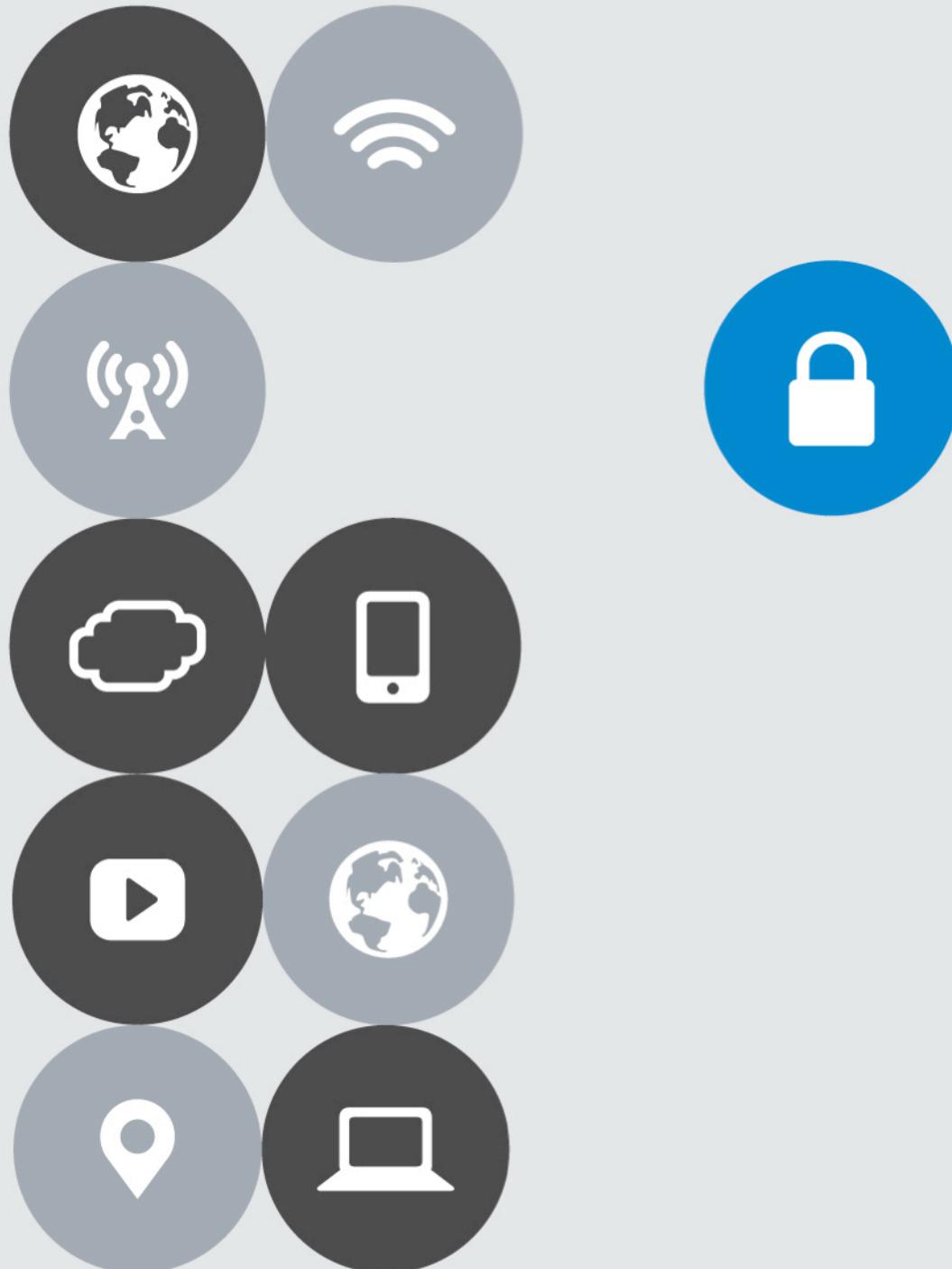




DEPLOYMENT GUIDE

vmware®

Load Balancing VMware Unified Access Gateway



Version History

Date	Version	Author	Description	Compatible Versions
Nov 2017	1.0	Matt Mabis	Initial Document with How-To Configure F5 LTM with VMware Unified Access Gateway (2)	VMware Access Point 2.5.x, 2.7.x, 2.8.x; Unified Access Gateway 2.9.x, 3.0.x (1)

NOTES:

(1) VMware Access Point was the name given to Unified Access gateway prior to 2.9.x Releases, it was changed after 2.9.0 to Unified Access Gateway and the branding will continue to be called Unified Access Gateway moving forward. This document will refer to Unified Access Gateway but is also applicable to VMware Access Point.

(2) This document will be using "Source IP Affinity" as its method for persistence.

(3) Functionality for Blast Extreme UDP is only supported in VMware Unified Access Gateway 3.0.x and above

(4) Functionality for Blast Extreme TCP is supported in VMware Access Point 2.8.0 and above and VMware Unified Access Gateway 3.0.x and above

Table of Contents

Version History	4
Overview.....	6
VMware Horizon Protocols	7
Primary Horizon Protocol	7
Secondary Horizon Protocols.....	7
Prerequisites.....	8
Importing the iApp Template into BIG-IP.....	9
Importing a Certificate into BIG-IP	12
Configuring your Horizon Environment for use with Unified Access Gateway.	14
iRule for the Horizon Origin Header	16
Creating/Deploying a Virtual IP for External Connections	18
Using the iApp to Deploy a Virtual Server for External Unified Access Gateway Servers	19
iApp Additional Configurations for Blast Extreme UDP and BEAT	25
Creating Monitors	25
Creating Pools.....	28
Creating a UDP Protocol Profile.....	30
Creating Virtual Servers.....	31
Final Configuration.....	34
Creating a Virtual Server for Unified Access Gateway Servers.....	35
Creating Monitors	35
Creating Pools.....	39
Creating Profiles	42
Creating Virtual Servers.....	49
Final Configuration.....	62
Testing the VMware Horizon Connection.....	63
References	65

Overview

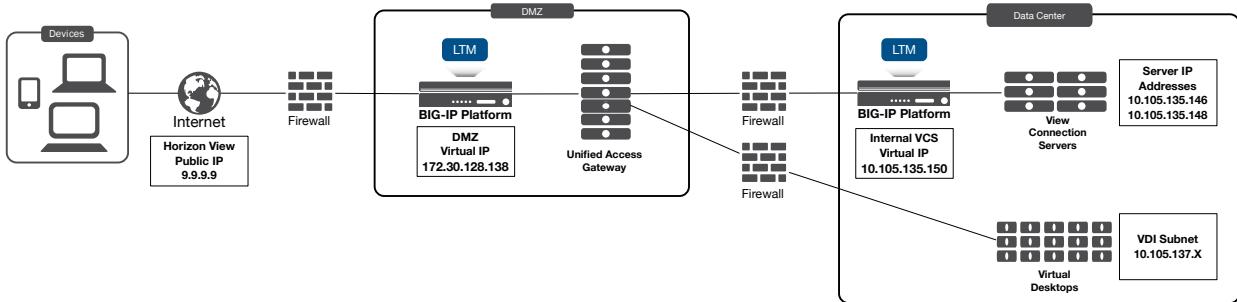


Figure 1 BIG-IP F5 LTM with Unified Access Gateway

VMware Unified Access Gateway (UAG), formerly known as VMware Access Point is an appliance that is typically installed in the demilitarized zone (DMZ). UAG is designed to provide safe and secure access to desktop and application resources for remote access. UAG simplifies gateway access and provides tunneled and proxied resources for the following VMware product suites.

- VMware Horizon (Formerly known as Horizon View)
- VMware Horizon Air (Formerly known as DAAS)
- VMware Horizon Air Hybrid Mode
- VMware Workspace One (Cloud and On-Premise)
- AirWatch Tunnel Gateway/Proxy

Typically, UAG is designed to run in the DMZ as the appliance has the following settings:

- Up-to-date Linux Kernel and software patches
- Multiple NIC support for Internet and Intranet traffic
- Disabled SSH
- Disabled FTP, Telnet, Rlogin, or Rsh services
- Disabled unwanted services

F5's products and solutions bring an improved level of reliability, scalability, and security to UAG deployments. For large Horizon deployments requiring multiple pods or several data centers, F5's products provide the load balancing and traffic management needed to satisfy the requirements of customers around the world. F5 and VMware continue to work together on providing customers best-of-breed solutions that allow for better and faster deployments as well as being prepared for future needs, requirements, and growth.

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

VMware Horizon Protocols

When a Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

Primary Horizon Protocol

The user enters a hostname at the Horizon Client which starts the primary Horizon protocol. This is a control protocol for authentication, authorization, and session management. It uses XML structured messages over HTTPS (HTTP over SSL). This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment as shown in Figure 1, the load balancer routes this connection to one of the UAG appliances. The load balancer usually selects the appliance based first on availability, and then out of the available appliances routes traffic based on the least number of current sessions. This evenly distributes the traffic from different clients across the available set of UAG appliances.

Secondary Horizon Protocols

After the Horizon Client has established secure communication to one of the UAG appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client.

These secondary connections can include:

- HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel (TCP 443).
- Blast Extreme display protocol (TCP 443 and UDP 443).
- PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same UAG appliance to which the primary Horizon protocol was routed. This is so UAG can authorize the secondary protocols based on the authenticated user session. An important security capability of UAG is that it only forwards traffic into the corporate datacenter if the traffic is on behalf of an authenticated user. If the secondary protocols were to be misrouted to a different UAG appliance (different from the one where primary protocols were handled) they would not be authorized and would therefore be dropped in the DMZ and the connection would fail. Misrouting the secondary protocols is a common problem if the load balancer is not configured correctly.

Prerequisites

The following are prerequisites for this solution and must be complete before proceeding with the configuration. Step-by-step instructions for prerequisites are outside the scope of this document, see the BIG-IP documentation on support.f5.com for specific instructions.

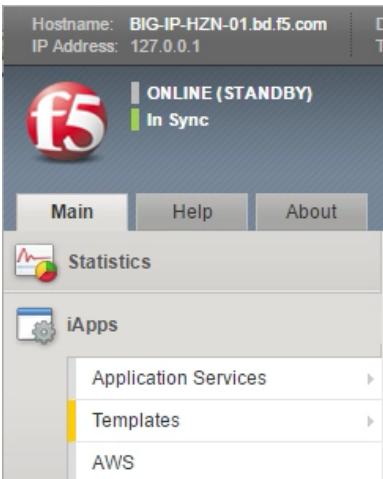
1. F5 recommends running this configuration using BIG-IP LTM version 12.x and 13.x, however it should run on earlier editions of BIG-IP LTM.
2. Create/import an SSL Certificate that contains the load-balanced FQDN that will be used for the Horizon instance.
3. Upload the following to the BIG-IP system:
 - o The SSL certificate.
 - o The Private Key used for the load balanced FQDN certificate.
 - o The Primary CA or Root CA for the SSL Certificate you uploaded to the BIG-IP.
4. Ensure the new FQDN for Horizon is in DNS with both forward and reverse records, and points to the Virtual Server IP address on the BIG-IP that will be used for load balancing the Horizon environment.
5. VMware Horizon deployed and functional within the environment. This includes Horizon Connection Servers, VDI, and Unified Access Gateway Servers.
6. Download the latest F5 iApp templates and extract to an accessible location at
https://downloads.f5.com/esd/ecc.sv?sw=BIG-IP&pro=iApp_Templates&ver=iApps&container=iApp-Templates
7. An internal virtual server configured for Connection Servers - **To create the Virtual IP (VIP) for the Internal Connection Server, refer to the Load Balancing VMware Horizon Connection Servers guide on F5's website.**
8. Firewall ports have been configured for External DMZ Access (Front-End Firewall Rules) and firewall ports have been configured from DMZ to Internal Environment/VDI Network (Back-End Firewall Rules) to allow access to the environment as per VMware KB <https://kb.vmware.com/kb/1027217>.
9. For Single Namespace, internal vs external DNS need to be configured correctly for the Zones (Internet) to point at the Unified Access Gateway Servers Virtual IP (VIP) and the Internal DNS (LAN) would typically point at the Connection Servers Virtual IP (VIP).

Importing the iApp Template into BIG-IP

1. Login to the F5 Configuration utility.



2. On the Main tab, click **iApps > Templates**.



3. Click the **Import** button on the right upper side of the window.

The screenshot shows a table of templates with columns for Name, Validity, Associated Application Services, Verification, Certificate, System-supplied, and Partition / Path. Several templates have warning icons next to them. At the top right of the table, there is a 'Import...' button which is highlighted with a red circle.

Name	Validity	Associated Application Services	Verification	Certificate	System-supplied	Partition / Path
f5.bea_weblogic	None			Yes	Common	
f5.cifs	None		⚠️	Yes	Common	
f5.diameter	None			Yes	Common	
f5.dns	None		⚠️	Yes	Common	
f5.ftp	None		⚠️	Yes	Common	
f5.http	None			Yes	Common	
f5.ip_forwarding	None			Yes	Common	
f5.ldap	None			Yes	Common	
f5.microsoft_is	None			Yes	Common	
f5.microsoft_sharepoint_2010	None			Yes	Common	

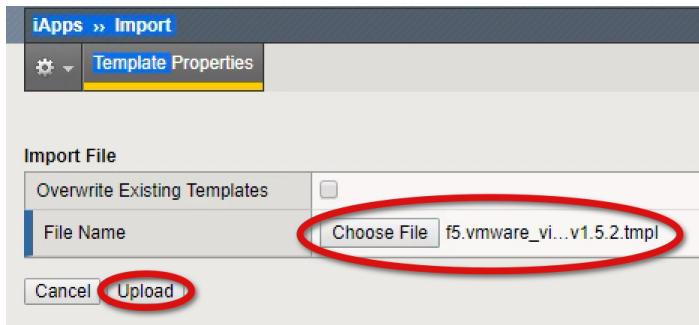
4. Click the **Choose File** button.

The screenshot shows the 'Import File' section of the template properties. It includes an 'Overwrite Existing Templates' checkbox and a 'File Name' input field containing 'f5.vmware_view.v1.5.2.tpl'. Below the input field is a 'Choose File' button, which is highlighted with a red circle.

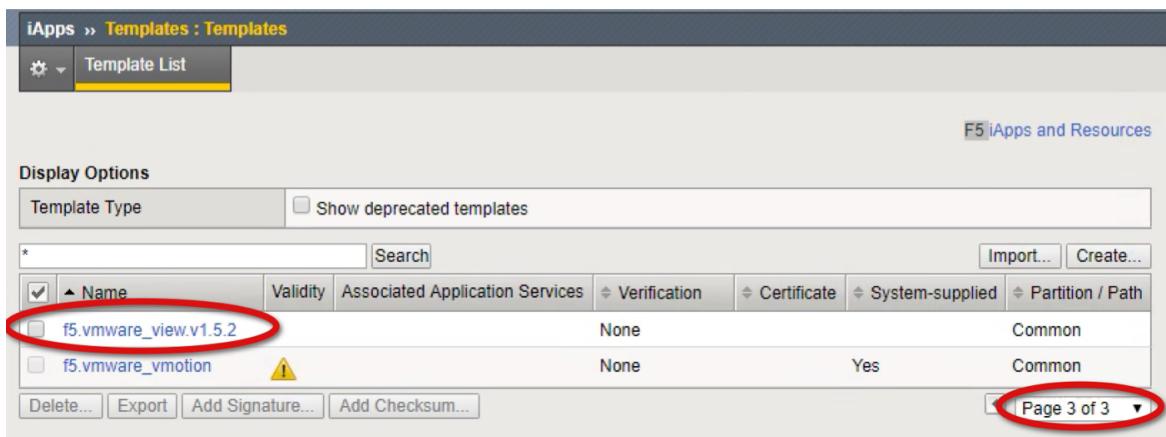
5. Browse to the location where you extracted F5 iApp templates. For more information see the [Prerequisites](#) section.

The screenshot shows a Windows file explorer window with the path 'Downloads > iapps-1.0.0.488.0 > VMware > View'. The 'Downloads' folder is selected. Inside 'Downloads', there are several files: 'Previous Versions', 'f5.vmware_view.v1.5.2.md5', 'f5.vmware_view.v1.5.2 README.txt', and 'f5.vmware_view.v1.5.2.tpl'. The 'f5.vmware_view.v1.5.2.tpl' file is highlighted with a red circle. At the bottom of the window, there is a 'File name:' dropdown and 'Open' and 'Cancel' buttons.

6. Once the TMPL file is selected, the file name appears next to the Choose File button. Once that is correct, click **Upload**.



7. Once the upload is complete ensure the template is available. Depending on your BIG-IP settings, the template is most likely on the last page of the Templates List section.



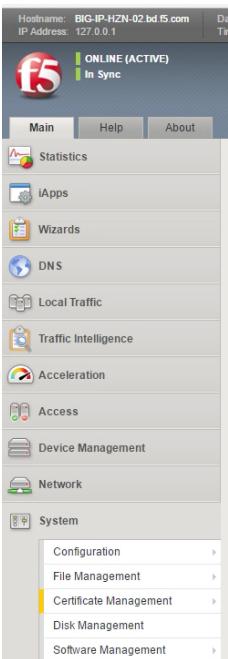
Importing a Certificate into BIG-IP

The next task is to import the certificate onto the BIG-IP.

1. Login to the F5 Configuration utility.



2. On the Main tab click **System > Certificate Management**.



3. Click the **Import** button on the upper right side of the window.



4. Complete the SSL Certificate/Key Source options. In this use case, we are importing a P12/PFX based file to the BIG-IP:

- From the **Import Type** list, select a certificate type.
- In the **Name** field, type a unique name for the certificate.
- Click the **Choose File** button and then locate your certificate file.
- In the **Password** field, type the password to decrypt the key in the file.
- Click **Import**.

SSL Certificate/Key Source	
Import Type	PKCS 12 (IIS) ▾
Certificate Name	<input checked="" type="radio"/> Create New <input type="radio"/> Overwrite Existing Wildcard-Public
Certificate Source	Choose File <input type="file" value="wildcard.bd.f5.com.p12"/>
Password	*****
Key Security	Normal ▾
Free Space on Disk	197 MB
<input type="button" value="Cancel"/> <input type="button" value="Import"/>	

After the import is completed you see your certificate in the window. Click the certificate to verify all the information in it.

			Import...	Create...			
	Status	Name	Contents	Common Name	Organization	Expiration	Partition / Path
MyHZN-InternalCA	Active	MyHZN-InternalCA	RSA Certificate & Key	MyHZN.bd.f5.com		Mar 6, 2019	Common
Wildcard-Public	Active	Wildcard-Public	RSA Certificate & Key	bd.f5.com	F5 Networks Inc	Jul 25, 2018	Common
ca-bundle	Active	ca-bundle	Certificate Bundle			Dec 31, 2029 - Oct 6, 2046	Common
default	Active	default	RSA Certificate & Key	localhost:ca:domain	MyCompany	Feb 13, 2027	Common
f5-inle	Active	f5-inle	RSA Certificate	support.f5.com	F5 Networks	Aug 13, 2031	Common

5. Verify the information in the Certificate/Key.

General Properties	
Name	Wildcard-Public.crt
Partition / Path	Common
Certificate Subject(s)	bd.f5.com, F5 Networks Inc. Entrust Certification Authority - L1K, Entrust, Inc.
<input type="button" value="Import..."/> <input type="button" value="Export..."/> <input type="button" value="Renew..."/> <input type="button" value="Update Status Monitoring"/> <input type="button" value="Delete OCSP Cache..."/> <input type="button" value="Delete"/>	

Certificate Properties	
Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jul 25 2018 18:55:31 GMT
Version	3
Serial Number	8e:ca:62:80:9a:81:bf:b5:00:00:00:00:50:d8:fb:75
Subject	Common Name: bd.f5.com Organization: F5 Networks Inc. Division: See www.entrust.net/legal-terms Locality: Seattle State Or Province: Washington Country: US
Issuer	Common Name: Entrust Certification Authority - L1K Organizational Unit: Entrust, Inc. Division: See www.entrust.net/legal-terms Locality: State Or Province: Country:
Email	Subject Alternative Name: DNS *.bd.f5.com, DNS:bd.f5.com
<input type="button" value="Import..."/> <input type="button" value="Export..."/> <input type="button" value="Renew..."/> <input type="button" value="Update Status Monitoring"/> <input type="button" value="Delete OCSP Cache..."/> <input type="button" value="Delete"/>	

Monitoring Properties	
Monitoring Type	<input type="checkbox"/> OCSP
Issuer Certificate	None
OCSP	+ None
Status	<input checked="" type="checkbox"/>
<input type="button" value="Import..."/> <input type="button" value="Export..."/> <input type="button" value="Renew..."/> <input type="button" value="Update Status Monitoring"/> <input type="button" value="Delete OCSP Cache..."/> <input type="button" value="Delete"/>	

Configuring your Horizon Environment for use with Unified Access Gateway.

1. Login to the VMware Horizon Admin using the FQDN or individual broker webpage.

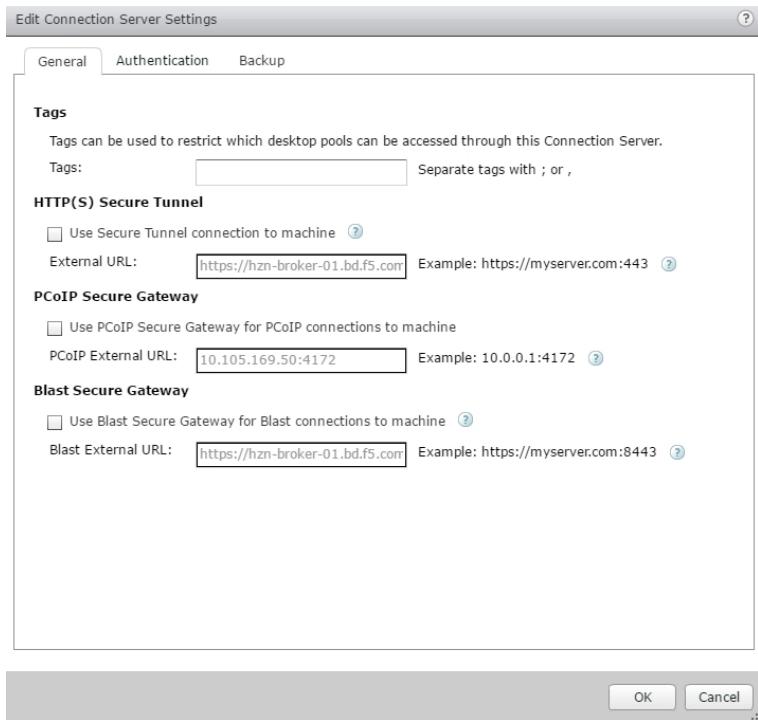
The screenshot shows the VMware Horizon 7 Administrator login interface. It features a blue header with the text "VMware Horizon™ 7 Administrator". On the left, there are three input fields: "User name:", "Password:", and "Domain:". The "Domain:" field contains "BD1". Below these fields is a checkbox labeled "Remember user name". At the bottom right is a blue "Log In" button.

2. In the Horizon Admin Window select a Broker, and then click **Edit**.

The screenshot shows the VMware Horizon 7 Administrator window with the "Servers" tab selected. The left sidebar displays system statistics: Sessions (1), Problem vCenter VMs (0), Problem RDS Hosts (0), Events (0 red, 13 yellow), and System Health (16 green, 0 grey, 0 blue). The main pane shows a table of connection servers:

Connection Server	Version	PCoIP Secure...	State
HZN-BROKER-01	7.0.3-47094	Installed	Enabled
HZN-BROKER-02	7.0.3-47094	Installed	Enabled

3. Ensure that the Checkboxes for **Use Secure Tunnel connection to machine**, **PCoIP Secure Gateway**, and **Use Blast Secure Gateway for Blast connections to machine** are **UNCHECKED**, as having any of these checked will cause connection issues.



4. In the Horizon Admin Window, edit any additional brokers that will be a part of the pool used to connect to the Unified Access Gateway Servers virtual server, and modify them in the same way as Step 3 (ensuring all boxes are unchecked).

Connection Server	Version	PCoIP Secure...	State
HZN-BROKER-01	7.0.3-47094	Installed	Enabled
HZN-BROKER-02	7.0.3-47094	Installed	Enabled

iRule for the Horizon Origin Header

With the release of Horizon 7, a new implementation for accessing the Horizon admin page and HTML5 Blast was added. These changes require an additional implementation done either by the F5 BIG-IP as an iRule, or a configuration that must be done on each Connection Server to allow load balanced configurations to work correctly.

F5 has provided a KB <https://support.f5.com/csp/article/K65620682> for resolution of this issue.

VMware has also provided a KB <https://kb.vmware.com/kb/2144768> for resolution of this issue.

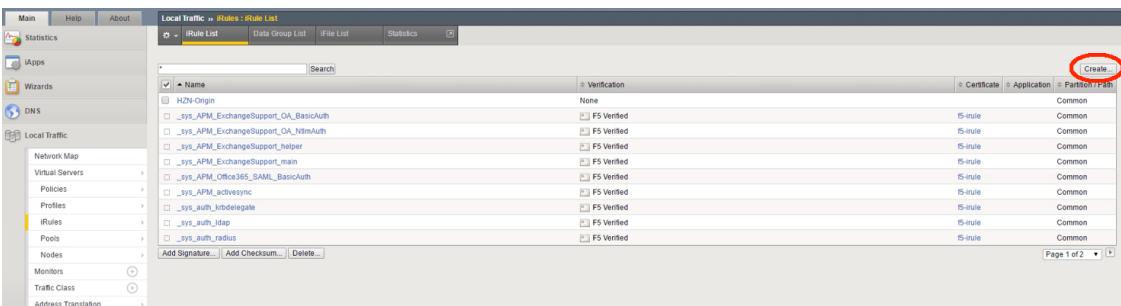
NOTE: Only one of these two methods are necessary.

Implementing an F5 iRule for Horizon Origin Header

1. Login to the BIG-IP Configuration utility.

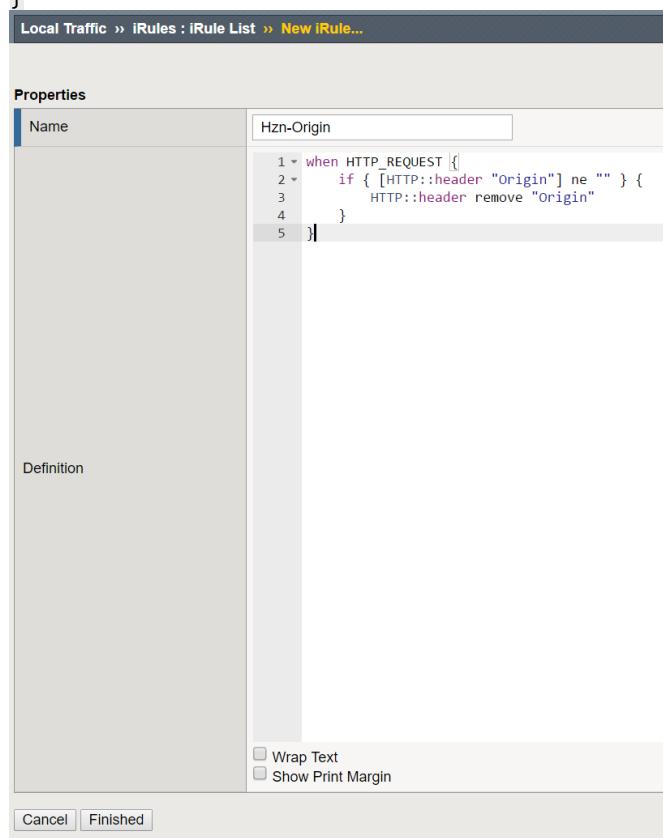


2. On the Main tab, click Local Traffic > iRules and then click Create.



3. In the **Name** field, type a unique name for the iRule.
 4. In the **Description** field, type or copy/paste the following iRule (found in the KB article referenced above):

```
when HTTP_REQUEST {
    if { [HTTP::header "Origin"] ne "" } {
        HTTP::header remove "Origin"
    }
}
```



5. Click **Finished**. Once created you should see your newly created iRule in the list.

Local Traffic » iRules : iRule List	
iRule List	
<input checked="" type="checkbox"/>	Name
<input type="checkbox"/>	None
<input type="checkbox"/>	HZN-Origin
<input type="checkbox"/>	_sys_APM_ExchangeSupport_OA_BasicAuth
<input type="checkbox"/>	_sys_APM_ExchangeSupport_OA_NtlmAuth
<input type="checkbox"/>	_sys_APM_ExchangeSupport_helper
<input type="checkbox"/>	_sys_APM_ExchangeSupport_main
<input type="checkbox"/>	_sys_APM_Office365_SAML_BasicAuth
<input type="checkbox"/>	_sys_APM_activesync
<input type="checkbox"/>	_sys_auth_krbdelegate
<input type="checkbox"/>	_sys_auth_ldap
<input type="checkbox"/>	_sys_auth_radius
Add Signature... Add Checksum... Delete...	

Creating/Deploying a Virtual IP for External Connections

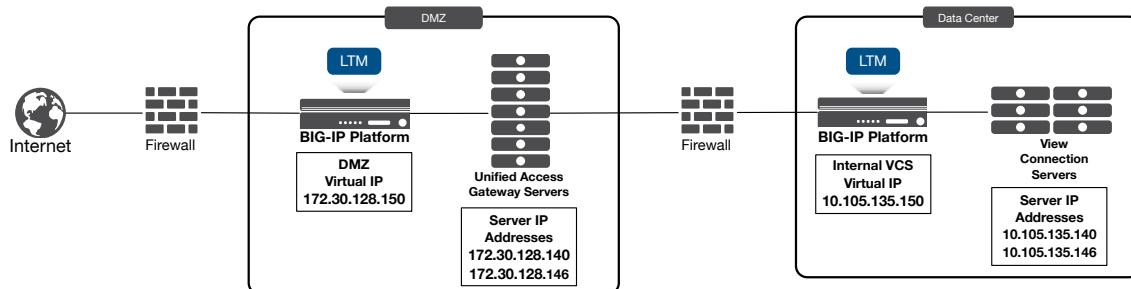


Figure 2 BIG-IP F5 LTM with Unified Access Gateway for External Connections

As part of the workflow, the configuration has LTM placed in the front and behind the Unified Access Gateway (UAG) Servers. This is because in production scenarios, multiple UAG servers require load balancing. Connection servers that manage the Horizon environment in the datacenter must also be load balanced to prevent Single Points of Failure (SPoF).

A load balanced configuration is recommended, and an FQDN configured in DNS must be setup prior to deploying Unified Access Gateway. This ensures the Unified Access Gateway servers can access the load balanced Connection servers to prevent single points of failure.

Use this section to configure the BIG-IP for the UAG Servers for external use.

NOTE: There must be an internal Virtual IP (VIP) for the Horizon Connection Servers prior to configuring the UAG Servers. See Section [Prerequisites](#) for more details.

Using the iApp to Deploy a Virtual Server for External Unified Access Gateway Servers

Before beginning this task, ensure you have previously imported the iApp Template as described in the [Importing iApp Template into BIG-IP](#) section.

Note: The Health Monitor for determining if a UAG node is in Quiesce Mode (Maintenance Mode) is NOT included in the iApp and must be configured manually (with Strict Updates disabled). See [HTTPS - Second Monitor](#) in the Manual Configuration section for instructions on creating the monitor after deploying the iApp.

1. On the Main tab, click **iApps > Application Services > Create**.



2. In the Template Selection section of the template, complete the following.

- a. In the **Name** field, type a unique name.
- b. From the **Template** list, select the template **f5.vmware_view.v1.5.2** (or a newer version if available).

The screenshot shows the 'New Application Service...' dialog. In the 'Template Selection' dropdown, 'Basic' is selected. The 'Name' field contains 'MyHZN-LTM-APM' and the 'Template' dropdown shows 'f5.vmware_view.v1.5.2' selected. Both the 'Name' field and the 'Template' dropdown are circled in red. At the bottom right of the dialog is a 'Create' button.

Welcome to the iApp template for VMware Horizon View

Introduction	Use this template to configure availability, encryption, and remote access for View. This template configures the BIG-IP Local Traffic Manager (LTM) module as well as Access Policy Manager (APM) for environments using VMware Unified Access Gateways (UAGs) in conjunction with Connection Servers or Connection Servers only.
Check for updates	Ensure you are using the most recent template before continuing. Check for newer versions online at https://support.f5.com/kb/en-us/solutions/public/15000/000/so15041.html or DevCentral: https://devcentral.f5.com/wiki/App.VMware-Checkpoints.ashx .
VMware Compatibility	Please follow online support at https://support.f5.com/csp/ttech-documents , select the product 'BIG-IP APM', Release version and only 'Manual' checkbox. And then click 'View Selected'. In the search results, look for BIG-IP APM Client Compatibility Matrix document to view the supported versions.
Prerequisites	Before using this iApp you must ensure that the following prerequisites are met: <ul style="list-style-type: none">The View environment must be fully configured and tested to verify clients are able to access the available Desktops via each View Connection Server or UAG that will be a part of this deployment.Ensure that your Active Directory server is properly configured and all View Clients have the appropriate credentials to access the View environment.Ensure that DNS and NTP servers are properly configured on the BIG-IP system. See the deployment guide or BIG-IP documentation for instructions.If you plan on using this template to configure the BIG-IP system for processing encrypted web traffic (HTTPS), you need to import an SSL certificate and key that correspond to all fully-qualified DNS names that you are using for the HTTPS traffic. Importing SSL certificates and keys is not a part of this template; see System > File Management >> SSL Certificate List.
Additional features available	You do not currently have the BIG-IP Application Visibility Reporting Module (AVR) provisioned on the BIG-IP system. Provisioning AVR (also called Analytics) provides rich application statistics and reporting for your application deployments.

3. In the Template Options section, from the configuration mode question, select **Advanced – configure advanced** options.
4. In the BIG-IP Access Policy Manager section, select **No, do not deploy BIG-IP Access Policy Manager**.

Template Options	
Do you want to see inline help?	Show inline help text
This template offers extensive inline assistance, notes, and configuration tips. We strongly recommend reading the deployment options. Important notes are always shown no matter which selection you make here.	
Which configuration mode do you want to use?	Advanced - configure advanced options
This template supports two configuration modes. Basic mode automatically configures many options, such as user intervention. Advanced mode allows you to review and edit the F5 recommended settings before configuration.	
BIG-IP Access Policy Manager	
Do you want to deploy BIG-IP Access Policy Manager?	No, do not deploy BIG-IP Access Policy Manager
NOTE	
You can use the BIG-IP Access Policy Manager (APM) as a full PCoIP secure gateway proxy, or a DTLS Network View 5.2 or later and the BIG-IP system must be running version 11.4 or later.	
You must have fully licensed the BIG-IP APM to use the APM features in this template.	

5. In the SSL Encryption section, complete the following.
 - a. From the *How should the BIG-IP system handle encrypted traffic?* question, select **Terminate SSL for clients, re-encrypt to View Servers (SSL Bridging)**.
 - b. From the *Which Client SSL profile do you want to use?* question, select **Create a new Client SSL profile**.
 - c. From the *Which SSL certificate do you want to use?* and *Which SSL private key do you want to use?* questions, select the SSL certificate and key you imported in [Importing a Certificate into BIG-IP](#).
 - d. (Optional) If using an Internal CA, we recommend you select an intermediate certificate.

SSL Encryption	
How should the BIG-IP system handle encrypted traffic?	Terminate SSL for clients, re-encrypt to View servers (SSL bridging)
SSL is a cryptographic protocol used to secure client to server communications. Select how you want the BIG-IP system to more accurately persist connections based on granular protocol or application-specific variables. Before encryption between the BIG-IP system and the View servers, select SSL Offload to terminate the SSL session from the client and re-encrypt to the servers (SSL bridging). If security requirements do not allow the BIG-IP system to offload SSL, select to re-encrypt to the servers (SSL bridging).	
Which Client SSL profile do you want to use?	Create a new Client SSL profile
If you have already created an Client SSL profile that includes the appropriate certificate and key, you can select it here.	
Which SSL certificate do you want to use?	Wildcard-Public.crt
To establish encrypted communication, a client and server negotiate security parameters that are used for the session with an authority for authenticity before sending data. When the BIG-IP system is decrypting communication before it is sent to the client, it uses the certificate and key selected here.	
Which SSL private key do you want to use?	Wildcard-Public.key
Select the associated SSL key.	
NOTE:	If your key is password-protected, you must manually create a Client SSL profile outside the iApp, and then select it here.
Which intermediate certificate do you want to use?	Do not use an Intermediate certificate
Intermediate certificates, also called intermediate certificate chains or chain certificates, are used to help verify the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the certificate without having to trust the entire chain. Intermediate certificates must be created or imported onto this BIG-IP system prior to running this iApp. See Importing a Certificate into BIG-IP .	
Do you want to redirect inbound HTTP traffic to HTTPS?	Redirect HTTP to HTTPS
It is common for users to mistakenly attempt insecure access (HTTP) to a secure application (HTTPS). The BIG-IP system automatically handles this redirection.	
From which port should HTTP traffic be redirected?	80
Specify the HTTP port from which you want users redirected. The most common HTTP port is 80.	
Which Server SSL profile do you want to use?	Use F5's recommended Server SSL profile
With SSL Bridging, the BIG-IP system accepts encrypted (HTTPS) traffic from clients, decrypts it for processing, and then re-encrypts it to the View servers. You must have installed and managed certificates on both the servers and the BIG-IP system. Certificates that you install or import for SSL Bridging have different requirements than those that apply to public-facing traffic. You may need to import a certificate or key pair that is specific to the View servers. If you are using an internal CA, you must select an intermediate certificate.	

6. In the PC Over IP section, complete the following.
- From the *Should PCoIP connections go through the BIG-IP system?* question, select **Yes, PCoIP connection should go through the BIG-IP system.**
 - From the *Will PCoIP connections be proxied by the View Security Servers?* question, select **Yes, PCoIP connections are proxied by the VMware UAGs.**
 - From the *Will VMware View HTML 5 client connections go through the BIG-IP system?* question, select **Yes, support HTML 5 View clientless browser connections.**

PC Over IP	
Should PCoIP connections go through the BIG-IP system?	<input type="button" value="Yes, PCoIP connections should go through the BIG-IP system"/>
Will PCoIP connections be proxied by the VMware UAGs?	<input type="button" value="Yes, PCoIP connections are proxied by the VMware UAGs"/>
Will VMware View HTML 5 client connections go through the BIG-IP system?	<input type="button" value="Yes, support HTML 5 View clientless browser connections"/>

7. In the Virtual Servers and Pools section, complete the following.

- Type the IP address for the virtual server.
- Type the FQDN to which external clients will connect with the Horizon Client.

Virtual Servers and Pools	
What virtual server IP address do you want to use for remote, untrusted clients?	<input type="text" value="10.192.192.10"/>
What service port do you want to use for the virtual server(s)?	<input type="text" value="443"/>
What FQDN will clients use to access the View environment?	<input type="text" value="MyHZN.bd.f5.com"/>
Which persistence profile do you want to use?	<input type="button" value="Use F5's recommended persistence profile"/>
Which load balancing method do you want to use?	<input type="button" value="Least Connections (member)"/>
Should the BIG-IP system queue TCP requests?	<input type="button" value="No, do not enable TCP request queuing"/>
Use a Slow Ramp time for newly added servers?	<input type="button" value="Use Slow Ramp"/>

8. Virtual Servers and Pools configuration continued.

- In the *Which servers should be included in this pool* section, type the IP addresses of the nodes for the Unified Access Gateway Servers, and ensure that port 443 is automatically set (if it is set to port 80, then check previous step #3 and make sure **SSL Bridging** is selected and not **SSL Offload**). Click **Add** to include more servers.
- For the next two questions, select the options based on your environment.
- From the *Should the BIG-IP system insert the X-Forwarded-For header?* question, ensure **Yes**, **Insert the X-Forwarded-For HTTP header** is selected.

How many seconds should Slow Ramp time last?	300	Specify the duration (in seconds) for Slow Ramp time (the amount of time the system sends less traffic to a newly-enabled server) is very conservative in most cases.		
Do you want to give priority to specific groups of servers?	Do not use Priority Group Activation			
	Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system sends traffic to the servers in that priority group until the value you specify as the minimum. The BIG-IP system then sends traffic to the group. See the BIG-IP documentation for more details.			
Which servers should be included in this pool?	Node/IP address: 10.105.169.100	Port: 443	Conn limit: 0	X
	Node/IP address: 10.105.169.101	Port: 443	Conn limit: 0	X
	Add			
Where will the virtual servers be in relation to the View servers?	BIG-IP virtual server IP and View servers are on different subnets			
	It is important to ensure that responses to client requests made using the BIG-IP virtual server address are returned directly from the View server, the connection is dropped. The way the BIG-IP system handles this depends on your network configuration.			
	For environments in which the virtual server IP address is on a subnet different from the View servers, select BIG-IP virtual server IP and View servers are on different subnets.			
How have you configured routing on your View servers?	View servers do not have a route to clients through the BIG-IP			
	For environments in which the virtual server IP is on a subnet different from the View servers, information regarding the View server's default gateway is displayed.			
	If the View servers use the BIG-IP system as their default gateway, select View servers have a route for clients through the BIG-IP system.			
	If the View servers do not have a route through the BIG-IP system, select View servers do not have a route for clients through the BIG-IP system. This configuration results in the BIG-IP system replacing the client IP address of an incoming connection with its self IP address (using floating addresses when available), ensuring the server response returns through the BIG-IP system.			
Should the BIG-IP system insert the X-Forwarded-For header?	Yes, Insert the X-Forwarded-For HTTP header			
	If you choose to Insert the X-Forwarded-For header, the BIG-IP system inserts the original client IP address in the HTTP header required on the View server to log the value of the X-Forwarded-For header.			

9. In the Client Optimization section, leave all settings at the defaults.

Client Optimization	
Which Web Acceleration profile do you want to use for caching?	Do not use a Web Acceleration profile
	Caching is the local storage of data for re-use. Once an item is cached on the BIG-IP system, subsequent requests require less processing and reduce load associated with processing subsequent requests.
Which HTTP compression profile do you want to use?	Do not compress HTTP responses
	Compression improves performance and end user experience for Web applications that suffer from WAN latency and bandwidth constraints.
How do you want to optimize client-side connections?	Use F5's recommended optimizations for WAN clients
	The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the client's TCP behavior.

10. In the Server Optimization section, leave all settings at the defaults.

Server Optimization	
Which OneConnect profile do you want to use?	<input type="button" value="Do not use a OneConnect profile"/>
	OneConnect (connection pooling or multiplexing) improves server scalability by reducing load associated with connection which is used to send requests from multiple clients.
How do you want to optimize server-side connections?	<input type="button" value="Use F5's recommended optimizations for the LAN"/>
	The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling

11. In the Application Health section, we recommend you start with the simple health monitor to ensure that basic functionality is working prior to changing to the advanced monitor.

Application Health	
Create a new health monitor or use an existing one?	<input type="button" value="Create a simple health monitor"/>
	Monitors are used to determine the health of the application on each View server. If an application instance does not respond to a health check, the monitor will begin sending requests once the application responds correctly. Simple monitor verifies basic web functionality, and at least one available entitlement pool for the specified user is available. If you have manually created a health monitor, it can be selected here.
How many seconds should pass between health checks?	<input type="text" value="30"/>
	This is the duration, in seconds, of a single monitor cycle. At this interval, the system checks the health of the application.

12. If you created the iRule in [iRule for the Horizon Origin Header](#), from the Options list, select the iRule you created click the Add (<<) button to move it to the Selected list. Using the iRule removes the need to disable the origin header within the servers locked.properties.

Note: If you used the VMware Origin Header method, skip this step.

iRules					
CRITICAL	Improper use or misconfiguration of an iRule can result in unwanted application behavior and poor performance of the application. The BIG-IP system supports a scripting language to allow an administrator to instruct the system to intercept, inspect, and modify data flowing through it, either in the header or payload of a packet.				
	Correct event priority is critical when assigning multiple iRules. For more information about iRule event priority, see iRule Event Priority .				
Do you want to add any custom iRules to this configuration?	<table border="1"> <thead> <tr> <th>Selected</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>/Common HZN-Origin</td> <td><input type="button" value="<<"/></td> </tr> </tbody> </table>	Selected	Options	/Common HZN-Origin	<input type="button" value="<<"/>
Selected	Options				
/Common HZN-Origin	<input type="button" value="<<"/>				

13. In the Statistics and Logging section, leave the defaults and then click the **Finished** button.

Statistics and Logging	
Which HTTP request logging profile do you want to use?	<input type="button" value="Do not enable HTTP request logging"/>
	HTTP request logging enables customizable log messages to be sent to a syslog server for each HTTP request. Request logging profile is not a part of this template. See Local Traffic>>Profiles: Other: Request Log thoroughly tested in a staging environment prior to enabling on a production deployment.
Additional Steps	
Modifying your DNS Settings	You must configure a DNS entry with the fully qualified host name that clients will use to access the View application.
Configuring SSL settings on the servers	Depending on your service and application software, you may have to perform additional steps on your servers to avoid redirect loops and needless redirects. Also, the server software may need to be configured to support SSL.
Configuring the View Servers	You must configure the External URL setting on each View Server to use the IP address (or DNS name) of the View server. See Deployment Guide .
Apply Access Policy	If using BIG-IP APM, you may need to click the 'Apply Access Policy' link (in the upper left corner of the screen).
Troubleshooting	If you have deployed APM for secure network access and you are unable to login, ensure your AD domain is correctly configured.
	You can find common troubleshooting tips in the View 5 Deployment Guide: http://www.f5.com/pdf/deployment-guides/view5-deployment-guide.pdf
<input type="button" value="Cancel"/>	<input type="button" value="Finished"/>

14. After clicking Finished, the summary screen appears. You should see all monitored items with a green Available icon if configured correctly.

Object	Status	Description
MyHZN-LTM-AP	Available	Application Service
MyHZN-LTM-AP_https	Available	Virtual Server
MyHZN-LTM-AP_pool_1	Available	Pool
MyHZN-LTM-AP_https	Available	Monitor
10.105.169.100:443	Available	Pool Member
10.105.169.100	Unknown	Node
10.105.169.101:443	Available	Pool Member
10.105.169.101	Unknown	Node
10.192.192.10	Virtual Address	
MyHZN-LTM-AP_src_addr	Virtual Server Persistence Profile	
MyHZN-LTM-AP_http	Profile	
MyHZN-LTM-AP_server_ssl	Profile	
MyHZN-LTM-AP_client_ssl	Profile	
Wildcard-Public.key	Certificate Key File	
Wildcard-Public.crt	Certificate File	
Wildcard-Public	clients1_certkeychain	
Wildcard-Public.crt	Certificate File	
Wildcard-Public.key	Certificate Key File	
MyHZN-LTM-AP_lan_optimized_tcp	Profile	
MyHZN-LTM-AP_wan_optimized_tcp	Profile	
HZN-Origin	iRule	
MyHZN-LTM-AP_redirect	Unknown	Virtual Server
10.192.192.10	Virtual Address	
MyHZN-LTM-AP_http	Profile	
MyHZN-LTM-AP_wan_optimized_tcp	Profile	
MyHZN-LTM-AP_lan_optimized_tcp	Profile	
_sys_https_redirect	iRule	
15-rule.crt	Certificate File	
MyHZN-LTM-AP_tcp	Available	Virtual Server
MyHZN-LTM-AP_pcoip_pool	Available	Pool
MyHZN-LTM-AP_tcp	Monitor	
MyHZN-LTM-AP_udp	Monitor	
10.105.169.100:4172	Pool Member	
10.105.169.100	Node	
10.105.169.101:4172	Pool Member	
10.105.169.101	Node	
10.192.192.10	Virtual Address	
MyHZN-LTM-AP_src_addr	Virtual Server Persistence Profile	
MyHZN-LTM-AP_lan_optimized_tcp	Profile	
MyHZN-LTM-AP_wan_optimized_tcp	Profile	
MyHZN-LTM-AP_udp	Available	Virtual Server
MyHZN-LTM-AP_pcoip_pool	Available	Pool
MyHZN-LTM-AP_tcp	Monitor	
MyHZN-LTM-AP_udp	Monitor	
10.105.169.100:4172	Pool Member	
10.105.169.100	Node	
10.105.169.101:4172	Pool Member	
10.105.169.101	Node	
10.192.192.10	Virtual Address	
MyHZN-LTM-AP_src_addr	Virtual Server Persistence Profile	
MyHZN-LTM-AP_udp_profile	Profile	
MyHZN-LTM-AP_html5	Available	Virtual Server
MyHZN-LTM-AP_html5_pool	Available	Pool
MyHZN-LTM-AP_tcp	Monitor	
10.105.169.100:8443	Pool Member	
10.105.169.100	Node	
10.105.169.101:8443	Pool Member	
10.105.169.101	Node	
10.192.192.10	Virtual Address	
MyHZN-LTM-AP_src_addr	Virtual Server Persistence Profile	
MyHZN-LTM-AP_lan_optimized_tcp	Profile	
MyHZN-LTM-AP_wan_optimized_tcp	Profile	

Buttons at the bottom: Enable, Disable, Force Offline, Refresh.

iApp Additional Configurations for Blast Extreme UDP and BEAT

The current builds of the iApp v1.5.2 and lower do not have the Blast Extreme UDP enabled ports. These instructions allow you to add the additional Monitors, Pools, Profiles, and Virtual Servers necessary to make Blast Extreme UDP with BEAT (Blast Extreme Adaptive Transport) work.

Creating Monitors

TCP (Blast Extreme) - Monitor

1. Create a simple monitor for TCP (HTML5) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, select **TCP**.
 - d. Ensure the Parent Monitor is **tcp**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. Leave all other settings at the default and then click **Finished**.

General Properties	
Name	MyHZN-LTM-AP_BE_TCP
Description	
Type	TCP
Parent Monitor	tcp
Configuration: Basic	
Interval	30 seconds
Timeout	91 seconds
Send String	
Receive String	
Receive Disable String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	*
Adaptive	<input type="checkbox"/> Enabled
Cancel Repeat Finished	

UDP (Blast Extreme) - Monitor

1. Create a simple monitor for UDP (PCoIP) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, select **UDP**.
 - d. Ensure the Parent Monitor is **udp**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. In the **Send String** field, type (or copy and paste):
default send string
 - h. Leave all other settings at the default and then click **Finished**.

General Properties

Name	MyHZN-LTM-AP_BE_UDP
Description	
Type	UDP
Parent Monitor	udp

Configuration: Basic

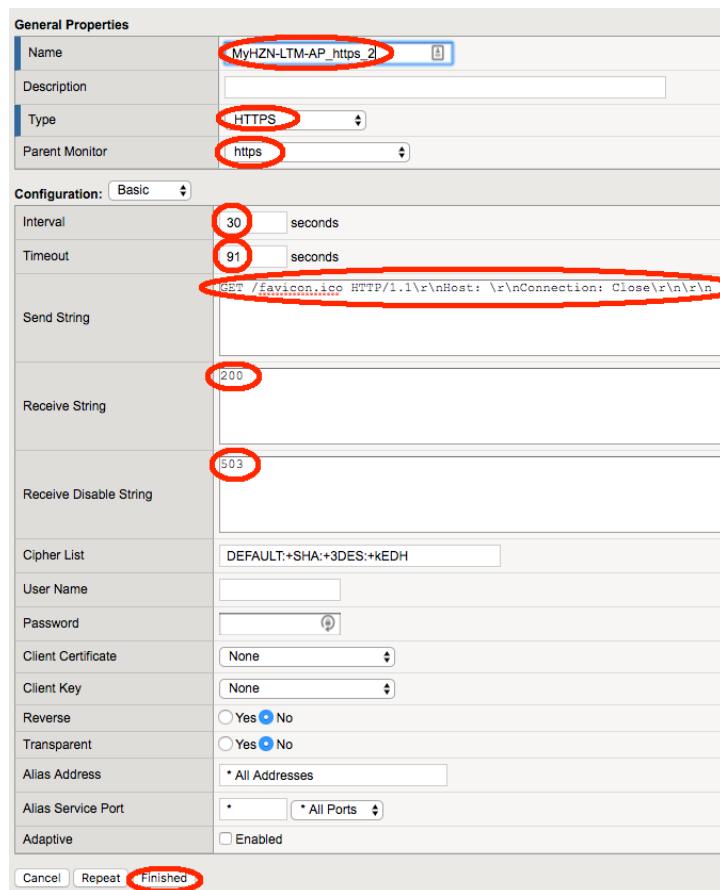
Interval	30	seconds
Timeout	91	seconds
Send String	default send string	
Receive String		
Receive Disable String		
Reverse	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Alias Address	* All Addresses	
Alias Service Port	*	* All Ports
Adaptive	<input type="checkbox"/> Enabled	

Buttons: Cancel Repeat **Finished**

HTTPS – Second Monitor

This monitor is used to identify when the UAG Node is in Quiesce Mode (Maintenance)

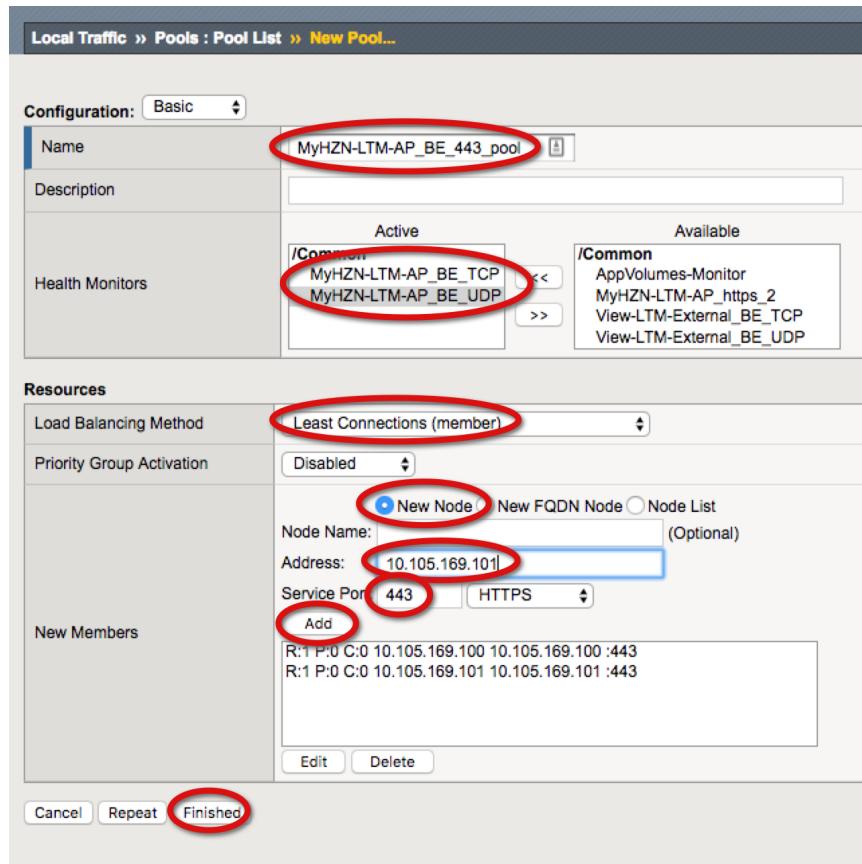
1. Create a simple HTTPS monitor using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name (different from the first).
 - c. From the **Type** list, select **HTTPS**.
 - d. Ensure the Parent Monitor is **https**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. In the **Send String** field, type (or copy and paste):
GET /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
 - h. In the **Receive String** field, type **200**
 - i. in the **Receive Disable String** field, type **503**
 - j. Leave all other settings at the default and then click **Finished**.



Creating Pools

UDP 443 (Blast Extreme) – Pool

1. Create a pool of servers for HTTPS, using the following guidance.
 - a. On the Main tab, click **Local Traffic > Pools > Create**.
 - b. In the **Name** field, type a unique name.
 - c. In the **Health Monitors** area, select the TCP and UDP monitor you created in the previous section and then click the Add (<<) button to move it to Active.
 - d. From the **Load Balancing Method** list, select **Least Connections (member)**.
 - e. In the **New Members** area, complete the following.
 - i. Click the **New Node** button.
 - ii. (Optional) In the **Node Name** field, type a name for the node.
 - iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
 - iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (443).
 - v. Click the **Add** button.
 - vi. Repeat Steps ii – v for additional Unified Access Gateway Servers.
- f. Click **Finished**.



The screenshot shows the 'New Pool...' configuration dialog for a UDP 443 pool. Key fields and settings highlighted with red circles are:

- Name:** MyHZN-LTM-AP_BE_443_pool
- Health Monitors:** MyHZN-LTM-AP_BE_TCP, MyHZN-LTM-AP_BE_UDP (selected)
- Load Balancing Method:** Least Connections (member)
- New Members:** Address: 10.105.169.101, Service Port: 443
- Buttons:** Cancel, Repeat, **Finished**

UDP 8443 (Blast Extreme) – Pool

1. Create a pool of servers for HTTPS, using the following guidance.
 - a. On the Main tab, click **Local Traffic > Pools > Create**.
 - b. In the **Name** field, type a unique name.
 - c. In the **Health Monitors** area, select the TCP and UDP monitor you created in the previous section and then click the Add (<<) button to move it to Active.
 - d. From the **Load Balancing Method** list, select **Least Connections (member)**.
 - e. In the **New Members** area, complete the following.
 - i. Click the **New Node** button.
 - ii. (Optional) In the **Node Name** field, type a name for the node.
 - iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
 - iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (8443).
 - v. Click the **Add** button.
 - vi. Repeat Steps ii – v for additional Unified Access Gateway Servers.
- f. Click **Finished**.

The screenshot shows the configuration of a pool named "MyHZN-LTM-AP_BE_8443_pool". The "Health Monitors" section displays two selected monitors: "MyHZN-LTM-AP_BE_TCP" and "MyHZN-LTM-AP_BE_UDP". The "Load Balancing Method" is set to "Least Connections (member)". A new member is being added with the address "10.105.169.101" and service port "8443". The "Resources" section indicates the configuration is set to "Basic". The bottom navigation bar includes "Cancel", "Repeat", and "Finished" buttons, with "Finished" circled in red.

Creating a UDP Protocol Profile

1. Create an UDP profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Protocol > UDP > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **udp** is selected.
 - d. Leave all other settings at the default and then click **Finished**.

General Properties	
Name	MyHZN-LTM-AP_E
Parent Profile	udp

Settings	
Proxy Maximum Segment	<input type="checkbox"/>
Idle Timeout	Specify... 60 seconds
IP ToS	Specify... 0
Link QoS	Specify... 0
Datagram LB	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>
TTL Mode	Proxy
Don't Fragment Mode	PMTU

Cancel **Repeat** **Finished**

Creating Virtual Servers

Blast Extreme 443 UDP - Virtual Server

1. Create an Blast Extreme 443 UDP virtual server using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **443** or select **HTTP** from the list.

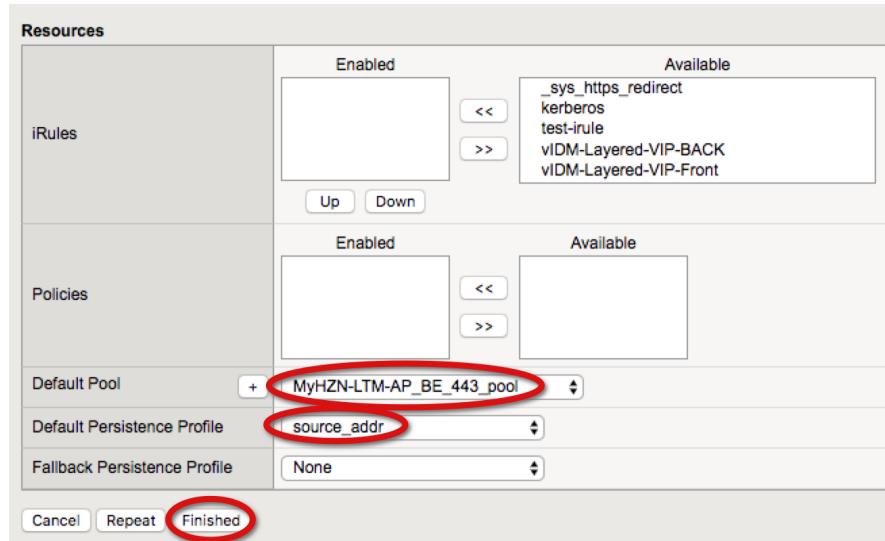
General Properties	
Name	MyHZN-LTM-AP_443_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **UDP**.
- g. From the **Protocol Profile (Client)** list, select the UDP Profile you created in the previous section
- h. From the **Protocol Profile (Server)** list, select **(Use Client Profile)**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic	
Protocol	UDP
Protocol Profile (Client)	MyHZN-LTM-AP_BE_udp_profile
Protocol Profile (Server)	(Use Client Profile)
SSL Profile (Client)	
SSL Profile (Server)	
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Netflow Profile	None <small> Warning: This feature is not enabled by the current license.</small>
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Creating a virtual server (continued)

- j. From the **Protocol Profile (Client)** list, select the 443 Pool you created in the previous section.
- k. From the **Default Persistence Profile** list, select **source_addr**.
- l. Leave all other settings at the defaults and then click **Finished**.



Blast Extreme 443 UDP - Virtual Server

1. Create an HTTP Redirect virtual server using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **443** or select **HTTP** from the list.

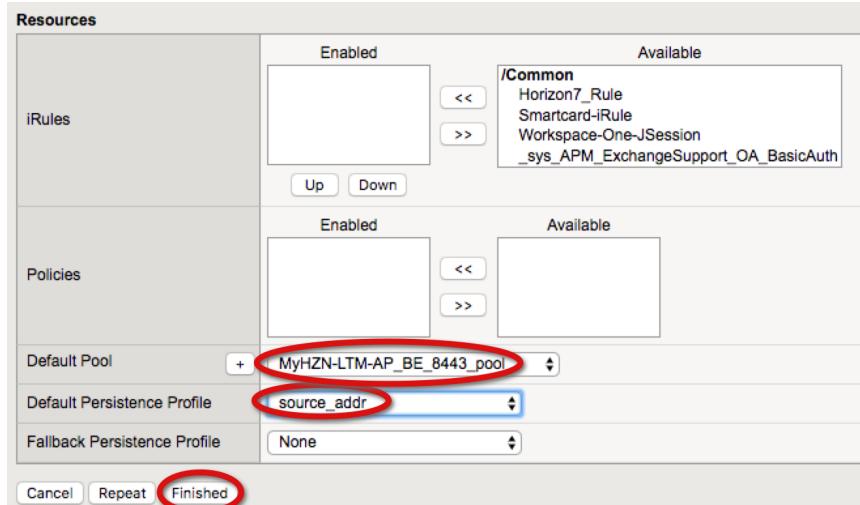
General Properties	
Name	MyHZN-LTM-AP_8443_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	8443
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **UDP**.
- g. From the **Protocol Profile (Client)** list, select the UDP Profile you created in the previous section
- h. From the **Protocol Profile (Server)** list, select **(Use Client Profile)**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic					
Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_BE_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL</td> </tr> </table>	Selected	Available		/Common AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL
Selected	Available				
	/Common AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL				
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common AppVolumes-ServersSSL am-default-serverssl crypto-client-default-serverssl pcip-default-serverssl</td> </tr> </table>	Selected	Available		/Common AppVolumes-ServersSSL am-default-serverssl crypto-client-default-serverssl pcip-default-serverssl
Selected	Available				
	/Common AppVolumes-ServersSSL am-default-serverssl crypto-client-default-serverssl pcip-default-serverssl				
SMTPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Netflow Profile	None <small> Warning: This feature is not enabled by the current license.</small>				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

Creating a virtual server (continued)

- j. From the **Protocol Profile (Client)** list, select the 443 Pool you created in the previous section.
- k. From the **Default Persistence Profile** list, select **source_addr**.
- l. Leave all other settings at the defaults and then click **Finished**.



Final Configuration

Once completed, the mixture of the iApp configuration and the additional virtual servers allow for the full configuration for F5 LTM with VMware Horizon Unified Access Gateway (UAG) for PCoIP and Blast Extreme TCP/UDP with BEAT (Blast Extreme Adaptive Transport).

Local Traffic >> Virtual Servers : Virtual Server List							
		Virtual Server List		Virtual Address List		Statistics	
<input checked="" type="checkbox"/>		Name	Description	Application	Destination	Service Port	Type
Status	▲ Name						Resources Partition / Path
<input type="checkbox"/>	● MyHZN-LTM-AP_443_UDP			10.192.192.10	443 (HTTPS)	Standard	Edit... Common
<input type="checkbox"/>	● MyHZN-LTM-AP_8443_UDP			10.192.192.10	8443	Standard	Edit... Common
<input type="checkbox"/>	● MyHZN-LTM-AP_html5	MyHZN-LTM-AP		10.192.192.10	8443	Standard	Edit... Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	● MyHZN-LTM-AP_https	MyHZN-LTM-AP		10.192.192.10	443 (HTTPS)	Standard	Edit... Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	■ MyHZN-LTM-AP_redirect	MyHZN-LTM-AP		10.192.192.10	80 (HTTP)	Standard	Edit... Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	● MyHZN-LTM-AP_tcp	MyHZN-LTM-AP		10.192.192.10	4172	Standard	Edit... Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	● MyHZN-LTM-AP_udp	MyHZN-LTM-AP		10.192.192.10	4172	Standard	Edit... Common/MyHZN-LTM-AP.app

At the bottom of the table, there are buttons for 'Enable', 'Disable', and 'Delete...'. The 'Virtual Server List' tab is currently selected.

Creating a Virtual Server for Unified Access Gateway Servers

Creating Monitors

HTTPS - Monitor

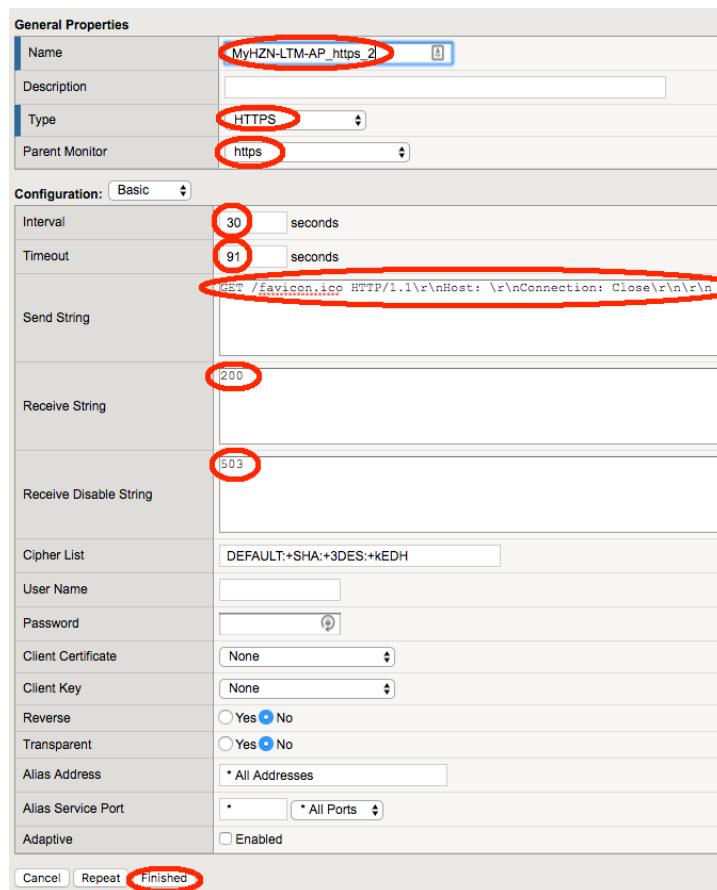
1. Create a simple HTTPS monitor using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, select **HTTPS**.
 - d. Ensure the Parent Monitor is **https**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. In the **Send String** field, type (or copy and paste):
GET /broker/xml/ HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
 - h. In the **Receive String** field, type **clientlaunch-default**.
 - i. Leave all other settings at the default and then click **Finished**.

The screenshot shows the 'New Monitor...' dialog box under the 'Local Traffic > Monitors' path. The 'General Properties' section is visible, showing the monitor's name as 'MyHZN-LTM-AP_https', type as 'HTTPS', and parent monitor as 'https'. The 'Configuration' section is set to 'Basic'. The 'Send String' field contains the value 'GET /broker/xml/ HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n'. The 'Receive String' field contains the value 'clientlaunch-default'. The 'Receive Disable String' field is empty. Other sections like 'Cipher List', 'User Name', 'Password', and 'Client Certificate' are also present but not filled. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons, with 'Finished' being highlighted.

HTTPS – Second Monitor

This monitor is used to identify when the Node is in Quiesce Mode (Maintenance)

1. Create a simple HTTPS monitor using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name (different from the first).
 - c. From the **Type** list, select **HTTPS**.
 - d. Ensure the Parent Monitor is **https**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. In the **Send String** field, type (or copy and paste):
GET /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
 - h. In the **Receive String** field, type **200**
 - i. in the **Receive Disable String** field, type **503**
 - j. Leave all other settings at the default and then click **Finished**.



TCP (PCoIP/Blast) - Monitor

1. Create a simple monitor for TCP (PCoIP/Blast) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, select **TCP**.
 - d. Ensure the Parent Monitor is **tcp**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. Leave all other settings at the default and then click **Finished**.

General Properties

Name	MyHZN-LTM-AP_tcp
Description	
Type	TCP
Parent Monitor	tcp
Configuration: Basic	
Interval	30 seconds
Timeout	91 seconds
Send String	
Receive String	
Receive Disable String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	*
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat **Finished**

UDP (PCoIP/Blast) - Monitor

1. Create a simple monitor for UDP (PCoIP/Blast) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Monitors > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, select **UDP**.
 - d. Ensure the Parent Monitor is **udp**.
 - e. In the **Interval** field, type **30**.
 - f. In the **Timeout** field, type **91**.
 - g. In the **Send String** field, type (or copy and paste):
default send string
 - h. Leave all other settings at the default and then click **Finished**.

General Properties

Name	MyHZN-LTM-AP_udp
Description	
Type	UDP
Parent Monitor	udp
Configuration:	Basic
Interval	30 seconds
Timeout	91 seconds
Send String	default send string
Receive String	
Receive Disable String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	*
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat **Finished**

Creating Pools

Port 443 - Pool

1. Create a pool of servers for Port 443, using the following guidance.
 - a. On the Main tab, click **Local Traffic > Pools > Create**.
 - b. In the **Name** field, type a unique name.
 - c. In the **Health Monitors** area, select all of the monitors created previously (https, https_2, tcp, udp) and then click the Add (<<) button to move them to Active.
 - d. From the **Load Balancing Method** list, select **Least Connections (member)**.
 - e. In the **New Members** area, complete the following.
 - i. Click the **New Node** button.
 - ii. (Optional) In the **Node Name** field, type a name for the node.
 - iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
 - iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (443).
 - v. Click the **Add** button.
 - vi. Repeat Steps ii – v for additional Unified Access Gateway Servers.
- f. Click **Finished**.

The screenshot shows the configuration dialog for creating a pool. Key fields and sections highlighted with red circles include:

- Name:** MyHZN-LTM-AP_443
- Health Monitors:** Common monitors (MyHZN-LTM-AP_https, MyHZN-LTM-AP_https_2, MyHZN-LTM-AP_udp, MyHZN-LTM-AP_tcp) moved to Active, and available monitors (/Common monitors: AppVolumes-Monitor, View-LTM-External_BE_TCP, View-LTM-External_BE_UDP, gateway_icmp).
- Resources:** Load Balancing Method set to Least Connections (member).
- New Members:** A new node is being added with Address 10.105.169.101 and Service Port 443. The 'Add' button is highlighted.
- Bottom Buttons:** Cancel, Repeat, and Finished (highlighted).

Port 8443 - Pool

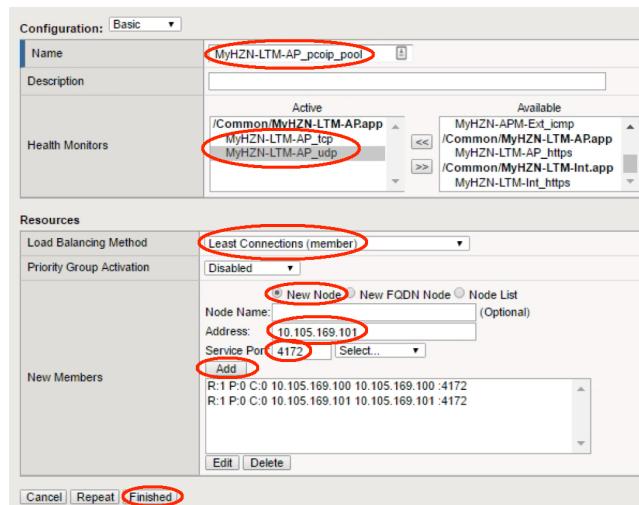
1. Create a pool of servers for Port 8443 using the following guidance.
 - a. On the Main tab, click **Local Traffic > Pools > Create**.
 - b. In the **Name** field, type a unique name.
 - c. In the **Health Monitors** area, select the TCP and UDP monitor you created previously and then click the Add (<<) button to move it to Active.
 - d. From the **Load Balancing Method** list, select **Least Connections (member)**.
 - e. In the New Members area, complete the following.
 - i. Click the **New Node** button.
 - ii. (Optional) In the **Node Name** field, type a name for the node.
 - iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
 - iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (8443).
 - v. Click the **Add** button.
 - vi. Repeat Steps ii – v for additional Unified Access Gateway Servers.
- f. Click **Finished**.

The screenshot shows the configuration dialog for creating a pool. Key fields and sections highlighted with red circles include:

- Name:** MyHZN-LTM-AP_8443
- Health Monitors:** /Common MyHZN-LTM-AP_tcp, /Common MyHZN-LTM-AP_udp (selected and moved to Active)
- Load Balancing Method:** Least Connections (member)
- New Members:** Address: 10.105.169.101, Service Port: 8443 (highlighted)
- Bottom Buttons:** Cancel, Repeat, Finished

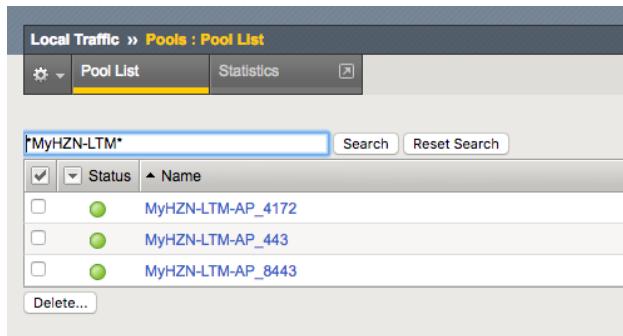
Port 4172 - Pool

1. Create a Pool of servers for Port 4172 using the following guidance.
 - a. On the Main tab, click **Local Traffic > Pools > Create**.
 - b. In the **Name** field, type a unique name.
 - c. In the **Health Monitors** area, select the TCP and UDP monitor you created previously and then click the Add (<<) button to move it to Active.
 - d. From the **Load Balancing Method** list, select **Least Connections (member)**.
 - e. In the New Members area, complete the following.
 - i. Click the **New Node** button.
 - ii. (Optional) In the **Node Name** field, type a name for the node.
 - iii. In the **Address** field, type the IP address of a Unified Access Gateway Server.
 - iv. In the **Service Port** field, type the port of the Unified Access Gateway Server (4172).
 - v. Click the **Add** button.
 - vi. Repeat Steps ii – v for additional Unified Access Gateway Servers.
- f. Click **Finished**.



Validate Pools Online

After a few minutes ensure all the statuses are green on the Pool Objects with the monitors to ensure that the Unified Access Gateway (UAG) Servers are online and functioning appropriately.



Creating Profiles

Creating a HTTP Profile

1. Create an HTTP profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Services > HTTP > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **http** is selected.
 - d. From the **Redirect Rewrite** row, click the **Custom** checkbox on the right, and then select **Matching** from the list.
 - e. From the **Insert X-Forwarded-For** row, click the **Custom** box and then select **Enabled**.
 - f. Leave all other settings at the default and then click **Finished**.

The screenshot shows the 'New HTTP Profile' configuration dialog. The 'General Properties' section includes fields for Name (MyHN-LTM-Int_h), Proxy Mode (Reverse), and Parent Profile (http). The 'Settings' section contains numerous options, many of which have been highlighted with red circles:

- Basic Auth Realm (disabled)
- Fallback Host (disabled)
- Fallback on Error Codes (disabled)
- Request Header Erase (disabled)
- Request Header Insert (disabled)
- Response Headers Allowed (Preserve)
- Request Chunking (Selective)
- Response Chunking (Enabled)
- OneConnect Transformations (Enabled)
- Redirect Rewrite (Matching)
- Encrypt Cookies (disabled)
- Cookie Encryption Passphrase (disabled)
- Confirm Cookie Encryption Passphrase (disabled)
- Insert X-Forwarded-For (Enabled)
- LWS Maximum Columns (80)
- LWS Separator (disabled)
- Maximum Requests (0)
- Send Proxy Via Header In Request (Preserve)
- Send Proxy Via Header In Response (Preserve)
- Accept XFF (disabled)
- XFF Alternative Names (disabled)
- Server Agent Name (BigIP)

At the bottom of the dialog, there are 'Cancel' and 'Repeat' buttons, and a prominent 'Finished' button which is also circled in red.

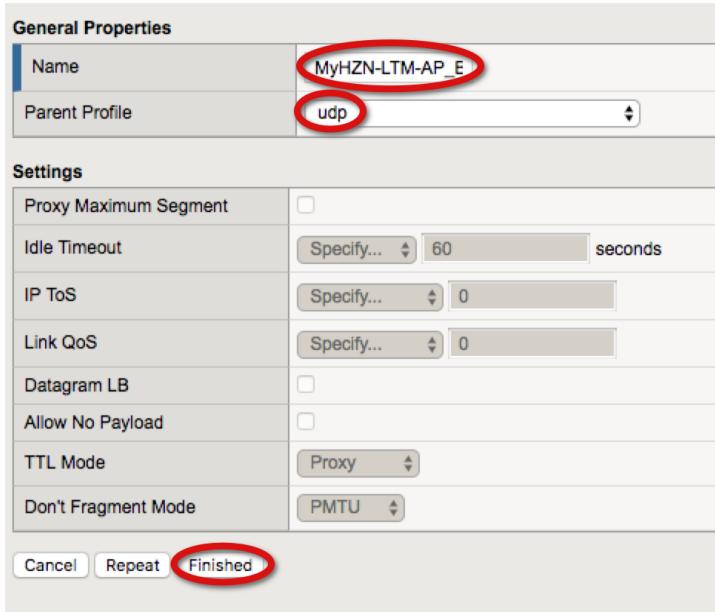
Creating a UDP Protocol Profile

1. Create an UDP profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Protocol > UDP > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **udp** is selected.
 - d. Leave all other settings at the default and then click **Finished**.

General Properties	
Name	MyHZN-LTM-AP_E
Parent Profile	udp

Settings	
Proxy Maximum Segment	<input type="checkbox"/>
Idle Timeout	Specify... 60 seconds
IP ToS	Specify... 0
Link QoS	Specify... 0
Datagram LB	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>
TTL Mode	Proxy
Don't Fragment Mode	PMTU

Cancel **Repeat** **Finished**



Creating a TCP-WAN-Optimized Profiles

1. Create an TCP profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Protocol > TCP > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **tcp-wan-optimized** is selected.
 - d. Leave all other settings at the default and then click **Finished**.

The screenshot shows the 'General Properties' dialog box. It has two main sections: 'Name' and 'Parent Profile'. The 'Name' field contains 'MyHZN-LTM-AP' and the 'Parent Profile' dropdown menu is set to 'tcp-wan-optimized'. Both the 'Name' field and the 'Parent Profile' dropdown are circled in red. At the bottom of the dialog, there are three buttons: 'Cancel', 'Repeat', and 'Finished', with 'Finished' also circled in red.

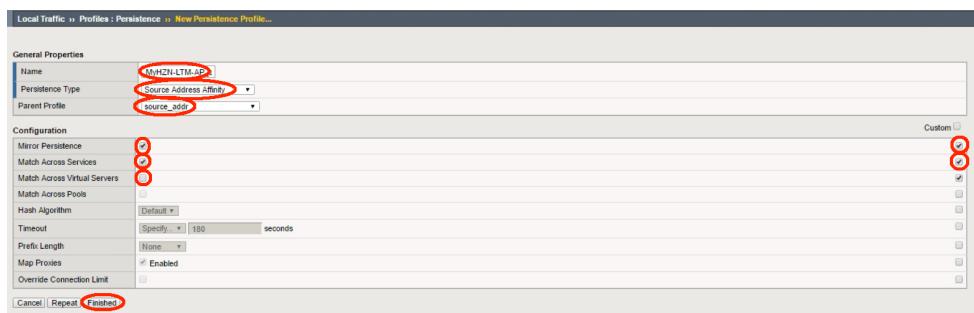
Creating a TCP-LAN-Optimized Profiles

1. Create an TCP profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Protocol > TCP > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **tcp-lan-optimized** is selected.
 - d. Leave all other settings at the default and then click **Finished**.

The screenshot shows the 'General Properties' dialog box. It has two main sections: 'Name' and 'Parent Profile'. The 'Name' field contains 'MyHZN-LTM-AP' and the 'Parent Profile' dropdown menu is set to 'tcp-lan-optimized'. Both the 'Name' field and the 'Parent Profile' dropdown are circled in red. At the bottom of the dialog, there are three buttons: 'Cancel', 'Repeat', and 'Finished', with 'Finished' also circled in red.

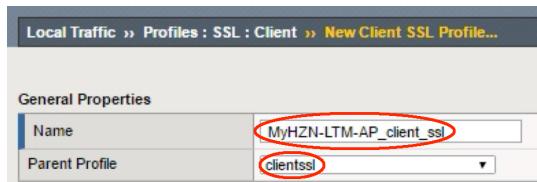
Creating a Persistence Profile

1. Creating a Persistence profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > Persistence > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Persistence Type** list, select **Source Address Affinity**.
 - d. From the **Parent Profile** list, ensure **source_addr** is selected.
 - e. If you have deployed a redundant pair of BIG-IP systems only:
From the **Mirror Persistence** row, click the **Custom** checkbox on the right, and then click the checkbox to enable persistence mirroring.
 - f. From the **Match Across Services** row, click the **Custom** checkbox, and then click the checkbox to enable matching across services.
 - g. From the **Match Across Virtual Servers** row, ensure the Match Across Virtual Servers box is UNCHECKED.
 - h. Click **Finished**.



Creating a Client SSL Profile

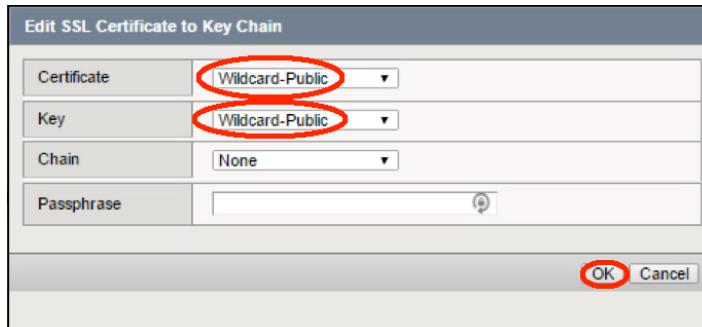
1. Create a Client SSL profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > SSL > Client > Create**.
 - b. In the **Name** field, type a unique name.



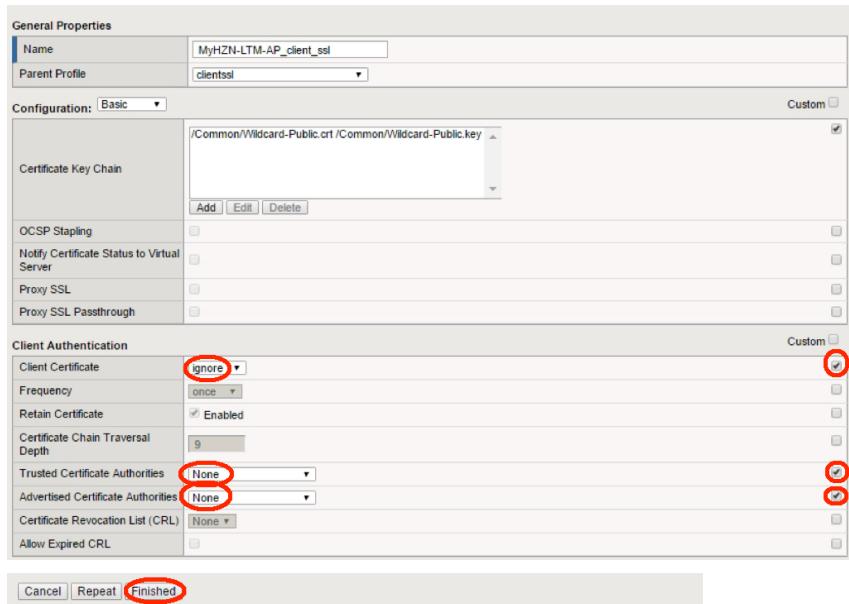
- c. From the **Certificate Key Chain** area, click the **Custom** checkbox and then click the **Add** button.



- d. In the Edit SSL Certificate to Key Chain box, complete the following.
 - i. From the **Certificate** list, select the certificate you imported in [Importing a Certificate into BIG-IP](#).
 - ii. From the **Key** list, select the key you imported in [Importing a Certificate into BIG-IP](#).
 - iii. (Optional) If you imported a chain certificate, select the Intermediate/Root Chain you imported in [Importing a Certificate into BIG-IP](#).
 - iv. (Optional) If your key is highly encrypted, in the **Passphrase** box, type the passphrase.
 - v. Click **OK**.

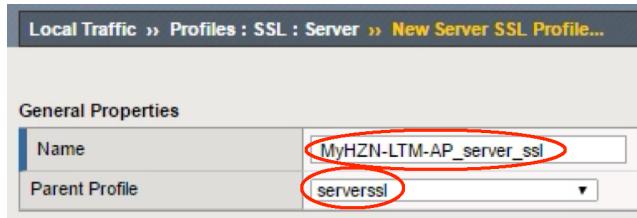


- e. From the **Client Certificate** row, click the **Custom** checkbox and then select **Ignore** from the list.
- f. From the **Trusted Certificate Authorities** row, click the **Custom** checkbox and then select **None** from the list.
- g. From the **Advertised Certificate Authorities** row, click the **Custom** checkbox and then select **None** from the list.
- h. Scroll to the bottom and click **Finished**.



Creating a Server SSL Profile

1. Create a Server SSL profile using the following guidance.
 - a. On the Main tab, click **Local Traffic > Profiles > SSL > Server > Create**.
 - b. In the **Name** field, type a unique name.
 - c. From the **Parent Profile** list, ensure **serverssl** is selected.



- d. From the **Configuration** list, select **Advanced**.
- e. In the **Ciphers** area, click the **Custom** box, and then click the **Cipher String** button.
- f. In the **Ciphers** field, type **DEFAULT:!DHE:@STRENGTH**
- g. Leave all other settings at the defaults and then click **Finished**.



Creating Virtual Servers

HTTP Redirect - Virtual Server

1. Create an HTTP Redirect virtual server using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **80** or select **HTTP** from the list.

The screenshot shows the 'General Properties' dialog box. It has a table with the following fields:

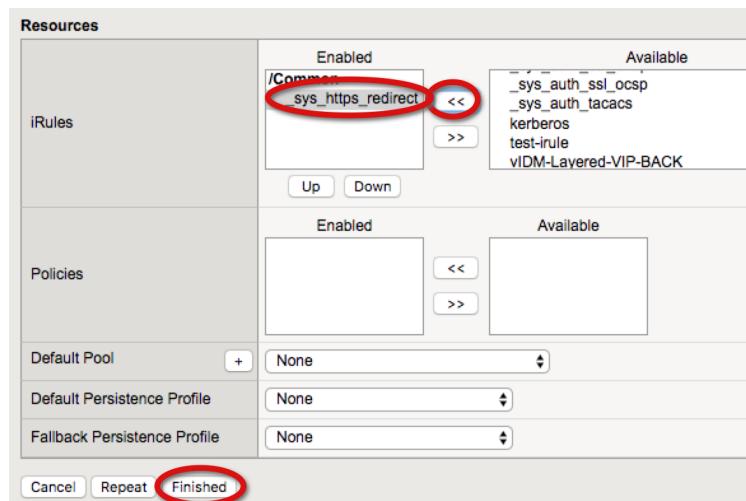
General Properties	
Name	MyHZN-LTM-AP_redirect
Description	(empty)
Type	Standard
Source Address	(empty)
Destination Address/Mask	10.192.192.10
Service Port	80
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **TCP**.
- g. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
- h. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
- i. From the **HTTP Profile** list, select the HTTP profile you created in [Creating a HTTP Profile](#).
- j. From the **Source Address Translation** list, select **Auto Map**.

The screenshot shows the 'Configuration' dialog box, specifically the 'Basic' tab. It contains the following settings:

Setting	Value
Protocol	TCP
Protocol Profile (Client)	MyHZN-LTM-AP_tcp_wan_optimized
Protocol Profile (Server)	MyHZN-LTM-AP_tcp_lan_optimized
HTTP Profile	MyHZN-LTM-AP_http
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: None Available: /Common MyHZN-LTM-AP_client_ssl, VPN-ClientSSL, Wildcard-ClientSSL, clientsssl
SSL Profile (Server)	Selected: None Available: /Common apm-default-serverssl, crypto-client-default-serverssl, pool-default-serverssl, serverssl, serverssl_insecure_compatible
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

- k. In the **iRules** area, from the **Available** list, select **_sys_https_redirect** and then click the Add (<<) button.
- l. Leave all other settings at the defaults and then click **Finished**.



Port 443 TCP - Virtual Server

1. Create the main virtual server (Port 443 TCP) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **443** or select **HTTPS** from the list.

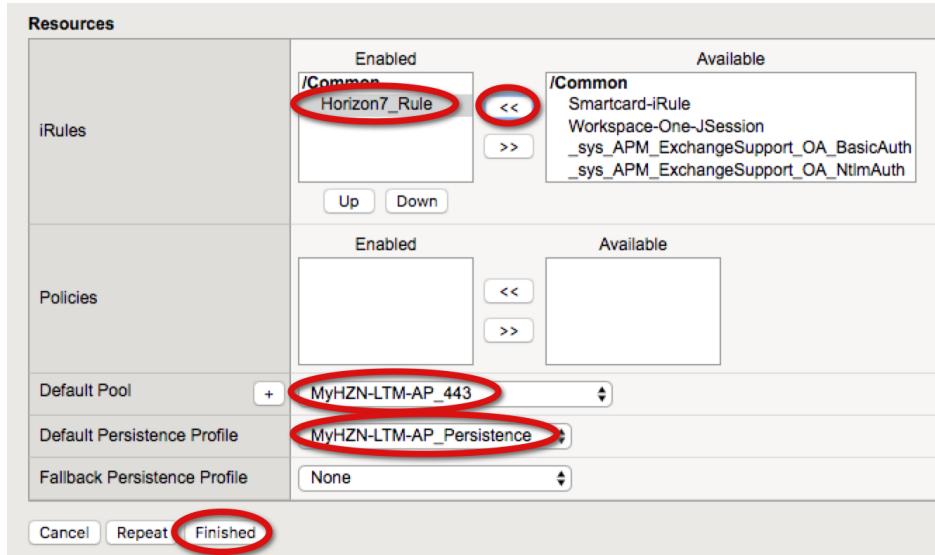
General Properties	
Name	MyHZN-LTM-AP_443_TCP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **TCP**.
- g. From the **Protocol Profile (Client)** list, select the **tcp-wan-optimized** profile you created previously.
- h. From the **Protocol Profile (Server)** list, select the **tcp-lan-optimized** profile you created previously.
- i. From the **HTTP Profile** list, select the **HTTP** profile you created previously.
- j. From the **SSL Profile (Client)** list, select the **clientssl** profile you created previously and click the Add (<<) button to move it to the Selected list.
- k. From the **SSL Profile (Server)** list, select the **serverssl** profile you created previously and click the Add (<<) button to move it to the Selected list.
- l. From the **Source Address Translation** list, select **Auto Map**.

Configuration:	Basic
Protocol	TCP
Protocol Profile (Client)	MyHZN-LTM-AP_tcp_wan_optimized
Protocol Profile (Server)	MyHZN-LTM-AP_tcp_lan_optimized
HTTP Profile	MyHZN-LTM-AP_http
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: /Common/MyHZN-LTM-AP_client_ssl Available: /Common/VPN-ClientSSL/Wildcard-ClientSSL/clientssl/clientssl-insecure-compatible
SSL Profile (Server)	Selected: /Common/MyHZN-LTM-AP_server_ssl Available: /Common/apm-default-serverssl/crypto-client-default-serverssl/pool-default-serverssl/serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Creating the main virtual server (continued)

- m. If you created the iRule for the Horizon Origin Header only: In the **iRules** area, select the iRule you created in [iRule for the Horizon Origin Header](#) and then click the Add (<<) button.
Note: If VMware Origin Header method was used skip this step.
- n. From the **Default Pool** list, select the pool you created in [Port 443 - Pool](#).
- o. From the **Default Persistence Profile** list, select the profile you created previously.
- p. Click **Finished**.



Port 443 UDP - Virtual Server

1. Create the main virtual server (Port 443 UDP) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **443** or select **HTTPS** from the list.

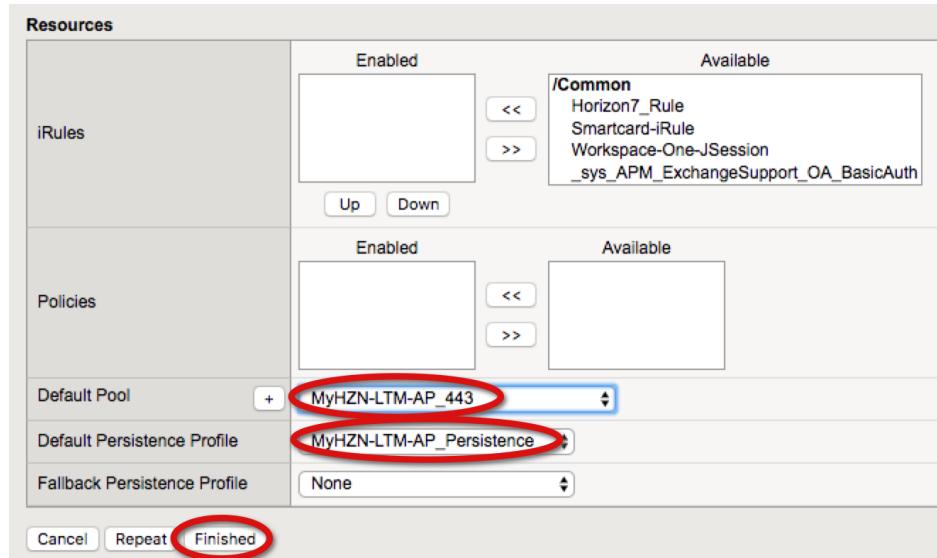
General Properties	
Name	MyHZN-LTM-AP_443_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **UDP**.
- g. From the **Protocol Profile (Client)** list, select the **udp profile** you created previously.
- h. From the **Protocol Profile (Server)** list, select **(Use Client Profile)**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic					
Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl
Selected	Available				
	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl				
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-ssl-default-serverssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-ssl-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-ssl-default-serverssl				
SMTPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Netflow Profile	None Warning: This feature is not enabled by the current license.				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

Creating the main virtual server (continued)

- j. From the **Default Pool** list, select the pool you created in [Port 443 - Pool](#).
- k. From the **Default Persistence Profile** list, select the profile you created previously.
- l. Click **Finished**.



Port 8443 TCP - Virtual Server

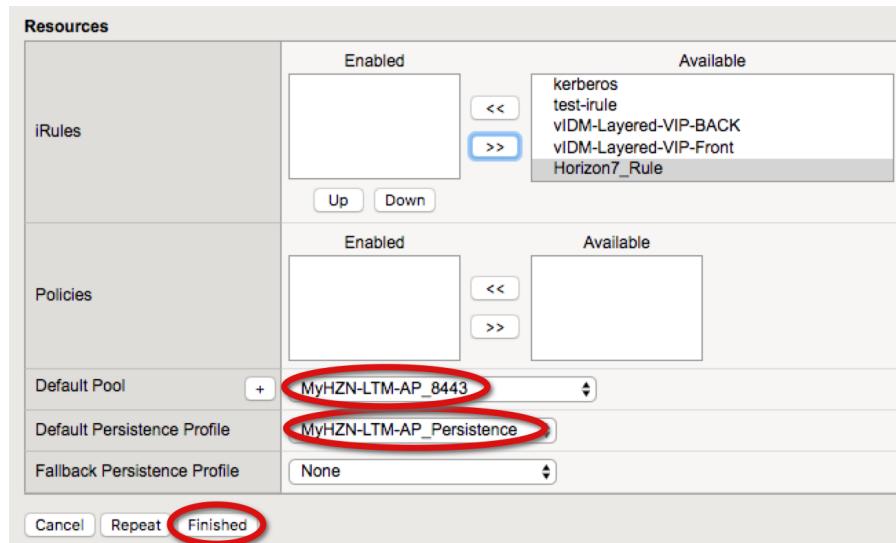
1. Creating the main virtual server for Port 8443 TCP
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **8443**.

General Properties	
Name	MyHZN-LTM-AP_8443_TCP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	8443
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **TCP**.
- g. From the **Protocol Profile (Client)** list, select the **tcp-wan-optimized** profile you created previously.
- h. From the **Protocol Profile (Server)** list, select the **tcp-lan-optimized** profile you created previously.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic					
Protocol	TCP				
Protocol Profile (Client)	MyHZN-LTM-AP_tcp_wan_optimized				
Protocol Profile (Server)	MyHZN-LTM-AP_tcp_lan_optimized				
HTTP Profile	None				
HTTP Proxy Connect Profile	None				
Traffic Acceleration Profile	None				
FTP Profile	None				
RTSP Profile	None				
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl
Selected	Available				
	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl				
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl				
SMTPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

- j. From the **Default Pool** list, select the pool you created in [Port 8443 - Pool](#).
- k. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
- l. Click **Finished**.



Port 8443 UDP - Virtual Server

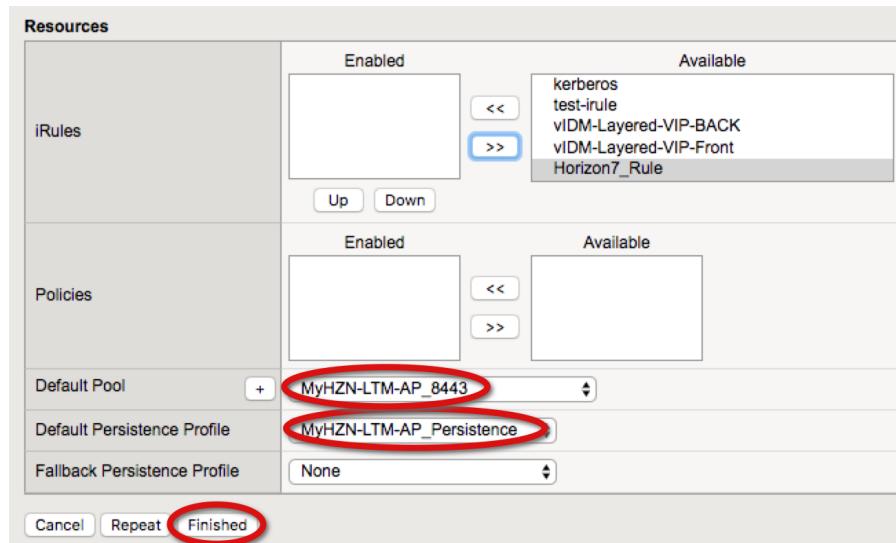
1. Creating the main virtual server for Port 8443 UDP
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **8443**.

General Properties	
Name	MyHZN-LTM-AP_8443_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	8443 Other:
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **UDP**.
- g. From the **Protocol Profile (Client)** list, select **udp**.
- h. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic					
Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl
Selected	Available				
	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl				
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_server_ssl appm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_server_ssl appm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_server_ssl appm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl				
SMTPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Netflow Profile	None <small>Warning: This feature is not enabled by the current license.</small>				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

- i. From the **Default Pool** list, select the pool you created in [Port 8443 - Pool](#).
- j. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
- k. Click **Finished**.



Port 4172 TCP - Virtual Server

1. Create the main virtual server (Port 4172 TCP) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **4172**.

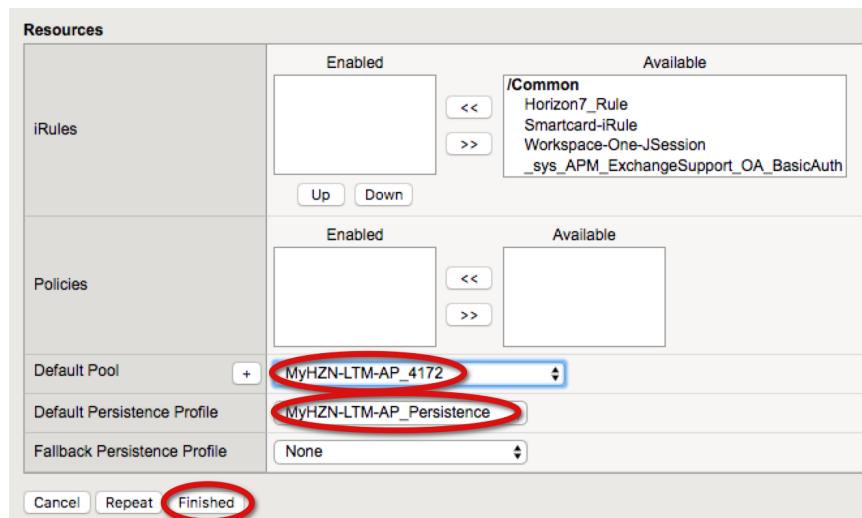
General Properties	
Name	MyHZN-LTM-AP_4172_TCP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	4172
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **TCP**.
- g. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
- h. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic										
Protocol	TCP									
Protocol Profile (Client)	MyHZN-LTM-AP_tcp_wan_optimized									
Protocol Profile (Server)	MyHZN-LTM-AP_tcp_lan_optimized									
HTTP Profile	None									
HTTP Proxy Connect Profile	None									
Traffic Acceleration Profile	None									
FTP Profile	None									
RTSP Profile	None									
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td></td> <td>Available</td> </tr> <tr> <td></td> <td><<</td> <td>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientsssl</td> </tr> <tr> <td></td> <td>>></td> <td></td> </tr> </table>	Selected		Available		<<	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientsssl		>>	
Selected		Available								
	<<	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientsssl								
	>>									
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td></td> <td>Available</td> </tr> <tr> <td></td> <td><<</td> <td>/Common MyHZN-LTM-AP_server_ssl apm-default-serversssl crypto-client-default-serversssl pcip-default-serversssl</td> </tr> <tr> <td></td> <td>>></td> <td></td> </tr> </table>	Selected		Available		<<	/Common MyHZN-LTM-AP_server_ssl apm-default-serversssl crypto-client-default-serversssl pcip-default-serversssl		>>	
Selected		Available								
	<<	/Common MyHZN-LTM-AP_server_ssl apm-default-serversssl crypto-client-default-serversssl pcip-default-serversssl								
	>>									
SMTPS Profile	None									
Client LDAP Profile	None									
Server LDAP Profile	None									
VLAN and Tunnel Traffic	All VLANs and Tunnels									
Source Address Translation	Auto Map									

Creating the PCoIP virtual server (continued)

- j. From the **Default Pool** list, select the pool you created in [Port 4172 - Pool](#).
- k. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
- l. Click **Finished**.



Port 4172 UDP - Virtual Server

1. Create the main virtual server (Port 4172 UDP) using the following guidance.
 - a. On the Main tab, click **Local Traffic > Virtual Servers > Create**
 - b. In the **Name** field, type a unique name.
 - c. From the **Type** list, ensure **Standard** is selected.
 - d. In the **Destination Address/Mask** field, type the IP Address for the virtual server.
 - e. In the **Service Port** field, type **4172**.

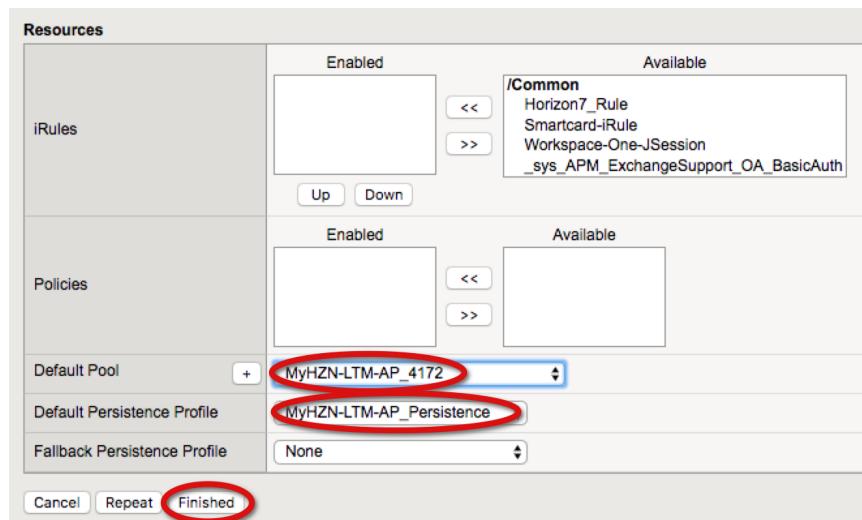
General Properties	
Name	MyHZN-LTM-AP_4172_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	4172 Other:
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

- f. From the **Protocol** list, select **UDP**.
- g. From the **Protocol Profile (Client)** list, select **udp**.
- h. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic					
Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl
Selected	Available				
	/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl				
SSL Profile (Server)	<table border="1"> <tr> <td>Selected</td> <td>Available</td> </tr> <tr> <td></td> <td>/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-default-serverssl</td> </tr> </table>	Selected	Available		/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcip-default-serverssl				
SMTPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Netflow Profile	None <small>Warning: This feature is not enabled by the current license.</small>				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

Creating the UDP virtual server (continued)

- i. From the **Default Pool** list, select the pool you created in [PCoIP - Pool](#).
- j. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
- k. Click **Finished**.



Final Configuration

Once Completed you should see the full configuration for F5 LTM with VMware Horizon Unified Access Gateway (UAG) for PCoIP and Blast Extreme TCP/UDP with BEAT (Blast Extreme Adaptive Transport).

Local Traffic >> Virtual Servers : Virtual Server List						
Virtual Server List		Virtual Address List		Statistics		
Status	Name	Description	Application	Destination	Service Port	Type
<input type="checkbox"/>	MyHZN-LTM-AP_4172_TCP			10.192.192.10	4172	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_4172_UDP			10.192.192.10	4172	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_443_TCP			10.192.192.10	443 (HTTPS)	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_443_UDP			10.192.192.10	443 (HTTPS)	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_8443_TCP			10.192.192.10	8443	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_8443_UDP			10.192.192.10	8443	Standard
<input type="checkbox"/>	MyHZN-LTM-AP_redirect			10.192.192.10	80 (HTTP)	Standard

Testing the VMware Horizon Connection

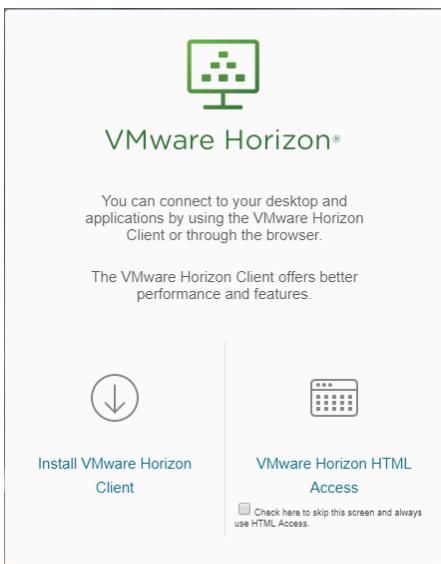
After setting up the Virtual IPs (VIPs) for the Unified Access Gateways, you can use the following methods validate that the External VIP is connecting and working properly. In this case, you are now using the new FQDN site name to connect to the Horizon Environment.

NOTE: This connection test should be done from an external computer on the Internet.

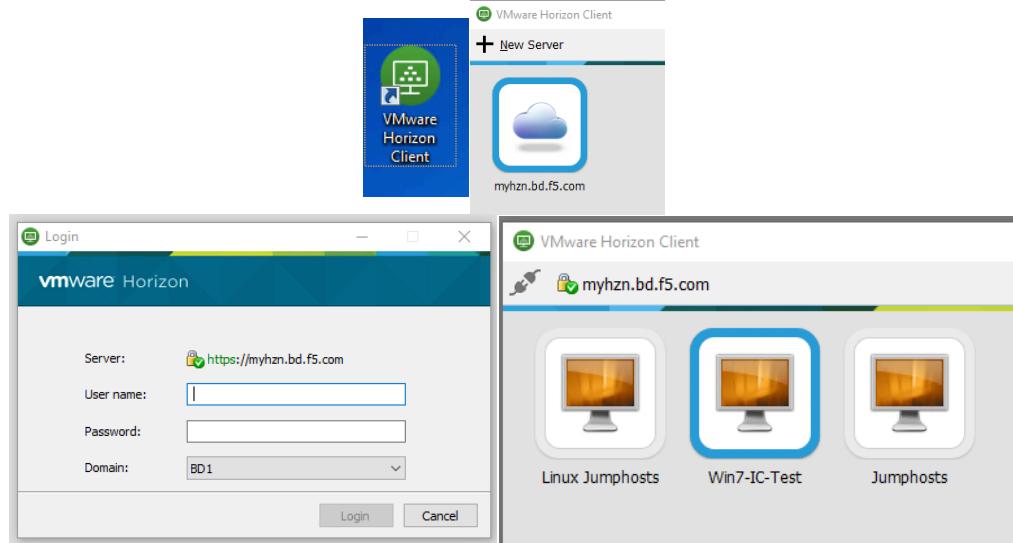
1. In a browser, type the FQDN for the VIP you previously created (for example, <https://myhzn.bd.f5.com>).

 <https://myhzn.bd.f5.com>

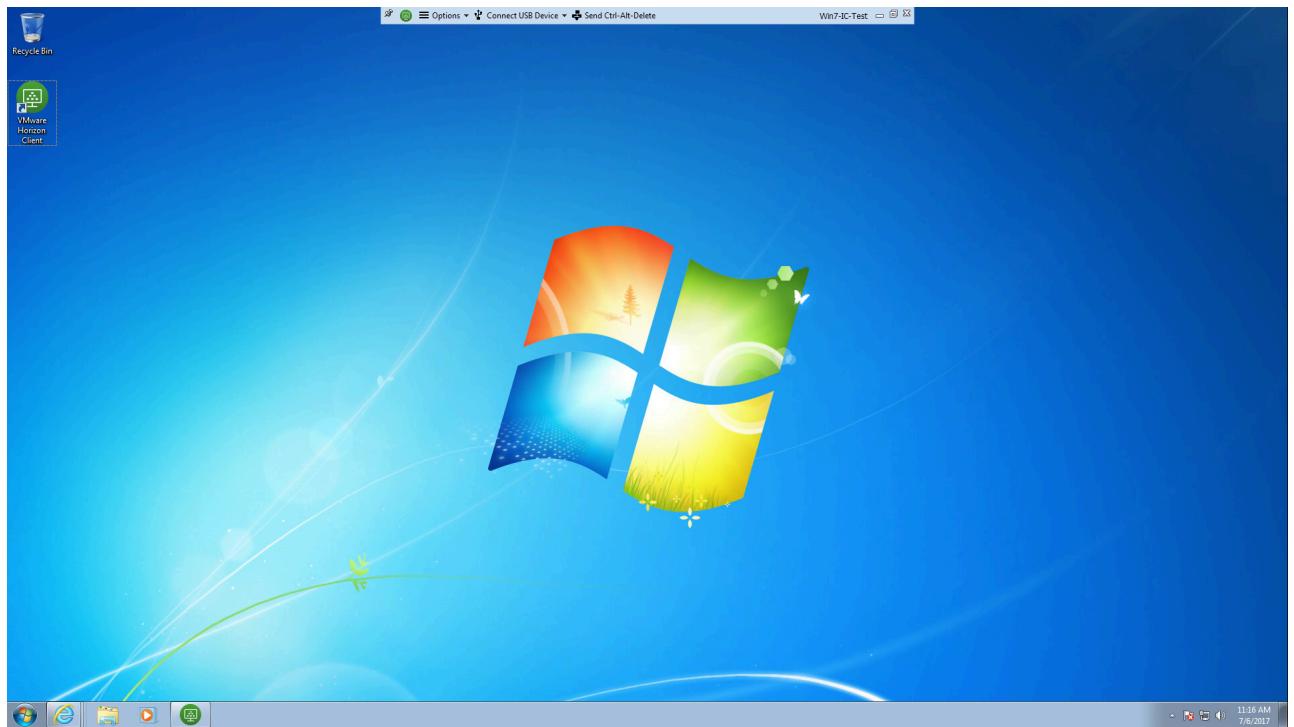
You should see the VMware Horizon Client/HTML5 Page. This confirms that your servers are working through the newly created virtual server.



2. You can also test the VMware Horizon Client to ensure accessibility to the Horizon Environment. After logging in you should see the apps/desktops associated with the user that logged on.



Select a Pool to validate connectivity and ensure that you can access a desktop. Once the connection is validated the environment is correctly setup for LTM with the Horizon servers.



References

Load Balancing across VMware Unified Access Gateway Appliances (formerly known as Access Point) – Mark Benson & Vish Kalsi

<https://communities.vmware.com/docs/DOC-32792>