

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

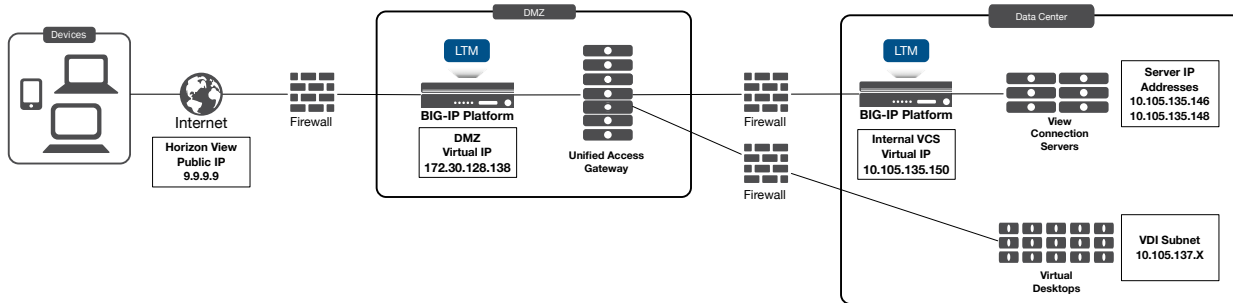


Figure 1 BIG-IP F5 LTM with Unified Access Gateway

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:
 - The SSL certificate.
 - The Private Key used for the load balanced FQDN certificate.
 - 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).

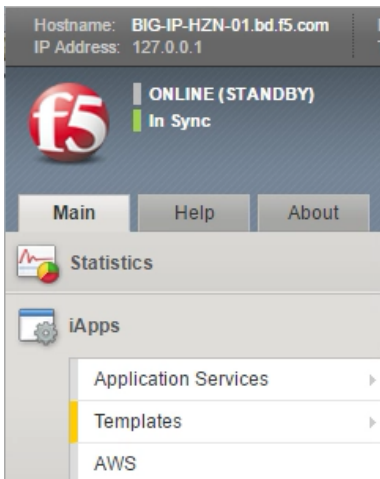
Importing the iApp Template into BIG-IP

1. Login to the F5 Configuration utility.

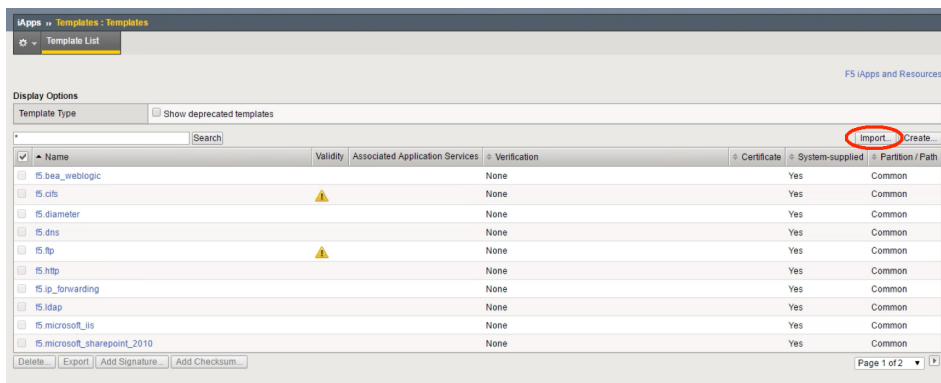


The screenshot shows the login interface of the BIG-IP Configuration Utility. At the top left is the F5 logo. To its right, the text reads "BIG-IP Configuration Utility" and "F5 Networks, Inc.". Below the logo, there are input fields for "Hostname" (pre-filled with "BIG-IP-HZN-01.bd.f5.com"), "IP Address" (pre-filled with "192.168.14.20"), "Username", and "Password". A "Log in" button is located below the password field. On the right side of the page, a welcome message states: "Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left."

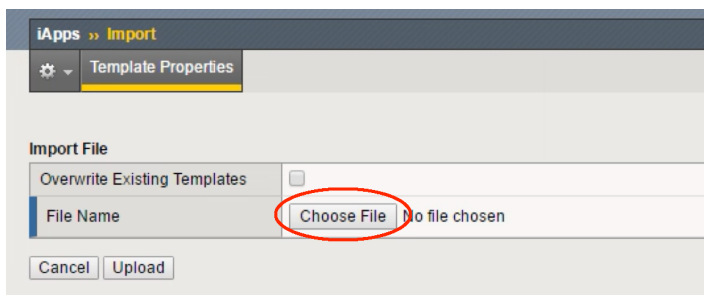
2. On the Main tab, click **iApps > Templates**.



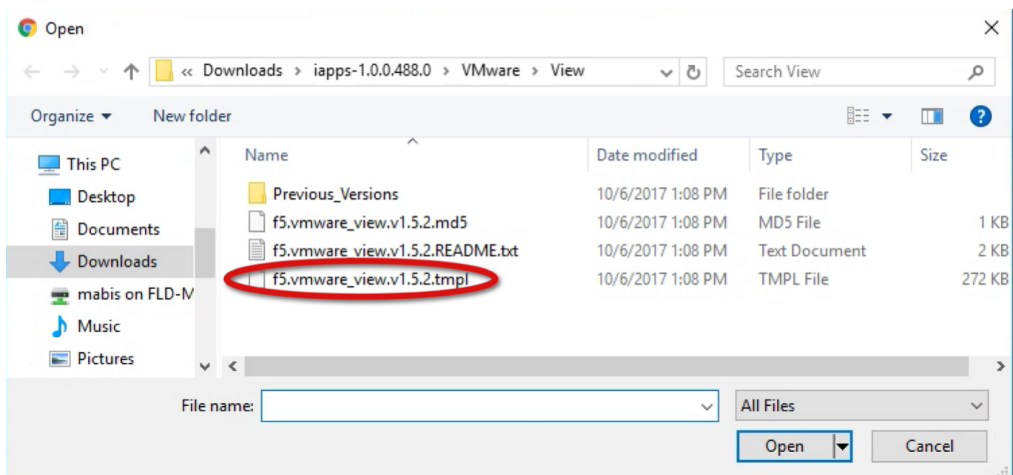
- Click the **Import** button on the right upper side of the window.



- Click the **Choose File** button.



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



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

The screenshot shows the 'iApps >> Import' dialog box with the 'Template Properties' tab selected. Under the 'Import File' section, the 'File Name' field displays 'f5.vmware_vi...v1.5.2.tmpl'. The 'Choose File' button is circled in red. At the bottom, the 'Upload' button is also circled in red.

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.

The screenshot shows the 'iApps >> Templates : Templates' page. The 'Template List' tab is selected. Under 'Display Options', the 'Show deprecated templates' checkbox is unchecked. A search bar is present. Below, a table lists templates. The first row, 'f5.vmware_view.v1.5.2', is circled in red. The second row, 'f5.vmware_vmotion', has a yellow warning icon. At the bottom right, the pagination shows 'Page 3 of 3', which is also circled in red.

<input checked="" type="checkbox"/>	Name	Validity	Associated Application Services	Verification	Certificate	System-supplied	Partition / Path
<input type="checkbox"/>	f5.vmware_view.v1.5.2			None			Common
<input type="checkbox"/>	f5.vmware_vmotion			None		Yes	Common

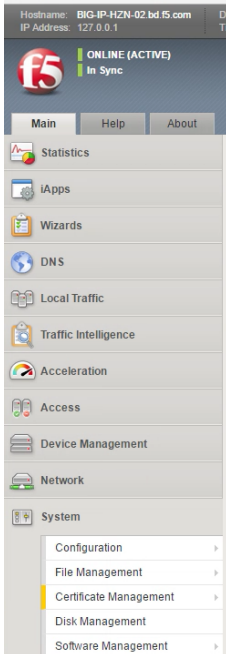
Importing a Certificate into BIG-IP

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

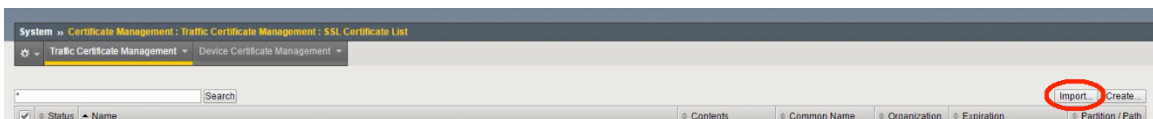
1. Login to the F5 Configuration utility.



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

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

Status	Name	Contents	Common Name	Organization	Expiration	Partition / Path
<input checked="" type="checkbox"/>	MyH2N-internalCA	RSA Certificate & Key	MyH2N.bd.f5.com		Mar 6, 2019	Common
<input checked="" type="checkbox"/>	Wildcard-Public	RSA Certificate & Key	bd.f5.com	F5 Networks Inc	Jul 25, 2018	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Dec 31, 2029 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	localhost.localdomain	MyCompany	Feb 13, 2027	Common
<input type="checkbox"/>	f5-internal	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.

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.bfb5.00.00.00.00.50.d8.tb.75
Subject	Common Name: bd.f5.com Organization: F5 Networks Inc Division: Seattle Locality: Washington State Or Province: US
Issuer	Common Name: Entrust Certification Authority - L1K Organizational Unit: Entrust, Inc. Division: See www.entrust.net/legal-terms Locality: US State Or Province: US Country: US
Email	
Subject Alternative Name	DNS:*.bd.f5.com, DNS:bd.f5.com

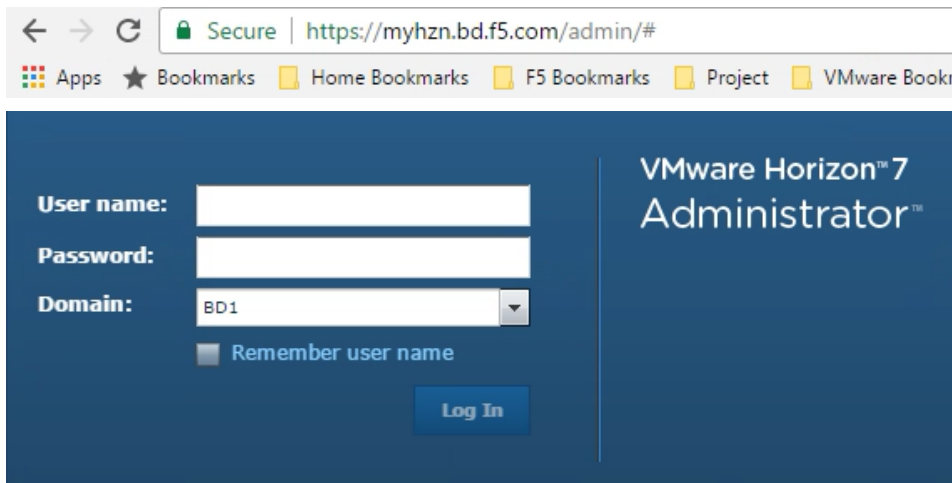
Monitoring Properties

Monitoring Type	<input type="checkbox"/> OCSP
Issuer Certificate	None
OCSP	None
Status	<input type="checkbox"/>

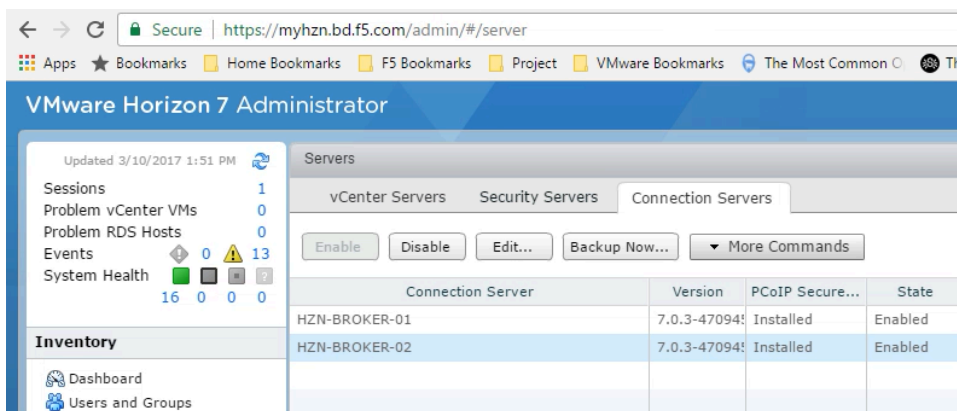
Buttons: Import, Export, Renew, Update Status Monitoring, Delete OCSP Cache, Delete

Configuring your Horizon Environment for use with Unified Access Gateway.

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



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



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

- 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.

Edit Connection Server Settings

General Authentication Backup

Tags

Tags can be used to restrict which desktop pools can be accessed through this Connection Server.

Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel

☐ Use Secure Tunnel connection to machine

External URL: Example: https://myserver.com:443

PCoIP Secure Gateway

☐ Use PCoIP Secure Gateway for PCoIP connections to machine

PCoIP External URL: Example: 10.0.0.1:4172

Blast Secure Gateway

☐ Use Blast Secure Gateway for Blast connections to machine

Blast External URL: Example: https://myserver.com:8443

OK Cancel

- 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).

VMware Horizon 7 Administrator

Updated 3/10/2017 1:51 PM

Sessions: 1
Problem vCenter VMs: 0
Problem RDS Hosts: 0
Events: 0
System Health: 16 0 0 0

Inventory: Dashboard, Users and Groups

Servers: vCenter Servers, Security Servers, Connection Servers

Enable Disable Edit... Backup Now... More Commands

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.

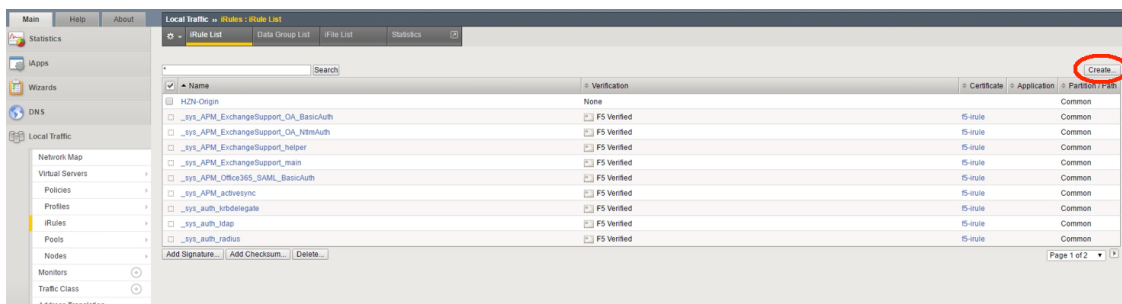
NOTE: Only one of these two methods are necessary.

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"
  }
}
```

Local Traffic » iRules : iRule List » New iRule...

Properties

Name: Hzn-Origin

```

1 when HTTP_REQUEST {
2   if { [HTTP::header "Origin"] ne "" } {
3     HTTP::header remove "Origin"
4   }
5 }
```

Definition

☐ Wrap Text
☐ Show Print Margin

Cancel Finished

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

Local Traffic » iRules : iRule List

iRule List Data Group List iFile List Statistics

Search

Name	Verification
HZN-Origin	None
_sys_APM_ExchangeSupport_OA_BasicAuth	F5 Verified
_sys_APM_ExchangeSupport_OA_NtimAuth	F5 Verified
_sys_APM_ExchangeSupport_helper	F5 Verified
_sys_APM_ExchangeSupport_main	F5 Verified
_sys_APM_Office365_SAML_BasicAuth	F5 Verified
_sys_APM_activesync	F5 Verified
_sys_auth_krbdelegate	F5 Verified
_sys_auth_ldap	F5 Verified
_sys_auth_radius	F5 Verified

Add Signature... Add Checksum... Delete...

Creating/Deploying a Virtual IP for External Connections

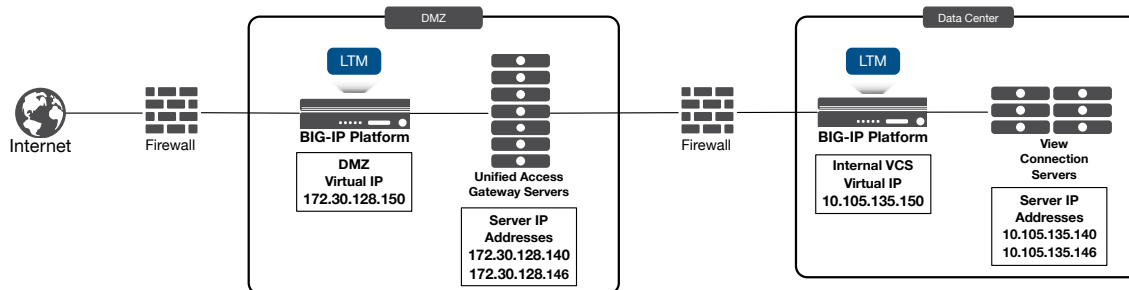


Figure 2 BIG-IP F5 LTM with Unified Access Gateway for External Connections

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.

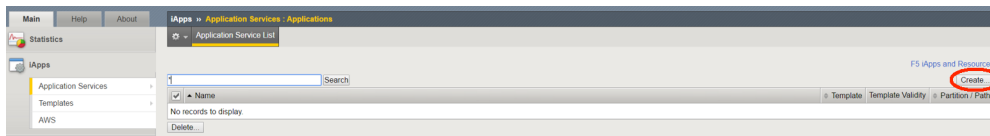
NOTE: There must be an internal Virtual IP (VIP) for the Horizon Connection Servers prior to configuring the UAG Servers. See Section [Prerequisites](#) for more details.

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).

iApps > Application Services > Applications > New Application Service...

Template Selection: Basic

Name: MyHZN-LTM-APM

Template: f5.vmware_view.v1.5.2

☐ Show deprecated templates

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/sol15041.html or DevCentral: https://devcentral.f5.com/wiki/iApp.VMware-Applications.ashx .
VMware Compatibility	Please follow online support at https://support.f5.com/csp/tech-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: 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?	<div> Show inline help text </div> <p>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.</p>
Which configuration mode do you want to use?	<div> Advanced - configure advanced options </div> <p>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 continuing.</p>

BIG-IP Access Policy Manager	
Do you want to deploy BIG-IP Access Policy Manager?	<div> No, do not deploy BIG-IP Access Policy Manager </div>
NOTE	<p>You can use the BIG-IP Access Policy Manager (APM) as a full PCoIP secure gateway proxy, or a DTLS NTP proxy. View 5.2 or later and the BIG-IP system must be running version 11.4 or later.</p> <p>You must have fully licensed the BIG-IP APM to use the APM features in this template.</p>

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 handle encrypted traffic.

If your environment requires clients use SSL and session persistence (which ensures requests from a single user 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 BIG-IP system.

If security requirements do not allow the BIG-IP system to offload SSL, select to re-encrypt to the servers (SSL Bridging). With SSL Bridging, you may experience inconsistent distribution of client requests.

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 from the list.

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 configured on the system.

Select the SSL certificate you imported for this deployment. Importing certificates and keys is not a part of this template.

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 from the list.

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 system administrators verify the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the certificate chain.

Intermediate certificates must be created or imported onto this BIG-IP system prior to running this iApp. See the Intermediate Certificates section of the BIG-IP System Administration Guide for more information.

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 can be configured to redirect HTTP traffic to HTTPS.

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 before sending it to the servers and the BIG-IP system. Certificates that you install or import must meet the encryption requirements are different than those that apply to public-facing traffic. You may need to import a certificate that meets the requirements for the servers and the BIG-IP system.

6. In the PC Over IP section, complete the following.
 - a. From the *Should PCoIP connections go through the BIG-IP system?* question, select **Yes, PCoIP connection should go through the BIG-IP system**.
 - b. From the *Will PCoIP connections be proxied by the View Security Servers?* question, select **Yes, PCoIP connections are proxied by the VMware UAGs**.
 - c. 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?	Yes, PCoIP connections should go through the BIG-IP system ▼
Select this option if PCoIP connections will be routed through the BIG-IP system.	
Will PCoIP connections be proxied by the VMware UAGs?	Yes, PCoIP connections are proxied by the VMware UAGs ▼
By selecting this option, the BIG-IP system does not create Forwarding virtual servers, but instead directs all PCoIP traffic back to the VMware properly, you must enable View secure tunnel option on the VMware UAGs, and enter the IP address entered in the next section with port 41192.0.2.100:4172.	
Will VMware View HTML 5 client connections go through the BIG-IP system?	Yes, support HTML 5 View clientless browser connections ▼
Choose Yes to enable support for both HTML 5 clientless browser connections and View Client connections to the Virtual Desktops. Choose Client connections and do not need to support the View HTML 5 client. When supporting HTML 5 clients, verify the View Connection Servers connections to BIG-IP virtual server address.	

7. In the Virtual Servers and Pools section, complete the following.
 - a. Type the IP address for the virtual server.
 - b. 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?	10.192.192.10
This IP address, combined with the port you specify below, becomes the BIG-IP virtual server address and port, vServers.	
What service port do you want to use for the virtual server(s)?	443
Specify the service port you want to use for the virtual server(s). The port you specify here is used for the remote, to the question asking how the system should handle SSL traffic.	
What FQDN will clients use to access the View environment?	MyHZN.bd.f5.com
The FQDN entered here will be used by the View Client to resolve to the virtual IP entered above.	
Which persistence profile do you want to use?	Use F5's recommended persistence profile ▼
With persistence, the BIG-IP system tracks and stores session data, such as the specific pool member that service direct all subsequent requests from a given client to the same View server in the pool. We recommend this method.	
Which load balancing method do you want to use?	Least Connections (member) ▼
A load balancing method is an algorithm that the BIG-IP system uses to select a pool member for processing a request. A number of current connections. This is ideal for environments in which pool members have similar performance.	
Should the BIG-IP system queue TCP requests?	No, do not enable TCP request queuing ▼
TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections and timeout for queued requests based on server capability, load, and need for shared resources.	
Use a Slow Ramp time for newly added servers?	Use Slow Ramp ▼
With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added View server balancing methods like Least Connections, as the BIG-IP system would otherwise send all new connections to a your server hardware and the behavior of your web services. The default setting of 300 seconds (5 minutes) is v	

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?	<input type="text" value="300"/>		
	Specify the duration (in seconds) for Slow Ramp time (the amount of time the system sends less traffic to a newly-enabled server). This value is very conservative in most cases.		
Do you want to give priority to specific groups of servers?	<input type="text" value="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 group with the highest priority that falls below the value you specify as the minimum. The BIG-IP system then sends traffic to the group with the next highest priority. For more details, see the BIG-IP documentation for more details.		
Which servers should be included in this pool?	Node/IP address: <input type="text" value="10.105.169.100"/>	Port: <input type="text" value="443"/>	Conn limit: <input type="text" value="0"/> <input type="button" value="X"/>
	Node/IP address: <input type="text" value="10.105.169.101"/>	Port: <input type="text" value="443"/>	Conn limit: <input type="text" value="0"/> <input type="button" value="X"/>
	<input type="button" value="Add"/>		
	Specify the IP address(es) of your View servers. If you have existing nodes on this BIG-IP system, you can select the nodes from the list. If you need to add a new node, click Add. If you have existing nodes on this BIG-IP system, you can select the nodes from the list. If you need to add a new node, click Add.		
Where will the virtual servers be in relation to the View servers?	<input type="text" value="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.		
	For environments in which the virtual server IP address provided is on the same subnet as the View servers in the pool, select BIG-IP virtual server IP and View servers are on the same subnet. This enables Secure Network Address Translation (SNAT Auto Map). 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.		
How have you configured routing on your View servers?	<input type="text" value="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 virtual server IP is required for the BIG-IP system configuration.		
	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. 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.		
	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?	<input type="text" value="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. The BIG-IP system also inserts the value of the X-Forwarded-For header in the HTTP 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?	<input type="text" value="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 for the same item are served from the cache, reducing the load associated with processing subsequent requests.
	Use a custom Web Acceleration profile only if you need to define specific URIs that should or should not be cached.
Which HTTP compression profile do you want to use?	<input type="text" value="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?	<input type="text" value="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 TCP connection parameters.

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

Server Optimization	
Which OneConnect profile do you want to use?	Do not use a OneConnect profile
	OneConnect (connection pooling or multiplexing) improves server scalability by reducing load associated with connections which is used to send requests from multiple clients.
How do you want to optimize server-side connections?	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?	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, the monitor will begin sending requests once the application responds correctly. Simple monitor verifies basic web functionality, and at least one available entitled pool for the specified user is available. If you have manually created a health monitor, you can select it from the list.
How many seconds should pass between health checks?	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 BIG-IP system.												
	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 the iRule Event Priority section in the BIG-IP Configuration Guide.												
Do you want to add any custom iRules to this configuration?	<table><thead><tr><th>Selected</th><th></th><th>Options</th></tr></thead><tbody><tr><td>/Common</td><td></td><td></td></tr><tr><td>HZN-Origin</td><td><<</td><td></td></tr><tr><td></td><td>>></td><td></td></tr></tbody></table>	Selected		Options	/Common			HZN-Origin	<<			>>	
Selected		Options											
/Common													
HZN-Origin	<<												
	>>												

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?	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 Logging for more information. Request logging has been 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 5 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 use the View 5 application.
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 BIG-IP system. See the View 5 deployment guide: http://www.f5.com/pdf/deployment-guides/vmware-view5-lapp-dg.pdf
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 View 5 application).
Troubleshooting	If you have deployed APM for secure network access and you are unable to login, ensure your AD configuration is correct. You can find common troubleshooting tips in the View 5 Deployment Guide: http://www.f5.com/pdf/deployment-guides/vmware-view5-lapp-dg.pdf
Cancel Finished	

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

The screenshot displays the BIG-IP configuration summary screen. The interface is divided into two main sections: a left pane showing a hierarchical tree of configuration objects, and a right pane showing the details of the selected object. The status of each object is indicated by a green circle with a checkmark (Available) or a blue square with an 'X' (Unknown).

Configuration Objects and Status:

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

Buttons: 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**.

The screenshot shows the 'General Properties' and 'Configuration' sections of the iApp configuration interface. The 'General Properties' section includes fields for Name, Description, Type, and Parent Monitor. The 'Configuration' section includes fields for Interval, Timeout, Send String, Receive String, Receive Disable String, Reverse, Transparent, Alias Address, Alias Service Port, and Adaptive. The 'Finished' button is highlighted with a red circle.

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	* All Ports
Adaptive	<input type="checkbox"/> Enabled

Buttons: 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

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**.

The screenshot shows the 'General Properties' and 'Configuration' tabs of the HTTPS Monitor configuration window. Red circles and a red underline highlight the following fields and values:

- Name:** MyHZN-LTM-AP_https_2
- Type:** HTTPS
- Parent Monitor:** https
- Interval:** 30 seconds
- Timeout:** 91 seconds
- Send String:** GET /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
- Receive String:** 200
- Receive Disable String:** 503
- Finished button:** Located at the bottom right of the configuration window.

Other visible fields include Description, Cipher List (DEFAULT:SHA:+3DES:+kEDH), User Name, Password, Client Certificate, Client Key, Reverse, Transparent, Alias Address, Alias Service Port, and Adaptive.

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**.

Local Traffic >> Pools : Pool List >> New Pool...

Configuration: Basic

Name: MyHZN-LTM-AP_BE_443_pool

Description:

Health Monitors:

Active:

- MyHZN-LTM-AP_BE_TCP
- MyHZN-LTM-AP_BE_UDP

Available:

- AppVolumes-Monitor
- MyHZN-LTM-AP_https_2
- View-LTM-External_BE_TCP
- View-LTM-External_BE_UDP

Resources:

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

New Members:

New Node (selected) New FQDN Node Node List

Node Name: (Optional)

Address: 10.105.169.101

Service Port: 443 HTTPS

Add

R:1 P:0 C:0 10.105.169.100 10.105.169.100 :443

R:1 P:0 C:0 10.105.169.101 10.105.169.101 :443

Edit Delete

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 displays the F5 LTM Configuration Utility interface for creating a new pool. The configuration is set to 'Basic'. The 'Name' field contains 'MyHZN-LTM-AP_BE_8443_pool'. The 'Health Monitors' section shows two monitors, 'MyHZN-LTM-AP_BE_TCP' and 'MyHZN-LTM-AP_BE_UDP', which have been moved from the 'Available' list to the 'Active' list. The 'Load Balancing Method' is set to 'Least Connections (member)'. The 'Priority Group Activation' is set to 'Disabled'. In the 'New Members' section, the 'New Node' radio button is selected. The 'Node Name' field is empty. The 'Address' field contains '10.105.169.101'. The 'Service Port' field contains '8443'. The 'Add' button is highlighted. Below the 'Add' button, a list of members is shown: 'R:1 P:0 C:0 10.105.169.100 10.105.169.100 :8443' and 'R:1 P:0 C:0 10.105.169.101 10.105.169.101 :8443'. The 'Finished' button is highlighted at the bottom.

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.

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

General Properties

Name	MyHZN-LTM-AP_443_UDP
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443 HTTPS
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)	<div>Selected: <div></div></div> <div>Available: /Common, AppVolumes-ClientSSL, AppVolumes-SSL, VPN-ClientSSL, Wildcard-ClientSSL</div>
SSL Profile (Server)	<div>Selected: <div></div></div> <div>Available: /Common, AppVolumes-ServerSSL, apm-default-serverssl, crypto-client-default-serverssl, pcolp-default-serverssl</div>
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 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**.

The screenshot shows the 'Resources' configuration window. The left sidebar contains 'iRules' and 'Policies'. The main area has two sections: 'iRules' and 'Policies'. Each section has an 'Enabled' list and an 'Available' list. The 'iRules' 'Available' list contains: _sys_https_redirect, kerberos, test-rule, vIDM-Layered-VIP-BACK, and vIDM-Layered-VIP-Front. Below these lists are 'Up' and 'Down' buttons. The 'Default Pool' dropdown is set to 'MyHZN-LTM-AP_BE_443_pool'. The 'Default Persistence Profile' dropdown is set to 'source_addr'. The 'Fallback Persistence Profile' dropdown is set to 'None'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons. The 'Finished' button is circled in red.

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.

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

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)	<div>Selected</div> <div>Available</div> <div>/Common AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL</div>
SSL Profile (Server)	<div>Selected</div> <div>Available</div> <div>/Common AppVolumes-ServerSSL apm-default-serverssl crypto-client-default-serverssl pcolp-default-serverssl</div>
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 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**.

Resources

iRules

Enabled: [] Available: /Common, Horizon7_Rule, Smartcard-iRule, Workspace-One-JSession, _sys_APM_ExchangeSupport_OA_BasicAuth

Up Down

Policies

Enabled: [] Available: []

Default Pool: + MyHZN-LTM-AP_BE_8443_pool

Default Persistence Profile: source_addr

Fallback Persistence Profile: None

Cancel Repeat **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

MyHZN-LTM* Search Reset Search Create...

✓	▼	Status	▲ Name	Description	Application	Destination	Service Port	Type	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_top		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

Enable Disable Delete...

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**.

Local Traffic > Monitors > New Monitor...

General Properties

Name: MyHZN-LTM-AP_https

Description:

Type: HTTPS

Parent Monitor: https

Configuration: Basic

Interval: 30 seconds

Timeout: 91 seconds

Send String: GET /broker/xml/ HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n

Receive String: clientlaunch-default

Receive Disable String:

Cipher List: DEFAULT:+SHA:+3DES:+KEDH

User Name:

Password:

Client Certificate: None

Client Key: None

Reverse: Yes No

Transparent: Yes No

Alias Address: * All Addresses

Alias Service Port: * All Ports

Adaptive: Enabled

Cancel Repeat Finished

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**.

The screenshot shows the 'General Properties' and 'Configuration' tabs of the HTTPS Monitor configuration window. Red circles highlight the following fields and values:

- Name:** MyHZN-LTM-AP_https_2
- Type:** HTTPS
- Parent Monitor:** https
- Interval:** 30 seconds
- Timeout:** 91 seconds
- Send String:** GET /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
- Receive String:** 200
- Receive Disable String:** 503
- Finished button:** Located at the bottom right of the window.

Other visible fields include Description, Cipher List (DEFAULT:SHA:+3DES:+kEDH), User Name, Password, Client Certificate (None), Client Key (None), Reverse (No), Transparent (No), Alias Address (* All Addresses), Alias Service Port (* All Ports), and Adaptive (Enabled).

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 checked="" type="radio"/> Yes <input type="radio"/> No
Transparent	<input checked="" type="radio"/> Yes <input type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	* All Ports
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**.

The screenshot shows the 'General Properties' dialog for creating a new monitor. The 'Name' field is set to 'MyHZN-LTM-AP_udp'. The 'Type' is set to 'UDP' and the 'Parent Monitor' is set to 'udp'. Under the 'Configuration' section, the 'Interval' is set to '30 seconds' and the 'Timeout' is set to '91 seconds'. The 'Send String' field contains the text 'default send string'. At the bottom, the 'Finished' button is highlighted.

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	* All Ports
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 displays the 'Create Pool' configuration wizard in the F5 LTM Configuration Utility. The 'Configuration: Basic' tab is active. The 'Name' field is set to 'MyHZN-LTM-AP_443'. The 'Health Monitors' section shows a list of monitors under the 'Active' tab, including 'Common', 'MyHZN-LTM-AP_https', 'MyHZN-LTM-AP_https_2', 'MyHZN-LTM-AP_udp', and 'MyHZN-LTM-AP_tcp'. The 'Load Balancing Method' is set to 'Least Connections (member)'. The 'Priority Group Activation' is set to 'Disabled'. The 'New Members' section shows the 'New Node' button selected, with the 'Node Name' field empty, 'Address' set to '10.105.169.101', and 'Service Port' set to '443'. The 'Add' button is highlighted. The 'Finished' button is highlighted at the bottom of the wizard.

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**.

Configuration: Basic

Name: MyHZN-LTM-AP_8443

Description:

Health Monitors:

Active	Available
/Common MyHZN-LTM-AP_tcp MyHZN-LTM-AP_udp	/Common AppVolumes-Monitor MyHZN-LTM-AP_https MyHZN-LTM-AP_https_2 View-LTM-External_BE_TCP

Resources:

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

New Members:

New Node New FQDN Node Node List

Node Name: (Optional)

Address: 10.105.169.101

Service Port: 8443

Add

Edit Delete

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**.

Configuration: Basic

Name: MyHZN-LTM-AP_pcoip_pool

Description:

Health Monitors:

Active: MyHZN-LTM-AP_tcp, MyHZN-LTM-AP_udp

Available: MyHZN-LTM-AP_https, MyHZN-LTM-Int_https

Resources:

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

New Members:

New Node: Node Name, Address: 10.105.169.101, Service Port: 4172, Add

Node List (Optional): R:1 P:0 C:0 10.105.169.100 10.105.169.100 :4172, R:1 P:0 C:0 10.105.169.101 10.105.169.101 :4172

Buttons: Cancel, Repeat, 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.

Local Traffic > Pools : Pool List

Pool List Statistics

Search: MyHZN-LTM* Search Reset Search

Status	Name
●	MyHZN-LTM-AP_4172
●	MyHZN-LTM-AP_443
●	MyHZN-LTM-AP_8443

Delete...

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**.

Local Traffic > Profiles > Services > HTTP > New HTTP Profile...

General Properties

Name: MyH2N-LTM-int-1
Proxy Mode: Reverse
Parent Profile: http

Settings Custom ☒ Default ☐

Basic Auth Realm		<input type="checkbox"/>
Fallback Host		<input type="checkbox"/>
Fallback on Error Codes		<input type="checkbox"/>
Request Header Erase		<input type="checkbox"/>
Request Header Insert		<input type="checkbox"/>
Response Headers Allowed		<input type="checkbox"/>
Request Chunking	Preserve	<input type="checkbox"/>
Response Chunking	Selective	<input type="checkbox"/>
OneConnect Transformations	Enabled	<input type="checkbox"/>
Redirect Rewrite	Matching	<input checked="" type="checkbox"/>
Encrypt Cookies		<input type="checkbox"/>
Cookie Encryption Passphrase		<input type="checkbox"/>
Confirm Cookie Encryption Passphrase		<input type="checkbox"/>
Insert X-Forwarded-For	Enabled	<input checked="" type="checkbox"/>
LVS Maximum Columns	80	<input type="checkbox"/>
LVS Separator		<input type="checkbox"/>
Maximum Requests	0	<input type="checkbox"/>
Send Proxy Via Header In Request	Preserve	<input type="checkbox"/>
Send Proxy Via Header In Response	Preserve	<input type="checkbox"/>
Accept XFF	<input type="checkbox"/>	<input type="checkbox"/>
XFF Alternative Names		<input type="checkbox"/>
Server Agent Name	BigIP	<input type="checkbox"/>

Cancel Repeat Finished

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**.

The screenshot shows the 'General Properties' and 'Settings' sections of a UDP profile configuration window. In the 'General Properties' section, the 'Name' field is set to 'MyHZN-LTM-AP E' and the 'Parent Profile' dropdown is set to 'udp'. Both fields are circled in red. The 'Settings' section contains several options: 'Proxy Maximum Segment' (unchecked), 'Idle Timeout' (60 seconds), 'IP ToS' (0), 'Link QoS' (0), 'Datagram LB' (unchecked), 'Allow No Payload' (unchecked), 'TTL Mode' (Proxy), and 'Don't Fragment Mode' (PMTU). At the bottom, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is circled in red.

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

Buttons: 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 for creating a TCP profile. The 'Name' field contains 'MyHZN-LTM-AP' and the 'Parent Profile' dropdown is set to 'tcp-wan-optimized'. At the bottom, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is 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 for creating a TCP profile. The 'Name' field contains 'MyHZN-LTM-AP' and the 'Parent Profile' dropdown is set to 'tcp-lan-optimized'. At the bottom, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is 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**.

Local Traffic > Profiles > Persistence > New Persistence Profile...

General Properties

Name: MIRROR-LTM-02

Persistence Type: Source Address Affinity

Parent Profile: source_addr

Configuration

Mirror Persistence: ☒

Match Across Services: ☒

Match Across Virtual Servers: ☐

Match Across Pools: ☒

Hash Algorithm: Default

Timeout: Specify: 180 seconds

Profile Length: None

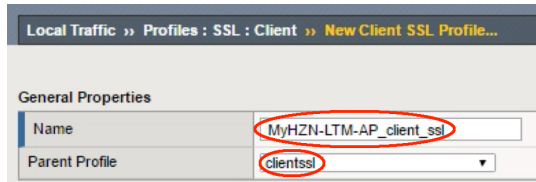
Map Probes: ☒ Enabled

Override Connection Limit: ☐

Cancel Repeat 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.



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

General Properties

Name	MyHZN-LTM-AP_client_ssl
Parent Profile	clientssl

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



Configuration: Basic Custom

Certificate Key Chain

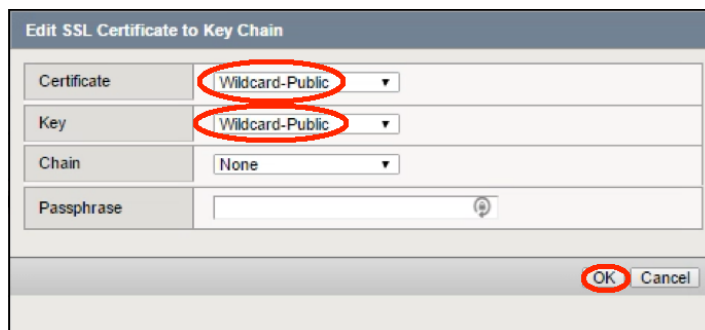
OCSP Stapling

Notify Certificate Status to Virtual Server

Proxy SSL

Proxy SSL Passthrough

- 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**.



Edit SSL Certificate to Key Chain

Certificate	Wildcard-Public
Key	Wildcard-Public
Chain	None
Passphrase	

OK Cancel

- 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**.

General Properties

Name: MyHZN-LTM-AP_client_ssl
Parent Profile: clientssl

Configuration: Basic Custom

Certificate Key Chain
/Common/Wildcard-Public.crl /Common/Wildcard-Public.key
Add Edit Delete

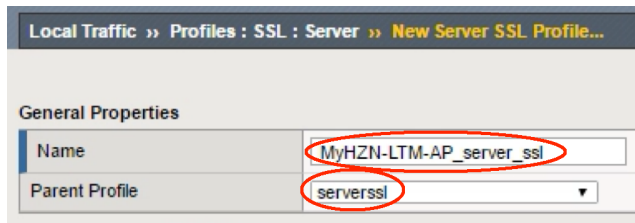
Client Authentication Custom

Client Certificate	Ignore	<input checked="" type="checkbox"/>
Frequency	once	<input type="checkbox"/>
Retain Certificate	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Certificate Chain Traversal Depth	9	<input type="checkbox"/>
Trusted Certificate Authorities	None	<input checked="" type="checkbox"/>
Advertised Certificate Authorities	None	<input checked="" type="checkbox"/>
Certificate Revocation List (CRL)	None	<input type="checkbox"/>
Allow Expired CRL	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Repeat **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.

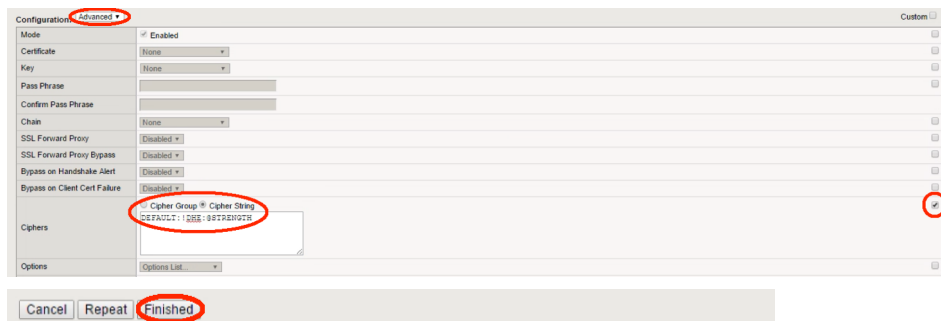


Local Traffic >> Profiles : SSL : Server >> New Server SSL Profile...

General Properties

Name	MyHZN-LTM-AP_server_ssl
Parent Profile	serverssl

- 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**.



Configuration: Advanced

Mode: ☒ Enabled

Certificate: None

Key: None

Pass Phrase:

Confirm Pass Phrase:

Chain: None

SSL Forward Proxy: Disabled

SSL Forward Proxy Bypass: Disabled

Bypass on Handshake Alert: Disabled

Bypass on Client Cert Failure: Disabled

Ciphers: ☒ Cipher Group ☒ Cipher String

Options: Options List

Cancel Repeat 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.

General Properties	
Name	MyHZN-LTM-AP_redirect
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	80 HTTP
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**.

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)	<div>Selected: <div></div> Available: <div>MyHZN-LTM-AP_client_ssl, VPN-ClientSSL, Wildcard-ClientSSL, clientssl</div></div>
SSL Profile (Server)	<div>Selected: <div></div> Available: <div>MyHZN-LTM-AP_server_ssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl, serverssl, serversslsecure-compatibility</div></div>
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**.

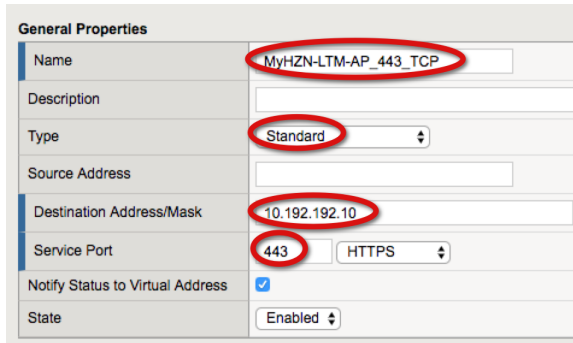
The screenshot shows the 'Resources' configuration window. The 'iRules' section has two lists: 'Enabled' and 'Available'. The 'Available' list contains the following items: `_sys_auth_ssl_ocsp`, `_sys_auth_tacacs`, `kerberos`, `test-inrule`, and `VIDM-Layered-VIP-BACK`. The item `_sys_https_redirect` is highlighted in the 'Available' list. A red circle is drawn around this item, and another red circle is drawn around the '<<' button, indicating the action to be taken. Below the 'Available' list is a '>>' button. The 'Policies' section has empty 'Enabled' and 'Available' lists with '<<' and '>>' buttons. The 'Default Pool' is set to 'None', 'Default Persistence Profile' is 'None', and 'Fallback Persistence Profile' is 'None'. At the bottom, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is circled in red.

Resources	
iRules	Enabled
	Available
Policies	Enabled
	Available
Default Pool	None
Default Persistence Profile	None
Fallback Persistence Profile	None

Cancel Repeat Finished

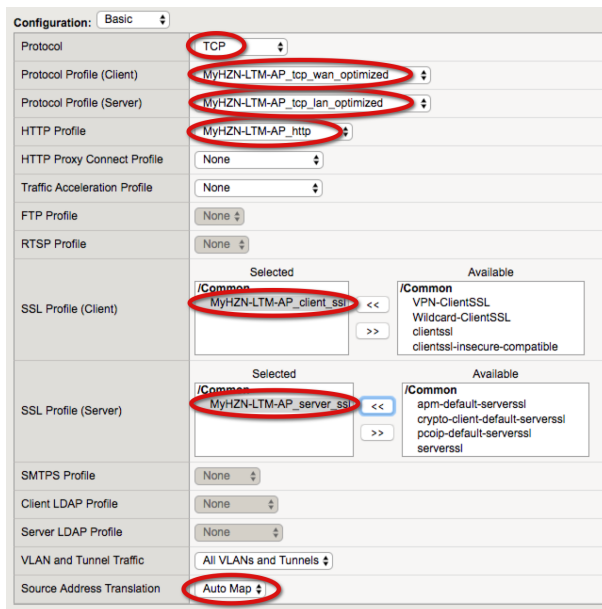
Port 443 TCP - Virtual Server

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 HTTPS
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: MyHZN-LTM-AP_client_ssl; Available: /Common VPN-ClientSSL, Wildcard-ClientSSL, clientssl, clientssl-insecure-compatible
SSL Profile (Server)	Selected: MyHZN-LTM-AP_server_ssl; Available: /Common apm-default-serverssl, crypto-client-default-serverssl, pcoip-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**.

The screenshot displays the 'Resources' configuration page in the NetScaler GUI. It is divided into two main sections: 'iRules' and 'Policies'. In the 'iRules' section, the 'Enabled' list contains 'Horizon7_Rule' (circled in red), and the 'Available' list contains several other rules. A red circle highlights the '<<' button used to move the rule from Available to Enabled. Below this, the 'Default Pool' is set to 'MyHZN-LTM-AP_443' (circled in red), and the 'Default Persistence Profile' is set to 'MyHZN-LTM-AP_Persistence' (circled in red). The 'Fallback Persistence Profile' is set to 'None'. At the bottom, the 'Finished' button is circled in red, indicating the final step in the configuration process.

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 HTTPS
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)	Selected: [Empty] Available: /Common, MyHZN-LTM-AP_client_ssl, VPN-ClientSSL, Wildcard-ClientSSL, clientssl
SSL Profile (Server)	Selected: [Empty] Available: /Common, MyHZN-LTM-AP_server_ssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl
SMTSPS 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**.

The screenshot shows the 'Resources' configuration window. It contains the following elements:

- iRules**: A section with 'Enabled' and 'Available' lists. The 'Available' list contains: /Common, Horizon7_Rule, Smartcard-iRule, Workspace-One-JSession, _sys_APM_ExchangeSupport_OA_BasicAuth. There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list.
- Policies**: A section with 'Enabled' and 'Available' lists. There are '<<' and '>>' buttons between the lists.
- Default Pool**: A dropdown menu with a '+' icon on the left. The selected value is 'MyHZN-LTM-AP_443', which is circled in red.
- Default Persistence Profile**: A dropdown menu. The selected value is 'MyHZN-LTM-AP_Persistence', which is circled in red.
- Fallback Persistence Profile**: A dropdown menu with the value 'None'.
- Buttons**: At the bottom, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is circled in red.

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**.

The screenshot shows the 'General Properties' tab of a virtual server configuration. The fields are as follows:

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**.

The screenshot shows the 'Configuration' tab of a virtual server configuration. The fields are as follows:

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)	<div>Selected: <div></div> Available: <div>MyHZN-LTM-AP_client_ssl, VPN-ClientSSL, Wildcard-ClientSSL, clientssl</div></div>
SSL Profile (Server)	<div>Selected: <div></div> Available: <div>MyHZN-LTM-AP_server_ssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl</div></div>
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**.

The screenshot shows the 'Resources' configuration page. The left sidebar contains the following items: 'iRules', 'Policies', 'Default Pool', 'Default Persistence Profile', and 'Fallback Persistence Profile'. The main configuration area is divided into two sections: 'iRules' and 'Policies'. The 'iRules' section has an 'Enabled' list (empty) and an 'Available' list containing 'kerberos', 'test-irule', 'vDM-Layered-VIP-BACK', 'vDM-Layered-VIP-Front', and 'Horizon7_Rule'. There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list. The 'Policies' section has an 'Enabled' list (empty) and an 'Available' list (empty), with '<<' and '>>' buttons between them. Below these sections are three dropdown menus: 'Default Pool' (set to 'MyHZN-LTM-AP_8443'), 'Default Persistence Profile' (set to 'MyHZN-LTM-AP_Persistence'), and 'Fallback Persistence Profile' (set to 'None'). The 'Default Pool' and 'Default Persistence Profile' dropdowns are circled in red. At the bottom of the page are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is circled in red.

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**.

The screenshot shows the 'General Properties' tab of a virtual server configuration. The following fields are highlighted with red circles:

- Name:** MyHZN-LTM-AP_8443_UDP
- Type:** Standard
- Destination Address/Mask:** 10.192.192.10
- Service Port:** 8443

Other visible fields include Description, Source Address, Notify Status to Virtual Address (checked), and 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**.

The screenshot shows the 'Configuration' tab of a virtual server. The following fields are highlighted with red circles:

- Protocol:** UDP
- Protocol Profile (Client):** MyHZN-LTM-AP_udp_profile
- Protocol Profile (Server):** (Use Client Profile)
- Source Address Translation:** Auto Map

Other visible fields include SSL Profile (Client), SSL Profile (Server), SMTPS Profile, Client LDAP Profile, Server LDAP Profile, Netflow Profile, and VLAN and Tunnel Traffic.

- 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**.

Resources

iRules	Enabled	Available	
	<div><< >> Up Down</div>	<div>kerberos test-irule vDM-Layered-VIP-BACK vDM-Layered-VIP-Front Horizon7_Rule</div>	
Policies	Enabled	Available	
	<div><< >></div>		
Default Pool	+	MyHZN-LTM-AP_8443	
Default Persistence Profile		MyHZN-LTM-AP_Persistence	
Fallback Persistence Profile		None	
<div>Cancel Repeat Finished</div>			

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-ian-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_ian_optimized
HTTP Profile	None
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	<div>Selected: <div></div></div> <div>Available: <div>MyHZN-LTM-AP_client_ssl, VPN-ClientSSL, Wildcard-ClientSSL, clientssl</div></div>
SSL Profile (Server)	<div>Selected: <div></div></div> <div>Available: <div>MyHZN-LTM-AP_server_ssl, apm-default-serverssl, crypto-client-default-serverssl, poaip-default-serverssl</div></div>
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 PColP 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**.

Resources

	Enabled	Available
iRules	<div><< >> Up Down</div>	<div>/Common Horizon7_Rule Smartcard-iRule Workspace-One-JSession _sys_APM_ExchangeSupport_OA_BasicAuth</div>
Policies	<div><< >></div>	
Default Pool	+ MyHZN-LTM-AP_4172	
Default Persistence Profile	MyHZN-LTM-AP_Persistence	
Fallback Persistence Profile	None	

Cancel Repeat **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)	<div>Selected</div> <div>Available</div> <div>/Common MyHZN-LTM-AP_client_ssl VPN-ClientSSL Wildcard-ClientSSL clientssl</div>
SSL Profile (Server)	<div>Selected</div> <div>Available</div> <div>/Common MyHZN-LTM-AP_server_ssl apm-default-serverssl crypto-client-default-serverssl pcopip-default-serverssl</div>
SMTSPS 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 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**.

The screenshot shows the 'Resources' configuration page for a virtual server. It includes sections for 'iRules' and 'Policies', each with 'Enabled' and 'Available' lists. Below these, the 'Default Pool' is set to 'MyHZN-LTM-AP_4172', the 'Default Persistence Profile' is set to 'MyHZN-LTM-AP_Persistence', and the 'Fallback Persistence Profile' is set to 'None'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons, with 'Finished' being the target of the final step.

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

MyHZN-LTM Search Reset Search Create...

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	●	MyHZN-LTM-AP_4172_TCP			10.192.192.10	4172	Standard	Edit...	Common
<input type="checkbox"/>	●	MyHZN-LTM-AP_4172_UDP			10.192.192.10	4172	Standard	Edit...	Common
<input type="checkbox"/>	●	MyHZN-LTM-AP_443_TCP			10.192.192.10	443 (HTTPS)	Standard	Edit...	Common
<input type="checkbox"/>	●	MyHZN-LTM-AP_443_UDP			10.192.192.10	443 (HTTPS)	Standard	Edit...	Common
<input type="checkbox"/>	●	MyHZN-LTM-AP_8443_TCP			10.192.192.10	8443	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_redirect			10.192.192.10	80 (HTTP)	Standard	Edit...	Common

Enable Disable Delete...

Testing the VMware Horizon Connection

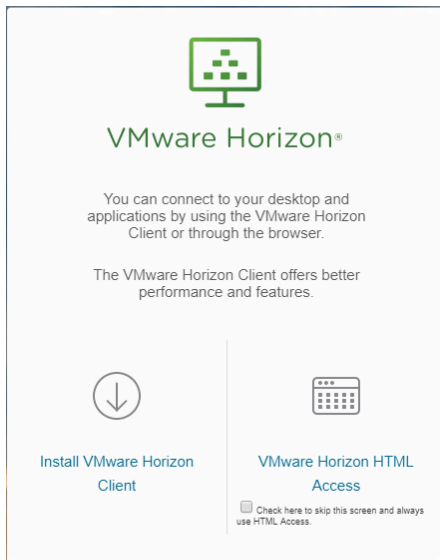
After setting up the Virtual IPs (VIPs) for the Unified Access Gateways, you can use the following methods validate that the External VIP is connecting and working properly. In this case, you are now using the new FQDN site name to connect to the Horizon Environment.

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

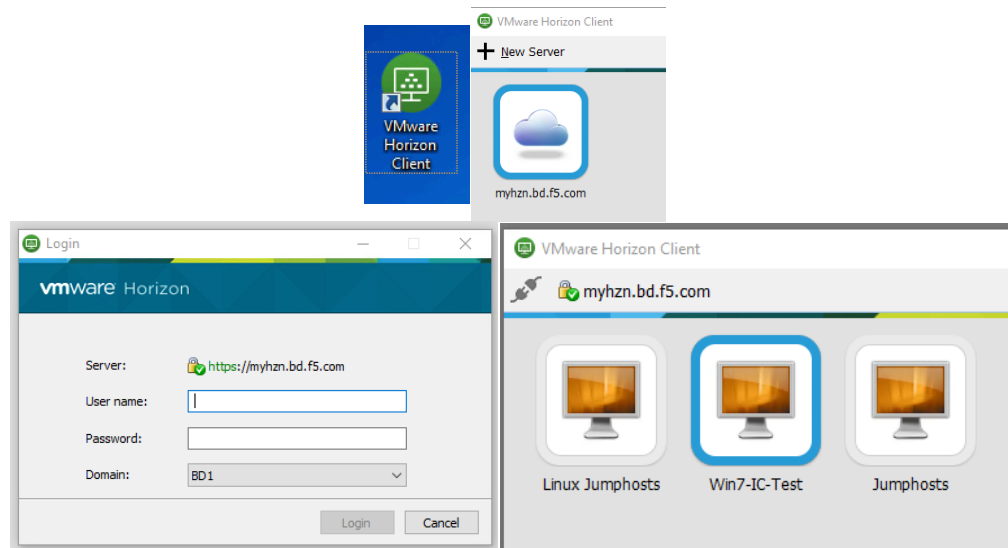
1. In a browser, type the FQDN for the VIP you previously created (for example, <https://myhzn.bd.f5.com>).

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

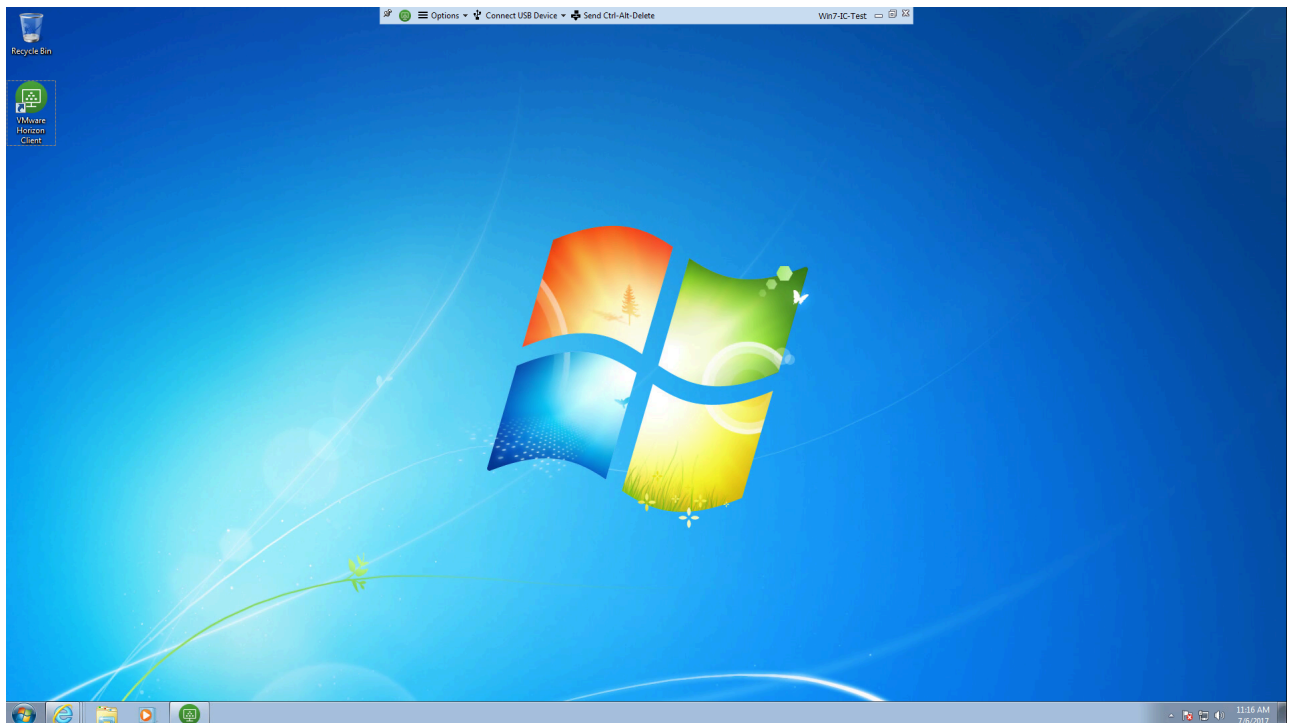
You should see the VMware Horizon Client/HTML5 Page. This confirms that your servers are working through the newly created virtual server.



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>