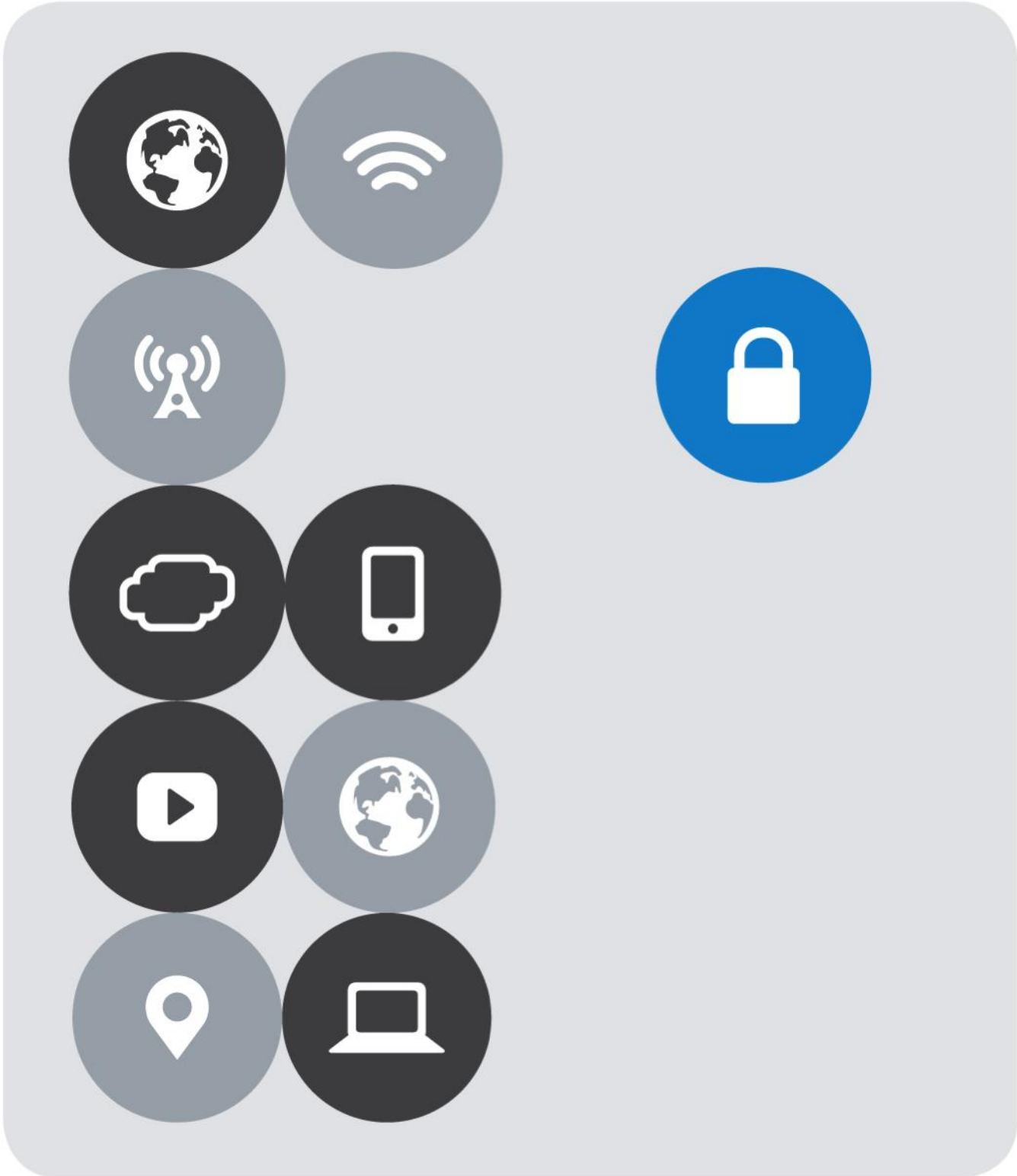




INTEGRATION GUIDE

Load Balancing VMware Unified Access Gateway



Version History

Date	Version	Author	Description	Compatible Versions
Dec 2020	3.0	Matt Mabis	Document Updates	Unified Access Gateway 2.x, 3.x, 2xxx (2)
Aug 2019	2.0	Matt Mabis	Document Updates and IAPP Integration Changes	Unified Access Gateway 2.x and 3.x (2)
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) (2) (3)

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.

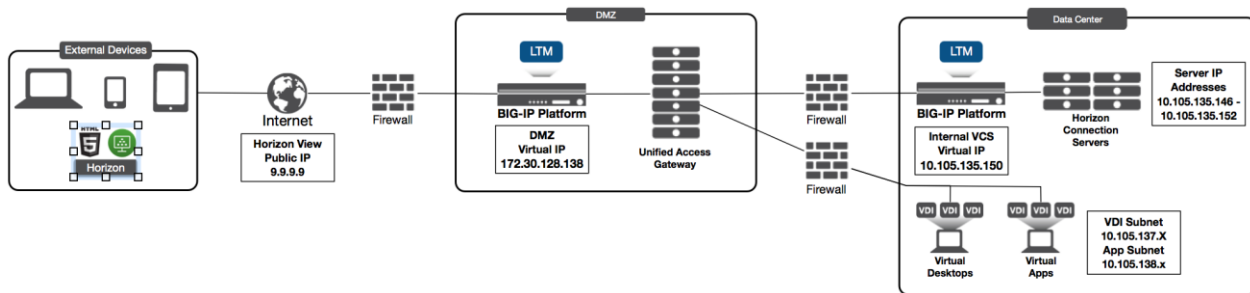
(2) Functionality for Blast Extreme UDP is only supported in VMware Unified Access Gateway 3.0.x and above

(3) 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	11
Configuring your Horizon 7 Environment for use with Unified Access Gateway.	13
Configuring your Horizon 8 Environment for use with Unified Access Gateway.	15
iRule for the Horizon Origin Header	17
Creating/Deploying a Virtual IP for External Connections	19
Using the iApp to Deploy a Virtual Server for UAG's	20
Final Configuration.....	26
Manually Creating a Virtual Server for UAG's	27
Creating Monitors.....	27
Creating Pools	31
Creating Profiles.....	34
Creating Virtual Servers.....	41
Final Configuration.....	55
Testing the VMware Horizon Connection	56
References	58

Overview



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 8443 and UDP 8443).
- 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.

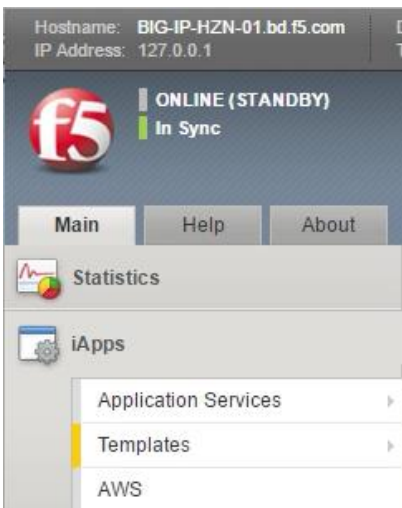
1. Create/import an SSL Certificate that contains the load balanced FQDN that will be used for the Horizon instance.
2. Upload the following to the BIG-IP system:
 - The SSL certificate.
 - The Private Key used for the load balanced FQDN certificate.
 - The Primary CA or Root CA for the SSL Certificate you uploaded to the BIG-IP.
3. 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.
4. VMware Horizon deployed and functional within the environment. This includes Horizon Connection Servers, VDI, and Unified Access Gateway Servers.
5. Download the latest F5 iApp templates and extract to an accessible location at https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=iApp_Templates
6. 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 at <https://www.f5.com/content/dam/f5/corp/global/pdf/deployment-guides/vmware-horizon-view-dg.pdf>
7. 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>. Also newest firewall rules can be referenced in VMware documentation for Unified Access Gateway in <https://docs.vmware.com/en/Unified-Access-Gateway>
8. For Single Namespace, internal vs external DNS need to be configured correctly for the Zones (Internet) to point at the Unified Access Gateway Servers Virtual IP (VIP) and the Internal DNS (LAN) would typically point at the Connection Servers Virtual IP (VIP).

Importing the iApp Template into BIG-IP

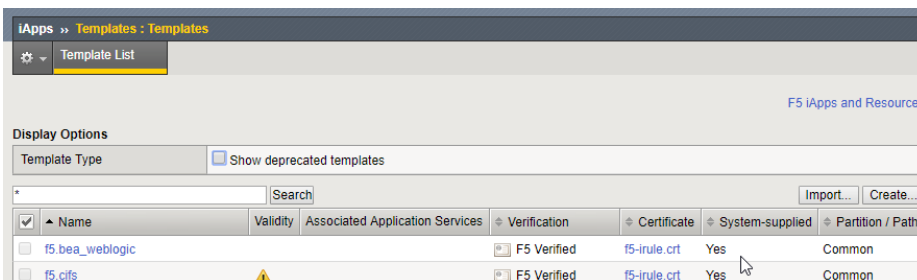
1. Login to the F5 Configuration utility.



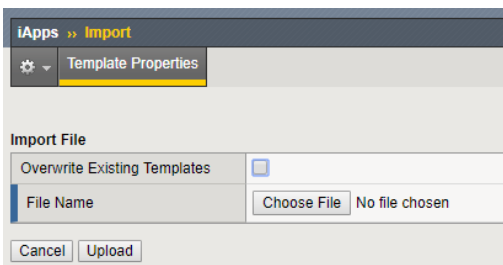
2. On the Main tab, click **iApps > Templates**.



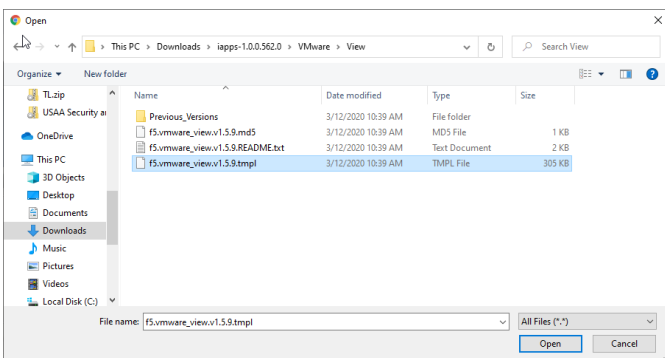
3. Click the **Import** button on the right upper side of the window.



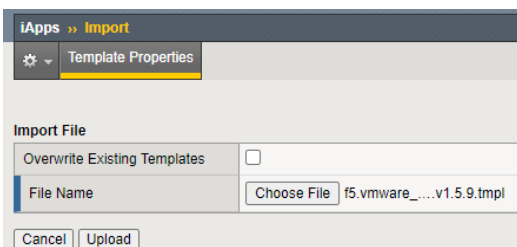
- Click the **Choose File** button.



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



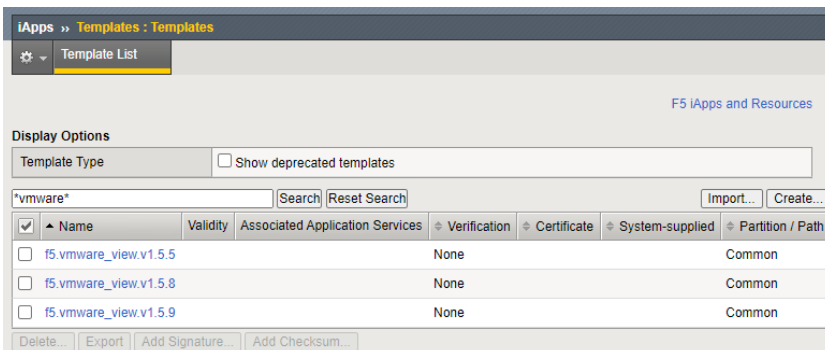
- Once the TMPL file is selected, the file name appears next to the Choose File button. Once that is correct, click **Upload** (Click **OK** on the Popup Prompt to install the configuration file).



This will install the configuration in the template file. Do you want to proceed?



- Once the upload is complete ensure the template is available. You can use the search `*vmware*` to find the template.



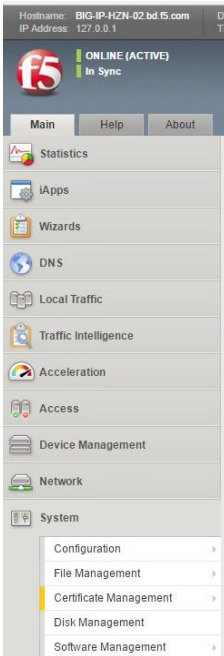
Importing a Certificate into BIG-IP

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

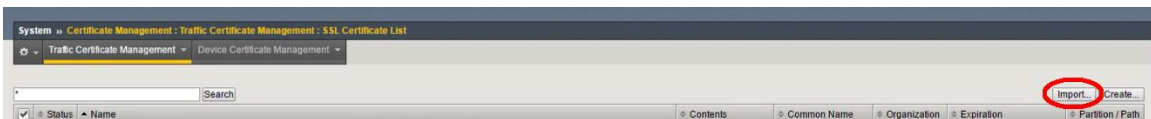
1. Login to the F5 Configuration utility.



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**.

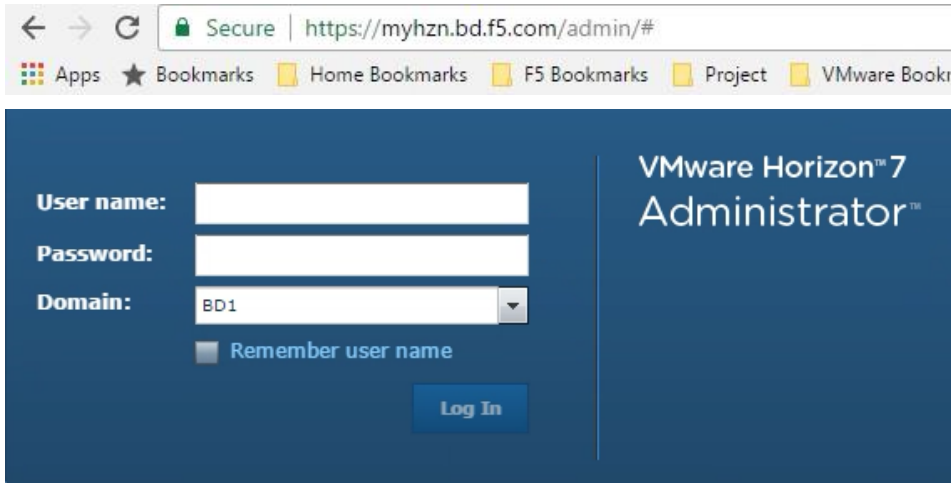
After the import is completed you see your certificate in the window. Click the certificate to verify all the information in it.

Status	Name	Contents	Common Name	Organization	Expiration	Partition / Path
<input checked="" type="checkbox"/>	MyHZN-internalCA	RSA Certificate & Key	MyHZN.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-tnlue	RSA Certificate	support.f5.com	F5 Networks	Aug 13, 2031	Common

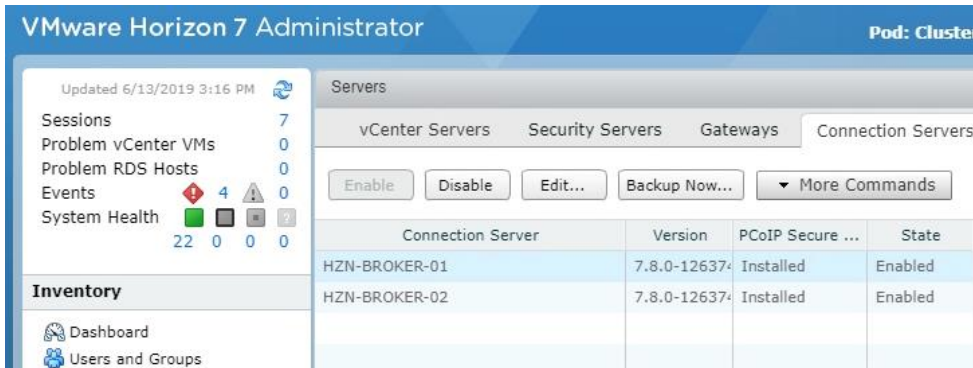
5. Verify the information in the Certificate/Key.

Configuring your Horizon 7 Environment for use with Unified Access Gateway.

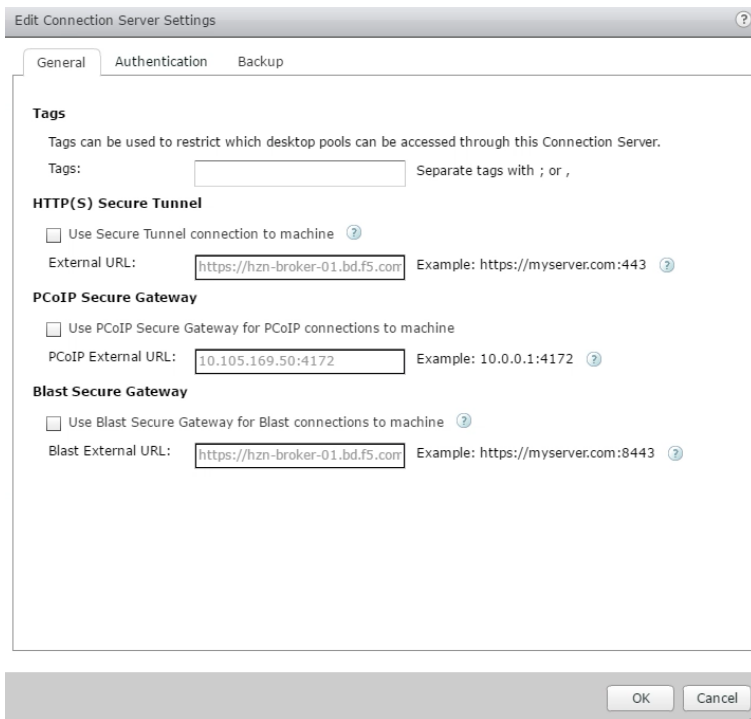
1. Login to the VMware Horizon Admin using the FQDN or individual broker webpage.



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



- 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.

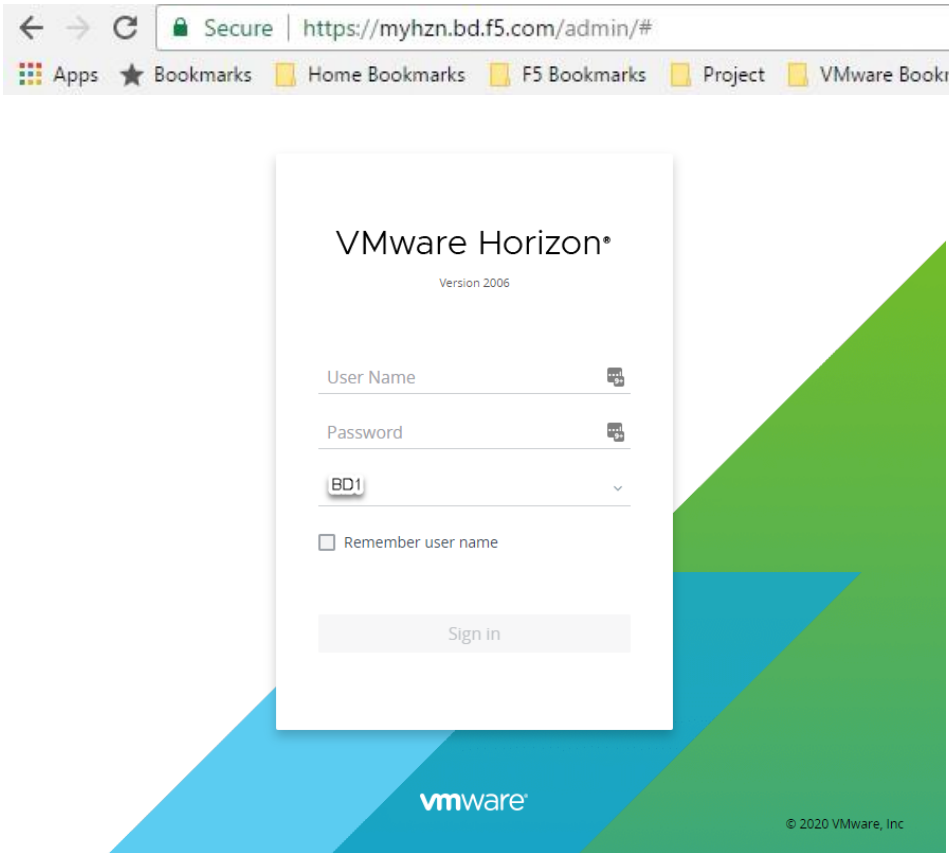


- In the Horizon Admin Window, edit any additional brokers that will be a part of the pool used to connect to the Unified Access Gateway Servers virtual server, and modify them in the same way as Step 3 (ensuring all boxes are unchecked).



Configuring your Horizon 8 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 go to (Settings → Servers → Connection Servers) select a Broker, and then click **Edit**.

Servers

vCenter Servers Gateways **Connection Servers**

Enable Disable Edit Backup Now

Filter


Connection Server	Version	PCoIP Secure Gate...	State	Settings	Last Backup
hzn-broker-01	8.0.0-16592062	Installed	Enabled	Smart card authentication: Optional, Automatic backup	✓ 12/09/2020, 12:00 AM
hzn-broker-02	8.0.0-16592062	Installed	Enabled	Smart card authentication: Optional, Automatic backup	✓ 12/09/2020, 12:00 AM

- Ensure that the Checkboxes for **Use Secure Tunnel connection to machine**, **PCoIP Secure Gateway** are **UNCHECKED**, and **Use Blast Secure Gateway** radio button is set to **Do not use Blast Secure Gateway** as having any of these checked/enabled 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 all Blast connections to machine 

Use Blast Secure Gateway for only HTML Access connections to machine 




Do not use Blast Secure Gateway 

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

- 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 protocols are unchecked and disabled).

Servers

vCenter Servers Gateways **Connection Servers**

Connection Server	Version	PCoIP Secure Gate...	State	Settings	Last Backup
hzn-broker-01	8.0.0-16592062	Installed	Enabled	Smart card authentication: Optional, Automatic backup	✓ 12/09/2020, 12:00 AM
hzn-broker-02	8.0.0-16592062	Installed	Enabled	Smart card authentication: Optional, Automatic backup	✓ 12/09/2020, 12:00 AM

iRule for the Horizon Origin Header

With the release of Horizon 7 and 8, an 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.

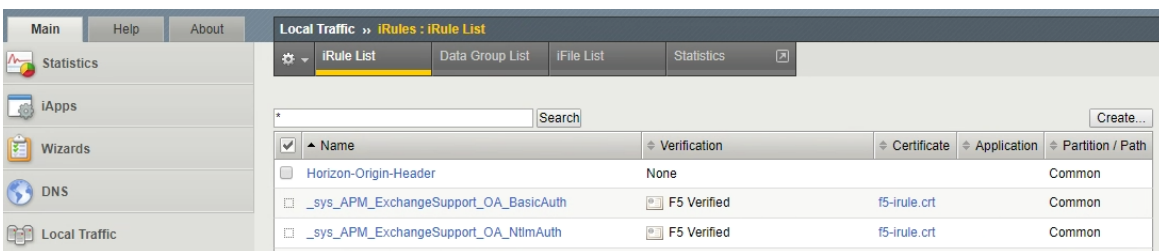
NOTE: Only one of these two methods are necessary.

Implementing an F5 iRule for Horizon Origin Header

1. Login to the BIG-IP Configuration utility.

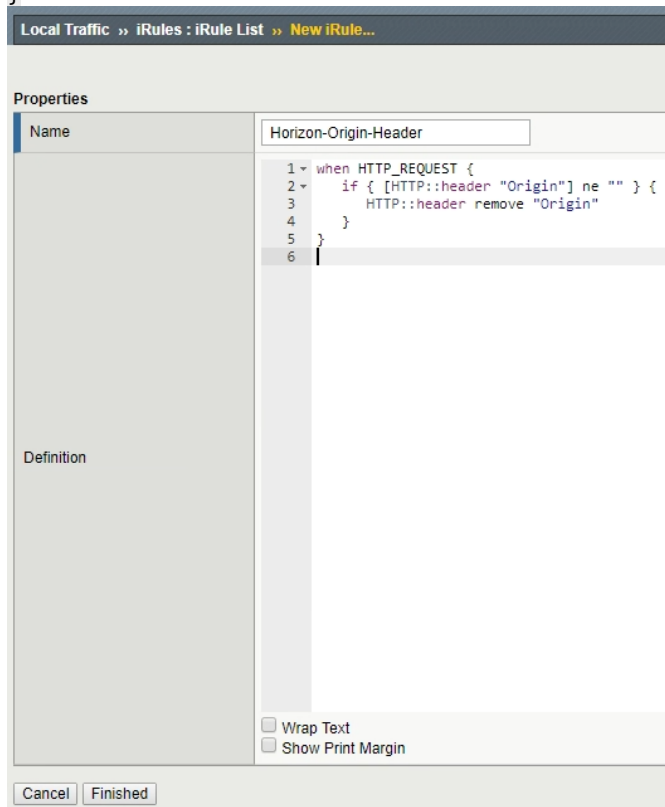


2. On the Main tab, click **Local Traffic > iRules** and then click **Create**.



- In the **Name** field, type a unique name for the iRule.
- 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"
  }
}
```

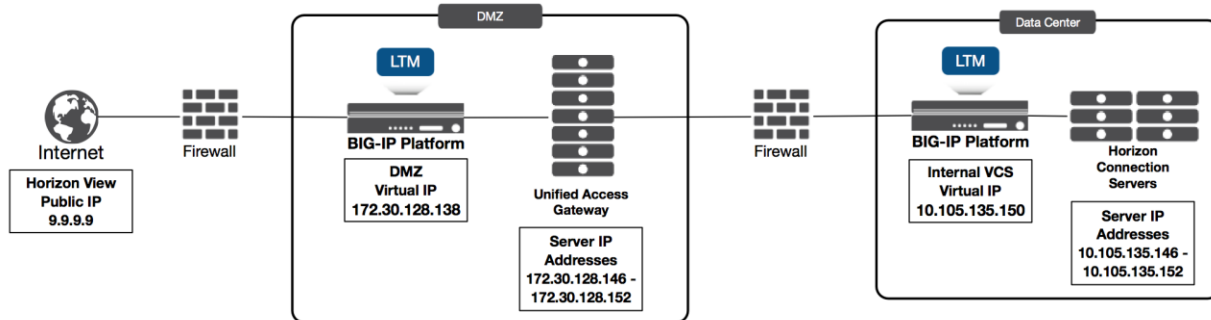


- Click **Finished**. Once created you should see your newly created iRule in the list.

The screenshot shows the 'iRule List' interface. A search bar is at the top left, and a 'Create...' button is at the top right. Below is a table listing the configured iRules:

Name	Verification	Certificate	Application	Partition / Path
<input checked="" type="checkbox"/> Horizon-Origin-Header	None			Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_OA_BasicAuth	F5 Verified	f5-irule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_OA_NtlmAuth	F5 Verified	f5-irule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_helper	F5 Verified	f5-irule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_main	F5 Verified	f5-irule.crt		Common

Creating/Deploying a Virtual IP 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.

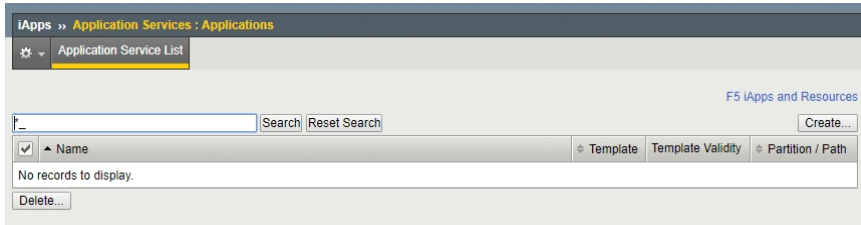
NOTE: There must be an internal Virtual IP (VIP) for the Horizon Connection Servers prior to configuring the UAG Servers. See Section [Prerequisites](#) for more details.

Using the iApp to Deploy a Virtual Server for UAG's

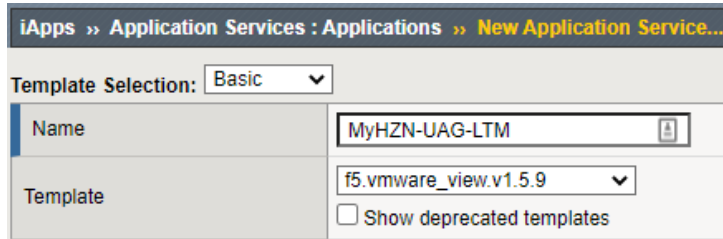
Before beginning this task, ensure you have previously imported the iApp Template as described in the [Importing iApp Template into BIG-IP](#) section.

Note: F5 Recommends using the latest iApp Available to ensure latest functionality and features are implemented, this build was using iApp Version 1.5.9

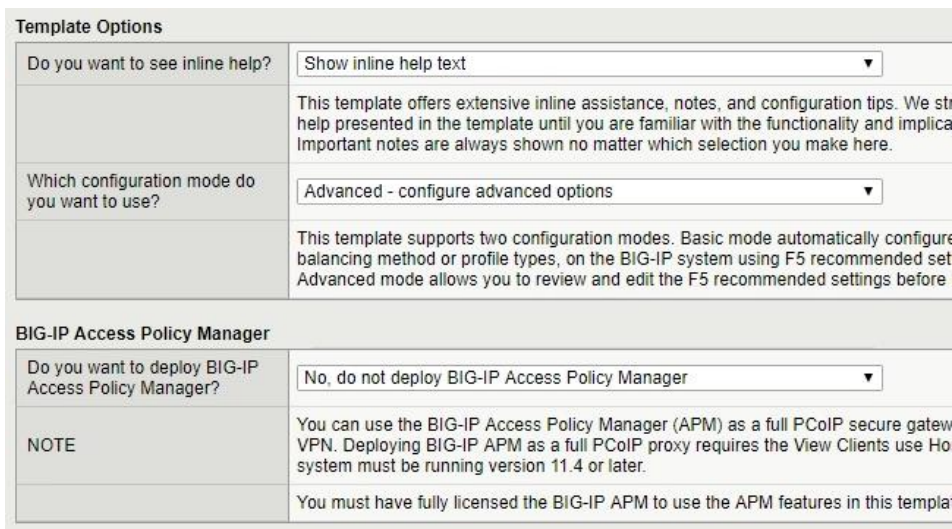
1. On the Main tab, click **iApps > Application Services > Create**.



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.v1.5.9** (or a newer version if available).



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**.



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?	<input type="text" value="Terminate SSL for clients, re-encrypt to View servers (SSL bridging)"/>
	<p>SSL is a cryptographic protocol used to secure client to server communications. Select how you want the BIG-IP system to handle encrypted traffic.</p> <p>If your environment requires clients use SSL and session persistence (which ensures requests from a single user are always distributed to the server on which they started), we recommend you configure the BIG-IP system for SSL offload. This allows the system to more accurately persist connections based on granular protocol or application-specific variables. Because encryption and decryption of SSL is computationally intensive and consumes server CPU resources, if your environment does not require encryption between the BIG-IP system and the View servers, select SSL Offload to terminate the SSL session from the client at the BIG-IP system and provide cleartext communication from the BIG-IP system to the servers.</p> <p>If security requirements do not allow the BIG-IP system to offload SSL, select to re-encrypt to the servers (SSL bridging). With this selection the system uses the SSL ID or Client/Server IP to enforce session persistence. Because these parameters are less granular, you may experience inconsistent distribution of client requests.</p>
Which Client SSL profile do you want to use?	<input type="text" value="Create a new Client SSL profile"/>
	<p>If you have already created a Client SSL profile that includes the appropriate certificate and key, you can select it from the list. Otherwise, the iApp creates a new Client SSL profile.</p>
Which SSL certificate do you want to use?	<input type="text" value="Wildcard"/>
	<p>To establish encrypted communication, a client and server negotiate security parameters that are used for the session. As part of this handshake, a certificate is provided by the server to the client to identify itself. The client can then validate the certificate with an authority for authenticity before sending data. When the BIG-IP system is decrypting communication between the client and server, an SSL certificate and key pair for each fully-qualified DNS name related to this application instance must be configured on the system.</p> <p>Select the SSL certificate you imported for this deployment. Importing certificates and keys is not a part of this template. See Local Traffic >> SSL Certificate List. To select any new certificates and keys you import, you need to restart or reconfigure this template.</p>
Which SSL private key do you want to use?	<input type="text" value="Wildcard"/>
	<p>Select the associated SSL key.</p>
NOTE:	<p>If your key is password-protected, you must manually create a Client SSL profile outside the iApp, and then select it from the list above.</p>
Which intermediate certificate do you want to use?	<input type="text" value="Do not use an Intermediate certificate"/>
	<p>Intermediate certificates, also called Intermediate certificate chains or chain certificates, are used to help systems which depend on SSL certificates for peer identification. These certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.</p> <p>Intermediate certificates must be created or imported onto this BIG-IP system prior to running this iApp. See http://support.f5.com/kb/en-us/solutions/public/13000/300/sol13302.html for help on creating an intermediate certificate chain.</p>
Do you want to redirect inbound HTTP traffic to HTTPS?	<input type="text" value="Redirect HTTP to HTTPS"/>
	<p>It is common for users to mistakenly attempt insecure access (HTTP) to a secure application (HTTPS). The BIG-IP system can automatically redirect these connections to use an encrypted connection.</p>
From which port should HTTP traffic be redirected?	<input type="text" value="80"/>

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 VMware UAGs?* question, select **Yes, PCoIP connections are proxied by the VMware UAGs.**
 - c. From the *Should Blast connections go through the BIG-IP system?* question, select **Yes, Blast connection should go through the BIG-IP system.**
 - d. From the *Will Blast connections be proxied by the VMware UAGs?* question, select **Yes, Blast connections are proxied by the VMware UAGs.**

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 UAGs. For this option to function properly, you must enable View secure tunnel option on the VMware UAGs, and enter the IP address entered in the next section with port 4172 appended. For example, 192.0.2.100:4172.	
Configure the Blast Display Protocol	
Should Blast connections go through the BIG-IP system?	Yes, Blast connections should go through the BIG-IP system
Select this option if Blast connections will be routed through the BIG-IP system.	
Will Blast connections be proxied by the VMware UAGs?	Yes, Blast 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 Blast traffic back to the VMware UAGs. For this option to function properly, you must enable View secure tunnel option on the VMware UAGs, and enter the IP address entered in the next section with port 8443 appended. For example, 192.0.2.100:8443.	
HTML5 Use Case	
HTML5 uses the same virtual server and port created for the Blast Configuration. No additional configuration is necessary.	

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.
 - c. If a longer persistence is required due to longer global timeouts it is recommended to create a persistence profile and modify the setting. If using a default configuration leave the default recommended persistence profile. (See VMware KB - <https://kb.vmware.com/s/article/56636>)

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, which public clients use to access the application. The system intercepts requests to this IP:Port and distributes them to the View Connection Servers.	
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, untrusted client virtual server, as well as for the optional internal, trusted virtual server. The default value displayed here is based your answer 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 serviced a client request. The F5 recommended method for tracking View sessions is Source Address persistence, which uses the source address to direct all subsequent requests from a given client to the same View server in the pool. We recommend this method, unless you have a specific reason to use another profile.	

8. Virtual Servers and Pools configuration continued.

- a. 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.
- b. For the next two questions, select the options based on your environment.
- c. 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.

Which servers should be included in this pool?	Node/IP address	10.105.169.100	Port	443	Conn limit	0	X
	Node/IP address	10.105.169.101	Port	443	Conn limit	0	X
Add							
Specify the IP address(es) of your View servers. If you have existing nodes on this BIG-IP system, you can select them from the list, otherwise type the addresses. Depending on your previous selections, you may need to add a Priority or Connection Limit. Click Add to include additional servers.							
Where will the virtual servers be in relation to the View servers?	BIG-IP virtual server IP and View servers are on different subnets						
It is important to ensure that responses to client requests made using the BIG-IP virtual server address are returned through the BIG-IP system. If the client receives a response directly from the View server, the connection is dropped. The way the BIG-IP system handles this depends on your network topology.							
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 the 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 associated pool, select BIG-IP virtual server IP and the 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?	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 IP setting of the View servers is required to ensure the correct 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. In this scenario, no configuration is needed to support your environment to ensure correct server response handling.							
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. 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.							
Should the BIG-IP system insert the X-Forwarded-For header?	Yes, insert the X-Forwarded-For HTTP header						
If you choose to insert the X-Forwarded-For header, the BIG-IP system inserts the original client IP address in the HTTP header for logging purposes. Additional configuration may be required on the View server to log the value of the X-Forwarded-For header.							

9. In the Client and Server Optimization sections, leave all settings at the defaults.

Client Optimization	
Which Web Acceleration profile do you want to use for caching?	Do not use a Web Acceleration profile
Caching is the local storage of data for re-use. Once an item is cached on the BIG-IP the same data are served from local storage. This can improve client request response scalability by reducing load associated with processing subsequent requests.	
Use a custom Web Acceleration profile only if you need to define specific URIs that share	
Which HTTP compression profile do you want to use?	Do not compress HTTP responses
Compression improves performance and end user experience for Web applications that throughput bottlenecks. Compression reduces the amount of traffic sent to the client to	
How do you want to optimize client-side connections?	Use F5's recommended optimizations for WAN clients
The client-side TCP profile optimizes the communication between the BIG-IP system and behavior of the traffic which results in higher transfer rates, improved connection reliability.	
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 concurrent connections and connection rate to View servers. When enabled, the BIG-IP connection to each View server 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 behavior of the traffic which results in higher transfer rates, improved connection reliability.	

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

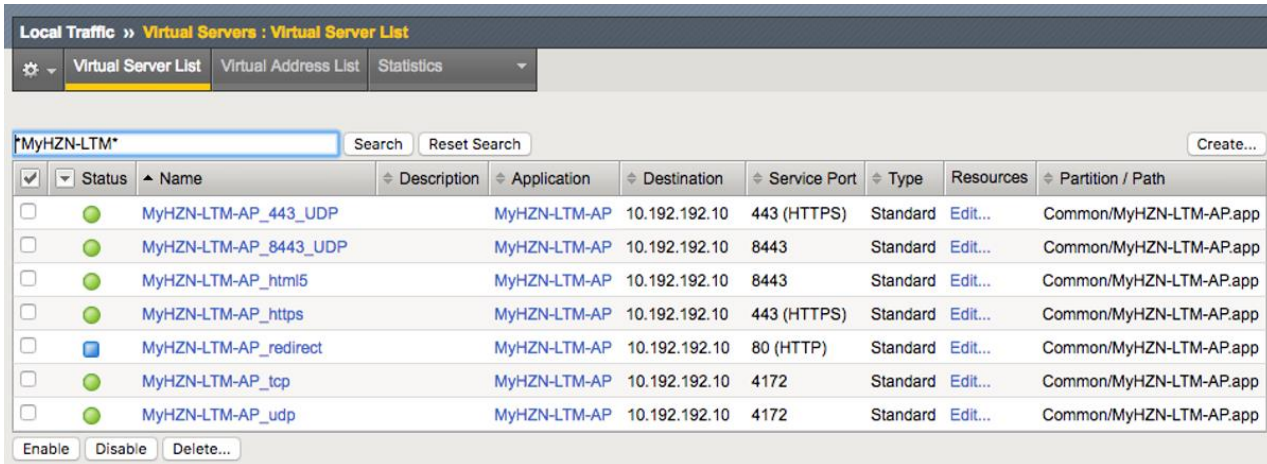
The screenshot displays the configuration summary for a BIG-IP system. The interface is organized into two main sections, each with a tree view on the left and a list of objects on the right. The status of each object is indicated by a colored icon: a green circle for 'Available' and a blue square for 'Unknown'.

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

At the bottom of the window, there are four buttons: **Enable**, **Disable**, **Force Offline**, and **Refresh**.

Final Configuration

Once completed, you should the iApp (1.5.9) will create the below configuration for F5 LTM with VMware Horizon Unified Access Gateway (UAG) for PCoIP and Blast Extreme TCP/UDP with BEAT (Blast Extreme Adaptive Transport).



The screenshot shows the F5 LTM configuration interface for a Virtual Server List. The search filter is set to "MyHZN-LTM*". The table lists eight virtual servers, all of which are in a "Up" status (indicated by a green dot). Each server is of type "Standard" and is located in the "Common/MyHZN-LTM-AP.app" partition. The servers are configured for various protocols and ports: 443 (HTTPS), 8443, 80 (HTTP), and 4172 (TCP/UDP).

<input type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	Up	MyHZN-LTM-AP_443_UDP		MyHZN-LTM-AP	10.192.192.10	443 (HTTPS)	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_8443_UDP		MyHZN-LTM-AP	10.192.192.10	8443	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_html5		MyHZN-LTM-AP	10.192.192.10	8443	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_https		MyHZN-LTM-AP	10.192.192.10	443 (HTTPS)	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_redirect		MyHZN-LTM-AP	10.192.192.10	80 (HTTP)	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_tcp		MyHZN-LTM-AP	10.192.192.10	4172	Standard	Edit...	Common/MyHZN-LTM-AP.app
<input type="checkbox"/>	Up	MyHZN-LTM-AP_udp		MyHZN-LTM-AP	10.192.192.10	4172	Standard	Edit...	Common/MyHZN-LTM-AP.app

Buttons: Enable, Disable, Delete...

Manually Creating a Virtual Server for UAG's

This Section is for customers who wish to manually configure the Virtual Servers for integrating a VMware UAG with F5. **Note: If you previously created an iApp deployment with the information in previous sections you do NOT need to follow these steps.**

Creating Monitors

As per VMware KB <https://kb.vmware.com/s/article/56636> the method used for the HTTPS monitor is an alternate way to identify if the Horizon environment is running correctly. F5 has used this method for many years on many VMware View and VMware Horizon versions. It is **NOT recommended** to change the interval time to anything less than 30 seconds as this can cause instabilities in the Horizon Connection Servers.

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) **{FQDN}** is replaced by **FQDN for VIP: GET /broker/xml/ HTTP/1.1\r\nHost: {FQDN}\r\nConnection: Close\r\n\r\n**
 - h. In the **Receive String** field, type **clientlaunch-default**.
 - i. Leave all other settings at the default and then click Finished.

The screenshot shows the 'New Monitor...' configuration window in the F5 management console. The 'General Properties' section is expanded, showing the following fields: Name (MyHZN-LTM-AP_https), Description (empty), Type (HTTPS), and Parent Monitor (https). The 'Configuration' section is set to 'Basic' and includes: Interval (30 seconds), Timeout (91 seconds), Send String (GET /broker/xml/ HTTP/1.1\r\nHost: myhzn.bd.f5.com\r\nConnection: Close\r\n\r\n), Receive String (clientlaunch-default), and Receive Disable String (empty). The 'User Name' and 'Password' fields are empty. The 'Reverse' and 'Transparent' options are set to 'No'. The 'Alias Address' is set to '* All Addresses' and the 'Alias Service Port' is set to '* All Ports'. The 'Adaptive' checkbox is unchecked. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons.

UAG Maintenance - Monitor

This monitor is used to identify when the Node is in Quiesce Mode (Maintenance). Depending on your version of VMware Horizon you could use VMware KB <https://kb.vmware.com/s/article/56636> to use HEAD instead of GET. The Received Disable String on an F5 BIG-IP is an error 503.

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 'New Monitor...' configuration window in VMware Horizon. The 'General Properties' section is expanded, showing the following fields:

- Name:** MyHZN-LTM-AP_uag_maintenance
- Description:** (empty)
- Type:** HTTPS
- Parent Monitor:** https

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

- 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
- User Name:** (empty)
- Password:** (empty)
- Reverse:** No (selected)
- Transparent:** No (selected)
- Alias Address:** * All Addresses
- Alias Service Port:** * All Ports
- Adaptive:** Not enabled

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

TCP (PCoIP/Blast) - Monitor

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

Local Traffic >> Monitors >> New Monitor...

General Properties

Name	MyHZN-LTM-AP_tcp
Description	
Type	TCP
Parent Monitor	tcp

Configuration: Basic

Interval	30 seconds
Timeout	91 seconds
Send String	
Receive String	
Receive Disable String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	* * 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**.

Local Traffic » Monitors » New Monitor...

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, uag_maintenance) 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**.

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

Configuration: Basic

Name: MyHZN-LTM-AP_443_pool

Description:

Health Monitors

Active	Available
/Common	/Common
MyHZN-LTM-AP_tcp	Mirage-Monitor
MyHZN-LTM-AP_udp	MyHZN-LTM-AP_https
MyHZN-LTM-AP_uag_maintenance	WS1-Monitor
	gateway_icmp

Resources

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

New Members

New Node New FQDN Node Node List

Node Name: (Optional)

Address: 192.168.30.59

Service Port: 443

Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
192.168.30.58	192.168.30.58	443		0
192.168.30.59	192.168.30.59	443		0

Edit Delete

Cancel Repeat Finished

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**.

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

Configuration: Basic

Name: MyHZN-LTM-AP_8443_pool

Description:

Health Monitors:

Active	Available
/Common	MyHZN-LTM-AP_udp_maintenance
MyHZN-LTM-AP_tcp	WS1-Monitor
MyHZN-LTM-AP_udp	gateway_icmp
	http
	http_head_f5
	https

Resources:

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

New Members:

New Node New FQDN Node Node List

Node Name: (Optional)

Address: 192.168.30.59

Service Port: 8443

Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
192.168.30.58	192.168.30.58	8443		0
192.168.30.59	192.168.30.59	8443		0

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**.

The screenshot shows the 'New Pool' configuration window. The 'Name' field is 'MyHZN-LTM-AP_pcoip_pool'. The 'Health Monitors' section shows two monitors selected: 'MyHZN-LTM-AP_tcp' and 'MyHZN-LTM-AP_udp'. The 'Load Balancing Method' is set to 'Least Connections (member)'. The 'New Members' section shows two nodes added:

Node Name	Address:FQDN	Service Port	Auto Populate	Priority
	192.168.30.58	4172		0
	192.168.30.59	4172		0

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.

The screenshot shows the 'Pool List' view. The search filter is '*LTM-AP*'. The table shows three pool objects, all with a green status icon:

✓	Status	Name
<input type="checkbox"/>	●	MyHZN-LTM-AP_443_pool
<input type="checkbox"/>	●	MyHZN-LTM-AP_8443_pool
<input type="checkbox"/>	●	MyHZN-LTM-AP_pcoip_pool

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	MyHZN-LTM-AP_H
Proxy Mode	Reverse
Parent Profile	http

Settings Custom

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	<input checked="" type="checkbox"/> 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"/>
LWS Maximum Columns	80	<input type="checkbox"/>
LWS 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**.

Local Traffic >> Profiles : Protocol : UDP >> New UDP Profile...

General Properties

Name	MyHZN-LTM-AP_U
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
Max Buffer Bytes	655350
Max Buffer Packets	0
Send Buffer	655350

Cancel Repeat Finished

Creating a TCP-WAN-Optimized Profiles

1. Create a 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. In **Data Transfer** section in the **Nagle's Algorithm** row, click the **Custom** checkbox on the right, and then select **Enable** from the list.
 - e. Leave all other settings at the default and then click **Finished**.

Local Traffic » Profiles : Protocol : TCP » New TCP Profile...

General Properties

Name	MyHZN-LTM-AP_w
Parent Profile	tcp-wan-optimized

Data Transfer Custom

Acknowledge on Push	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Delayed Acks	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Don't Fragment Flag (DF)	Pmtu	<input type="checkbox"/>
Initial Receive Window Size	3 MSS units	<input type="checkbox"/>
Max Segment Size (MSS)	1460 bytes	<input type="checkbox"/>
Nagle's Algorithm	Enabled	<input checked="" type="checkbox"/>
PUSH Flag	Default	<input type="checkbox"/>
Time To Live (TTL)	Proxy	<input type="checkbox"/>
Time To Live (TTL) v4	255	<input type="checkbox"/>
Time To Live (TTL) v6	64	<input type="checkbox"/>

Cancel Repeat Finished

Creating a TCP-LAN-Optimized Profiles

1. Create a 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**.

Local Traffic » Profiles : Protocol : TCP » New TCP Profile...

General Properties

Name	MyHZN-LTM-AP_la
Parent Profile	tcp-lan-optimized

Cancel Repeat Finished

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. **(Optional)** Timeout can be increased for environments who increase in Horizon the “Global Session Timeout” variable (when increased the heartbeats in Horizon are lengthened and its recommended to increase the Timeout variable to accommodate) – VMware KB <https://kb.vmware.com/s/article/56636>
 - i. Click **Finished**.

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

General Properties

Name	MyHZN-LTM-AP_s1
Persistence Type	Source Address Affinity
Parent Profile	source_addr

Configuration Custom

Mirror Persistence	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input type="checkbox"/>
Hash Algorithm	Default	<input type="checkbox"/>
Timeout	Specify... 180 seconds	<input type="checkbox"/>
Prefix Length	None	<input type="checkbox"/>
Map Proxies	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input type="checkbox"/>

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_clientsssl
Parent Profile	clientsssl

- c. From the **Configuration** list, select **Advanced**
- d. From the **Certificate Key Chain** area, click the **Custom** checkbox and then click the **Add** button.

Configuration:	Advanced	Custom <input checked="" type="checkbox"/>
Mode	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Certificate Key Chain	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>	<input checked="" type="checkbox"/>
	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

- e. 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 **ADD**.

Add SSL Certificate Key Chain	
Certificate	Wildcard
Key	Wildcard
Chain	None
Passphrase	
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

- f. In the **Ciphers** area, click the **Custom** box, and then click the **Cipher String** button.
- g. In the **Ciphers** field, type **DEFAULT:!RC4:!MEDIUM:@STRENGTH**
- h. In the **Options** field, click the **Custom** box (leave defaults)
- i. In the **Handshake Timeout** field, click the **Custom** box, and **specify 10 seconds**

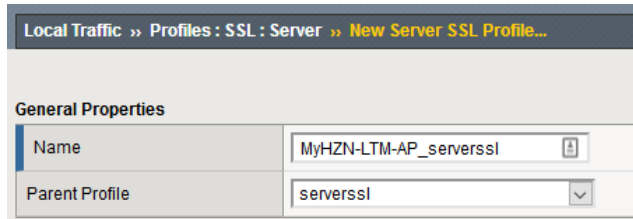
Configuration: Advanced		Custom <input type="checkbox"/>
Mode	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Certificate Key Chain	<input type="text" value="/Common/Wildcard /Common/Wildcard"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input checked="" type="checkbox"/>
OCSP Stapling	<input type="checkbox"/>	<input type="checkbox"/>
Notify Certificate Status to Virtual Server	<input type="checkbox"/>	<input type="checkbox"/>
Ciphers	<input type="radio"/> Cipher Group <input checked="" type="radio"/> Cipher Suites <input type="text" value="DEFAULT:!RC4:!MEDIUM:@STRENGTH"/>	<input checked="" type="checkbox"/>
Options	<input type="text" value="Options List..."/>	<input checked="" type="checkbox"/>
Options List	Enabled Options <input type="text" value="Don't insert empty fragments"/> <input type="text" value="No TLSv1.3"/> <input type="button" value="Disable"/> Available Options <input type="text" value="Netscape@ reuse cipher change bug workarou"/> <input type="text" value="Microsoft@ big SSLv3 buffer"/> <input type="text" value="Microsoft@ IE SSLv2 RSA padding"/> <input type="text" value="SSLLeay 080 client DH bug workaround"/> <input type="text" value="TLS D5 bug workaround"/> <input type="button" value="Enable"/>	
Proxy SSL	<input type="checkbox"/>	<input type="checkbox"/>
Proxy SSL Passthrough	<input type="checkbox"/>	<input type="checkbox"/>
ModSSL Methods	<input type="checkbox"/>	<input type="checkbox"/>
Cache Size	<input type="text" value="262144"/> sessions	<input type="checkbox"/>
Cache Timeout	<input type="text" value="3600"/> seconds	<input type="checkbox"/>
Alert Timeout	<input type="text" value="Indefinite"/>	<input type="checkbox"/>
Handshake Timeout	<input type="text" value="Specify..."/> <input type="text" value="10"/> seconds	<input checked="" type="checkbox"/>

- j. From the **Client Certificate** row, click the **Custom** checkbox and then select **Ignore** from the list.
- k. From the **Trusted Certificate Authorities** row, click the **Custom** checkbox and then select **None** from the list.
- l. From the **Advertised Certificate Authorities** row, click the **Custom** checkbox and then select **None** from the list.
- m. Scroll to the bottom and click **Finished**.

Client Authentication		Custom <input type="checkbox"/>
Client Certificate	<input type="text" value="Ignore"/>	<input checked="" type="checkbox"/>
Frequency	<input type="text" value="once"/>	<input type="checkbox"/>
Retain Certificate	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Certificate Chain Traversal Depth	<input type="text" value="9"/>	<input type="checkbox"/>
Trusted Certificate Authorities	<input type="text" value="None"/>	<input checked="" type="checkbox"/>
Advertised Certificate Authorities	<input type="text" value="None"/>	<input checked="" type="checkbox"/>
CRL File	<input type="text" value="None"/>	<input type="checkbox"/>
Allow Expired CRL File	<input type="checkbox"/>	<input type="checkbox"/>

Creating a Server SSL Profile

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

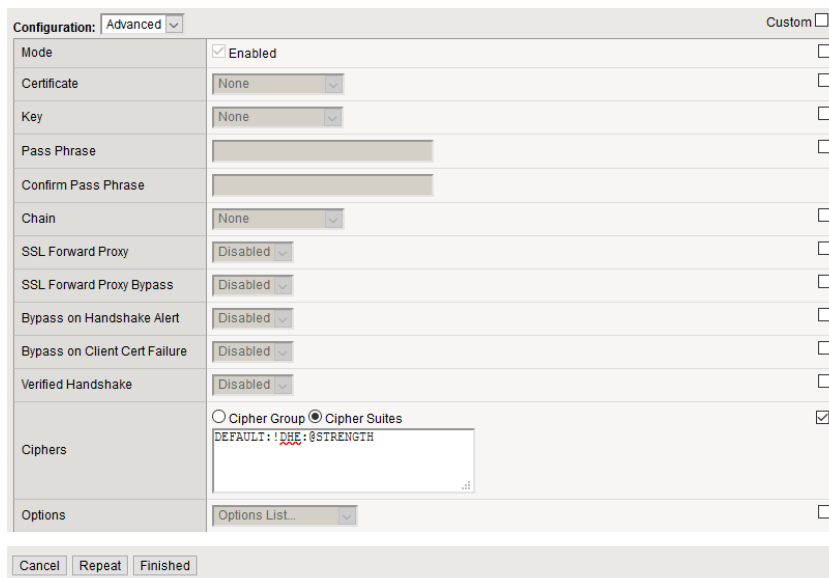


Local Traffic » Profiles : SSL : Server » New Server SSL Profile...

General Properties

Name	MyHZN-LTM-AP_serverssl
Parent Profile	serverssl

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



Configuration: Advanced Custom

Mode	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Certificate	None	<input type="checkbox"/>
Key	None	<input type="checkbox"/>
Pass Phrase		<input type="checkbox"/>
Confirm Pass Phrase		
Chain	None	<input type="checkbox"/>
SSL Forward Proxy	Disabled	<input type="checkbox"/>
SSL Forward Proxy Bypass	Disabled	<input type="checkbox"/>
Bypass on Handshake Alert	Disabled	<input type="checkbox"/>
Bypass on Client Cert Failure	Disabled	<input type="checkbox"/>
Verified Handshake	Disabled	<input type="checkbox"/>
Ciphers	<input type="radio"/> Cipher Group <input checked="" type="radio"/> Cipher Suites DEFAULT:!DHE:@STRENGTH	<input checked="" type="checkbox"/>
Options	Options List...	<input type="checkbox"/>

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.

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

General Properties	
Name	MyHZN-LTM-AP_redirect
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	80 Other:
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 previously created.
- h. From the **Protocol Profile (Server)** list, select the TCP-LAN-Optimized profile previously created.
- i. From the **HTTP Profile** list, select the HTTP profile previously created.
- j. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	MyHZN-LTM-AP_wan_optimized_tcp
Protocol Profile (Server)	MyHZN-LTM-AP_lan_optimized_tcp
HTTP Profile	MyHZN-LTM-AP_HTTP
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: /Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible
SSL Profile (Server)	Selected: Available: /Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
SMTPS Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP 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**.

Resources					
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><i>/Common</i> _sys_https_redirect</td><td>_sys_auth_radius _sys_auth_ssl_cc_ldap _sys_auth_ssl_cridp _sys_auth_ssl_ocsp _sys_auth_tacacs</td></tr></tbody></table> <p>Up Down</p>	Enabled	Available	<i>/Common</i> _sys_https_redirect	_sys_auth_radius _sys_auth_ssl_cc_ldap _sys_auth_ssl_cridp _sys_auth_ssl_ocsp _sys_auth_tacacs
	Enabled	Available			
<i>/Common</i> _sys_https_redirect	_sys_auth_radius _sys_auth_ssl_cc_ldap _sys_auth_ssl_cridp _sys_auth_ssl_ocsp _sys_auth_tacacs				
Policies	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Enabled	Available		
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_https
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443 Other:
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 **clientsssl** 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 **serversssl** 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_wan_optimized_tcp
Protocol Profile (Server)	MyHZN-LTM-AP_lan_optimized_tcp
HTTP Profile	MyHZN-LTM-AP_HTTP
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Selected</p> <ul style="list-style-type: none"> /Common MyHZN-LTM-AP_clientsssl </div> <div style="width: 45%;"> <p>Available</p> <ul style="list-style-type: none"> /Common Wildcard-SSL clientsssl clientsssl-insecure-compatible clientsssl-secure </div> </div>
SSL Profile (Server)	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Selected</p> <ul style="list-style-type: none"> /Common MyHZN-LTM-AP_serversssl </div> <div style="width: 45%;"> <p>Available</p> <ul style="list-style-type: none"> /Common apm-default-serverssl crypto-client-default-serverssl pcop-default-serverssl serversssl </div> </div>
SMTPS Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP 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**.

Resources

iRules	Enabled	Available
	<ul style="list-style-type: none">/CommonHorizon-Origin-Header	<ul style="list-style-type: none">/CommonLog-IP-MirageNewHorizon_sys_APM_ExchangeSupport_OA_BasicAuth_sys_APM_ExchangeSupport_OA_NtlmAuth
Policies	Enabled	Available
Default Pool	+ MyHZN-LTM-AP_443_pool	
Default Persistence Profile	MyHZN-LTM-AP_src_addr	
Fallback Persistence Profile	None	

Cancel Repeat Finished

Port 443 UDP - Virtual Server

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

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

General Properties	
Name	MyHZN-LTM-AP_udp_blast_443
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	443 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 the **udp profile** you created previously.
- h. From the **Protocol Profile (Server)** list, select **(Use Client Profile)**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic

Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> /Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible </td> </tr> </tbody> </table>	Selected	Available		/Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible
Selected	Available				
	/Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible				
SSL Profile (Server)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> /Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl </td> </tr> </tbody> </table>	Selected	Available		/Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl				
SMTSP Profile	None				
POP3 Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Service Profile	None				
SMTP Profile	None				
Netflow Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

Creating the main virtual server (continued)

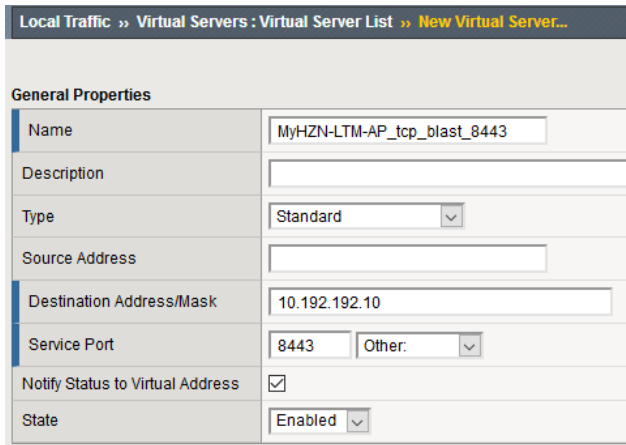
- j. From the **Default Pool** list, select the pool you created in [Port 443 - Pool](#).
- k. From the **Default Persistence Profile** list, select the profile you created previously.
- l. Click **Finished**.

Resources					
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth</td></tr></tbody></table> <p>Up Down</p>	Enabled	Available		<i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth
Enabled	Available				
	<i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth				
Policies	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Enabled	Available		
Enabled	Available				
Default Pool	MyHZN-LTM-AP_443_pool				
Default Persistence Profile	MyHZN-LTM-AP_src_addr				
Fallback Persistence Profile	None				

Cancel Repeat Finished

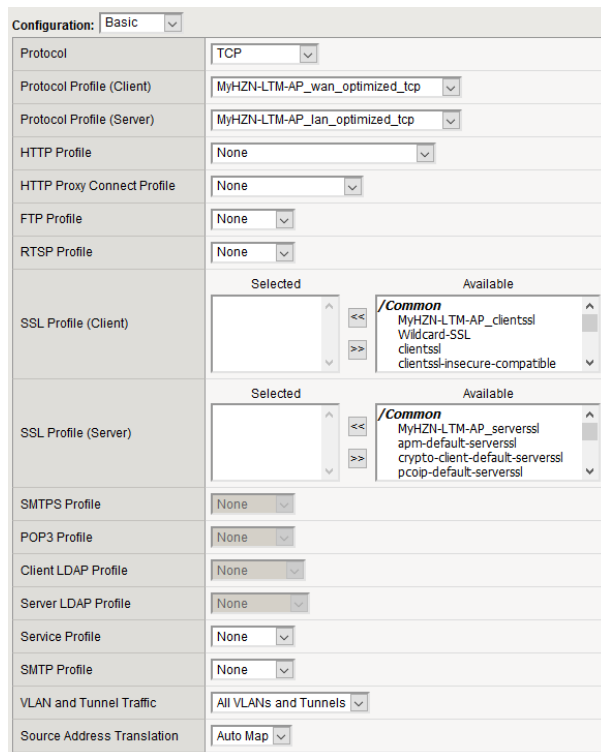
Port 8443 TCP - Virtual Server

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



General Properties	
Name	MyHZN-LTM-AP_tcp_blast_8443
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	8443 Other:
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

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



Configuration: Basic	
Protocol	TCP
Protocol Profile (Client)	MyHZN-LTM-AP_wan_optimized_tcp
Protocol Profile (Server)	MyHZN-LTM-AP_lan_optimized_tcp
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: /Common, MyHZN-LTM-AP_clientssl, Wildcard-SSL, clientssl, clientssl-insecure-compatible
SSL Profile (Server)	Selected: /Common, MyHZN-LTM-AP_serverssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl
SMTPS Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP 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**.

Resources					
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth</td></tr></tbody></table> <p>Up Down</p>	Enabled	Available		<i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth
Enabled	Available				
	<i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth				
Policies	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Enabled	Available		
Enabled	Available				
Default Pool	+ MyHZN-LTM-AP_8443_pool				
Default Persistence Profile	MyHZN-LTM-AP_src_addr				
Fallback Persistence Profile	None				

Cancel Repeat Finished

Port 8443 UDP - Virtual Server

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

General Properties	
Name	MyHZN-LTM-AP_udp_blast_8443
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.192.192.10
Service Port	8443 Other: ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

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

Configuration: Basic					
Protocol	UDP				
Protocol Profile (Client)	MyHZN-LTM-AP_udp_profile				
Protocol Profile (Server)	(Use Client Profile)				
SSL Profile (Client)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td></td><td>/Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible</td></tr></tbody></table>	Selected	Available		/Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible
Selected	Available				
	/Common MyHZN-LTM-AP_clientssl Wildcard-SSL clientssl clientssl-insecure-compatible				
SSL Profile (Server)	<table border="1"><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td></td><td>/Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl</td></tr></tbody></table>	Selected	Available		/Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
Selected	Available				
	/Common MyHZN-LTM-AP_serverssl apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl				
SMTSP Profile	None				
POP3 Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
Service Profile	None				
SMTP Profile	None				
Netflow Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map				

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

Resources					
iRules	<table border="1"> <thead> <tr> <th>Enabled</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> /Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth </td> </tr> </tbody> </table> <p>Up Down</p>	Enabled	Available		/Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth
Enabled	Available				
	/Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth				
Policies	<table border="1"> <thead> <tr> <th>Enabled</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Enabled	Available		
Enabled	Available				
Default Pool	MyHZN-LTM-AP_8443_pool				
Default Persistence Profile	MyHZN-LTM-AP_src_addr				
Fallback Persistence Profile	None				

Cancel Repeat Finished

Port 4172 TCP - Virtual Server

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

Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...	
General Properties	
Name	MyHZN-LTM-AP_pcoip_tcp
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 TCP profile you created previously.
- g. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
- h. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
- i. From the **Source Address Translation** list, select **Auto Map**.

Configuration: Basic	
Protocol	TCP
Protocol Profile (Client)	MyHZN-LTM-AP_wan_optimized_tcp
Protocol Profile (Server)	MyHZN-LTM-AP_lan_optimized_tcp
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: /Common, MyHZN-LTM-AP_clientssl, Wildcard-SSL, clientssl, clientssl-insecure-compatible
SSL Profile (Server)	Selected: Available: /Common, MyHZN-LTM-AP_serverssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl
SMTPS Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP 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 4172 - Pool](#).
- k. From the **Default Persistence Profile** list, select the profile you created in [Creating a Persistence Profile](#).
- l. Click **Finished**.

Resources							
iRules	<table border="1"> <thead> <tr> <th>Enabled</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td> <ul style="list-style-type: none"> /Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth </td> </tr> <tr> <td style="text-align: center;"> <input type="button" value="Up"/> <input type="button" value="Down"/> </td> <td></td> </tr> </tbody> </table>	Enabled	Available	<input type="text"/>	<ul style="list-style-type: none"> /Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth 	<input type="button" value="Up"/> <input type="button" value="Down"/>	
Enabled	Available						
<input type="text"/>	<ul style="list-style-type: none"> /Common Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth 						
<input type="button" value="Up"/> <input type="button" value="Down"/>							
Policies	<table border="1"> <thead> <tr> <th>Enabled</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Enabled	Available	<input type="text"/>	<input type="text"/>		
Enabled	Available						
<input type="text"/>	<input type="text"/>						
Default Pool	MyHZN-LTM-AP_pcoip_pool						
Default Persistence Profile	MyHZN-LTM-AP_src_addr						
Fallback Persistence Profile	None						
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="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**.

Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...	
General Properties	
Name	MyHZN-LTM-AP_pcoip_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 profile you created previously.
- 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)	Selected: Available: /Common, MyHZN-LTM-AP_clientssl, Wildcard-SSL, clientssl, clientssl-insecure-compatible
SSL Profile (Server)	Selected: Available: /Common, MyHZN-LTM-AP_serverssl, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl
SMTSP Profile	None
POP3 Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
Service Profile	None
SMTP Profile	None
Netflow Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

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

Resources									
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><div style="border: 1px solid gray; height: 40px;"></div></td><td><div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth</div></td></tr><tr><td colspan="2" style="text-align: center;"><< >></td></tr><tr><td colspan="2" style="text-align: center;">Up Down</td></tr></tbody></table>	Enabled	Available	<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth</div>	<< >>		Up Down	
Enabled	Available								
<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> Horizon-Origin-Header Log-IP-Mirage NewHorizon _sys_APM_ExchangeSupport_OA_BasicAuth</div>								
<< >>									
Up Down									
Policies	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><div style="border: 1px solid gray; height: 40px;"></div></td><td><div style="border: 1px solid gray; height: 40px;"></div></td></tr><tr><td colspan="2" style="text-align: center;"><< >></td></tr></tbody></table>	Enabled	Available	<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; height: 40px;"></div>	<< >>			
Enabled	Available								
<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; height: 40px;"></div>								
<< >>									
Default Pool	<div style="border: 1px solid gray; padding: 2px;">+ MyHZN-LTM-AP_pcoip_pool</div>								
Default Persistence Profile	<div style="border: 1px solid gray; padding: 2px;">MyHZN-LTM-AP_src_addr</div>								
Fallback Persistence Profile	<div style="border: 1px solid gray; padding: 2px;">None</div>								
Cancel Repeat Finished									

Final Configuration

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

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List | Virtual Address List | Statistics

MyHZN Search Reset Search Create...

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	Up	MyHZN-LTM-AP_redirect			10.192.192.10	80 (HTTP)	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_udp_blast_443			10.192.192.10	443 (HTTPS)	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_https			10.192.192.10	443 (HTTPS)	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_pcoip_udp			10.192.192.10	4172	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_pcoip_tcp			10.192.192.10	4172	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_udp_blast_8443			10.192.192.10	8443	Standard	Edit...	Common
<input type="checkbox"/>	Up	MyHZN-LTM-AP_tcp_blast_8443			10.192.192.10	8443	Standard	Edit...	Common

Enable Disable Delete...

Testing the VMware Horizon Connection

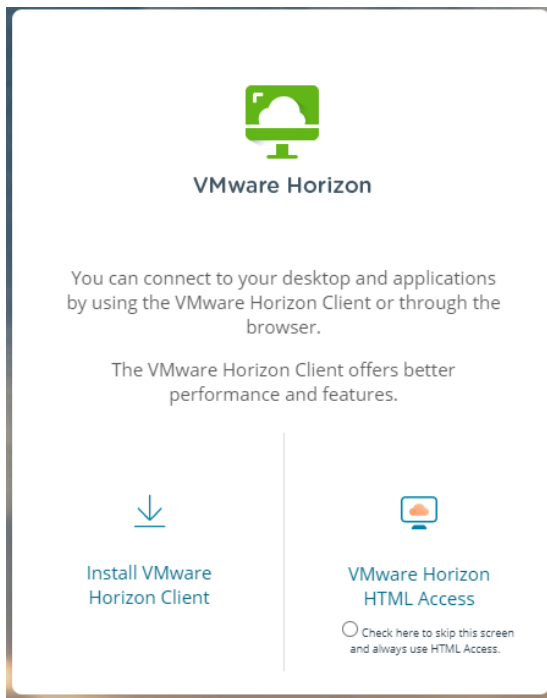
After setting up the Virtual IPs (VIPs) for the Unified Access Gateways, you can use the following methods validate that the External VIP is connecting and working properly. In this case, you are now using the new FQDN site name to connect to the Horizon Environment.

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

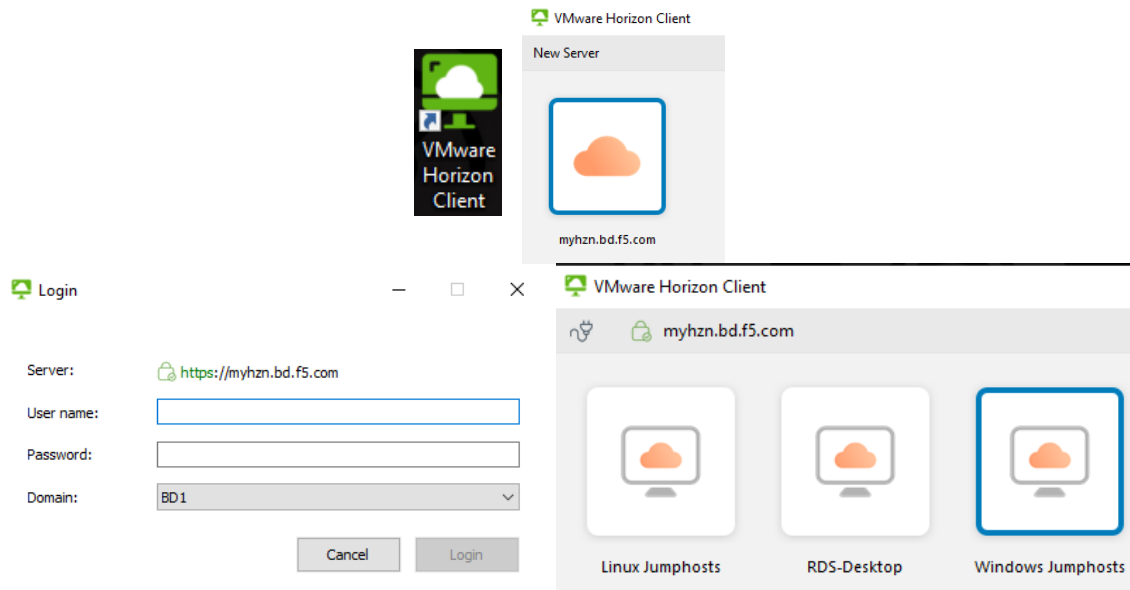
1. In a browser, type the FQDN for the VIP you previously created (for example, <https://myhzn.bd.f5.com>).

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

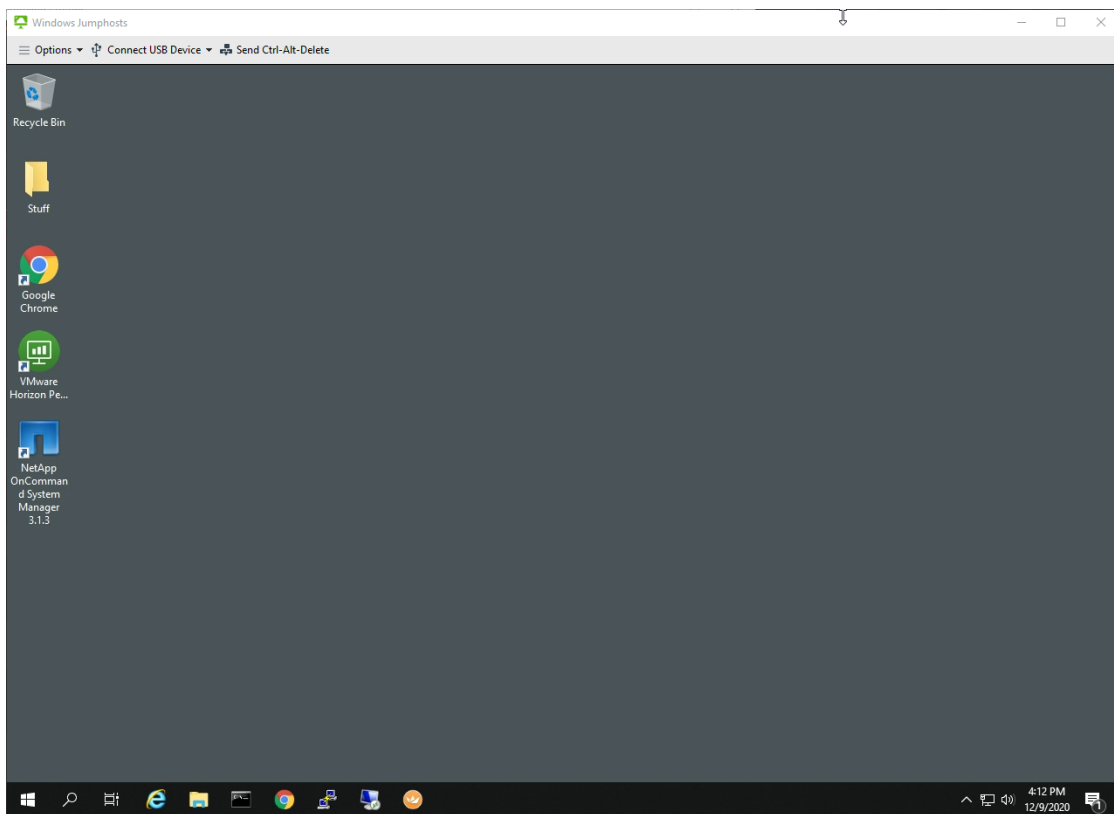
You should see the VMware Horizon Client/HTML5 Page. This confirms that your servers are working through the newly created virtual server.



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>