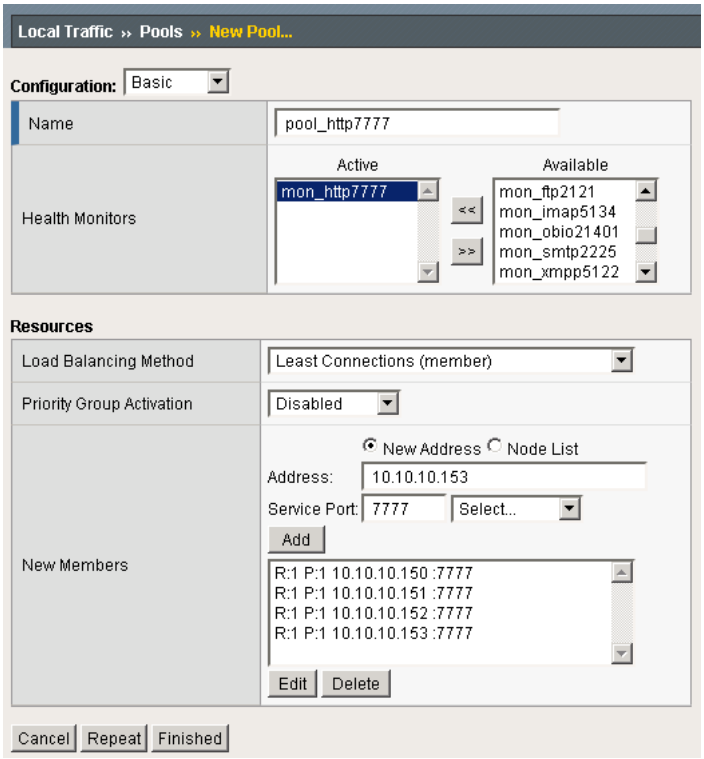

Figure 3 *Configuring the BIG-IP pool*

Creating the TCP profiles

The next step is to create a TCP profile. A profile is an F5 object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as TCP or HTTP connections. Using

profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient. It also allows for different characteristics to be matched to specific client or applications.

◆ Note

*The TCP profile uses an **Idle Timeout** setting of 30 minutes (1800 seconds) for the TCP timeout settings. The Idle Timeout setting determines how long the BIG-IP holds open a TCP connection to a Beehive service after there is no activity on the connection. This is a general recommendation that you may need to change to match your network environment.*

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, select **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 unique name for this profile. We recommend prefacing the profile name with *tcp_* and then including the Beehive Service and TCP port number from Table 1. For example, **tcp_http7777**.
5. In the **Idle Timeout** row, check the **Custom** box. Leave the list set to **Specify**, and in the box, type **1800**.
6. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.
7. Click the **Finished** button (see Figure 4).

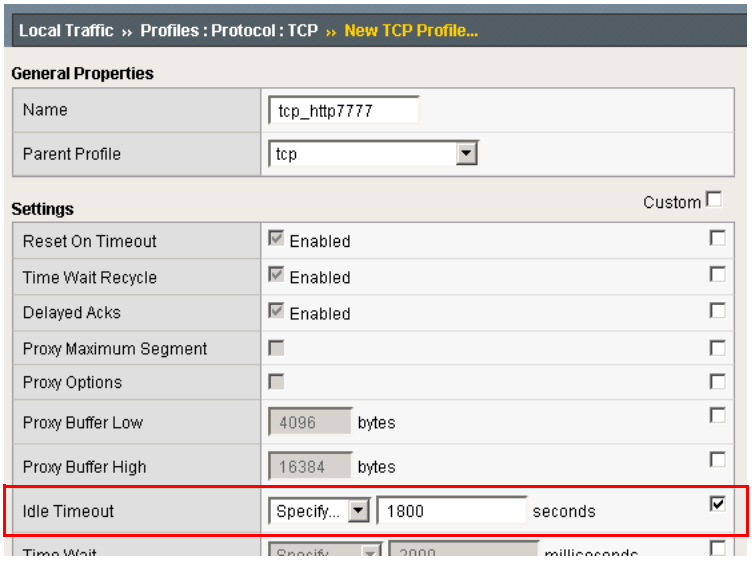

***Figure 4** Configuring the TCP profile (truncated)*

Tip

*If majority of your clients are connecting over a wide area network (WAN), consider selecting **tcp-wan-optimized** from the **Parent Profile** list.*

Creating the persistence profile for the Beekeeper service

There is one additional profile needed for the Beekeeper server; a persistence profile. For this profile, we use cookie persistence. In the following example, we use the default settings, but you can modify settings, such as the cookie expiration, if applicable.

Important

*This profile is **only** necessary for the Beekeeper service. You do not need to create a persistence profile for any of the other Beehive services.*

To create the persistence profile for Beekeeper

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Persistence**.
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 **cookie-beekeeper**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
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.

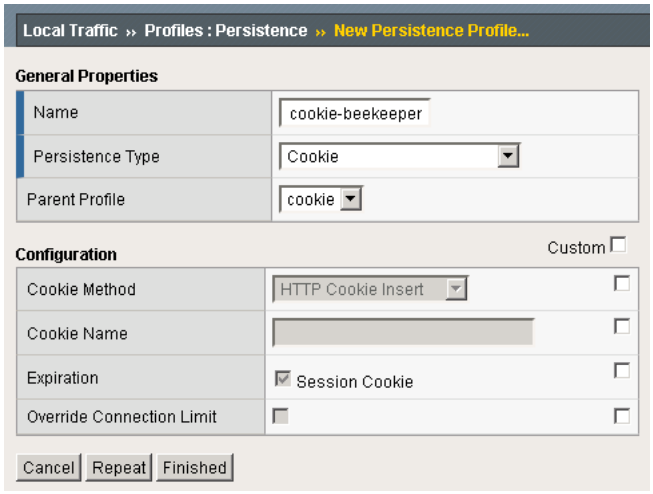

***Figure 5** Configuring the Beekeeper cookie persistence profile*

Creating the virtual servers

The final step in this section is to define a virtual server that references the profile and pool you created. A virtual server with its virtual address and port number, is the client addressable host name or IP address through which members of a load balancing pool are made available to a client. This procedure uses entries from the **VIP TCP Port** column in the tables above.

To create the virtual servers

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a unique name for this virtual server. We recommend prefacing the profile name with *vs_* and then including the Beehive Service and TCP port number from Table 1. For example, **vs_http7777**.
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 **10.10.10.101**.
6. In the **Service Port** box, type the service number from the **VIP TCP Port** column in the table above. For example, if you are configuring the Beehive HTTP virtual server, use port **80**.
   Note: This port does not always match the port used for the pool.
7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the profile you created for this service in *Creating the TCP profiles*, on page 8.

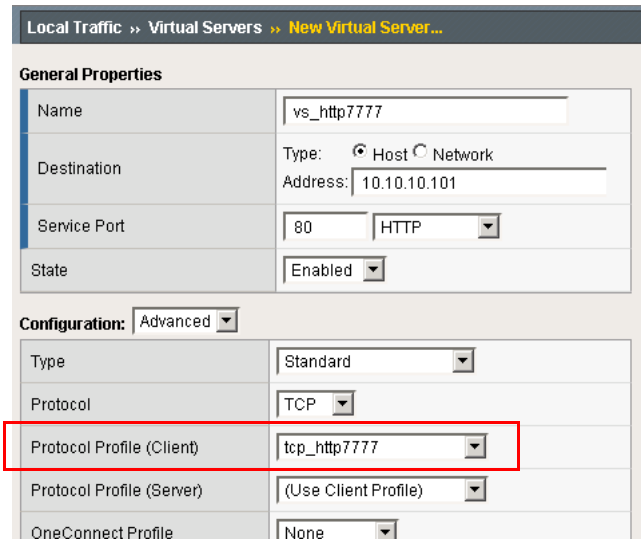

Figure 6 *Configuring the virtual server (truncated)*

9. For **Beehive HTTP** and **Beekeeper HTTP** services only:
   From the **HTTP Profile** list, select **http**.
   Note: If the clients are attaching to the Beehive HTTPS services over a WAN (wide-area network), select the **http-wan-optimized-compression** profile from the list.
10. From the **SNAT Pool** list, select **Auto Map**.
11. In the Resources section, from the **Default Pool** list, select the pool you made for this service in *Creating the Beehive pools*, on page 7.
12. If you are configuring the Beekeeper virtual server, from the **Default Persistence Profile** list, select **cookie-beekeeper**. This is only necessary for the Beekeeper virtual server(s).
13. Configure any other settings as appropriate for your configuration.
14. Click the **Finished** button.

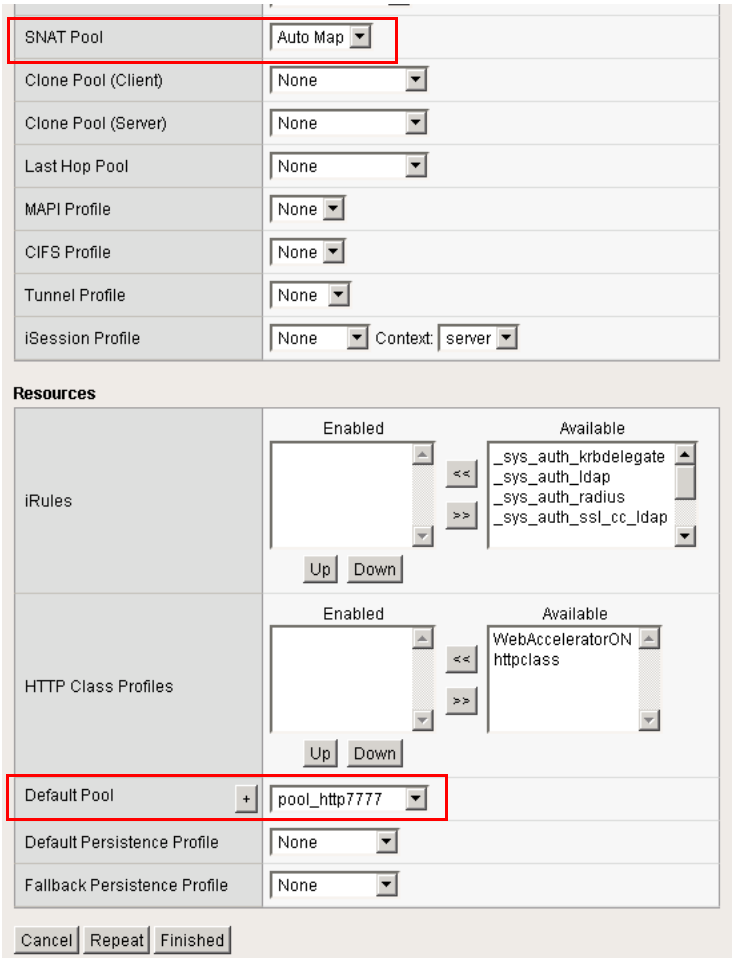

Figure 7 *Configuring the virtual server SNAT pool and default pool.*

Return to *Creating the health monitors*, on page 5 and using Table 1, on page 5, repeat all of the procedures for each of the Beehive services applicable to your configuration. If you configured all Beehive Services, when you are finished with all of the BIG-IP LTM configuration objects, you should have 9 health monitors, 9 pools, 9 tcp profiles, 1 persistence profile, and 7 virtual servers. Note there are more virtual servers if you are offloading SSL (see *Configuring the BIG-IP LTM to offload SSL (optional)*, on page 18).

Synchronizing the BIG-IP configuration if using a redundant system

When you have completed the configuration of your virtual servers and related objects, and if you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

The method of synchronizing the BIG-IP configuration depends on your version, see the appropriate BIG-IP LTM manual, available on Ask F5 (*https://support.f5.com/kb/en-us/products/big-ip_ltm.html*).

Continue with the following section, *Configuring Oracle Beehive for the BIG-IP LTM*, on page 14

Configuring Oracle Beehive for the BIG-IP LTM

Follow the steps in this section to configure Beehive to work with the F5 BIG-IP LTM. Perform the tasks in this section before you clone any other application nodes so that you do not have to duplicate these steps on the other application nodes. At the end of these steps, be sure to activate the changes and commit them to the local configuration.

All of the commands in the following procedures are performed from the Beehive system as an administrator. The procedures are provided for your convenience. For further information, see the Oracle documentation.

Configuring Set Ports

If you do not want to use privileged ports directly, set ports as follows:

```
list_properties --component _VIRTUAL_SERVER
beectl modify_property --component _EmailService:SMTPProperties --name Port --value 2225
beectl modify_property --component _VIRTUAL_SERVER --name SmtpPort --value 2225
beectl modify_property --component _EmailService:IMAPProperties --name Port --value 5143
beectl modify_property --component _VIRTUAL_SERVER --name ImapPort --value 5143
```

The commands above are set to the Oracle HTTP Server (OHS) virtual port. To see what the HTTP listening port is set to, see *Setting the HTTP Listening Port* , on page 14.

```
beectl modify_property --component _VIRTUAL_SERVER --name HttpPort --value 80
list_properties --component _VIRTUAL_SERVER
```

You see a list of property names and property values. In this case, you will notice that the changes you made above have been changed, but not yet activated (as noted by an asterisk). The example below shows changed values only:

Property Name	Property Value
*ImapPort	5143
*SmtpPort	2225
*HttpPort	80

Table 2 *Changed properties in the virtual server list*

Setting the HTTP Listening Port

Setting the HTTP listening port is necessary only if the current listening port is not what you want.

To set the HTTP Listening Port

1. Get the Beehive instance name using the following command:

   beectl list_components --type BeehiveInstance

   You see a list like the following:

Component Type	Component Identifier
BeehiveInstance	beehive_instance_maaXtst.dscbac07.us.oracle.com

Table 3 *Beehive Instance name*

2. Get the OHS component name using the following command:

beectl list_properties --component beehive_instance_maaXtst.dscbac07.us.oracle.com --name HttpServer

You see a list like the following:

Property Name	Property Value
HttpServer	ohs_maaXtst.dscbac07.us.oracle.com

Table 4 *OHS component name*

3. Get the current HTTP listener port using the following command:

beectl list_properties --component ohs_maaXtst.dscbac07.us.oracle.com --name HttpListenPort

You see a list like the following:

Property Name	Property Value
HttpListen Port	7779

Table 5 *HTTP listener port*

4. Change the listening port using the following command:

beectl modify_property --component ohs_maaXtst.dscbac07.us.oracle.com --name HttpListenPort --value 7777

5. Activate the configuration using the following command:

   beectl activate_configuration

6. Modify the local configuration files using the following command:

   beectl modify_local_configuration_files

Setting the Beehive Virtual Server

The next step is to set the Beehive virtual server.

To set the Beehive virtual server

1. Set the Beehive virtual server using the following command:

```
beectl modify_property --component _VIRTUAL_SERVER --name ServerName --value beehive.example.com
beectl list_properties --component _VIRTUAL_SERVER
```

You see a list of property names and property values. In this case, you will notice that the change you made above has been changed, but not yet activated (as noted by an asterisk). The example below shows changed value only:

Property Name	Property Value
*ServerName	beehive.example.com

Table 6 *Setting the virtual server*

2. Type the following command:

```
beectl activate_configuration
```

You should see the following message

```
Now attempting to get writable configuration with maximum
wait time 30 seconds.
Got writable configuration successfully.
Now attempting to activate writable configuration and
releasing the lock. Updated new configuration repository
successfully. Local configuration files are not in sync
with system model. Please run
"modify_local_configuration_files" manually.
Proposed configuration is saved successfully and
activated now.
```

3. Type the following command:

```
beectl modify_local_configuration_files
```

You should see the following message:

```
Note: All validators registered for
"modify_local_configuration_files" command will be
executed now.

Note : The validation results will be accumulated and
analyzed at the end.

Executing "HostName" validator ...

Successfully executed all validators registered for
"modify_local_configuration_files" command.

Now analyzing the validation results ... … Successfully
ran the command in oracle home
/u01/app/oracle/product/1.5.0.0.0/beehive_1. Please run
this command on all midtier instances.
```

Setting the Beekeeper Virtual Server

To configure multiple instances of Oracle Beekeeper with a virtual host through the BIG-IP LTM so that all your Oracle Beekeeper instances will be accessed by a single point of access, configure the virtual host on the Beehive Beekeeper application nodes using the following procedure:

To set the Beekeeper virtual server

1. Edit the file **<*Oracle_Beekeeper_home*>/j2ee/home/config/default-web-site.xml** and specify the virtual host name and port number in the ***<frontend>*** child element of ***<web-site>*** using the following syntax:

```
<web-site xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=
"http://xmlns.oracle.com/oracleas/schema/11/web-site-11_1.xsd"
port="7778"
secure="false"
protocol="http"
display-name="Default Web Site"
schema-major-version="11"
schema-minor-version="1">
...
<frontend host="beekeeper.example.com" port="80" />
...
</web-site>
```

   In this example, **beekeeper.example.com** is the host name of the BIG-IP LTM virtual host and 80 is the port number.

2. Restart beekeeper using the following commands:

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall
```

This completes the Oracle Beehive configuration changes, unless you are offloading SSL to the BIG-IP LTM. If you are offloading SSL, there is one additional procedure found in *Configuring the BIG-IP LTM to offload SSL (optional)*, on page 18.

Configuring the BIG-IP LTM to offload SSL (optional)

This section describes how to configure the BIG-IP LTM system as an SSL proxy for Beehive Services deployment. It also includes one modification to the Oracle Beehive device to allow SSL offload by the BIG-IP LTM. If you are not using the BIG-IP LTM system to offload SSL traffic, you do not need to perform the procedures in this section.

Prerequisites and Configuration Notes

This section lists additional prerequisites for SSL offload:

- You need an SSL certificate for your site that is compatible with the BIG-IP LTM system. For more information, visit the F5 BIG-IP Product Documentation, available on the F5 Technical Support site, *Ask F5*.
- For Oracle Beehive, you need two unique SSL certificates:
  - One SSL certificate is used to secure client connections for all the SSL enabled services.
  - One SSL certificate is used exclusively for the Beekeeper Administration Secure Console.
- The SSL virtual servers use the same configuration objects you created in the procedures above, so there is no need to re-create these.

Important

When using the BIG-IP LTM for SSL offload, for each Beehive Service deployed behind LTM, configure that service to use the new HTTPS protocol header. For SSL offload, you must have URLs defined as ***https://<FQDN>****, where FQDN is the name associated in DNS with the appropriate Virtual Server, and assigned to the SSL certificate in the Client SSL profile.*

Beehive Service	Use Pool created for:	Profiles	Redirect iRule?	Virtual Server Port
Beehive HTTPS	Beehive HTTP	TCP, main Client SSL	Yes	443
IMAPS	IMAP	TCP, main Client SSL	No	993
SMTPS	SMTP	TCP, main Client SSL	No	465
FTPS	FTP	TCP, main Client SSL	No	990
Beekeeper HTTPS	Beekeeper HTTP	TCP, persistence, Beekeeper Client SSL	Yes	443

Table 7 *Table of Beehive services and associated BIG-IP configuration objects*

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 secure 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.

You need to complete this procedure twice, once for the Beekeeper Administration Secure Console and again for the other Beehive services.

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**.
8. If you imported the certificate, repeat this procedure for the key.
9. Repeat the entire procedure so you have one certificate and key for the Beekeeper console and one for the other Beehive services.

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. Again, you need to complete this procedure twice, once for the Beekeeper Administration Secure Console and again to create a Client SSL profile for the other Beehive services.

To create a new Client SSL 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 **SSL** menu, select **Client**.
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 **beehive_clientssl**.
5. In the Configuration section, check the **Certificate** and **Key Custom** boxes.
6. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section for the Beehive services.
7. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
8. Click the **Finished** button.
9. Repeat the entire procedure for the Beekeeper console Client SSL profile. In our example, we name this profile **beekeeper_clientssl** and select the appropriate certificate and key in steps 6 and 7.

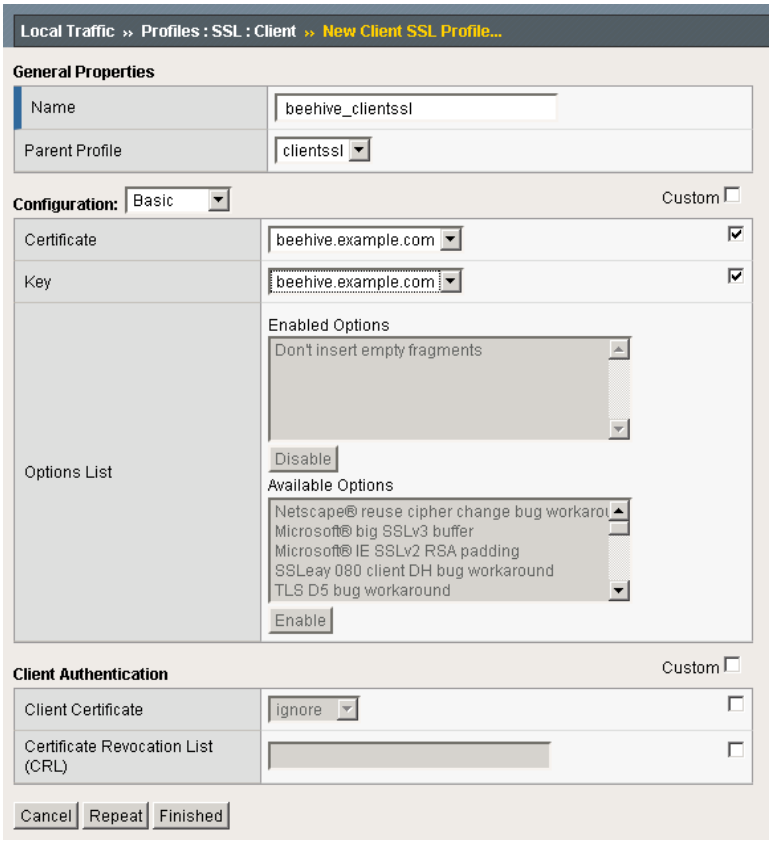

Figure 8 *Creating the Client SSL profile*

Creating the Beehive Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects the requests to the correct HTTPS (secure) virtual server, without user interaction. This Redirect iRule is used with both the Beehive HTTP service and the Beekeeper HTTP service, to redirect clients to the matching SSL Secured Beehive Service.

To create the Redirect iRule

1. On the Main tab, expand **Local Traffic** and click **iRules**.
2. In the upper right portion of the iRule screen, click **Create**.
3. In the Name field on the New iRule screen, enter a name for your iRule. In our example, we use **Beehive_httptohttps**.
4. 4. In the **Definition** section, copy and paste the following iRule:

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

5. Click **Finished**.

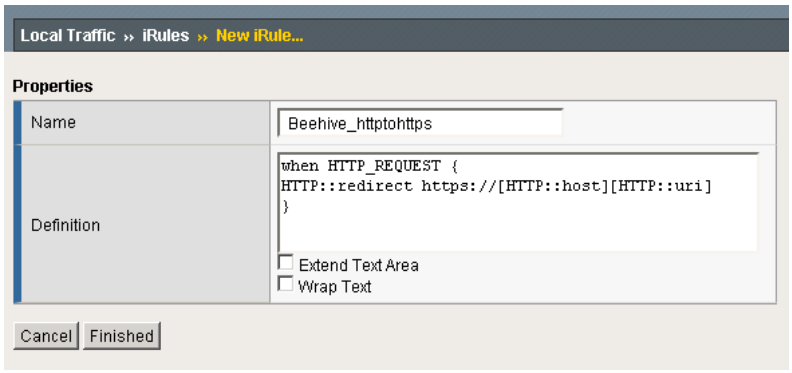

Figure 9 *Creating the redirect iRule*

Creating the SSL virtual servers

We now create a new SSL virtual server for each of the Beehive services the BIG-IP LTM is offloading SSL. This virtual server references pools and profiles you created in the non-SSL section. If you have not yet configured those objects, you must do that first. This procedure uses entries from Table 7, on page 18.

To create the virtual servers

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.

3. In the **Name** box, type a unique name for this virtual server. We recommend prefacing the profile name with *vs_* and then including the Beehive Service and TCP port number from the VIP TCP port column of Table 7, on page 18. For example, **vs_https443**.
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 **10.10.10.101**.
6. In the **Service Port** box, type the service number from the **VIP TCP Port** column in the table above. For example, if you are configuring the Beehive HTTPS virtual server, use port **443**.
   Note: This port does not always match the port used for the pool.
7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the profile you created for this service in *Creating the TCP profiles*, on page 8. In our Beehive HTTPS example, we select **tcp_http7777**.
9. For the Beehive HTTPS and Beekeeper HTTPS virtual servers only, From the HTTP Profile list, select **http**.
   Note: If the clients are attaching to the Beehive HTTPS services over a WAN (wide-area network), select the **http-wan-optimized-compression** profile from the list.

Only for the Beehive HTTPS and Beekeeper HTTPS virtual servers

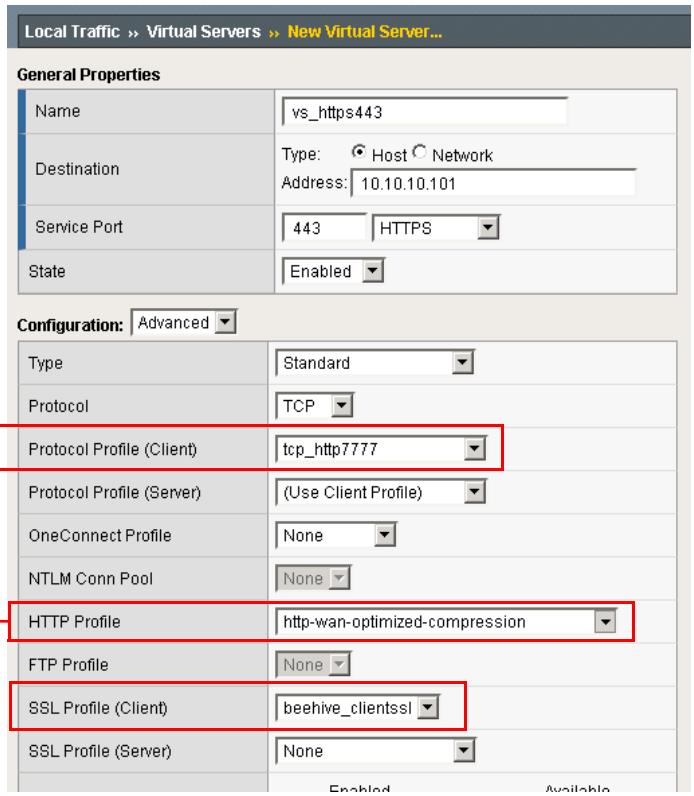

Figure 10 *Configuring the SSL virtual server (truncated)*

10. From the **SNAT Pool** list, select **Auto Map**.
11. For the Beehive HTTPS and Beekeeper HTTPS virtual servers only: In the **iRules** section, from the Available list, select the name of the iRule you created in *Creating the Beehive Redirect iRule*, on page 21, and click the Add (<<) button. In our example, we select **Beehive_httptohttps**.
12. In the Resources section, from the **Default Pool** list, select the pool you made for the non SSL service in *Creating the Beehive pools*, on page 7.
13. If you are configuring the Beekeeper virtual server, from the **Default Persistence Profile** list, select **cookie-beekeeper**. This is only necessary for the Beekeeper virtual server(s).
14. Configure any other settings as appropriate for your configuration.
15. Click the **Finished** button.

Only for the Beehive HTTPS and Beekeeper HTTPS virtual servers

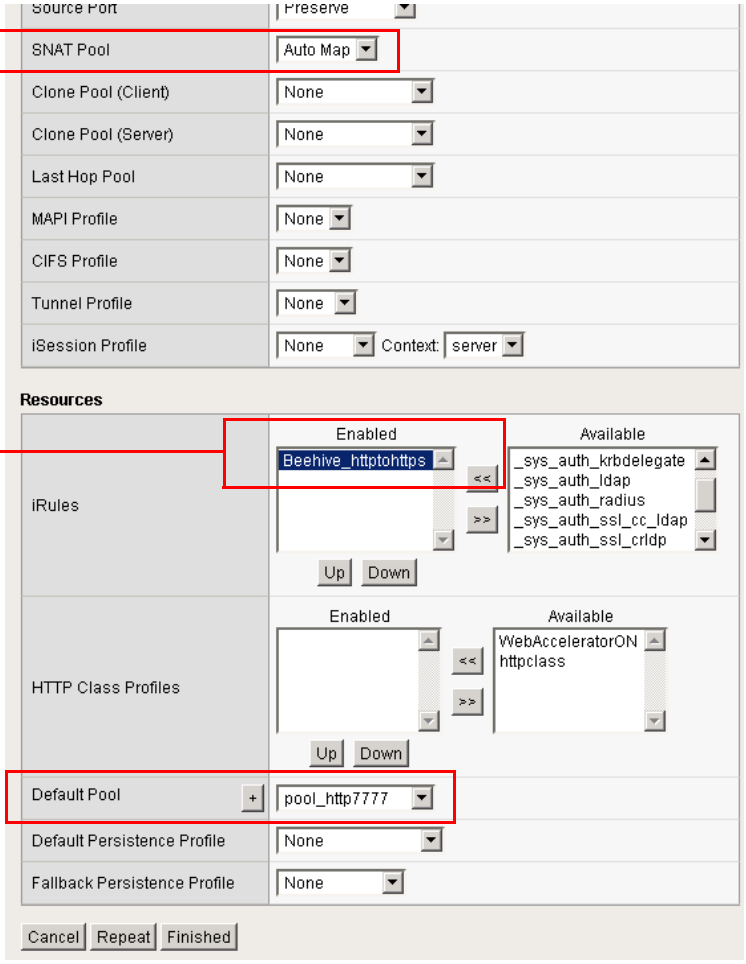

Figure 11 *Configuring the SSL virtual server, continued (truncated)*

Configuring Beehive for SSL Termination

Use the following procedure to configure Beehive for SSL termination.

To configure Beehive for SSL termination

1. Log onto the Beehive system as an administrator.
2. Set the **SslTerminatedByLoadBalancer** property of the **HttpServerCluster** component to **true**.
   For example:

```
beectl modify_property --component _current_site:HttpServerCluster --name\
    SslTerminatedByLoadBalancer --value true
```

3. Review the change using the following command:

```
beectl list_properties --component _CURRENT_SITE:HttpServerCluster
```

   You see a list similar to the following:

Property Name	Property Value
Alias	
HttpServerSslEnabled Port	**true**

Table 8 *HTTPServer cluster setting*

4. Commit the changes you made to the configuration:

```
beectl activate_configuration
beectl modify_local_configuration_files
```

This completes the SSL configuration.

Appendix B: Additional screenshots

The following are additional screenshots of some of the BIG-IP configuration objects.

IMAP Health Monitor

The IMAP monitor contains three additional configuration fields: User Name, Password, and Folder.

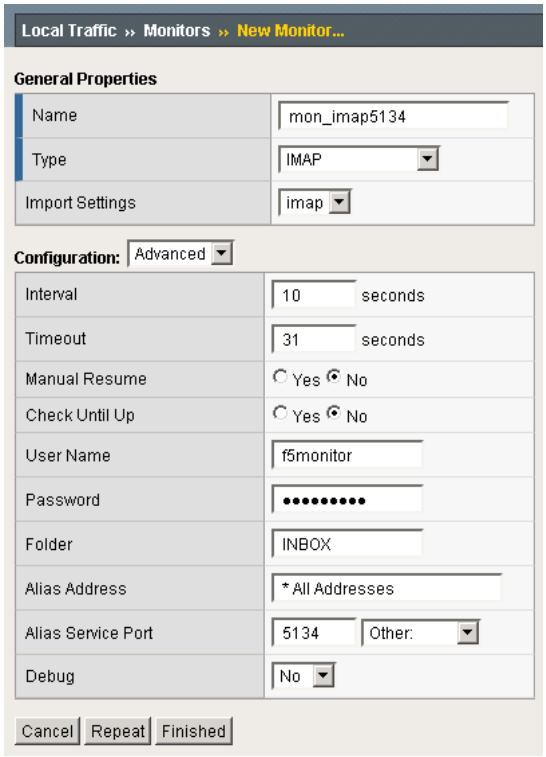

Figure 12 *Configuring the IMAP health monitor*

SMTP Monitor

The SMTP monitor contains one additional configuration field: Domain.

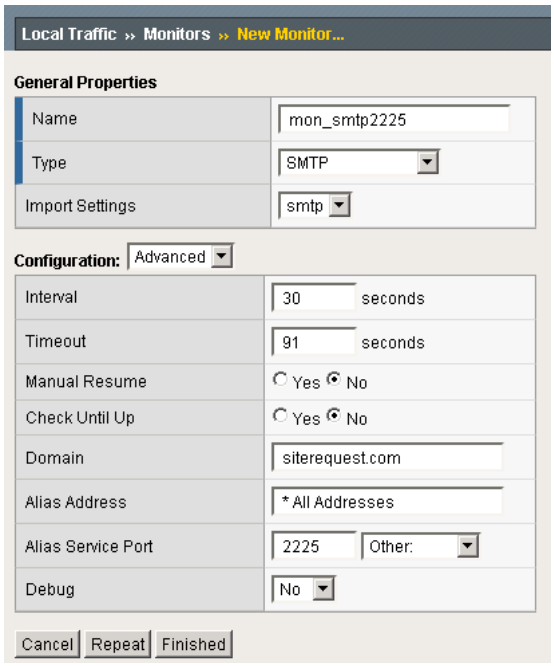

Figure 13 *Configuring the SMTP monitor*

FTP monitor

The FTP monitor contains three additional configuration fields: User Name, Password, and Path/Filename.

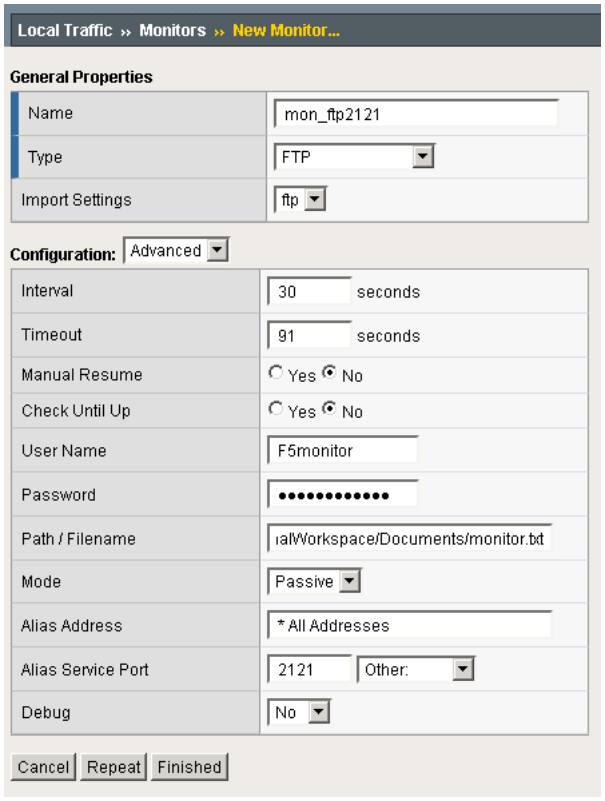

Figure 14 *Configuring the FTP monitor*