

Configuring Maximum Availability
Architecture for Beehive with F5
BIG-IP Global and Local Traffic
Manager: Beehive High
Availability

*Oracle Maximum Availability Architecture White Paper
March 2010*

Maximum Availability Architecture

Oracle Best Practices For High Availability

Executive Summary.....	4
Beehive Architecture Overview.....	4
Client Tier.....	6
Application Tier.....	7
Data Tier	8
Ancillary Tier.....	8
Best Practices	9
F5.....	9
Beehive	10
F5 Configuration Guide for Beehive.....	10
Using the Configuration Table	11
Document Naming Conventions	12
Configuring SSL	13
Configuring IMAP Email (Port 5143).....	13
Configuring SMTP Email (Port 2225).....	23
Configuring Oracle Beehive Transport Protocol (Port 21401)	30
Configuring Oracle Secure BTPS (Port 5224).....	32
Configuring XMPP Beehive Presence (Port 5222).....	35
Configuring FTP Service (Port 2121).....	39
Configuring Beehive HTTP and HTTPS (Port 7777)	44
Configuring Beekeeper (Port 7779)	51
F5 Monitor Configuration Summary	58
F5 TCP Profile Configuration Summary.....	58

F5 Persistence Profile Configuration Summary	59
F5 Pool Configuration Summary	60
F5 Virtual Server Configuration Summary.....	61
Configure Beehive to Work with the F5 BIG-IP LTM	62
Set the Virtual Server and Ports	62
Set the HTTP Listening Port	63
Set Beehive HTTP Server for SSL Termination	64
Setup TLS	65
Setup XMPP.....	66
Set the Beekeeper Virtual Server	67
Appendix A: Terminology for F5 BIG-IP Local Traffic Manager.....	69
Pool.....	69
Member	69
Virtual Server.....	69
Profile	70
Rule.....	70
Monitor	70
Persistence.....	71
Appendix B: Configuring BIG-IP for Beehive to Use SSL Offload	72
Prerequisites and Configuration Notes	72
Using SSL Certificates and Keys	72
Importing Certificates and Keys	73
Creating the Beehive Client SSL Profile	73

Creating the Beekeeper Client SSL Profile	75
Creating the Beehive Redirect iRule	76
Configuring Beehive for SSL Termination	77
Appendix C: F5 BIG-IP Example Configuration File	78
Appendix D: Beehive Host: Port and URL Summary	85
References	86
Oracle	86
F5 References	86

Executive Summary

Oracle Maximum Availability Architecture (MAA) [2] is the Oracle best practices blueprint for implementing Oracle high-availability technologies. The goal of this MAA white paper is to provide best practices for using Oracle Beehive 1.5 in an MAA deployment that includes: Oracle Database Real Application Clusters (Oracle RAC), multiple Oracle Beehive Application tier nodes and the F5 Networks BIG-IP Local Traffic Managers. This paper will focus on configuring a primary site and does not discuss the creation or the use of standby deployments and the F5 BIG-IP Global Traffic Manager (GTM). Future MAA white papers will provide detailed discussions about using Oracle Beehive and F5 BIG-IP in a full MAA deployment. The information in this white paper is based on BIG-IP Version 10.0.1, Build 283 software.

The primary Oracle Beehive high availability architecture solutions are:

- Deploying Oracle Beehive on Multiple Computers
- Deploying Oracle Beehive Across Network Zones

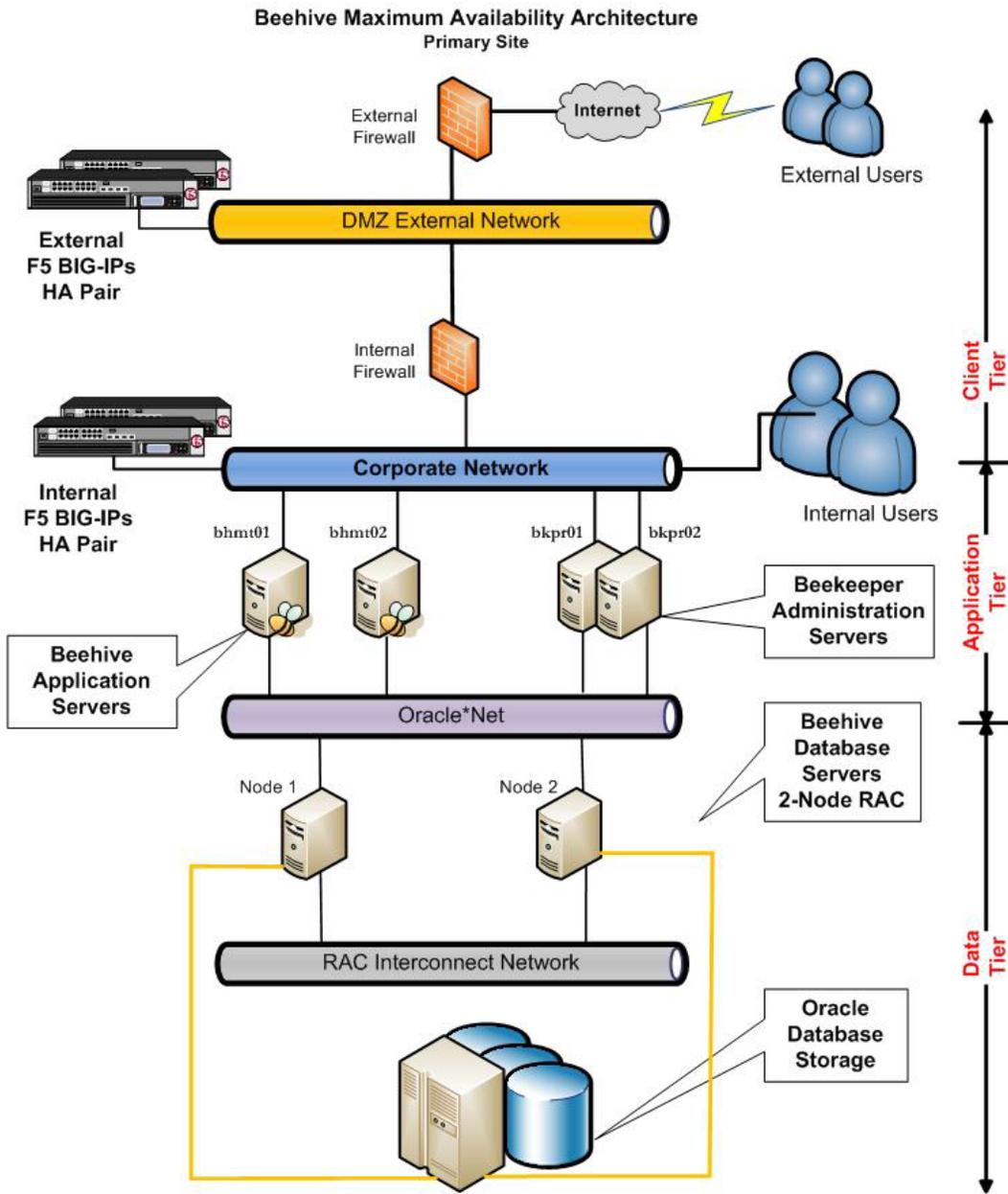
This paper has been jointly written by Oracle Corporation and F5 Networks and describes the configuration and operational best practices for using F5 BIG-IP as the application delivery controller with an Oracle Beehive MAA deployment. By using the technologies from Oracle and F5 together, you can deploy Beehive to meet your high availability service levels. MAA deployments eliminate guesswork and uncertainty when implementing a high availability architecture utilizing the full complement of Oracle High Availability (HA) technologies. The MAA best practices are described in a series of technical white papers and documentation to assist in designing, implementing, and managing optimum high availability architectures. The MAA series of papers are available at <http://www.oracle.com/technology/ deploy/availability/htdocs/maa.htm>.

Note: This document assumes that you are familiar with F5 Networks BIG-IP. See [Appendix A](#) for a quick terminology reference. For detailed information, see the [BIG-IP Solutions Guide](#) and [BIG-IP Configuration Guide](#).

Beehive Architecture Overview

As illustrated in [Figure 1](#), the architecture of an MAA Beehive deployment provides superior data protection and availability by minimizing or eliminating planned and unplanned downtime at all technology stack layers, including hardware and software components.

Figure 1: Beehive Architecture Diagram



The hardware application delivery controller is an integral component for providing High Availability. F5's BIG-IP provides the necessary application delivery controller features for Oracle Beehive high availability load balancing and monitoring.

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

Client Tier

The Client Tier is the face of the system and includes all supported clients and devices, including end-user clients, such as Oracle Beehive Workspaces Client, and system administration clients, such as Oracle Beekeeper and `beectl`. Oracle Beehive provides a common model that enables a wide variety of clients and devices to connect with the platform. Once connected to the platform, supported clients and devices can access and leverage the collaborative services and data that it provides. Oracle Beehive also supports several standardized protocols, enabling organizations to integrate and deploy standards-based clients, as well as mobile devices, easily with the platform. Oracle Beehive supports clients and devices that leverage the following standardized protocols:

- 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)
- Push Internet Message Access Protocol (P-IMAP)
- Open Mobile Alliance Data Synchronization (OMA-DS)
- Open Mobile Alliance Device Management (OMA-DM)

Oracle Beehive also provides several out-of-the-box client options for enterprise users.

Organizations can also integrate and deploy custom clients or incorporate Oracle Beehive clients into existing interfaces such as portals. The following is a list of some of the end-user clients and devices that Oracle Beehive supports:

- Oracle Beehive Extensions for Outlook (OBEO)
- Oracle Beehive Extensions for Explorer (OBEE)
- Oracle Beehive Zimbra
- Oracle Beehive Central
- Oracle Beehive Conferencing
- Oracle Beehive Workspaces Client

- Mobile Devices Supported by Oracle Beehive
- Standards-based and Open Source Clients Supported by Oracle Beehive
- Telephony Clients Supported by Oracle Beehive

For a complete overview of the Beehive end-user clients see Chapter 7 “Oracle Beehive End-User Clients” in the [Oracle Beehive Concepts](#) guide.

Application Tier

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 compliant containers that provide an infrastructure for deploying, undeploying, and redeploying J2EE-compliant applications and modules. Oracle Beehive services are deployed in OC4J containers.

This paper focuses on the Beehive Application Tier with the F5 BIG-IP LTM providing traffic management for the aforementioned Beehive end-user clients and standardized protocols to connect to the Beehive services/components.

Each Oracle Beehive server instance also includes the Beehive Transport Infrastructure (BTI), which enables connectivity between supported clients and Oracle Beehive through its proprietary multiplexor protocol (MX). BTI also has a secure transport option.

Oracle Beehive Extensions for Outlook (OBEO) on the Client Tier (see the Beehive Concepts Guide, Oracle Beehive Architecture) communicates with Oracle Beehive through the Beehive Transport Infrastructure (BTI) and the proprietary MX protocol that the BTI provides. Thus, Oracle Beehive Extensions for Outlook users can either connect directly to an Oracle Beehive deployment or they can be tunneled through standard HTTPS. This is also true for Beehive Conferencing.

[Table 1](#) describes the protocols used by different Beehive Services:

TABLE 1: BEEHIVE SERVICE PROTOCOLS

SERVICE NAME	PROTOCOLS USED
Content Management Services	WebDAV
Email Services	IMAP IMAPS SMTP SMTPS
Instant Messaging and Presence Service	XMP
Time Management Services	CalDAV
Mobile Data Synchronization	OMA-DS P-IMAP
Oracle HTTP Server <ul style="list-style-type: none"> • Workspace Client • Zimbra 	HTTP HTTPS
Beehive Integration for Outlook Beehive Conferencing	Beehive Transport Protocol (BTP)
Other	TCP, Beehive Transport Infrastructure (BTI) using proprietary multiplexor protocol (MX)

Data Tier

The Data Tier is the information store for Oracle Beehive and contains the Oracle Database, either as a single, standalone database instance or an Oracle Real Application Cluster (Oracle RAC). For MAA a RAC database is used. All system configuration and collaborative data for Oracle Beehive is stored in the Oracle Database.

The Data Tier provides Oracle Database a layer of separation from the other tiers, ensuring, among other things, optimized security and system performance. Beehive utilizes a Database Access Framework. The Database Access Framework controls all access to the database through a connection pool that it manages. Services request connections to the database through the connection pool. Once a service receives the requested information, it returns the connection back to the connection pool. The Database Access Framework leverages Java Database Connectivity (JDBC) for these connections (see "[Overview of the Database Access Framework](#)").

Ancillary Tier

The Ancillary Tier is not diagrammed in [Figure 1](#) but described for completeness. The Ancillary Tier contains any optional servers and applications that are external to the Oracle Beehive server.

Typically, components in this tier are optional because Oracle Beehive already provides many of these capabilities, such as user directories, e-mail, and time management.

Oracle Beehive supports Ancillary Tier components to provide enterprises flexibility in their deployment choices, especially for those that want to leverage existing or specialized component investments. In either case, enterprises can choose to implement the components of this tier to coexist with or access key aspects of Oracle Beehive.

Best Practices

The following configuration and operational best practices were used to compile this white paper and are recommended when using F5 BIG-IP as the application delivery controller with an Oracle Beehive MAA deployment.

F5

Use the following F5 best practices:

- Install the F5 BIG-IP units in identical pairs, configured as active/standby, to provide hardware-level redundancy. For further details, consult the BIG-IP documentation: [Configuring High Availability](#).
- Use a naming standard to ease maintenance and monitoring. An example standard is described in the [“Document Naming Conventions”](#) section of this white paper.
- Configure each Beehive protocol with a unique monitor, a unique TCP profile, and any other specific settings tuned for each protocol. This allows for more granular tuning of network communications for each Beehive protocol.
- To monitor the configuration, the rule of thumb is to set the BIG-IP LTM Health Monitor “Timeout” setting as:

$$(3 * \text{“Interval”}) + 1$$

Where Interval is the Health Monitor property that specifies the frequency at which the system issues the monitor check. This Timeout setting allows for the monitor to fail three times before marking a pool member as down.

- For the TCP profiles, use 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.

- Some Beehive services use an HTTP to HTTPS redirect iRule to redirect clients to the SSL secured service whenever possible. This includes the Beehive HTTP service and the Beehive Beekeeper service.

Beehive

Use the following Beehive recommendations:

- Configure the first application node before cloning other application nodes to save repetition of the Beehive application node configuration steps. By completing the configuration steps detailed in “Configure Beehive to Work with the F5 BIG-IP LTM” before cloning any other nodes you will eliminate the need to redo those commands on other Beehive application nodes.
- Create a Beehive generic user for BIG-IP LTM monitors to utilize for more granular service level monitoring.

F5 Configuration Guide for Beehive

This section describes how to configure the BIG-IP application delivery controller for Beehive services. At a high level, the steps to configure F5 for Beehive are as follows:

1. Install a single-application node of Beehive.
2. Configure F5 BIG-IP LTM for SSL (optional)
3. Configure F5 BIG-IP LTM for each Beehive service, including:
 - a. Creating a [monitor](#) for the service.
 - b. Creating a [TCP profile](#) for the service.
 - c. Creating a [Pool](#) for the service, adding the members.
 - d. Creating the [Virtual Server](#) for the service, selecting the associated items previously created.
 - e. Optionally, adding a second Virtual Server for secure connections over SSL.

Some of the Beehive services will add a second Virtual Server for secure connections over SSL. This is optional and only required when using SSL secured services. See the "Configuring the BIG-IP for Beehive 1.5 to use SSL Offload" section in [Appendix B](#) for more information.
4. Configure Beehive to work with the F5 BIG-IP LTM.
5. Clone the Beehive application node.

Using the Configuration Table

[Table 2](#) summarizes the F5 and Beehive protocols, objects, and configurations used in this white paper. For example, the “TCP Port” column in Table 2 is the port configured on the Beehive Application tier nodes. The “F5 Virtual Server Name:Port” column shows the virtual server name and the port used by the clients accessing Beehive services.

TABLE 2: CONFIGURATION SUMMARY FOR ORACLE BEEHIVE SERVICES

Beehive Protocol	TCP Port	F5 Monitor Name	F5 Profile Name	F5 Pool Name	F5 Virtual Server		SSL Cert
					Name	Port	
Beehive HTTP	7777	mon_bhhttp7777	tcp_bhhttp7777	pool_bhhttp7777	vs_bhhttp80	80	No ³
Beehive HTTPS	7777	mon_bhhttp7777	tcp_bhhttp7777	pool_bhhttp7777	vs_bhhttps443	443	Yes
IMAP	5143	mon_bhimap5143	tcp_bhimap5143	pool_bhimap5143	vs_bhimap143	143	No ²
IMAPS	5143	mon_bhimap5143	tcp_bhimap5143	pool_bhimap5143	vs_bhmaps993	993	Yes
SMTP	2225	mon_bhsmt2225	tcp_bhsmt2225	pool_bhsmt2225	vs_bhsmt25	25	No ²
SMTPS	2225	mon_bhsmt2225	tcp_bhsmt2225	pool_bhsmt2225	vs_bhsmts465	465	Yes
BTP	21401	mon_bhbt21401	tcp_bhbt21401	pool_bhbt21401	vs_bhbt21401	21401	No ²
BTPS	5224	mon_bhbtps5224	tcp_bhbtps5224	pool_bhbtps5224	vs_bhbtps5224	5224	No
XMPP	5222	mon_bhxmp5222	tcp_bhxmp5222	pool_bhxmp5222	vs_bhxmp5222	5222	No ²
XMPPS	5223	mon_bhxmps5223	tcp_bhxmps5223	pool_bhxmps5223	vs_bhxmps5223	5223	No
FTP	2121	mon_bhftp2121	tcp_bhftp2121	pool_bhftp2121	vs_bhftp2121	2121	No ²
FTPS	2121	mon_bhftp2121	tcp_bhftp2121	pool_bhftp2121	vs_bhfts990	990	No
Beekeeper HTTP	7779	mon_bhbekeeper7779	tcp_bhbekeeper7779 cookie_beekeeper ¹	pool_bhbekeeper7779	vs_bhbekeeper80	80	No ³
Beekeeper HTTPS	7779	mon_bhbekeeper7779	tcp_bhbekeeper7779 cookie_beekeeper ¹	pool_bhbekeeper7779	vs_bhbekeeper443	443	Yes

¹ Persistence Profile.

² For completeness we have documented both secure and unsecure connections. For secure best practices, we recommend using only secure connections.

³ HTTP is redirected through HTTPS with an iRule.

Tip: Print [Table 2](#) for easy reference while you configure F5 BIG-IP.

The examples in this document describe how to create the first two services, IMAP and IMAPS, and provide a screenshot showing what each object looks like using the BIG-IP Configuration

Utility. However, to save space, this document does not show the F5 configuration screenshots for all Beehive services. If you plan to use the SSL offload features of the F5 BIG-IP product, then first consult [Appendix B](#), in the “Configuring the BIG-IP for Beehive 1.5 to use SSL Offload” section.

For a summary of the URL’s and server port configurations used to configure the client tier, see [Appendix D](#).

[Table 3](#) lists the IP addresses and hostnames for the example used throughout this white paper, and includes the purpose that each address and hostname serves for Beehive access.

TABLE 3: IP ADDRESS AND HOSTNAME PLANNING TABLE

HOSTNAME	IP ADDRESS	PURPOSE
bhmt01.example.com	10.10.10.151	Beehive Application tier node
bhmt02.example.com	10.10.10.152	Beehive Application tier node
beehive.example.com	10.10.10.101	Beehive Virtual Server for LTM
bkpr01.example.com	10.10.10.161	Beekeeper Application Tier Node
bkpr02.example.com	10.10.10.162	Beekeeper Application Tier Node
Beekeeper.example.com	10.10.10.102	Beekeeper Virtual Server for LTM

The last subsections in this section (“F5 Configuration Guide for Beehive”) show F5 summary screenshots that depict a completed F5 configuration for all of the Beehive virtual servers.

Document Naming Conventions

Each Beehive service managed by F5 BIG-IP requires that you configure the following objects:

- [Health monitor](#)
- [TCP profile](#)
- [Pool](#)
- [Virtual server](#) or servers

To keep the configuration consistent, easy to read, and easy to administer, you should use a naming convention for your F5 configurations. Your organization may already use naming standards (which your Network Operations team can provide if necessary), or you can create naming conventions or adopt the ones used in this white paper.

[Table 4](#) shows the naming conventions used by the MAA example in this white paper.

TABLE 4: NAMING CONVENTIONS

SERVICE	PREFIX USED IN THE MAA EXAMPLE	EXAMPLE NAMES FOR THE BEEHIVE IMAP SERVICE
Health monitors	mon_	mon_bhimap5143
TCP Profiles	tcp_	tcp_bhimap5143
Pools	pool_	pool_bhimap5143
Virtual services	vs_	vs_bhimap5143

In the MAA example:

- The Beehive Services use the “bh” notation, and each service has been given a shorthand name.
- If the Beehive service is secured with SSL, the letter “s” is appended to the shorthand name.
- Each name is terminated with the TCP port number as a suffix. Pool port numbers face the Beehive servers. Virtual Server port numbers face the Beehive clients.

Thus, in the example of the Beehive IMAP service, the shorthand name is “bhimap,” the TCP port number is 5143 for the servers, and 143 for the virtual server, and 993 for the second virtual server with SSL enabled:

- vs_bhimap5143
- vs_bhimaps993 (optional if using SSL)

These values match what is shown in [Table 2](#).

Configuring SSL

The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you are planning to run any Beehive services with SSL Offload, you **MUST** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. Please see [Appendix B](#) for full details on configuring SSL on the BIG-IP.

Configuring IMAP Email (Port 5143)

This section provides step-by-step procedures to configure F5 to support the Internet Message Access Protocol (IMAP) Service for the Oracle Beehive system.

Configure a health monitor for the IMAP service

To create a health monitor:

1. On the Main tab of the BIG-IP Configuration Utility, expand the **Local Traffic** option on the menu bar, and then click **Monitors**.
2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, type a unique name for this Monitor. The MAA example uses mon_bhimap5143.
4. From the Type list, select **IMAP**.

The Monitor configuration options appear. The IMAP monitor verifies the IMAP by attempting to open a specified mail folder on the server.

5. From the Configuration list, select **Advanced**.
6. In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The example in this white paper uses an Interval of 10 and a Timeout of 31.
7. In the Username field, enter the name of a dedicated monitor account. The MAA example uses F5monitor.
8. In the Password field, enter a password for the F5monitor account. In the MAA example we entered F5monitor.
9. In the Alias Service Port field, enter **5143**.
10. All other configuration settings are optional; specify the values that are applicable for your deployment.
11. Click **Finished**.

Local Traffic » Monitors » New Monitor...

General Properties

Name	mon_bhimap5143
Type	IMAP
Import Settings	imap

Configuration: **Advanced**

Interval	10 seconds
Timeout	31 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Check Until Up	<input type="radio"/> Yes <input checked="" type="radio"/> No
User Name	F5monitor
Password	*****
Folder	INBOX
Alias Address	* All Addresses
Alias Service Port	5143 Other:
Debug	No

Cancel Repeat Finished

Create a new TCP profile for the IMAP service

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile: The MAA example uses tcp_bhimap5143.
6. In the Idle Timeout row, check the **Custom** option on the far right. In the second's field, enter **1800**.
7. Click **Finished**.

General Properties	
Name	tcp_bhimap5143
Parent Profile	tcp

Settings	
Reset On Timeout	<input checked="" type="checkbox"/> Enabled
Time Wait Recycle	<input checked="" type="checkbox"/> Enabled
Delayed Acks	<input checked="" type="checkbox"/> Enabled
Proxy Maximum Segment	<input type="checkbox"/>
Proxy Options	<input type="checkbox"/>
Proxy Buffer Low	4096 bytes
Proxy Buffer High	16384 bytes
Idle Timeout	Specify... 1800 seconds

Create the IMAP pool on the BIG-IP system

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. The example configuration in this white paper creates one pool for the Beehive IMAP nodes.

To create the IMAP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**.
Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings, as applicable, for your network.
3. In the Name field of the New Pools screen, enter a unique name for your pool. The MAA example uses `pool_bhimap5143`.
4. In the Health Monitors section, select the name of the monitor you created in the “[Configure the IMAP health monitor for the IMAP service](#)” step, and click **Add (<<)**. In the MAA example, we selected `mon_bhimap5143`.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) In our example, we selected Least Connections (member).
6. For this pool, we leave the Priority Group Activation Disabled.
7. In the New Members section, make sure the New Address option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses: `10.10.10.151`.
9. In the Service Port field, enter the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example used `5143`.
10. Click **Add** to add the member to the list.
11. Repeat the previous three steps for each server you want to add to the pool.
The MAA example in this white paper repeats this step once to add the remaining server: `10.10.10.152`.
12. Click **Finished**.

Create the IMAP virtual server

This step configures the following two IMAP virtual servers:

- MAP standard connection on port 143
- SSL secured connections on port 993

Each IMAP virtual server references the monitor, profiles, and pool created in the preceding steps.

To configure the IMAP virtual servers:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click Create.
3. In the Name field of the New Virtual Servers screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhimap143.
4. In the Destination section, select the **Host** option.

5. In the Address field, type the IP address of this virtual server. The MAA example uses: 10.10.10.101.
6. In the Service Port field, type 143.
Note: In the example, the IMAP pool is configured for port 5143, but the Virtual Server is configured for port 143. You may need to modify the port numbers to match your Beehive installation.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list, select the name of the profile you created in the “[Create a new TCP profile for the IMAP service](#)” step. The MAA example selected tcp_bhimap5143.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the IMAP pool on the BIG-IP system](#)” step. In the MAA example, we selected pool_bhimap5143.
13. Click **Finished**.

The screenshot shows the 'New Virtual Server...' configuration window in the F5 BIG-IP management console. The window is divided into 'General Properties' and 'Configuration' sections. In the 'General Properties' section, the 'Name' field is set to 'vs_bhimap143', the 'Destination' is 'Host' with address '10.10.10.101', the 'Service Port' is '143', and the 'State' is 'Enabled'. In the 'Configuration' section, the 'Configuration' dropdown is set to 'Advanced', the 'Type' is 'Standard', the 'Protocol' is 'TCP', and the 'Protocol Profile (Client)' is 'tcp_bhimap5143'. Red boxes highlight the 'Service Port' field and the 'Protocol Profile (Client)' dropdown.

Local Traffic » Virtual Servers » New Virtual Server...	
General Properties	
Name	vs_bhimap143
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	143 Other: <input type="button" value="v"/>
State	Enabled <input type="button" value="v"/>
Configuration: <input type="button" value="v"/> Advanced <input type="button" value="v"/>	
Type	Standard <input type="button" value="v"/>
Protocol	TCP <input type="button" value="v"/>
Protocol Profile (Client)	tcp_bhimap5143 <input type="button" value="v"/>

SNAT Pool	Auto Map						
Clone Pool (Client)	None						
Clone Pool (Server)	None						
Last Hop Pool	None						
iSession Profile	None Context: server						
Resources							
iRules	<table border="1"> <tr> <td>Enabled</td> <td>Available</td> </tr> <tr> <td></td> <td>Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap</td> </tr> <tr> <td>Up Down</td> <td></td> </tr> </table>	Enabled	Available		Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap	Up Down	
Enabled	Available						
	Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap						
Up Down							
HTTP Class Profiles	<table border="1"> <tr> <td>Enabled</td> <td>Available</td> </tr> <tr> <td></td> <td>httpclass</td> </tr> <tr> <td>Up Down</td> <td></td> </tr> </table>	Enabled	Available		httpclass	Up Down	
Enabled	Available						
	httpclass						
Up Down							
Default Pool	pool_bhimap5143						
Default Persistence Profile	None						
Fallback Persistence Profile	None						
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>							

Create the IMAPS virtual server

This step configures an IMAPS virtual server that references the monitor, profiles, and pool created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you plan to run any Beehive services with SSL Offload, you **must** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. See [Appendix B](#) for full details about configuring SSL on the F5 BIG-IP.

To create the IMAPS virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand Local Traffic, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name box on the New Virtual Server screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhimps993.

4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example used 10.10.10.101.
6. In the Service Port field, type **993**.
Note: In the MAA example, the IMAP pool is configured for port 5143, but the Virtual Server is configured for port 993. You may need to modify the port numbers to match your Beehive installation.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options display.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the "[Create a new TCP profile for the IMAP service](#)" step. The MAA example selected tcp_bhimap5143.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the SSL Profile (Client) list, select the name of the SSL profile you created in the [Create a Beehive Client SSL profile](#) section. The MAA example selected Beehive_clientssl.
12. Change the SNAT Pool setting to **Auto Map**.
13. In the Resources section, from the Default Pool list, select the pool you created in the "[Create the IMAP pool on the BIG-IP system](#)" step. The MAA example uses pool_bhimap5143.
14. Click **Finished**.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhimap993
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	993 Other: <input type="button" value="v"/>
State	Enabled <input type="button" value="v"/>

Configuration:

Type	Standard <input type="button" value="v"/>
Protocol	TCP <input type="button" value="v"/>
Protocol Profile (Client)	tcp_bhimap5143 <input type="button" value="v"/>
Protocol Profile (Server)	(Use Client Profile) <input type="button" value="v"/>
OneConnect Profile	None <input type="button" value="v"/>
NTLM Conn Pool	None <input type="button" value="v"/>
HTTP Profile	None <input type="button" value="v"/>
FTP Profile	None <input type="button" value="v"/>
SSL Profile (Client)	Beehive_clientssl <input type="button" value="v"/>
SSL Profile (Server)	None <input type="button" value="v"/>

SNAT Pool	Auto Map						
Clone Pool (Client)	None						
Clone Pool (Server)	None						
Last Hop Pool	None						
iSession Profile	None Context: server						
Resources							
iRules	<table border="1"> <tr> <td>Enabled</td> <td>Available</td> </tr> <tr> <td></td> <td>Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap</td> </tr> <tr> <td>Up Down</td> <td><< >></td> </tr> </table>	Enabled	Available		Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap	Up Down	<< >>
Enabled	Available						
	Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap						
Up Down	<< >>						
HTTP Class Profiles	<table border="1"> <tr> <td>Enabled</td> <td>Available</td> </tr> <tr> <td></td> <td>httpclass</td> </tr> <tr> <td>Up Down</td> <td><< >></td> </tr> </table>	Enabled	Available		httpclass	Up Down	<< >>
Enabled	Available						
	httpclass						
Up Down	<< >>						
Default Pool	pool_bhmap5143						
Default Persistence Profile	None						
Fallback Persistence Profile	None						
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>							

Configuring SMTP Email (Port 2225)

This section describes procedures you can use to configure the F5 to support the SMTP Service for the Oracle Beehive system.

Step 1: Create the SMTP health monitor

To configure a health monitor for the SMTP service:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens
2. Click **Create**. The New Monitor screen opens.
3. In the Name field, type a unique name for this Monitor. The MAA example uses mon_bhsmtp2225.
4. From the Type list, select **SMTP**.

The Monitor configuration options appear.

5. From the Configuration list, select **Advanced**.
6. In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the

interval and the timeout. The example in this white paper uses an Interval of 30 and a Timeout of 91.

7. In the Domain field, enter the name of your SMTP domain. The MAA example uses example.com.
8. In the Alias Service Port field, enter 2225.
9. All other configuration settings are optional, configure as applicable for your deployment.
10. Click **Finished**.

Step 2: Create a new TCP profile for the SMTP service

To create a TCP profile, our example bases the TCP profile on the default TCP profile, and uses the default settings for all of the options. You can configure these options as appropriate for your network.

To create the new TCP profile for the SMTP service:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.
5. In the Name field on the New TCP Profile screen, enter a unique name for this profile. The MAA example uses tcp_bhsmtp2225.
6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings, as applicable for your network. See the online help for more information on the configuration options. The MAA example used the default settings.
8. Click **Finished**.

Step 3: Create the SMTP pool

To create the SMTP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pool screen, click **Create**.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.

3. In the Name field of the New Pool screen, enter a unique name for your pool. The MAA example uses pool_bhsmtp2225.
4. In the Health Monitors section, select the name of the monitor you created in the Creating the SMTP health monitor section, and click **Add (<<)**. The MAA example selected mon_bhsmtp2225.
5. From the Load Balancing Method list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In our example, we selected **Least Connections (member)**.
6. For this pool, the MAA example leaves the Priority Group Activation set to **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 2225.
10. Click **Add** to add the member to the list.
11. Repeat the previous three steps for each server to be added to the pool.
The MAA example repeated this step only one time to add the remaining server: 10.10.10.152.
12. Click **Finished**.

Step 4: Create the SMTP virtual server

This step configures two SMTP virtual servers: one for standard connections over port 25, and another virtual server for SSL secured connections over port 465. Each virtual server references the monitor, profiles, and pool you created in the preceding procedures. To create the SMTP virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhsmtp25.
4. In the Destination section, select the **Host** option.

5. In the Address field, type the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, type **25**.
Note: In our example, the SMTP pool is configured for port 2225, but the Virtual Server is configured for port 25. You may need to modify these port numbers to match your Beehive installation.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options display.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the Creating a TCP profile section. The MAA example selected tcp_bhsmtp2225.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the [“Create the SMTP pool”](#) step. The MAA example selected pool_bhsmtp2225.
13. Click **Finished**.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhsmt25
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	25 SMTP
State	Enabled

Configuration: **Advanced**

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp_bhsmt2225
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	None
FTP Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None

SNAT Pool	Auto Map
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None Context: server

Resources

iRules	<div style="display: flex; justify-content: space-between;"> <div>Enabled</div> <div>Available</div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid gray; width: 100px; height: 40px;"></div> <div style="text-align: center;"> << >> </div> <div style="border: 1px solid gray; padding: 2px;"> Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_ldap </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
HTTP Class Profiles	<div style="display: flex; justify-content: space-between;"> <div>Enabled</div> <div>Available</div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid gray; width: 100px; height: 40px;"></div> <div style="text-align: center;"> << >> </div> <div style="border: 1px solid gray; padding: 2px;"> httpclass </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
Default Pool	pool_bhsmt2225
Default Persistence Profile	None
Fallback Persistence Profile	None

Step 5: Create the SMTPS virtual server

This step configures a SMTPS virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you are planning to run any Beehive services with SSL Offload, you **MUST** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. Please see the Appendix for full details on configuring SSL on the BIG-IP.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhsmtps465.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, type **465**.

Note: In our example, the SMTP pool is configured for port 2225, but the Virtual Server is configured for port 465. You may need to modify the port numbers to match your Beehive installation.

7. From the Configuration list, select **Advanced**.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the Creating a TCP profile section. The MAA example selected tcp_bhsmtp2225.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the SSL Profile (Client) list, select the name of the SSL profile you created in the [Create a Beehive Client SSL profile](#) section. The MAA example selected Beehive_clientssl.
12. Change the SNAT Pool setting to **Auto Map**.
13. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the SMTP pool](#)” step. The MAA example selected pool_bhsmtp2225.
14. Click **Finished**.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhsmtps465
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	465 Other: <input type="text"/>
State	Enabled

Configuration:

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp_bhsmtps2225
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	None
FTP Profile	None
SSL Profile (Client)	Beehive_clientssl
SSL Profile (Server)	None

SNAT Pool	Auto Map
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None Context: server

Resources

iRules	<div style="display: flex; justify-content: space-between;"> <div>Enabled</div> <div>Available</div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid gray; width: 100px; height: 30px;"></div> <div style="text-align: center;"> <input type="button" value="←"/> <input type="button" value="→"/> </div> <div style="border: 1px solid gray; padding: 2px;"> Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> <input type="button" value="Up"/> <input type="button" value="Down"/> </div>
HTTP Class Profiles	<div style="display: flex; justify-content: space-between;"> <div>Enabled</div> <div>Available</div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid gray; width: 100px; height: 30px;"></div> <div style="text-align: center;"> <input type="button" value="←"/> <input type="button" value="→"/> </div> <div style="border: 1px solid gray; padding: 2px;"> httpclass </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> <input type="button" value="Up"/> <input type="button" value="Down"/> </div>
Default Pool	pool_bhsmtps2225
Default Persistence Profile	None
Fallback Persistence Profile	None

Configuring Oracle Beehive Transport Protocol (Port 21401)

This section provides step-by-step procedures to configure F5 to support the Oracle Beehive Transport Protocol (BTP) port for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the BTP service

1. On the Main tab of the BIG-IP Configuration Utility, expand Local Traffic, and click **Monitors**.
2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses mon_bhbtp21401.
4. From the Type list, select **TCP**.

The Monitor configuration options display.

5. From the Configuration list, select **Advanced**.

In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The example in this white paper uses an Interval of 30 and a Timeout of 91.

6. In the Alias Service Port box, enter **21401**.
7. All other configuration settings are optional, configure as applicable for your deployment.
8. Click **Finished**.

Step 2: Create a new TCP profile for the BTP

This step creates a TCP profile. In our example, the TCP profile is based on the default TCP profile and uses all of default settings. You can configure these options as appropriate for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. The MAA example uses tcp_bhbtp21401.

6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
8. Click **Finished**.

Step 3: Create the BTP pool

To create the BTP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.
Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.
3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhbt21401.
4. In the Health Monitors section, select the name of the monitor you created in the "[Create the BTP health monitor](#)," step, and click **Add (<<)**. The MAA example selected mon_bhbt21401.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) In our example, we selected **Least Connections (member)**.
6. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 21401.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.

The MAA example in this white paper repeats this step once to add the remaining server: 10.10.10.152.

12. Click **Finished**.

Step 4: Create the BTP virtual server

This step configures a BTP virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhbt21401.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, type 21401
7. From the Configuration list, select **Advanced**.

The Advanced configuration options appear.

8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “[Create a TCP profile for BTP](#)” step. The MAA example selected tcp_bhsmtp2225.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the BTP pool](#)” step The MAA example selected pool_bhbt21401.
13. Click **Finished**.

Configuring Oracle Secure BTPS (Port 5224)

This section provides step-by-step procedures to configure F5 to support the Secure Oracle Beehive Transport Protocol (BTPS) port for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the BTPS service

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and click **Monitors**.

2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses mon_bhbtps5224.
4. From the Type list, select **TCP**.

The Monitor configuration options display.

5. From the Configuration list, select **Advanced**.

In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The example in this white paper uses an Interval of 30 and a Timeout of 91.

6. In the Alias Service Port box, enter **5224**.
7. All other configuration settings are optional, configure as applicable for your deployment.
8. Click **Finished**.

Step 2: Create a new TCP profile for the BTPS

This step creates a TCP profile. In our example, the TCP profile is based on the default TCP profile and uses all of default settings. You can configure these options as appropriate for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. The MAA example uses tcp_bhbtps5224.
6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
8. Click **Finished**.

Step 3: Create the BTPS pool

To create the BTPS pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.
Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.
3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhbtps5224.
4. In the Health Monitors section, select the name of the monitor you created in the “[Create the BTPS health monitor](#)” step, and click **Add (<<)**. The MAA example selected mon_bhbtps5224.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) In our example, we selected **Least Connections (member)**.
6. For this pool, we leave the Priority Group Activation set to **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 5224.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.
The MAA example in this white paper repeats this step once to add the remaining server: 10.10.10.152.
12. Click **Finished**.

Step 4: Create the BTPS virtual server

This step configures a BTPS virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhbtps5224.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, type **5224**.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “Create a TCP profile for BTPS” step. The MAA example selected tcp_bhbtps5224.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the BTPS pool](#)” step. The MAA example selected pool_bhbtps5224.
13. Click **Finished**.

Configuring XMPP Beehive Presence (Port 5222)

This section provides step-by-step procedures to configure F5 to support the Beehive Presence Service for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the Beehive Presence (XMPP) service

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and click **Monitors**.
2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses mon_bhxmpp5222.
4. From the Type list, select **TCP**.

The Monitor configuration options appear.

5. From the Configuration list, select **Advanced**.

In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The example in this white paper uses an Interval of 30 and a Timeout of 91.

6. In the Alias Service Port box, enter **5222**.
7. All other configuration settings are optional, configure as applicable for your deployment.
8. Click **Finished**.

Step 2: Create a new TCP profile for the XMPP service

This step creates a TCP profile. You can configure these options as appropriate for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. The MAA example uses tcp_bhxmpp5222.
6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
8. Click **Finished**.

Step 3: Create the XMPP pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. The MAA example configuration created one pool for the Beehive XMPP devices.

To create the XMPP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.
Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.
3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhxmpp5222.
4. In the Health Monitors section, select the name of the monitor you created in the “[Create the XMPP health monitor](#)” step, and click **Add (<<)**. The MAA example selected mon_bhxmpp5222.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) In our example, we selected **Least Connections (member)**.
6. For this pool, we leave the Priority Group Activation setting at **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 5222.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.
The MAA example in this white paper repeats this step once to add the remaining server: 10.10.10.152.
12. Click **Finished**.

Step 4: Create the XMPP virtual server

This step configures an XMPP virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.

3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhxmpp5222.
4. In the Destination section, select the **Host** option.
5. In the Address field, enter the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, enter **5222**
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “[Create a TCP profile for XMPP](#)” step. The MAA example selected tcp_bhxmpp5222.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the XMPP pool](#)” step. The MAA example selected pool_bhxmpp5222.
13. Click **Finished**.

Step 5: Create the XMPPS virtual server

This step configures an XMPPS virtual server that references the monitor, profiles, and pool created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you plan to run any Beehive services with SSL Offload, you **must** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. See [Appendix B](#) for full details about configuring SSL on the F5 BIG-IP.

To create the XMPPS virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name box on the New Virtual Server screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhxmpss5223.
4. In the Destination section, select the **Host** option.

5. In the Address field, type the IP address of this virtual server. The MAA example used 10.10.10.101.
6. In the Service Port field, type **5223**.
Note: In the MAA example, the XMPP pool is configured for port 5222, but the Virtual Server is configured for port 5223. You may need to modify the port numbers to match your Beehive installation.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the "[Create a new TCP profile for the XMPP service](#)" step. The MAA example selected tcp_bhxmpp5222.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the SSL Profile (Client) list, select the name of the SSL profile you created in the [Create a Beehive Client SSL profile](#) section. The MAA example selected Beehive_clientssl.
12. Change the SNAT Pool setting to **Auto Map**.
13. In the Resources section, from the Default Pool list, select the pool you created in the "[Create the XMPP pool](#)" step. The MAA example uses pool_bhxmpp5222.
14. Click **Finished**.

Configuring FTP Service (Port 2121)

This section describes the procedure to configure the F5 to support the Beehive FTP Service for the Oracle Beehive system.

This section provides step-by-step procedures to configure F5 to support the Beehive Presence Service for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the FTP service

1. On the Main tab of the BIG-IP Configuration Utility, expand Local Traffic, and click **Monitors**.
2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses mon_bhftp2121.
4. From the Type list, select **FTP**.

The Monitor configuration options appear.

5. From the Configuration list, select **Advanced**.

In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The example in this white paper uses an Interval of 30 and a Timeout of 91.

6. In the Username field, enter the name of a dedicated monitor account. The MAA example uses `F5monitor`.
7. In the Password field, enter a password for the `F5monitor` account. The MAA example uses `F5monitor`.
8. In the Path/Filename field, enter the path and file for testing downloads. The MAA example uses:

```
/Oracle/F5monitor's Personal Workspace/Documents/monitor.txt
```

9. In the Alias Service Port box, enter **2121**.
10. All other configuration settings are optional. Configure them, as applicable, for your deployment.
11. Click **Finished**.

The screenshot shows the configuration page for a monitor named 'mon_bhftp2121'. The breadcrumb navigation is 'Local Traffic >> Monitors >> mon_bhftp2121'. There are two tabs: 'Properties' (selected) and 'Instances'. The 'General Properties' section includes:

Name	mon_bhftp2121
Partition	Common
Type	FTP

The 'Configuration' section is set to 'Basic' and includes the following fields:

Interval	30	seconds
Timeout	91	seconds
User Name	F5monitor	
Password	●●●●●●●●	
Path / Filename	ersonal Workspace/Documents/monitor.txt	
Mode	Passive	

At the bottom, there are 'Update' and 'Delete' buttons.

Step 2: Create a new TCP profile for the FTP service

This step creates a TCP profile for the MAA example configuration. The MAA example bases the TCP profile on the default TCP profile, and using the default settings for all of the options. You should configure the options appropriately for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.

The HTTP Profiles screen opens.

3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. The MAA example uses tcp_bhftp2121.
6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
8. Click **Finished**.

Step 3: Create the FTP pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. The MAA example configuration created one pool for the Beehive FTP devices.

To create the FTP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.

Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.

3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhftp2121.

4. In the Health Monitors section, select the name of the monitor you created in the “[Create and configure the FTP health monitor](#)” step, and click **Add (<<)**. The MAA example selected `mon_bhxmpp5222`.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) The MAA example selected **Least Connections (member)**.
6. For this pool, we leave the Priority Group Activation setting at **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses `10.10.10.151`.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses `2121`.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.
The MAA example in this white paper repeats this step once to add the remaining server: `10.10.10.152`.
12. Click **Finished**.

Step 4: Create the FTP virtual server

This step configures an FTP virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses `vs_bhftp2121`.
4. In the Destination section, select the **Host** option.
5. In the Address field, enter the IP address of this virtual server. The MAA example uses `10.10.10.101`.
6. In the Service Port field, enter **2121**.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options display.

8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “[Create a TCP profile for FTP](#)” step. The MAA example selected tcp_bhftp2121.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the “[Create the FTP pool](#)” step. The MAA example selected pool_bhftp2121.
13. Click **Finished**.

Step 5: Create the FTPS virtual server

This step configures an FTPS virtual server that references the monitor, profiles, and pool created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you plan to run any Beehive services with SSL Offload, you **must** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. See [Appendix B](#) for full details about configuring SSL on the F5 BIG-IP.

To create the FTPS virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name box on the New Virtual Server screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhftps990.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example used 10.10.10.101.
6. In the Service Port field, type **990**.

Note: In the MAA example, the FTPS pool is configured for port 2121, but the Virtual Server is configured for port 990. You may need to modify the port numbers to match your Beehive installation.

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.

9. From the Protocol Profile (Client) list, select the name of the profile you created in the "[Create a new TCP profile for the FTP service](#)" step. The MAA example selected tcp_bhftp2121.
10. Leave the Protocol Profile (Server) option at the default setting.
11. Change the SNAT Pool setting to **Auto Map**.
12. In the Resources section, from the Default Pool list, select the pool you created in the "[Create the FTP pool](#)" step. The MAA example uses pool_bhftp2121.
13. Click **Finished**

Configuring Beehive HTTP and HTTPS (Port 7777)

This section provides step-by-step procedures to configure F5 to support the Standard Beehive HTTP Service for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the Beehive HTTP service

1. On the Main tab of the BIG-IP Configuration Utility, expand Local Traffic, and click **Monitors**.
2. On the Monitors screen, click **Create**.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses mon_bhhttp7777.
4. From the Type list, select **HTTP**.
The Monitor configuration options display.
5. From the Configuration list, select **Advanced**.
In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The MAA example in this white paper uses an Interval of 30 and a Timeout of 91.
6. In the Alias Service Port box, enter **7777**.
7. All other configuration settings are optional, configure as applicable for your deployment.
8. Click **Finished**.

Step 2: Create a new TCP profile for the Beehive HTTP service

This step creates a TCP profile for the MAA example configuration. The MAA example bases the TCP profile on the default TCP profile, and using the default settings for all of the options. You should configure the options appropriately for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the Protocol menu, select **TCP**.
4. In the upper right portion of the screen, click **Create**.
The New TCP Profile screen opens.
5. In the Name field, enter a unique name for this profile. The MAA example uses tcp_bhhttp7777.
6. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
7. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
8. Click **Finished**.

Step 3: Create the Beehive HTTP pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. The MAA example configuration created one pool for the Beehive HTTP devices.

To create the HTTP pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.
Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.
3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhhttp7777.
4. In the Health Monitors section, select the name of the monitor you created in the [“Create and configure the \(Unsecure\) Beehive HTTP health monitor”](#) step, and click **Add (<<)**. The MAA example selected mon_bhhttp7777.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a

particular network.) The MAA example selected **Least Connections (member)**.

6. For this pool, we leave the Priority Group Activation setting at **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 7777.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.

The MAA example in this white paper repeats this step once to add the remaining server: 10.10.10.152.

12. Click **Finished**.

Step 4: Create the Beehive HTTP virtual server

This step configures a Beehive HTTP virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhhttp80.
4. In the Destination section, select the **Host** option.
5. In the Address field, enter the IP address of this virtual server. The MAA example uses 10.10.10.101.
6. In the Service Port field, enter **80**.
7. From the Configuration list, select **Advanced**.

The Advanced configuration options display.

8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “[Create a TCP profile for Beehive HTTP Service](#)” step. The MAA example selected tcp_bhhttp7777.

10. Leave the Protocol Profile (Server) option at the default setting.
11. From the HTTP Profile list, select **http**.
Note: If the clients will be attaching to the Beehive HTTP services over a WAN (wide-area network), select the **http-wan-optimized-compression** profile.
12. Change the SNAT Pool setting to **Auto Map**.
13. In the Resources section, from the Available list, select the iRule you created in the “[Creating the Beehive Redirect iRule](#)” section. In the MAA example, we select **Beehive_httptohttps**, and click and click **Add (<<)** to add it to the Enabled list. This iRule redirects all clients to the SSL virtual server for Beehive HTTP on port 443.
14. From the Default Pool list, select the pool you created in the “[Create the Beehive HTTP pool](#)” step. The MAA example selected pool_bhhttp7777.
15. Click **Finished**.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhhttp80
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	80 HTTP
State	Enabled

Configuration: **Advanced**

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp_bhhttp7777
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http-wan-optimized-compression
FTP Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None

SNAT Pool	Auto Map
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None Context: server

Resources

iRules	Enabled	Available
	Beehive httphttps	_sys_auth_krbdelegate _sys_auth_ssl_cc_idap
HTTP Class Profiles	Enabled	Available
		httpclass
Default Pool	pool_bhhttp7777	
Default Persistence Profile	None	
Fallback Persistence Profile	None	

Cancel Repeat Finished

Step 5: Create the HTTPS virtual server

This step configures an HTTPS virtual server that references the monitor, profiles, and pool created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you plan to run any Beehive services with SSL Offload, you **must** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. See [Appendix B](#) for full details about configuring SSL on the F5 BIG-IP.

To create the HTTPS virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name box on the New Virtual Server screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhhttps443.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example used 10.10.10.101.
6. In the Service Port field, type **443**.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list, select the name of the profile you created in the "[Create a new TCP profile for the Beehive HTTP service](#)" step. The MAA example selected tcp_bhhttp7777.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the SSL Profile (Client) list, select the name of the SSL profile you created in the [Create a Beehive Client SSL profile](#) section. The MAA example selected Beehive_clientssl.
12. From the HTTP Profile list, select **http**.
Note: If the clients will be attaching to the Beehive HTTPS services over a WAN (wide-area network), select the **http-wan-optimized-compression** profile.
13. Change the SNAT Pool setting to **Auto Map**.
14. In the Resources section, from the Default Pool list, select the pool you created in the "[Create the HTTP pool](#)" step. The MAA example uses pool_bhhttp7777.

15. Click **Finished**

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhhttps443
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.10.101
Service Port	443 HTTPS
State	Enabled

Configuration: Advanced

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp_bhhttp7777
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http-wan-optimized-compression
FTP Profile	None
SSL Profile (Client)	Beehive_clientssl
SSL Profile (Server)	None

SNAT Pool	Auto Map
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None Context: server

Resources

iRules	<table border="1"> <tr> <th>Enabled</th> <th>Available</th> </tr> <tr> <td></td> <td>Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap</td> </tr> </table>	Enabled	Available		Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap
Enabled	Available				
	Beehive_httphttps _sys_auth_krbdelegate _sys_auth_ssl_cc_idap				
HTTP Class Profiles	<table border="1"> <tr> <th>Enabled</th> <th>Available</th> </tr> <tr> <td></td> <td>httpclass</td> </tr> </table>	Enabled	Available		httpclass
Enabled	Available				
	httpclass				
Default Pool	pool_bhhttp7777				
Default Persistence Profile	None				
Fallback Persistence Profile	None				

Cancel Repeat Finished

Configuring Beekeeper (Port 7779)

This section provides step-by-step procedures to configure F5 to support the Standard Beekeeper Service for the Oracle Beehive system.

Step 1: Create and configure a health monitor for the Beekeeper service

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and click **Monitors**.
2. On the Monitors screen, click **Create**. The New Monitor screen opens.
3. In the Name field on the New Monitor screen, enter a unique name for this Monitor. The MAA example uses `mon_bhbeekeeper7779`.
4. From the Type list, select **HTTP**.

The Monitor configuration options display.

5. From the Configuration list, select **Advanced**.

In the Configuration section, enter values in the Interval and Timeout fields. The recommendation is to specify a minimum 1:3 +1 ratio between the interval and the timeout. The MAA example in this white paper uses an Interval of 30 and a Timeout of 91.

6. In the Alias Service Port box, enter **7779**.
7. All other configuration settings are optional, configure as applicable for your deployment.
8. Click **Finished**.

Step 2: Create a new TCP profile for the unsecure Beekeeper service

This step creates a TCP profile for the MAA example configuration. The MAA example bases the TCP profile on the default TCP profile, and using the default settings for all of the options. You should configure the options appropriately for your network.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic** and click **Profiles**.

The HTTP Profiles screen opens.

2. On the Menu bar, from the Protocol menu, select **TCP**.
3. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

4. In the Name field, enter a unique name for this profile. The MAA example uses `tcp_bhbeekeeper7779`.

5. In the Idle Timeout row, check **Custom**. In the second's field, enter **1800**.
6. Modify any of the settings as applicable for your network. See the online help for more information about the configuration options. The MAA example uses the default settings.
7. Click **Finished**.

Step 3: Create a new Beekeeper cookie persistence profile

This step creates a Cookie Persistence profile based on the default profile. We recommend using the default cookie method for this profile (HTTP cookie insert), but you can change other settings, such as specifying a cookie expiration.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic** and click **Profiles**.

The HTTP Profiles screen opens.

2. On the Menu bar, from the Protocol menu, click **Persistence**.
3. In the upper right portion of the Persistence Profiles screen, click **Create**.
4. In the Name field on the New Persistence Profile screen, enter a unique name for this profile. The MAA example uses `cookie_beekeeper`.
5. From the Persistence Type list, select **Cookie**.

The configuration options for cookie persistence display.

6. Click **Finished**.

For more information about creating or modifying profiles, or for general information about applying profiles, see the F5 BIG-IP Product Documentation [3] at

<http://www.f5.com/products/big-ip/>

Local Traffic >> Profiles : Persistence >> New Persistence Profile...	
General Properties	
Name	cookie_beekeeper
Persistence Type	Cookie
Parent Profile	cookie
Configuration	
Cookie Method	HTTP Cookie Insert
Cookie Name	
Expiration	<input checked="" type="checkbox"/> Session Cookie
Override Connection Limit	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Step 4: Create the Beekeeper pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. The MAA example configuration created one pool for the Beehive HTTP devices.

To create the Beekeeper pool:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Pools**.
2. In the upper right portion of the Pools screen, click **Create**. The New Pool screen opens.
Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure the settings, as applicable, for your network.
3. In the Name field, enter a unique name for your pool. The MAA example uses pool_bhbeekeeper7779.
4. In the Health Monitors section, select the name of the monitor you created in the “[Create and configure the \(Unsecure\) Beekeeper health monitor](#)” step, and click **Add (<<)**. The MAA example selected mon_bhbeekeeper7779.
5. From the Load Balancing Method list, choose your preferred load balancing method. (Different load balancing methods may yield optimal results for a particular network.) The MAA example selected **Least Connections (member)**.
6. For this pool, the MAA example left the Priority Group Activation setting at **Disabled**.
7. In the New Members section, make sure the **New Address** option is selected.
8. In the Address field, add the first server to the pool. The MAA example uses 10.10.10.161.
9. In the Service Port field, type the service port you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 7779.
10. Click **Add** to add the member to the list.
11. Repeat the three previous steps for each server you want to add to the pool.
The MAA example in this white paper repeats this step once to add the remaining server: 10.10.10.162.
12. Click **Finished**.

Step 5: Create the unsecure Beekeeper HTTP virtual server

This step configures an unsecure Beekeeper HTTP virtual server that references the monitor, profiles, and pool that you created in the preceding procedures.

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name field on the New Virtual Server screen, enter a unique name for this virtual server. The MAA example uses vs_bhbeekeeper80.
4. In the Destination section, select the **Host** option.
5. In the Address field, enter the IP address of this virtual server. The MAA example uses 10.10.10.102.
6. In the Service Port field, enter **80**.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list select the name of the profile you created in the “[Create a TCP profile for Beekeeper](#)” step. The MAA example selected tcp_bhbeekeeper7779.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the HTTP Profile list, select **http**.
12. Change the SNAT Pool setting to **Auto Map**.
13. In the Resources section, from the Available list, select the select the iRule you created in the “[Creating the Beehive Redirect iRule](#)” section. In the MAA example, we select **Beehive_httptohttps**, and click (**<<**) to add it to the Enabled list. This iRule redirects all clients to the SSL virtual server for Beekeeper on port 443.
14. From the Default Pool list, select the pool you created in the “Create the Beekeeper pool” step. The MAA example selected pool_bhbeekeeper7779.
15. From the Default Persistence Profile list, select the Cookie profile you created in the “[Create the cookie persistence profile for Beekeeper](#)” step. In our example, we select **cookie_beekeeper**.
16. Click **Finished**.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vs_bhbeekeeper80		
Destination	Type:	<input checked="" type="radio"/> Host <input type="radio"/> Network	
	Address:	10.10.10.102	
Service Port	80	HTTP	
State	Enabled		

Configuration: Advanced

Type	Standard		
Protocol	TCP		
Protocol Profile (Client)	tcp_bhbeekeeper7778		
Protocol Profile (Server)	(Use Client Profile)		
OneConnect Profile	None		
NTLM Conn Pool	None		
HTTP Profile	http		
FTP Profile	None		
SSL Profile (Client)	None		
SSL Profile (Server)	None		

SNAT Pool	Auto Map		
Clone Pool (Client)	None		
Clone Pool (Server)	None		
Last Hop Pool	None		
iSession Profile	None	Context: server	

Resources

iRules	Enabled	Beehive httpstohttps	Available	_sys_auth_krbdelegate _sys_auth_ssl_cc_idap
HTTP Class Profiles	Enabled		Available	httpclass
Default Pool	pool_bhbeekeeper7778			
Default Persistence Profile	cookie_beekeeper			
Fallback Persistence Profile	None			

Cancel Repeat Finished

Step 6: Create the Beekeeper HTTP Secure virtual server

This step configures a Beekeeper Secure virtual server that references the monitor, profiles, and pool created in the preceding procedures.

Note: The creation of a virtual server using the SSL offload features of BIG-IP is optional. If you plan to run any Beehive services with SSL Offload, you **must** configure the BIG-IP for SSL before creating any SSL enabled virtual servers. See [Appendix B](#) for full details about configuring SSL on the F5 BIG-IP.

To create the Beekeeper Secure virtual server:

1. On the Main tab of the BIG-IP Configuration Utility, expand **Local Traffic**, and then click **Virtual Servers**.
2. In the upper right portion of the Virtual Servers screen, click **Create**.
3. In the Name box on the New Virtual Server screen, type a unique name for this virtual server. In the MAA example, we entered vs_bhbeekeepers443.
4. In the Destination section, select the **Host** option.
5. In the Address field, type the IP address of this virtual server. The MAA example used 10.10.10.102.
6. In the Service Port field, type **443**.
7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. In the Type field, ensure the default setting, **Standard**, is selected.
9. From the Protocol Profile (Client) list, select the name of the profile you created in the “[Create a new TCP profile for the Beekeeper service](#)” step. The MAA example selected tcp_bhbeekeeper7779.
10. Leave the Protocol Profile (Server) option at the default setting.
11. From the SSL Profile (Client) list, select the name of the SSL profile you created in the [Create a Beekeeper Client SSL profile](#) section. The MAA example selected Beekeeper_clientssl. Make sure you use the Beekeeper SSL profile, and not the Beehive SSL profile.
12. From the HTTP Profile list, select **http**.
13. Change the SNAT Pool setting to **Auto Map**.

14. In the Resources section, from the Default Pool list, select the pool you created in the ["Create the Beekeeper pool"](#) step. The MAA example uses pool_bhbeekeeper7779.
15. **Click Finished.**

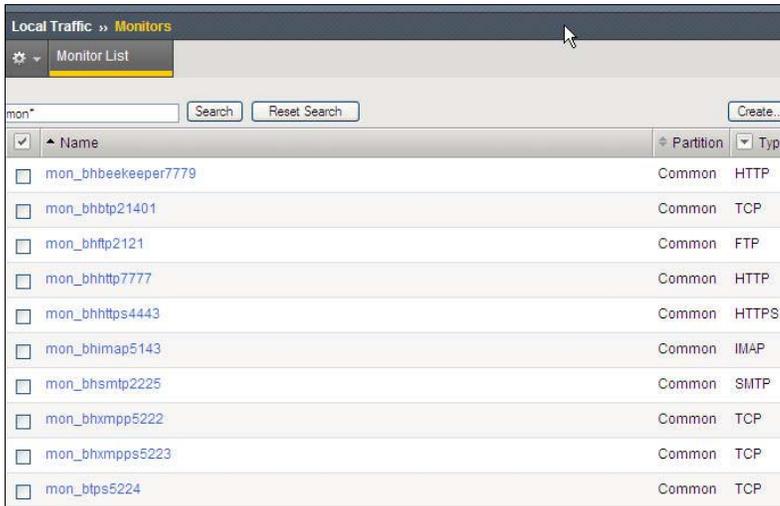
The screenshot shows the configuration page for a new virtual server in the F5 Local Traffic Manager. The interface is divided into several sections:

- General Properties:** Name is 'vs_bhbeekeeper443', Destination Type is 'Host' with address '10.10.10.102', Service Port is '443' with protocol 'HTTPS', and State is 'Enabled'.
- Configuration:** Type is 'Standard', Protocol is 'TCP', Protocol Profile (Client) is 'tcp_bhbeekeeper7778', Protocol Profile (Server) is '(Use Client Profile)', OneConnect Profile is 'None', NTLM Conn Pool is 'None', HTTP Profile is 'http', FTP Profile is 'None', SSL Profile (Client) is 'Beekeeper_clientsl', and SSL Profile (Server) is 'None'.
- SNAT Pool:** Set to 'Auto Map'.
- Clone Pools:** Client, Server, and Last Hop are all set to 'None'.
- iSession Profile:** Set to 'None' with Context 'server'.
- Resources:**
 - iRules:** An 'Available' list contains 'Beehive_httphttps', '_sys_auth_krbdelegate', and '_sys_auth_ssl_cc_idap'.
 - HTTP Class Profiles:** An 'Available' list contains 'httpclass'.
 - Default Pool:** A dropdown menu is set to 'pool_bhbeekeeper7778'.
 - Default Persistence Profile:** Set to 'cookie_beekeeper'.
 - Fallback Persistence Profile:** Set to 'None'.

At the bottom, there are buttons for 'Cancel', 'Repeat', and 'Finished'.

F5 Monitor Configuration Summary

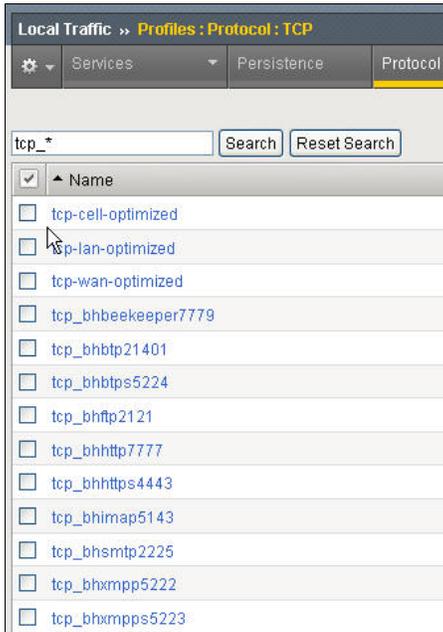
After finishing the configuration of all Beehive services, you should have a list of monitors similar to the one in the following screenshot from the MAA example.



<input checked="" type="checkbox"/>	Name	Partition	Type
<input type="checkbox"/>	mon_bhbeekeeper7779	Common	HTTP
<input type="checkbox"/>	mon_bhbtcp21401	Common	TCP
<input type="checkbox"/>	mon_bhttp2121	Common	FTP
<input type="checkbox"/>	mon_bhttp7777	Common	HTTP
<input type="checkbox"/>	mon_bhhttps4443	Common	HTTPS
<input type="checkbox"/>	mon_bhimap5143	Common	IMAP
<input type="checkbox"/>	mon_bsmtp2225	Common	SMTP
<input type="checkbox"/>	mon_bxmpp5222	Common	TCP
<input type="checkbox"/>	mon_bxmpps5223	Common	TCP
<input type="checkbox"/>	mon_btpps5224	Common	TCP

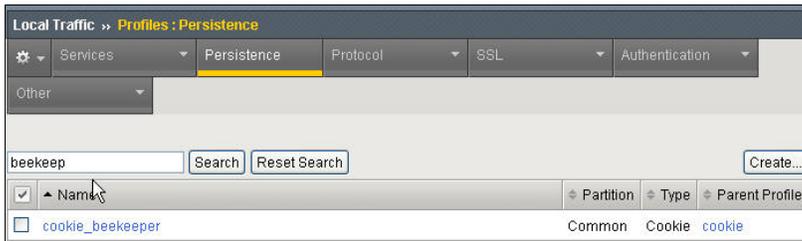
F5 TCP Profile Configuration Summary

After finishing the configuration of all Beehive services, you should have a list of TCP profiles similar to the one in the following screenshot from the MAA example.



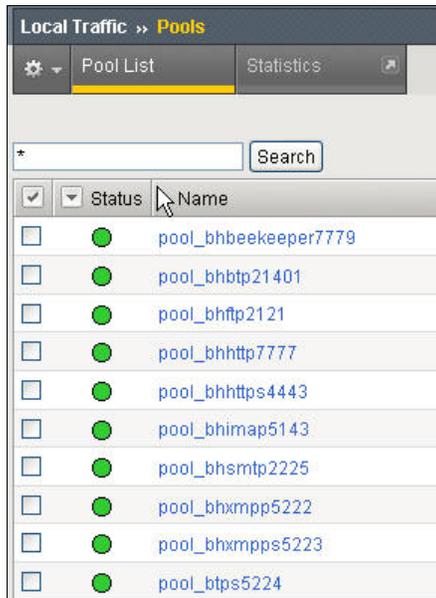
F5 Persistence Profile Configuration Summary

After finishing the configuration of all Beehive services, you should have a list of persistence profiles similar to the one in the following screenshot from the MAA example.



F5 Pool Configuration Summary

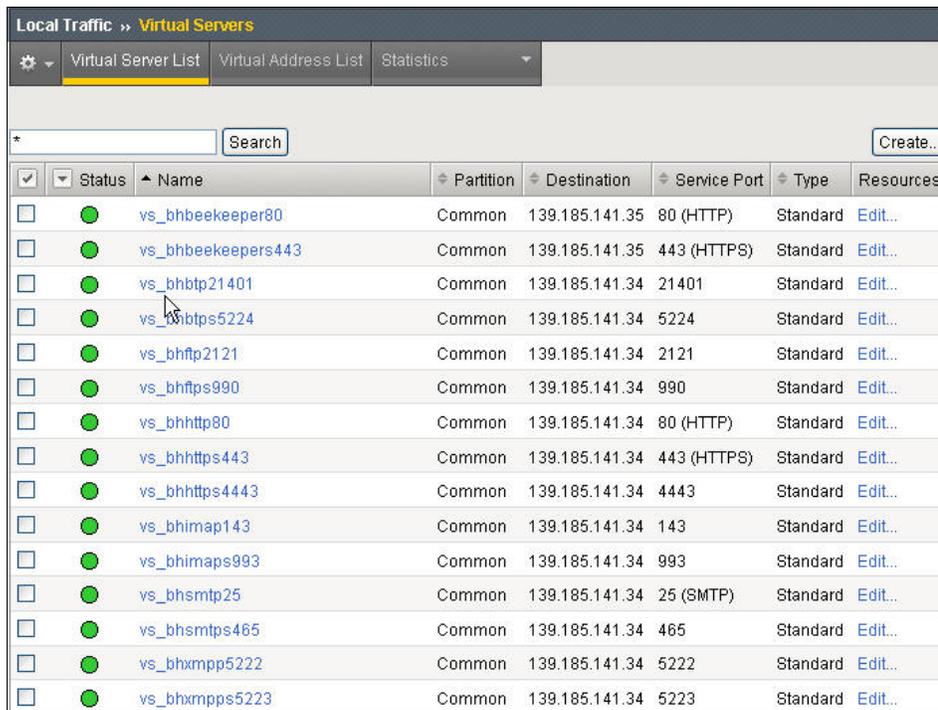
After finishing the configuration of all Beehive services, you should have a list of pools similar to the one in the following screenshot from the MAA example.



Local Traffic >> Pools		
Pool List		Statistics
* <input type="text"/> <input type="button" value="Search"/>		
<input checked="" type="checkbox"/>	Status	Name
<input type="checkbox"/>	●	pool_bhbeekeeper7779
<input type="checkbox"/>	●	pool_bhbtp21401
<input type="checkbox"/>	●	pool_bhftp2121
<input type="checkbox"/>	●	pool_bhhttp7777
<input type="checkbox"/>	●	pool_bhhttps4443
<input type="checkbox"/>	●	pool_bhimap5143
<input type="checkbox"/>	●	pool_bhsmtip2225
<input type="checkbox"/>	●	pool_bhxmp5222
<input type="checkbox"/>	●	pool_bhxmps5223
<input type="checkbox"/>	●	pool_btps5224

F5 Virtual Server Configuration Summary

After finishing the configuration of all Beehive services, you should have a list of virtual servers with IP addresses and port numbers similar to the one in the following screenshot from the MAA example.



<input type="checkbox"/>	Status	Name	Partition	Destination	Service Port	Type	Resources
<input type="checkbox"/>	●	vs_bhbeekeeper80	Common	139.185.141.35	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	vs_bhbeekeeper443	Common	139.185.141.35	443 (HTTPS)	Standard	Edit...
<input type="checkbox"/>	●	vs_bhhtp21401	Common	139.185.141.34	21401	Standard	Edit...
<input type="checkbox"/>	●	vs_bhtps5224	Common	139.185.141.34	5224	Standard	Edit...
<input type="checkbox"/>	●	vs_bhtp2121	Common	139.185.141.34	2121	Standard	Edit...
<input type="checkbox"/>	●	vs_bhtps990	Common	139.185.141.34	990	Standard	Edit...
<input type="checkbox"/>	●	vs_bhhttp80	Common	139.185.141.34	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	vs_bhhttps443	Common	139.185.141.34	443 (HTTPS)	Standard	Edit...
<input type="checkbox"/>	●	vs_bhhttps4443	Common	139.185.141.34	4443	Standard	Edit...
<input type="checkbox"/>	●	vs_bhimap143	Common	139.185.141.34	143	Standard	Edit...
<input type="checkbox"/>	●	vs_bhimaps993	Common	139.185.141.34	993	Standard	Edit...
<input type="checkbox"/>	●	vs_bhsmtp25	Common	139.185.141.34	25 (SMTP)	Standard	Edit...
<input type="checkbox"/>	●	vs_bhsmtps465	Common	139.185.141.34	465	Standard	Edit...
<input type="checkbox"/>	●	vs_bhxmp5222	Common	139.185.141.34	5222	Standard	Edit...
<input type="checkbox"/>	●	vs_bhxmps5223	Common	139.185.141.34	5223	Standard	Edit...

Configure Beehive to Work with the F5 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.

Set the Virtual Server and Ports

Set the ports to match [Table 2](#) as follows

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

Note: The HttpPort is set to the Oracle HTTP Server (OHS) virtual port. Since SSL is terminated at the BigIP LTM, set the HttpPort to 443 and ensure that SSL is enabled for the Beehive virtual server. Enabling SSL is for redirect URL's that copy the settings that the active request used.

To see what the HTTP listening port is set to, see the “[Setting the HTTP and HTTPS Listening Ports](#)” section.

```
beectl modify_property --component _VIRTUAL_SERVER --name HttpPort --value 443
beectl modify_property --component _VIRTUAL_SERVER --name HttpSslEnabled --value true
beectl list_properties --component _VIRTUAL_SERVER
```

Property Name	Property Value
*ImapPort	5143
*Smtpport	2225
Alias	_VIRTUAL_SERVER
BtiClientPort	21401
BtiSecureClientPort	21451
FtpPort	2121
*HttpPort	443

*HttpSslEnabled	false
HttpSslPort	443
IPAddress	
ImapSslEnabled	false
ImapSslPort	993
*ServerName	beehive.example.com
SmtplAuthRequired	false
SmtplSslEnabled	false
SmtplSslPort	465
XmppPort	5222
XmppSslEnabled	false
XmppSslPort	5223

Note:- An asterisk (*) indicates that property value is changed and change is not yet activated.

Set the HTTP Listening Port

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

1. Get the Beehive instance name:

```
beectl list_components --type BeehiveInstance
```

Component type	Component identifier
BeehiveInstance	beehive_instance_maatst.bhmt01.example.com

2. Get the OHS component name:

```
beectl list_properties --component beehive_instance_maatst.bhmt01.example.com --name HttpServer
```

Property name	Property value
HttpServer	ohs_maatst.bhmt01.example.com

3. Get the current HTTP listener port:

```
beectl list_properties --component ohs_maatst.bhmt01.example.com --name HttpListenPort
```

Property name	Property value
HttpListenPort	7779

4. Change the HTTP listening port:

```
beectl modify_property
--component ohs_maastst.bhmt01.example.com --name HttpListenPort --value 7777
```

5. Activate the configuration:

```
beectl activate_configuration
```

6. Modify the local configuration files:

```
beectl modify_local_configuration_files
```

Set Beehive HTTP Server for SSL Termination

1. Set the `SslTerminatedByLoadBalancer` property of the `HttpServerCluster` component to **true**:

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

2. Review the changes:

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

Property name	Property value
Alias	
HttpServerSslEnabled	false
HttpServers	ohs_maastst.bhmt01.example.com
Site	_CURRENT_SITE
*SslTerminatedByLoadBalancer	true

Note:- An asterisk (*) indicates that property value is changed and change is not yet activated.

3. Commit changes made to the configuration:

```
beectl activate_configuration
beectl modify_local_configuration_files
```

Setup TLS

See Chapter 21 of the Beehive Installation guide for further details.

1. Enable auto login for default wallet on each mid-tier

```
orapki wallet create -wallet $ORACLE_HOME/Apache/Apache/conf/ssl.wlt/default/ -
auto_login -pwd welcome
```

2. Configure each instance to use Oracle Wallet:

- a) Get instance names

```
beectl list_components --type BeehiveInstance
```

```
-----+-----
Component type | Component identifier
-----+-----
BeehiveInstance | beehive_instance_maatst.bhmt01.example.com
-----+-----
```

- b) Set instance property:

```
beectl modify_property \
--component beehive_instance_maatst.bhmt01.example.com \
--name WalletDir \
--value /u01/app/oracle/product/1.5/beehive_1/Apache/Apache/conf/ssl.wlt/default
```

- c) Verify settings:

```
beectl list_properties --component beehive_instance_maatst.bhmt01.example.com \
--name WalletDir
```

```
-----+-----
Property name  | Property value
-----+-----
WalletDir      | /u01/app/oracle/product/1.5/beehive_1/Apache/Apache/
conf/ssl.wlt/default
-----+-----
```

Setup XMPP

- 1) Verify settings:

```
beectl list_properties --component _XmppService
```

Property name	Property value
Alias	_XmppService
Database	
DomainName	example.com
DomainNames	example.com
Language	en
LightweightThreadCount	10
LightweightThreadPriority	5
MessagesOnInvalidAction	
RetryCount	6
RetryTimeout	5
SearchFields	first , last , email
ServiceApplication	svcapp_xmpp
ServiceInstances	instance_xmpp_BEEAPP_maastst.bhmt01.example .com
Site	_CURRENT_SITE
Status	ENABLED
SupportedAgents	uds
VersionRules	
XmppPort	5222
XmppSslPort	5223
XmppTimerKeepAliveTime	5

- 2) Change domain, if desired

```
beectl modify_property --component _XmppService \  
--name DomainName --value example.com
```

```
beectl modify_property --component _XmppService \  
--name DomainNames --value example.com
```

- 3) Change ports, if desired:


```
beectl modify_property --component _XmppService \  
--name XmppPort --value 5222  
beectl modify_property --component _XmppService \  
--name XmppSslPort --value 5223
```
- 4) Activate the configuration:


```
beectl activate_configuration  
beectl modify_local_configuration_files
```

Set 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 as follows:

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>` as follows:

```

<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="7779"
  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:

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

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

Appendix A: Terminology for F5 BIG-IP Local Traffic Manager

This appendix discusses the basic terminology to help with discussions in this white paper. For detailed information, see the BIG-IP Solutions Guide and the BIG-IP Configuration Guide at <http://www.f5.com/solutions/resources/deployment-guides/>

The version of BIG-IP software used for the rest of the discussion is BIG-IP Version 10.0.1, Build 283. Terms are identical between Version 9 and 10 of the BIG-IP software, but specific commands may have slightly different syntax.

Pool

A *pool* is a set of nodes grouped together to receive traffic on a specific TCP port using a load balancing method. Each pool can have its own unique characteristic for a persistence definition and the load-balancing algorithm used. The preferred setting of the load balance algorithm for all Beehive pools is Least Connections (Member).

Pools are associated with specific virtual servers directly or by rules (see later). As a result, the traffic coming to a virtual server is directed to one of the associated pools, and ultimately to one of the pool members.

Member

A *member* of the pool is defined as a node, as a destination for traffic, with an IP address and a port definition, expressed as `a.b.c.d:xx`, or 192.168.1.200:80 for a Web server with IP address 192.168.1.200 and listening on port 80. There must be at least two members in every pool to provide high availability. If one of the pool members is unavailable or offline, traffic is sent to the remaining member or members.

Virtual Server

A *virtual server*, with its virtual address and port number, is the client addressable hostname or IP address through which members of a load balancing pool are made available to a client. After a virtual server receives a request, it directs the request to a member of the pool based on a chosen load balancing method. After a virtual server receives traffic, either directly or through a rule, the virtual server can optionally perform a number of different operations, such as inserting or modifying a header into an HTTP request, setting a persistence record, or redirecting the request to another site or fallback destination.

Before creating a virtual server, you must configure a load balancing pool of the actual physical devices (members) you wish to forward the traffic to. You can then create the virtual server, specifying that pool as the destination for any traffic coming from this virtual server. Also, if you want some of the traffic from that virtual server to go to multiple pools based on a pre-determined criterion, then you can create a rule specifying the criteria, and BIG-IP would

forward the traffic to a pool matching the rule's criteria. A virtual server is configured to a specific port or to accept *any* ports.

A given application delivery controller device may contain one or more virtual servers.

Profile

BIG-IP version 9.0 and later uses profiles. 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 connections 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. For example, one HTTP profile could be configured for Internet Explorer browsers, a different profile for Mozilla browsers, and yet another profile for hand held mobile browsers. You would have complete control over all the HTTP options in each profile, to match the characteristics of these different browser types.

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.

Rule

A *rule* is a user-written script that uses criteria to choose among one or more pools. In the BIG-IP software, it is called an iRule. For an incoming request to a virtual server, the iRule is evaluated, and selects the pool to send the request to. F5 iRules provide a powerful and more granular level of control over traffic management. For more information on F5 iRules, see the “[Creating the Beehive Redirect iRule](#)” section in this white paper, and the F5 DevCentral Website [8] at <http://devcentral.f5.com/Default.aspx?tabid=75>.

Monitor

Monitors are used to verify the operational state of pool members. Monitors verify connections and services on nodes that are members of load-balancing pools. A monitor is designed to check the status of a node or service on an ongoing basis, at a set interval. If the node or service being checked does not respond within a specified timeout period, or the status of the node indicates that the performance of the node has degraded, the BIG-IP system automatically takes it out of the pool and chooses the other members of the pool. When the node or service becomes available again, the monitor detects this and the member is automatically accessible to the pool and able to handle traffic. Monitors can be as simple as an ICMP ping to a server's IP address, to a TCP three-way handshake to a service port, or as sophisticated as an HTTP Get Request with parameters, or SSL session negotiation. F5 monitors can also be custom programmed for specific needs.

Persistence

Certain types of applications may require the same client returning to the same pool member, this is called persistence, or “stickiness”. It can be configured using a persistence profile, and applied to the virtual server.

Note: For Oracle Beehive services, you do not need to configure persistence, except for the Beekeeper Administration Console.

Appendix B: Configuring BIG-IP for Beehive to Use SSL Offload

This section describes how to configure the BIG-IP LTM system as an SSL proxy for Beehive Services deployment. 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.

This appendix contains the following information about configuring the BIG-IP system for SSL offload:

- [Prerequisites and Configuration Notes](#)
- [Using SSL certificates and keys](#)
- [Importing certificates and keys](#)
- [Creating a Beehive Client SSL profile](#)
- [Creating the Beekeeper Client SSL profile](#)
- [Creating the Beehive Redirect iRule](#)
- [Configuring Beehive for SSL Termination](#)

Prerequisites and Configuration Notes

This section lists additional prerequisites when using the BIG-IP LTM system for SSL offload:

- You need an SSL certificate for your site that is compatible with the BIG-IP LTM system. For more information, consult the F5 BIG-IP Product Documentation [3].
- 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.

In the MAA example, these two certificates are named `beehive.example.com`, and `beekeeper.example.com`, respectively.

- **Important:** When using the BIG-IP LTM system for SSL offload, for each Beehive Service that will be 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 within the Client SSL profile.

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

device. This white paper assumes that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system.

For information about generating certificates, or using the BIG-IP system to generate a request for a new certificate and key from a certificate authority, see the “Managing SSL Traffic” chapter in the *Configuration Guide for Local Traffic Management*.

Importing Certificates and Keys

Once you have obtained both SSL certificates, you can import these certificates into the BIG-IP LTM system using the **BIG-IP 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** and click **SSL Certificates**.
This displays the list of existing certificates.
2. In the upper right corner of the screen, click **Import**.
3. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
4. In the **Certificate** (or **Key**) **Name** field, enter a unique name for the certificate or key. In the MAA example, we entered **beehive.example.com**.
5. In the **Certificate** (or **Key**) **Source** field, choose to either upload the file or paste the text.
6. Click **Import**.

After you import the certificate, repeat the procedure for the key. Follow the procedure a second time for the **beekeeper.example.com** certificate and key.

Creating the Beehive Client SSL Profile

The next step in this configuration is to create an SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic. This Profile will be used on multiple Beehive services, including IMAPS, SMTPS, FTPS, Beehive HTTP Secure.

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

1. On the Main tab, expand **Local Traffic** and click **Profiles**.
The HTTP Profiles screen opens.
2. On the Menu bar, from the SSL menu, select **Client**.

The Client SSL Profiles screen opens.

3. In the upper right portion of the screen, click **Create**.

The New Client SSL Profile screen opens.

4. In the Name box, type a name for this profile. The MAA example uses `Beehive_clientssl`.
5. In the Configuration section, click to check the Certificate and Key Custom boxes on the far right.
6. From the Certificate list, select the name of the Certificate you imported in the Importing keys and certificates section. The MAA example uses `beehive.example.com`.
7. From the Key list, select the key you imported in the Importing keys and certificates section. The MAA example selected `beehive.example.com`.
8. Click **Finished**.

Local Traffic >> Profiles: SSL: Client >> New Client SSL Profile...

General Properties

Name: Beehive_clientssl

Parent Profile: clientssl

Configuration: Basic

Certificate: beehive.oracle.com

Key: beehive.oracle.com

Options List

Enabled Options

Don't insert empty fragments

Disable

Available Options

Netscape® reuse cipher change bug workaround

Microsoft® big SSLv3 buffer

Microsoft® IE SSLv2 RSA padding

SSLv2 080 client DH bug workaround

TLS D5 bug workaround

Enable

Client Authentication

Client Certificate: ignore

Certificate Revocation List (CRL):

Cancel Repeat Finished

Creating the Beekeeper Client SSL Profile

The next step in this configuration is to create a second SSL profile for the Beekeeper Administrator Console. This SSL profile uses a separate SSL certificate. In our example, the name is **beekeeper.example.com**. This profile contains the SSL certificate and Key information for offloading the SSL traffic. This Profile will be used only on the Beekeeper Secure virtual server.

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

1. On the Main tab, expand **Local Traffic** and click **Profiles**.
The HTTP Profiles screen opens.
2. On the Menu bar, from the SSL menu, select **Client**.
The Client SSL Profiles screen opens.
3. In the upper right portion of the screen, click **Create**.
The New Client SSL Profile screen opens.
4. In the Name field, type a name for this profile. The MAA example uses **Beekeeper_clientssl**.
5. In the Configuration section, click to check the Certificate and Key Custom options on the far right.
6. From the Certificate list, select the name of the Certificate you imported in the [“Importing Certificates and Keys”](#) section. The MAA example uses **beekeeper.example.com**.
7. From the Key list, select the key you imported in the Importing keys and certificates section. The MAA example selected **beekeeper.example.com**.
8. Click **Finished**.

The screenshot shows the 'New Client SSL Profile' configuration window in the F5 BIG-IP interface. The window is titled 'Local Traffic >> Profiles : SSL : Client >> New Client SSL Profile...'. It is divided into several sections:

- General Properties:**
 - Name: beeper_clientssl
 - Parent Profile: clientssl
- Configuration:**
 - Configuration: Basic
 - Certificate: beeper.oracle.com
 - Key: beeper.oracle.com
 - Options List:
 - Enabled Options: Don't insert empty fragments
 - Available Options: Netscape® reuse cipher change bug workaround, Microsoft® big SSLv3 buffer, Microsoft® IE SSLv2 RSA padding, SSLey 080 client DH bug workaround, TLS D5 bug workaround
- Client Authentication:**
 - Client Certificate: ignore
 - Certificate Revocation List (CRL):

At the bottom of the window are three buttons: Cancel, Repeat, and Finished.

For more information about creating or modifying [SSL profiles or SSL Certificates](#), see the BIG-IP documentation set [3].

Creating the Beehive Redirect iRule

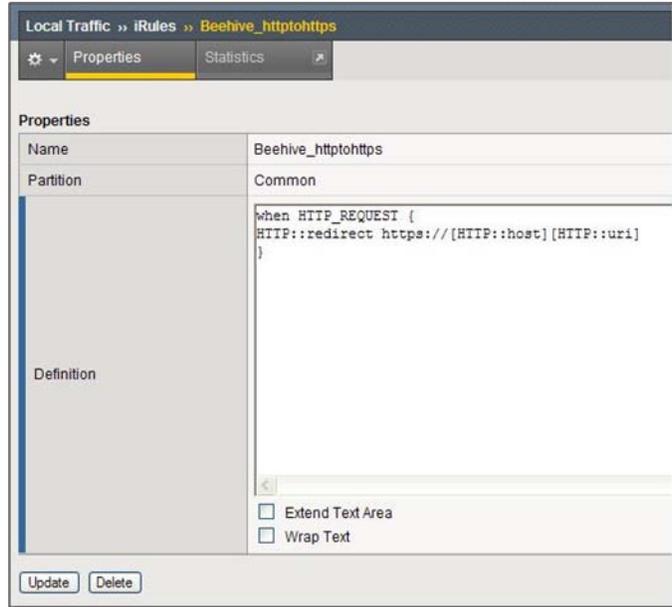
The Redirect iRule takes incoming HTTP requests (non-secure) and redirects the requests to the correct HTTPS (secure) virtual server, without user interaction. This Redirect iRule is used with both the Beehive HTTP service and the Beekeeper HTTP service, to redirect clients to the matching SSL Secured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

The MAA example uses `Beehive_httpstohttps`.

1. In the Definition section, type the iRule exactly as shown in the following screenshot:



2. Click **Finished**.

Configuring Beehive for SSL Termination

1. Set the `SslTerminatedByLoadBalancer` property of the `HttpServerCluster` component to **true**. For example:

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

2. Review the change:

```
beectl> list_properties --component _CURRENT_SITE:HttpServerCluster
-----+-----
Property name          | Property value
-----+-----
Alias                   |
* HttpServerSslEnabled | true
...

```

3. Commit the changes you made to the configuration:

```
beectl modify_local_configuration_files
```

Appendix C: F5 BIG-IP Example Configuration File

This appendix contains the F5 BIG-IP configuration file for the MAA example. The file was generated while following the instructions in this document.

```
monitor mon_bhbeekeeper7779 {
    defaults from http
    interval 30
    timeout 91
    dest *:7779
}
monitor mon_bhbtp21401 {
    defaults from tcp
    interval 30
    timeout 91
    dest *:21401
}
monitor mon_bhftp2121 {
    defaults from ftp
    interval 30
    timeout 91
    dest *:2121
    debug "no"
    get "/Oracle/qa.auto_9's Personal
Workspace/Documents/summary.html"
    password "Welcome1"
    username "qa.auto_9"
}
monitor mon_bhhttp7777 {
    defaults from http
    interval 30
    timeout 91
    dest *:7777
}
monitor mon_bhimap5143 {
    defaults from imap
    dest *:5143
    debug "no"
    password "Welcome1"
    username "qa.auto_9"
}
monitor mon_bhsmtpt2225 {
    defaults from smtp
```

```
    interval 30
    timeout 91
    dest *:2225
    debug "no"
}
monitor mon_bhxmpp5222 {
    defaults from tcp
    interval 30
    timeout 91
    dest *:5222
}
monitor mon_bhxmp5223 {
    defaults from tcp
    interval 30
    timeout 91
    dest *:5223
}
monitor mon_btps5224 {
    defaults from tcp
}
profile clientssl beehive_clientssl {
    defaults from clientssl
    key "beehive.example.com.key"
    cert "beehive.example.com.crt"
    chain none
    passphrase "$M$aE$F3a+ej5GbIDcfNPxjfkQ=="
}
profile clientssl beekeeper_clientssl {
    defaults from clientssl
}
profile persist cookie_beekeeper {
    defaults from cookie
    mode cookie
}
profile tcp tcp_bhbeekeeper7779 {
    defaults from tcp
    idle timeout 1800
}
profile tcp tcp_bhbtp21401 {
    defaults from tcp
    idle timeout 1800
}
profile tcp tcp_bhbtps5224 {
    defaults from tcp
    idle timeout 1800
}
profile tcp tcp_bhftp2121 {
    defaults from tcp
}
```

```
    idle timeout 1800
  }
profile tcp tcp_bhhttp7777 {
  defaults from tcp
  idle timeout 1800
}
profile tcp tcp_bhimap5143 {
  defaults from tcp
  idle timeout 1800
}
profile tcp tcp_bhsntp2225 {
  defaults from tcp
  idle timeout 1800
}
profile tcp tcp_bhxmp5222 {
  defaults from tcp
  idle timeout 1800
}
profile tcp tcp_bhxmps5223 {
  defaults from tcp
  idle timeout 1800
}
node 10.10.10.151{
  screen bhmt01.example.com
}
node 10.10.10.152{
  screen bhmt02.example.com
}
pool pool_bhbeekeeper7779 {
  lb method member least conn
  monitor all mon_bhbeekeeper7779
  members {
    10.10.10.151:7779 {}
    10.10.10.152:7779 {}
  }
}
pool pool_bhbtp21401 {
  lb method member least conn
  monitor all mon_bhbtp21401
  members {
    10.10.10.151:21401 {}
    10.10.10.152:21401 {}
  }
}
pool pool_bhftp2121 {
  lb method member least conn
  monitor all mon_bhftp2121
  members {
```

```
        10.10.10.151:2121 {}
        10.10.10.152:2121 {}
    }
}
pool pool_bhhttp7777 {
    lb method member least conn
    monitor all mon_bhhttp7777
    members {
        10.10.10.151:7777 {}
        10.10.10.152:7777 {}
    }
}
pool pool_bhimap5143 {
    lb method member least conn
    monitor all mon_bhimap5143
    members {
        10.10.10.151:5143 {}
        10.10.10.152:5143 {}
    }
}
pool pool_bhsntp2225 {
    lb method member least conn
    monitor all mon_bhsntp2225
    members {
        10.10.10.151:2225 {}
        10.10.10.152:2225 {}
    }
}
pool pool_bhxmp5222 {
    lb method member least conn
    monitor all mon_bhxmp5222
    members {
        10.10.10.151:5222 {}
        10.10.10.152:5222 {}
    }
}
pool pool_bhxmp5223 {
    lb method member least conn
    monitor all mon_bhxmp5223
    members {
        10.10.10.151:5223 {}
        10.10.10.152:5223 {}
    }
}
pool pool_btps5224 {
    lb method member least conn
    monitor all mon_btps5224
    members {
```

```
        10.10.10.151:5224 {}
        10.10.10.152:5224 {}
    }
}
rule beehive_HTTPtoHTTPS {
    when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
    }
}
virtual vs_bhbeekeeper80 {
    snat automap
    pool pool_bhbeekeeper7779
    destination 139.185.141.35:http
    ip protocol tcp
    rules beehive_HTTPtoHTTPS
    persist cookie_beekeeper
    profiles {
        http {}
        tcp_bhbeekeeper7779 {}
    }
}
virtual vs_bhbeekeeper443 {
    snat automap
    pool pool_bhbeekeeper7779
    destination 139.185.141.35:https
    ip protocol tcp
    profiles {
        beekeeper_clientssl {
            clientside
        }
        http {}
        tcp_bhbeekeeper7779 {}
    }
}
virtual vs_bhbtp21401 {
    snat automap
    pool pool_bhbtp21401
    destination 10.10.10.101:21401
    ip protocol tcp
    profiles tcp_bhbtp21401 {}
}
virtual vs_bhbtps5224 {
    snat automap
    pool pool_btps5224
    destination 10.10.10.101:5224
    ip protocol tcp
    profiles tcp_bhbtps5224 {}
}
```

```
virtual vs_bhftp2121 {
    snat automap
    pool pool_bhftp2121
    destination 10.10.10.101:2121
    ip protocol tcp
    profiles tcp_bhftp2121 {}
}
virtual vs_bhftps990 {
    snat automap
    pool pool_bhftp2121
    destination 10.10.10.101:990
    ip protocol tcp
    profiles {
        beehive_clientssl {
            clientside
        }
        tcp_bhftp2121 {}
    }
}
virtual vs_bhhttp80 {
    snat automap
    pool pool_bhhttp7777
    destination 10.10.10.101:http
    ip protocol tcp
    rules beehive_HTTPtoHTTPS
    profiles {
        http {}
        tcp_bhhttp7777 {}
    }
}
virtual vs_bhhttps443 {
    snat automap
    pool pool_bhhttp7777
    destination 10.10.10.101:https
    ip protocol tcp
    profiles {
        beehive_clientssl {
            clientside
        }
        http {}
        tcp_bhhttp7777 {}
    }
}
virtual vs_bhimap143 {
    snat automap
    pool pool_bhimap5143
    destination 10.10.10.101:imap
    ip protocol tcp
}
```

```
    profiles tcp_bhimap5143 {}
  }
virtual vs_bhimaps993 {
  snat automap
  pool pool_bhimap5143
  destination 10.10.10.101:imaps
  ip protocol tcp
  profiles {
    beehive_clientssl {
      clientside
    }
    tcp_bhimap5143 {}
  }
}
virtual vs_bhsmtp25 {
  snat automap
  pool pool_bhsmtp2225
  destination 10.10.10.101:smtp
  ip protocol tcp
  profiles tcp_bhsmtp2225 {}
}
virtual vs_bhsmtps465 {
  snat automap
  pool pool_bhsmtp2225
  destination 10.10.10.101:smtps
  ip protocol tcp
  profiles {
    beehive_clientssl {
      clientside
    }
    tcp_bhsmtp2225 {}
  }
}
virtual vs_bhxmpp5222 {
  snat automap
  pool pool_bhxmpp5222
  destination 10.10.10.101:5222
  ip protocol tcp
  profiles tcp_bhxmpp5222 {}
}
virtual vs_bhxmp5223 {
  snat automap
  pool pool_bhxmp5223
  destination 10.10.10.101:5223
  ip protocol tcp
  profiles tcp_bhxmp5223 {}
}
```

Appendix D: Beehive Host: Port and URL Summary

[Table 5](#) summarizes the URL's or `hostname:port` number used to set up Beehive clients.

TABLE 5: HOST PORT / URL MAPPING

VIRTUAL SERVER : PORT	PURPOSE
beehive.example.com:143	IMAP Server
beehive.example.com:993	IMAP Secure Server
beehive.example.com:25	SMTP Server
beehive.example.com:465	SMTP Secure Server
beehive.example.com:80	http://beehive.example.com
beehive.example.com:443	https://beehive.example.com
beehive.example.com:21401	OBEO, OBEE, P-IMAP and Web Conferencing
beehive.example.com:5224	OBEO, OBEE, P-IMAP and Web Conferencing Secure Access
beehive.example.com:5222	XMPP
beehive.example.com:5223	XMPP Secure Access
beehive.example.com:21	FTP
beehive.example.com:990	FTPS
beekeeper.example.com:80 http:// beekeeper.example.com/bkpr	Beekeeper
beekeeper.example.com:443 https:// beekeeper.example.com/bkpr	Beekeeper Secure

References

Oracle

1. Oracle Maximum Availability Architecture Web site
<http://www.otn.oracle.com/goto/maa>
2. *Oracle Database High Availability Overview (Part #B14210)*
<http://otn.oracle.com/pls/db111/db111.toc?partno=b28281>
3. *Oracle Database High Availability Best Practices (Part B25159)*
<http://otn.oracle.com/pls/db111/db111.toc?partno=b28282>
4. Oracle Beehive documentation library on OTN
http://download.oracle.com/docs/cd/E14897_01/index.htm

F5 References

1. F5 Networks Home Page
<http://www.f5.com>
2. F5 and Oracle Solutions Home Page
<http://www.f5.com/solutions/applications/oracle/>
3. F5 BIG-IP Product Documentation
<http://www.f5.com/products/big-ip/>
4. F5 Version 10 Software Configuration Guide
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/lm_configuration_guide_10_0_0.html
5. F5 Technical Support Knowledge Base
<https://support.f5.com/kb/en-us.html>
6. F5 and Oracle Cooperative Support Agreement
<http://www.f5.com/news-press-events/press/archive/20050725b.html>
7. F5 Training and Support
<http://www.f5.com/training-support/>
8. F5 DevCentral Web site
<http://devcentral.f5.com/Default.aspx?tabid=75>

ORACLE



Configuring Maximum Availability Architecture
for Beehive with F5 BIG-IP Global and Local
Traffic Manager
March 2010

Author: Ray Dutcher (Oracle), Chris Akker (F5)

Contributing Authors: Sudip Roy,
Frederic Daurelle

Editor: Viv Schupmann

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

0109