Introduction

This paper details the setup of F5 BIG IP 11.3 with Horizon Workspace 1.5 to load balance gateway-VAs for both internal and external access as well as load balancing kerberos enabled connector-VAs.

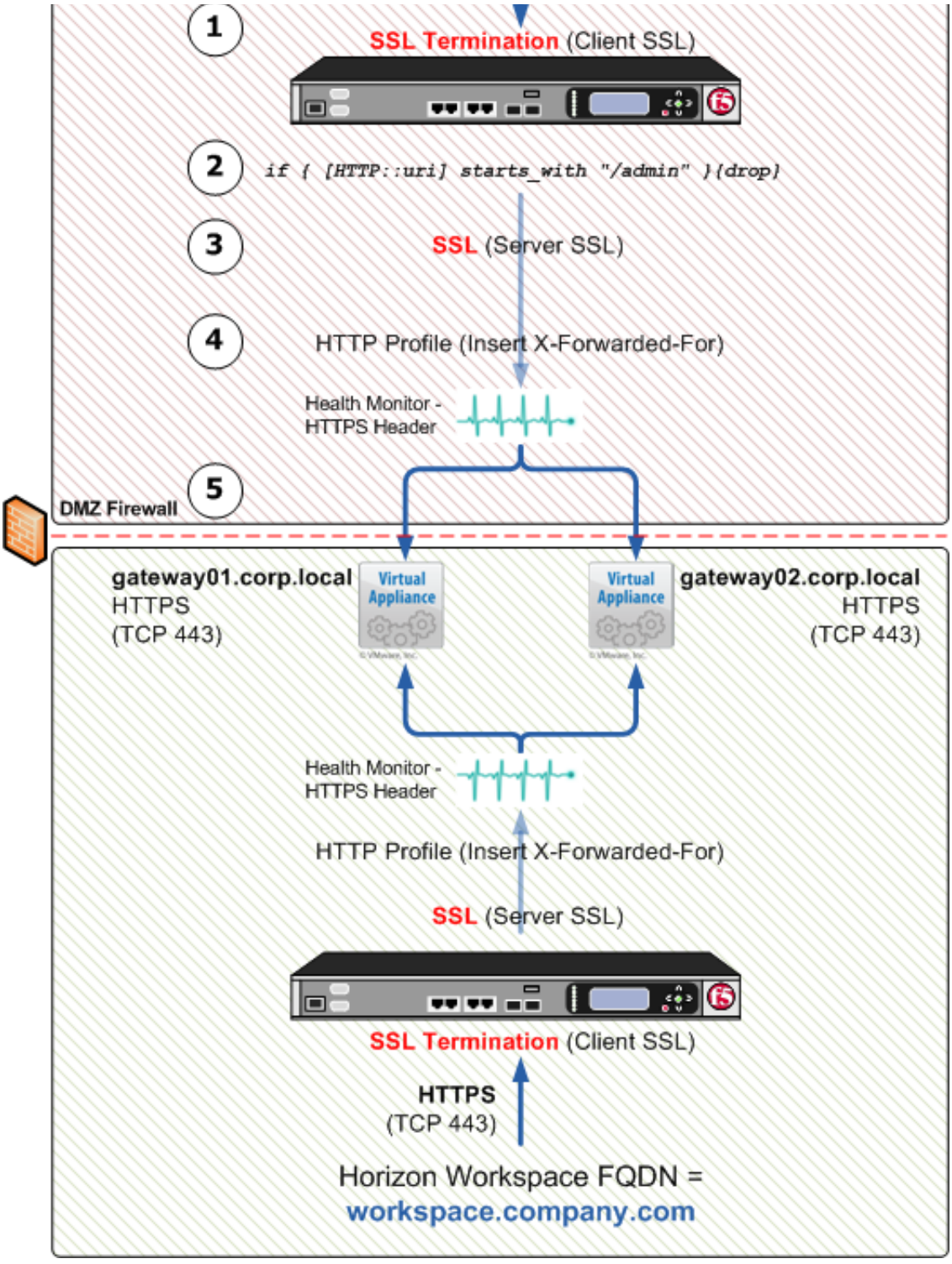
Objective

When setting up Horizon Workspace 1.5 for production usage a typical requirement is to have service level reduncancy for the different virtual appliances that makes up Horizon Workspace. This setup requires load balancers in front of the Gateway Virtual Appliance(s) as well as Connector Virtual Appliance(s) configured for Windows (Kerberos) Authentication.
If the Horizon Workspace will be used externally a Load Balancer also needs to be placed in the DMZ. It is not supported to place Gateway VA(s) the DMZ.

Solution

F5 offers load balancing solutions that covers the criterias above which means they can cover the load balancing requirements for multiple gateway-VAs, connector-VAs (Kerberos) and external access to Horizon Workspace by placing F5 in the DMZ and routing those requests to the internal gateway-VAs.
Below a brief solutions overview with a description of the flow.

1. A user goes to the Horizon Workspace URL - Which points to the F5 LTM VIP - SSL (HTTPS 433) traffic terminates at the F5 LTM.
2. If accessing the Horizon Workspace URL externally an iRule denies access to the admin part of Horizon Workspace (**Optional**)
3. F5 LTM continues to use SSL (HTTPS 443) against Horizon Workspace gateway-va(s)
4. X-Forwarded-For header is inserted with the requesting clients IP address
5. The users request is taken to an gateway-va which is available. This validation is based on a successful HTTPS header response.



NOTE: In the above diagram 2 F5 LTM appliances are pictured but they can be the same physical/virtual appliance with 2 logical configurations. In such a setup the VIP for providing external access would typically be defined on the 'Public' VLAN and the VIP for internal access to would be defined on the 'Private' VLAN.

The F5 deployment scenario does not matter in the case of using it for providing external

access to Horizon Workspace meaning that both "In-Line" and "One-Arm" deployments would work equilly well.

This document discusses the following:

1. Configuration of F5 BIG IP 11.3 and Horizon Workspace 1.5 to support:
    - Load balancing gateway-VAs
    - Load balancing Kerberos enabled connector-VAs (Windows Authentication, SSO)
2. Using proper CA signed certificates (not self-signed supplied with Horizon Workspace) for both gateways and connectors.

This tech-note assumes a requirement for using CA signed certificates and not the self-signed certificates by Horizon Workspace.

NOTE: This tech-note does not cover installation or deployment of any F5 BIG IP products. For F5 BIG IP deployment and configuration options please refer to the BIG-IP LTM / VE 11.3.0 Documentation

Pre-reqs

- All pre-reqs to meet a successfull Horizon Workspace deployment (Installing Horizon Workspace 1.5)
- F5 BIG IP 11.3 setup to integrate with your existing environment
- Certificates to be used with the Horizon Workspace deployment
- Admin access to F5 BIG IP 11.3 used for the deployment
- DNS A and PTR records pointing to the Horizon Workspace FQDN URL - The VIP configured on the F5 LTM
- DNS A and PTR records to be used for the Connector Identity Provider FQDN - Pointing to the VIP configured on the F5 LTM
- ICMP traffic allowed from Gateway-VAs to F5 IP (F5 BIG-IP Needs to be "pingable")

NOTE: These pre-reqs are for both load balancing gateways and connectors.

LOAD BALANCING - Gateway Virtual Appliances (VAs)

This section covers load balancing gateway-VAs

Import certificates on F5 BIG IP

This guides assumes the usage of a proper CA signed certificate that matches the FQDN of the Horizon Workspace URL eg. workspace.company.com including the full certificate chain (root, subordinate, issuing etc.) imported on the F5 BIG IP 11.3 as well.
Just as would be required for Horizon Workspace the following is needed:

- Certificate to match Horizon Workspace URL / FQDN
  - Including Private Key
- Root, and/or any issuing/subordinate certificate to build full trust chain

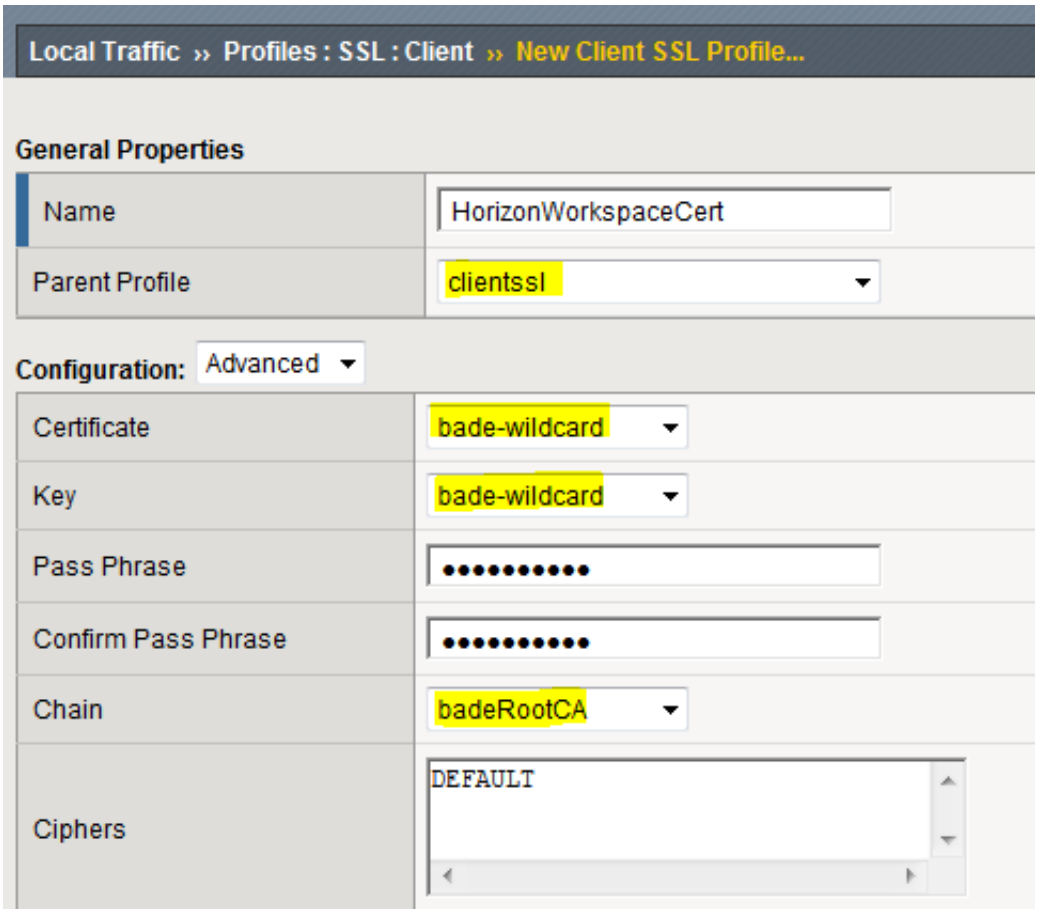
Go to System ›› File Management : SSL Certificate List ›› Import SSL Certificates and Keys and click "Import"

Here you have the options for importing your certificate, private key and certificate chain. Everything can be imported as PKCS12 if such a keystore is available containing all required certificates and private keys. If this is not available import the required certificates, keys and CA certificates individually.

Create Client SSL profile

Go to Local Traffic ›› Profiles : SSL : Client and click "Create".
Chose "Advanced" and click "Custom" to enable making changes.

Type a name thats going to be associated with the Client SSL profile and chose the Certificate, Private Key and Chain

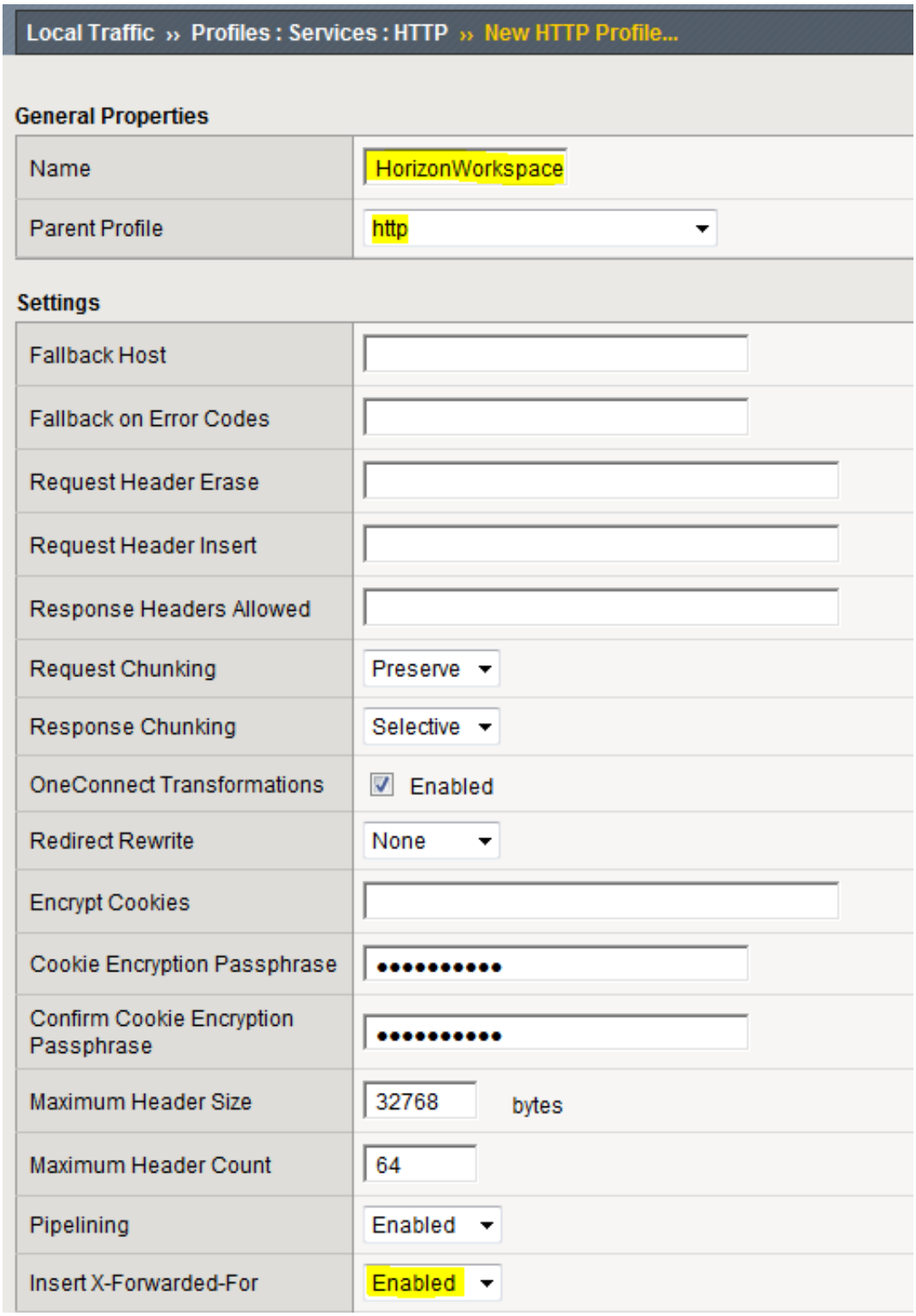


Scroll to the bottom and click "Finished"

Create HTTP Profile

Go to Local Traffic ›› Profiles : Services : HTTP and click "Create"
Click "Custom" to enable making changes.

Type a name thats going to be associated with this HTTP Profile and make sure Parent Profile is set to clientssl as well as enabling "Insert X-Forwarded-For"



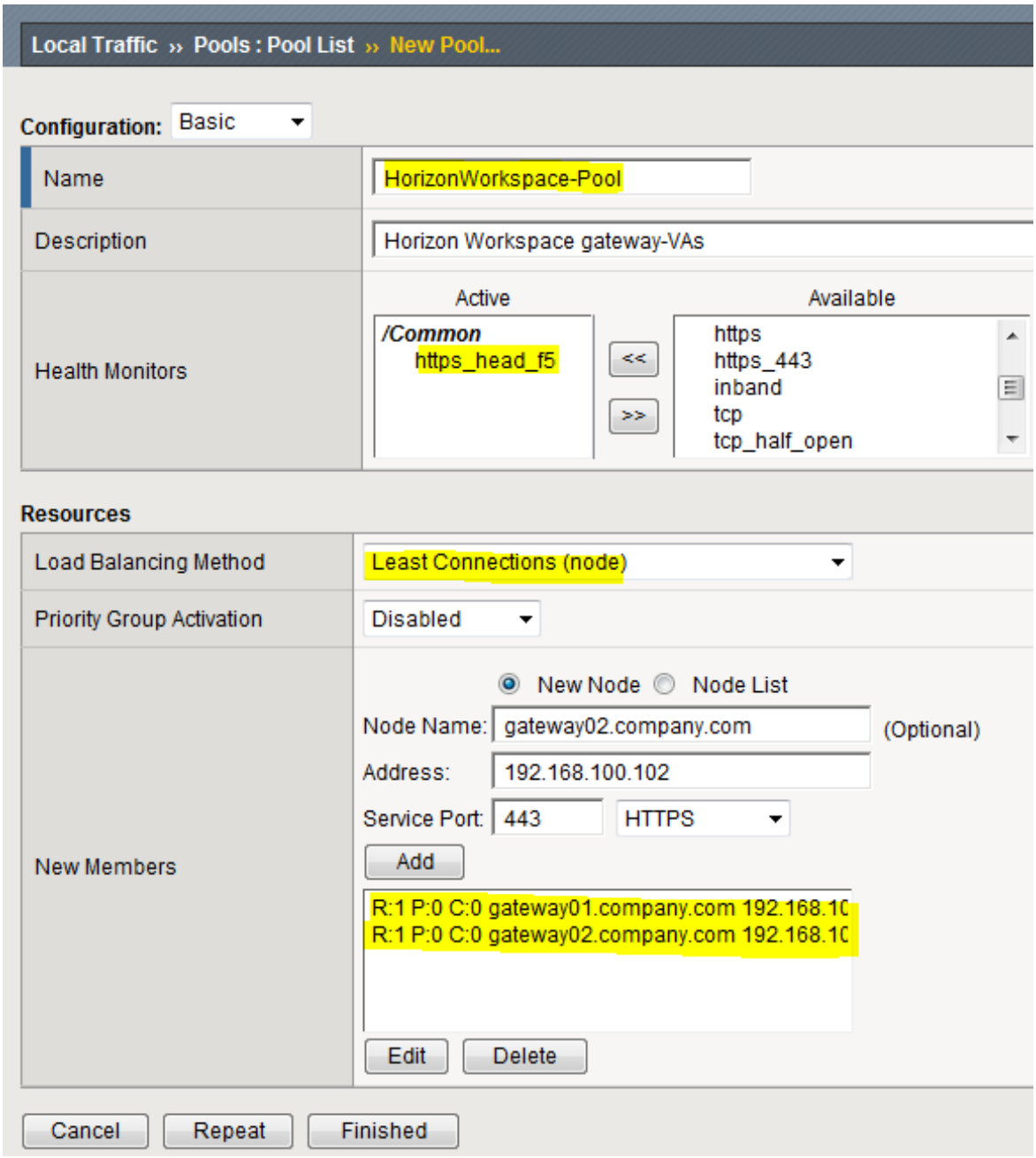
Scroll to the bottom and click "Finished"

Create Pool

Go to Local Traffic ›› Pools : Pool List and click "Create"

Type a name thats going to be associated with this pool and chose *https_head_f5* as health monitor and "Least Connections (node)" as load balanching method.

Then add the gateway-VA(s) filling node name and the IP of the gateway-VA(s)



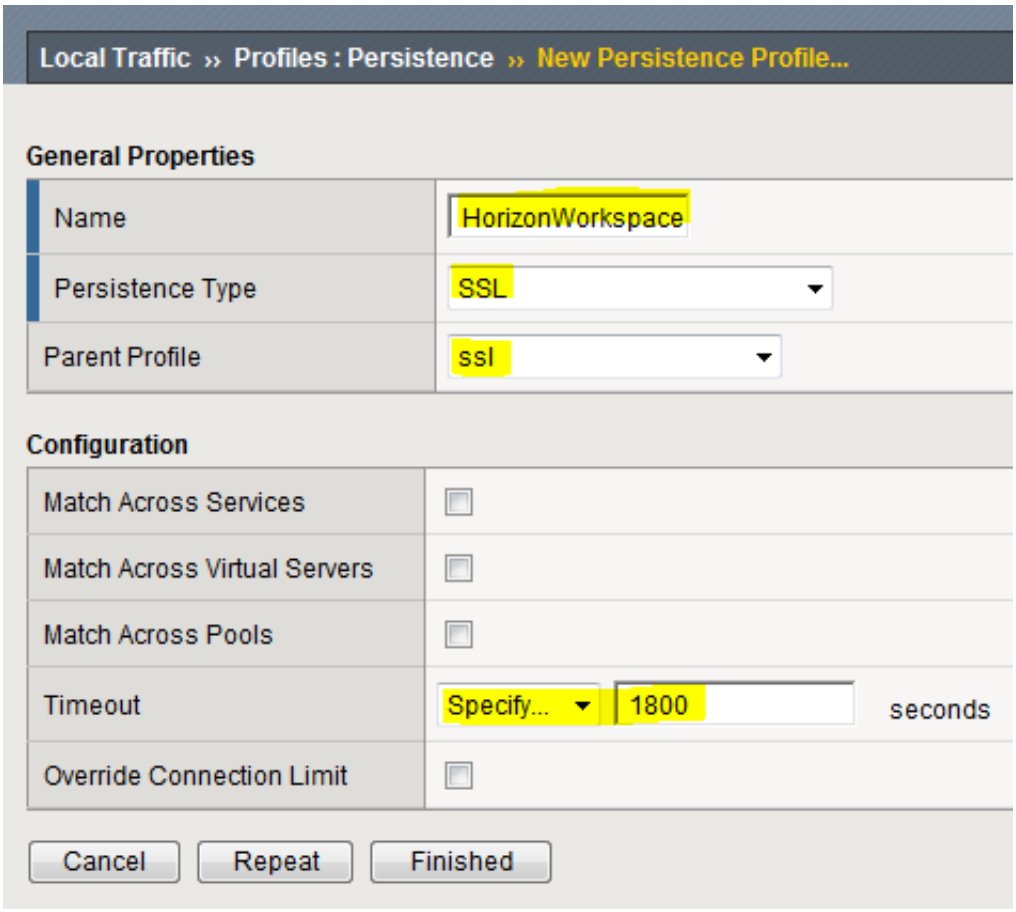
Scroll to the bottom and click "Finished"

Create Persistence Profile

Go to Local Traffic ›› Profiles : Persistence and click "Create"

Chose SSL as "Persistence Type" and "ssl" as Parent Profile.

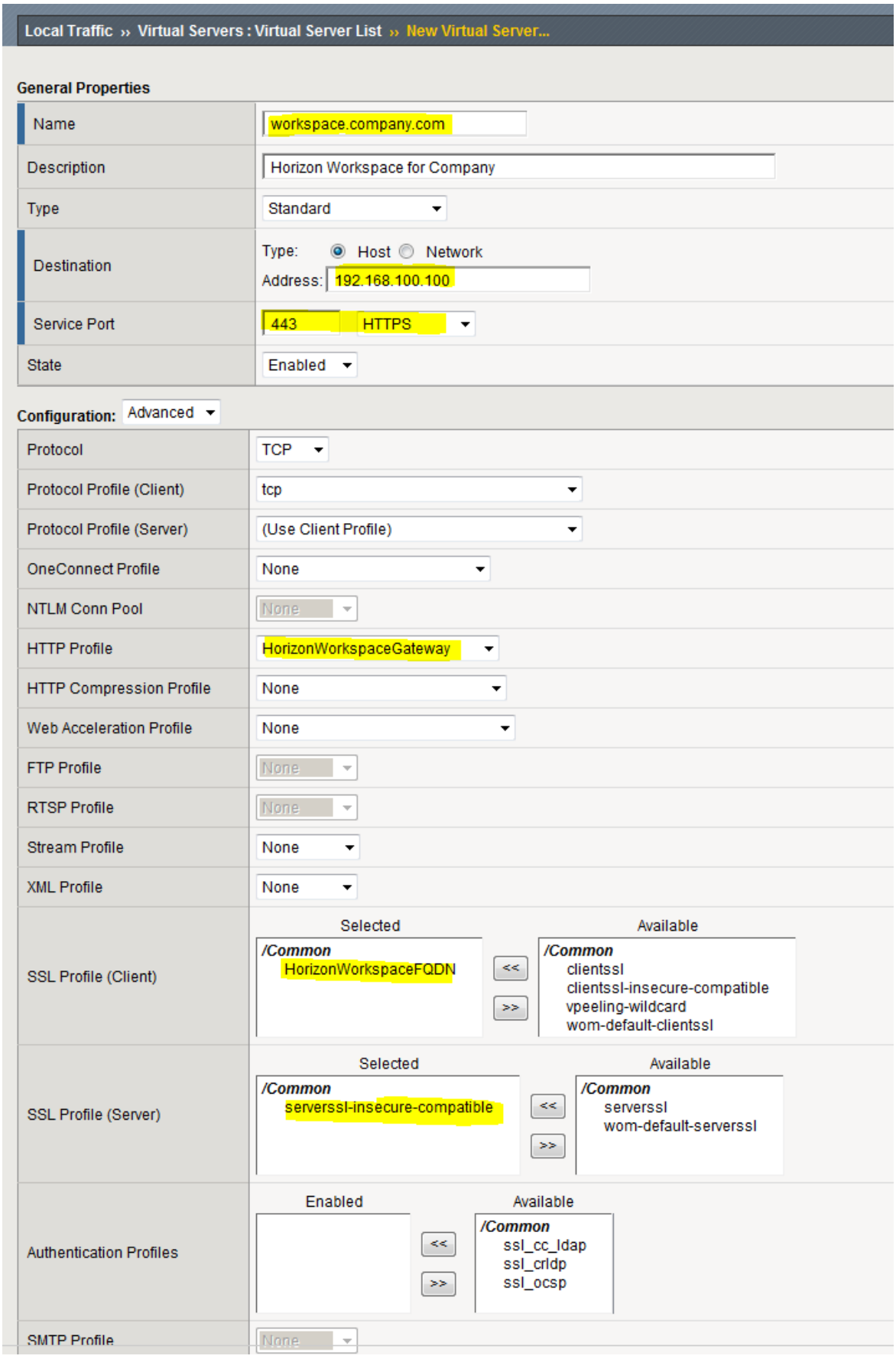
Under "Timeout" specify 1800 seconds (30 min). This will keep user sessions tied to the same gateway-VA for up to 30 min to avoid timeout errors like: “502 error: The service is currently unavailable."



Scroll to the bottom and click "Finished"

Create Virtual Server

Go to Local Traffic ›› Virtual Servers : Virtual Server List and click "Create".
Chose "Advanced" under Configuration and configure with the different settings as created above. Make sure yo use the correct Client SSL Profile, HTTP profile, Pool and Persistence Profile.


Local Traffic ›› Virtual Servers : Virtual Server List ›› New Virtual Server...
General Properties
Name
workspace.company.com
Description
Horizon Workspace for Company
Type
Standard
Destination
Type: Host Network
Address: 192.168.100.100
Service Port
443
HTTPS
State
Enabled
Configuration: Advanced
Protocol
TCP
Protocol Profile (Client)
tcp
Protocol Profile (Server)
(Use Client Profile)
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
HorizonWorkspaceGateway
HTTP Compression Profile
None
Web Acceleration Profile
None
FTP Profile
None
RTSP Profile
None
Stream Profile
None
XML Profile
None
SSL Profile (Client)
Selected
/Common
HorizonWorkspaceFQDN
<<
>>
Available
/Common
clientssl
clientssl-insecure-compatible
vpeeling-wildcard
wom-default-clientssl
SSL Profile (Server)
Selected
/Common
serverssl-insecure-compatible
<<
>>
Available
/Common
serverssl
wom-default-serverssl
Authentication Profiles
Enabled
<<
>>
Available
/Common
ssl_cc_ldap
ssl_crldp
ssl_ocsp
SMTP Profile
None

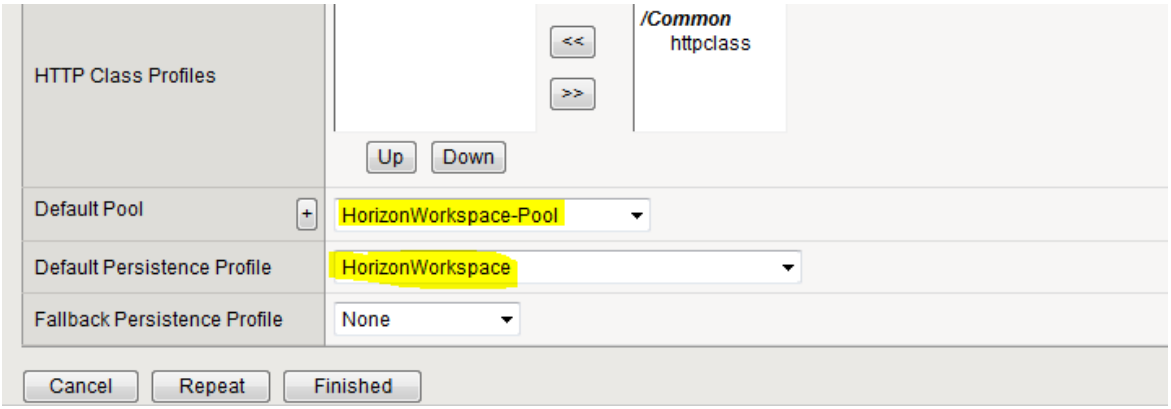
DNS Profile	None
Diameter Profile	None
SIP Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
SNAT Pool	Auto Map
Rate Class	None
Traffic Class	Enabled / Available << >>
Connection Limit	0
Address Translation	Enabled
Port Translation	Enabled
Source Port	Preserve
Clone Pool (Client)	None
Clone Pool (Server)	None
Auto Last Hop	Default
Last Hop Pool	None
Analytics Profile	None **Warning:** The Application Visibility and Reporting module (HTTP Analytics) is
NAT64	Enabled
Request Logging Profile	None

Access Policy

Access Profile	None
Connectivity Profile	None
Rewrite Profile	None
Citrix & Java Support	Enabled
OAM Support	Enabled

Resources

iRules	Enabled / Available << >> /Common HEADER-CHECK SSO-Admin SSO-Persistance _sys_APM_ExchangeSupport_OA_BasicAuth Up Down
	Enabled / Available



Scroll to the bottom and click "Finished"

Validate that the Horizon Workspace FQDN is accessible.

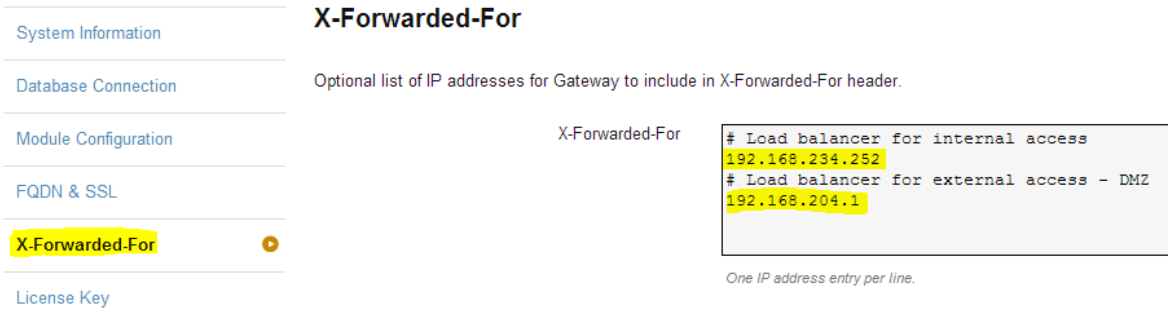
Configure X-Forwarded-For

Horizon Workspace supports multiple authentication mechanisms and for it to be able to determine which one to use it checks the requesting clients IP address and validates that against the Identify Provider (idP) setup.
Each configurator has a defined range of IP addresses which the gateway checks the clients source IP against to know which authentication mechanism should be used for the requesting client.
For this to work properly with the gateway's being placed behind a Load Balancer or reverse proxy the X-Forwarded-For option needs to be set. This options allows the load balancer to send the clients IP as part of the header which the gateway's then in turn uses to match up against the idP configuration of the different connectors.
Defining the X-Forwarded-For also configures the "real_ip" settings as part of nginx which makes the gateway's trust traffic from the Load Balancer allowing access to reports from the Horizon Workspace Admin pages.

The option to configure X-Forwarded-For is defined on the configurator VA web page.

Go to the URL of the configurator VA and login.

Click on X-Forwarded-For in the menu on the left page and paste in the IP address of each of the load balancers being used. A typical scenario could be having 2 load balancers: One for providing the internal access and one for providing the external access. This is shown in the example screenshot below.



It is possible to add comments using hashtags (#).

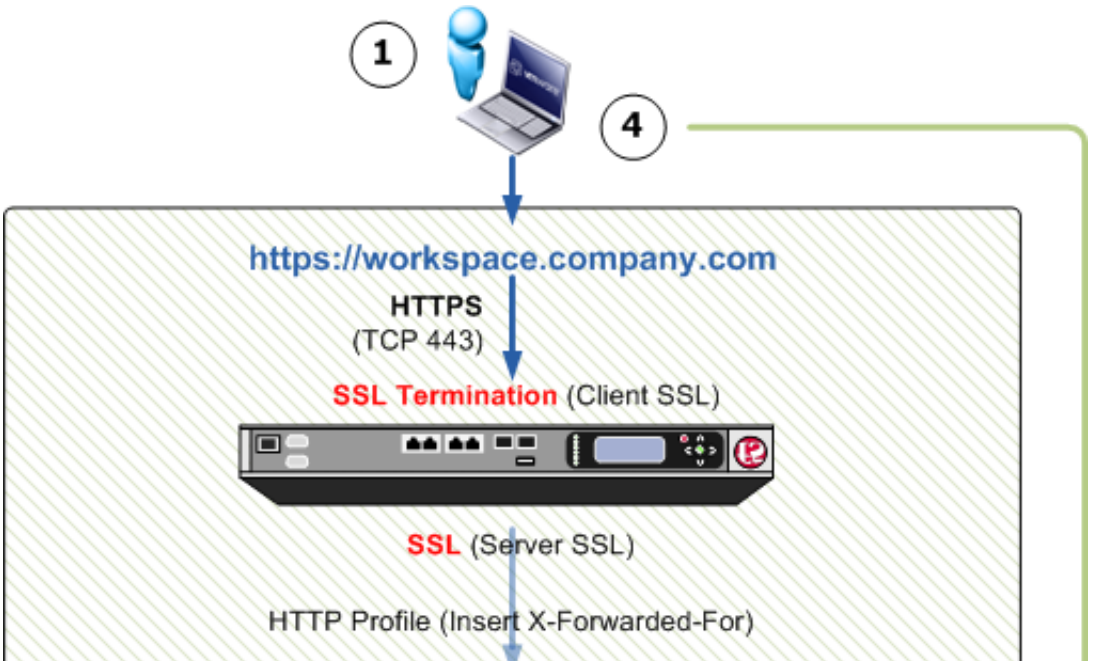
NOTE: There can only be one IP specified per line.

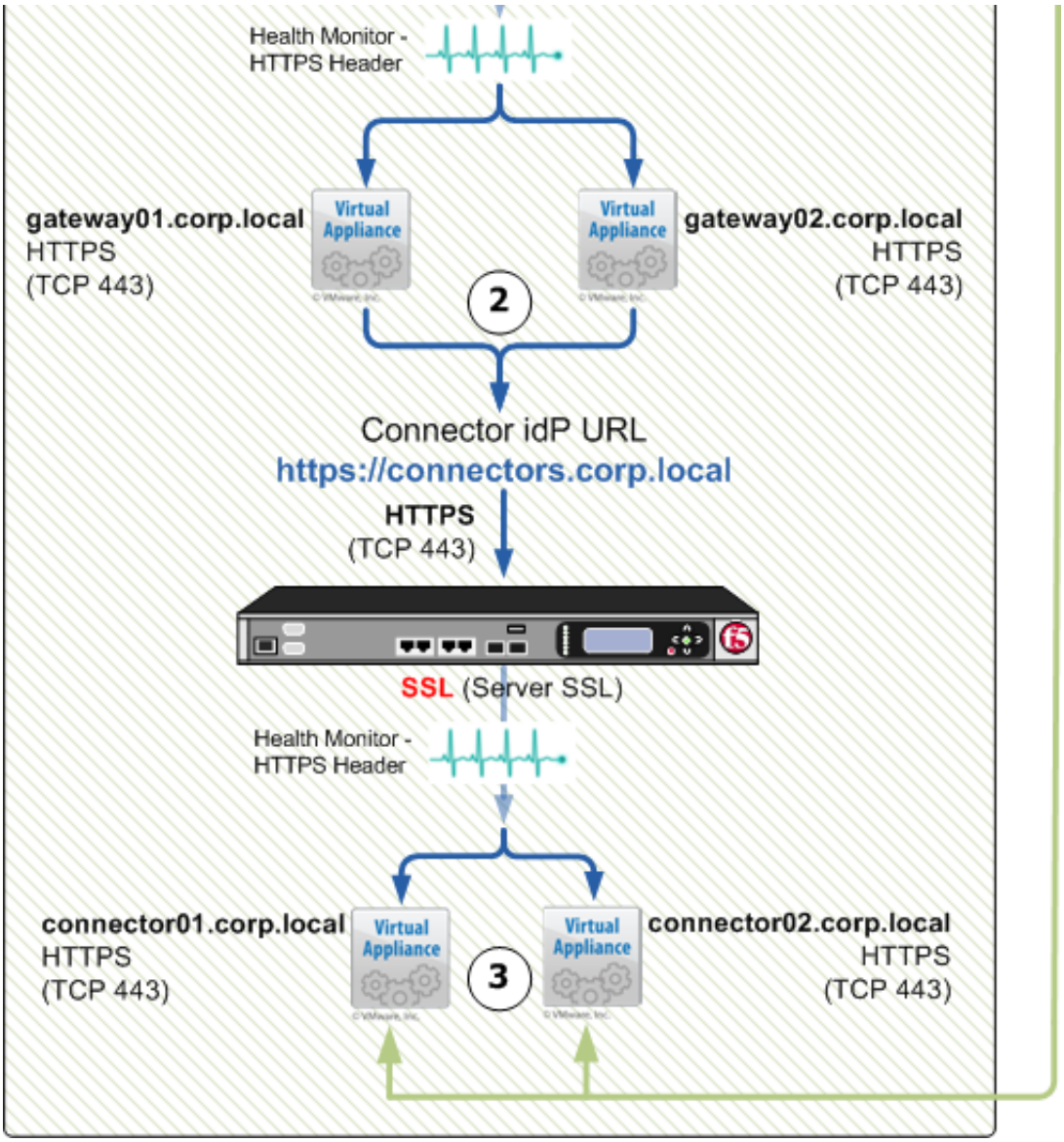
Once the IP information has been entered press save and wait a few minutes for the changes to be active on all the gateways.
If the changes does not happen within a few minutes reboot all the gateways.

LOAD BALANCING - Connector Virtual Appliances (VAs)

This section covers load balancing Connector VAs used for Windows authentication (Kerberos, SSO) Below a brief solutions overview with a description of the flow.

NOTE: Before beginning this part of the configuration make sure that the load balancing of gateway VAs and X-Forwarded-For is setup correctly. Refer to the troubleshooting section to solve any issues.





1. A user goes to the Horizon Workspace URL - Which points to the F5 LTM VIP - SSL (HTTPS 443)
2. The F5 LTM takes the user request to an available gateway and passes the client IP (X-Forwarded-For) to the gateway so it can determine which connectors to use for authentication. The client is then redirected to the idP URL as configured.
3. Once an available connector gets the request it initiates an HTTPS redirect to have the client target the connectors own specific FQDN.
4. The client redirects via HTTPS to the FQDN of the available connector and the connector validates the request against Active Directory using Kerberos. The reason for the HTTPS redirect is due to a requirement where the SPN value needs to match that of the connectors FQDN when it takes the requests to Active Directory via Kerberos.

Add Connectors and change idP settings

Add connectors to the Horizon Workspace implementation by following the VMware Horizon Workspace Documentation and make sure to use the *useGatewayAsIDP=n* option with hznAdminTool so the connectors can be used for Kerberos SSO authentication.

Once the connectors have been added login to each connectors admin webinterface which is running on HTTPS port 8443 (eg. https://connector01.corp.local:8443/)

Join the connectors to the domain and afterwards enable Windows Authentication.
NOTE: Make sure to check the "Enable Redirect" option under "Windows Auth" on all connectors.

Once the connectors have been configured log into the Horizon Workspace Admin interface and go to "Identity Providers" under the "Settings" tab.
Click on each of newly added connectors and change it's provider name and description. This is an optional step but it makes it easier to locate the individual connectors later.

Stay on the "Identify Providers" page and edit the newly created connectors IP range settings to match the clients you wish to be authenticated by these connectors. Make sure that the settings match on all the newly added connectors as they will all be serving the same clients and purpose.

After changing idP and IP range settings re-arrange the order of the connectors so that the newly added connectors are at the top of the list. The main thing to note here is that the default connector with it's 0.0.0.0/255.255.255.255 cannot have a higher priority than the connectors used for Windows Authentication.

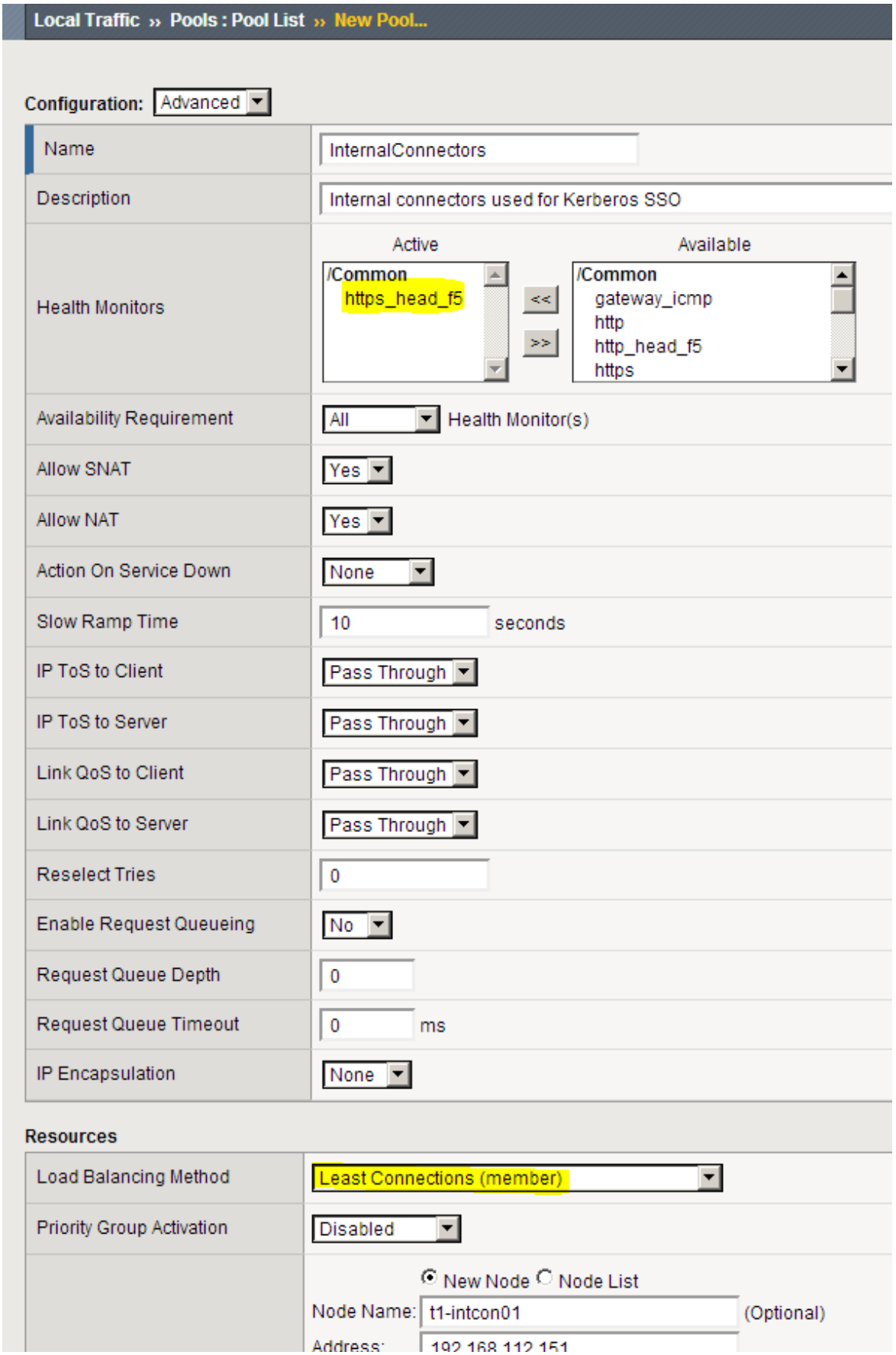
Before continuing to the next step verify that when accessing the Horizon Workspace FQDN from a client matching the IP range specified directs you to one of the connectors prompting for username and password.

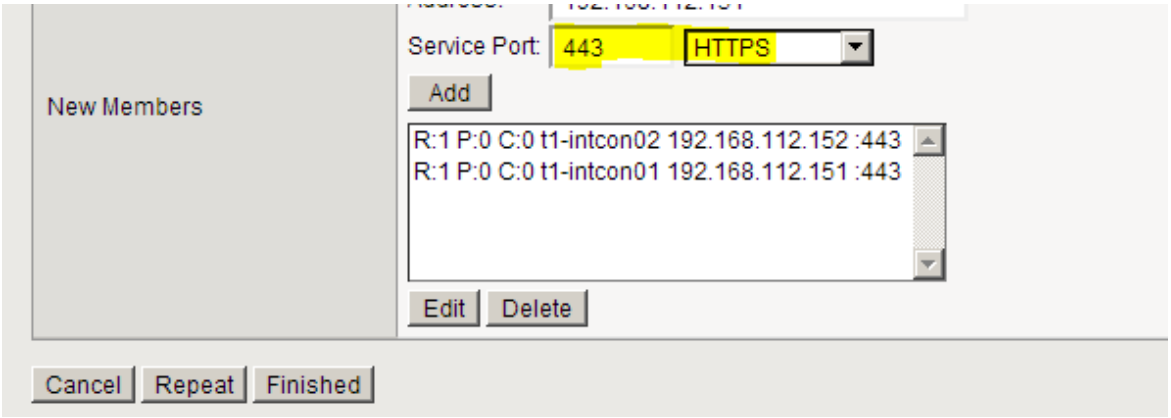
Create Pool on F5 LTM

Go to Local Traffic ›› Pools : Pool List and click "Create"

Type a name thats going to be associated with this pool for Connector VAs and chose *https_head_f5* as health monitor and "Least Connections (member)" as load balanching method.

Then add the Connector VAs filling node name and the IP of the individual Connectors.

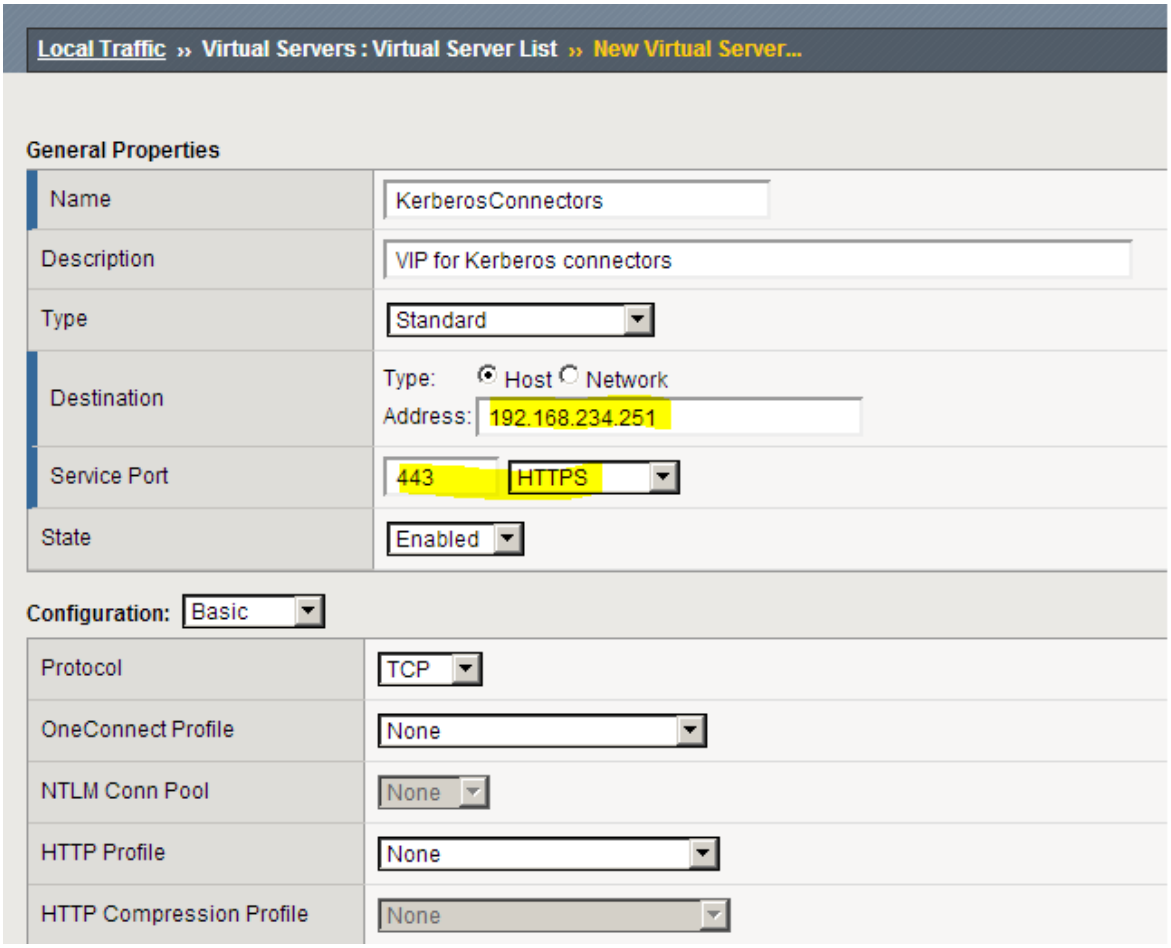

Local Traffic ›› Pools : Pool List ›› New Pool...
Configuration: Advanced
Name
InternalConnectors
Description
Internal connectors used for Kerberos SSO
Health Monitors
Active
Available
/Common
https_head_f5
<<
>>
/Common
gateway_icmp
http
http_head_f5
https
Availability Requirement
All
Health Monitor(s)
Allow SNAT
Yes
Allow NAT
Yes
Action On Service Down
None
Slow Ramp Time
10
seconds
IP ToS to Client
Pass Through
IP ToS to Server
Pass Through
Link QoS to Client
Pass Through
Link QoS to Server
Pass Through
Reselect Tries
0
Enable Request Queueing
No
Request Queue Depth
0
Request Queue Timeout
0
ms
IP Encapsulation
None
Resources
Load Balancing Method
Least Connections (member)
Priority Group Activation
Disabled
New Node
Node List
Node Name:
t1-intcon01
(Optional)
Address:
192.168.112.151

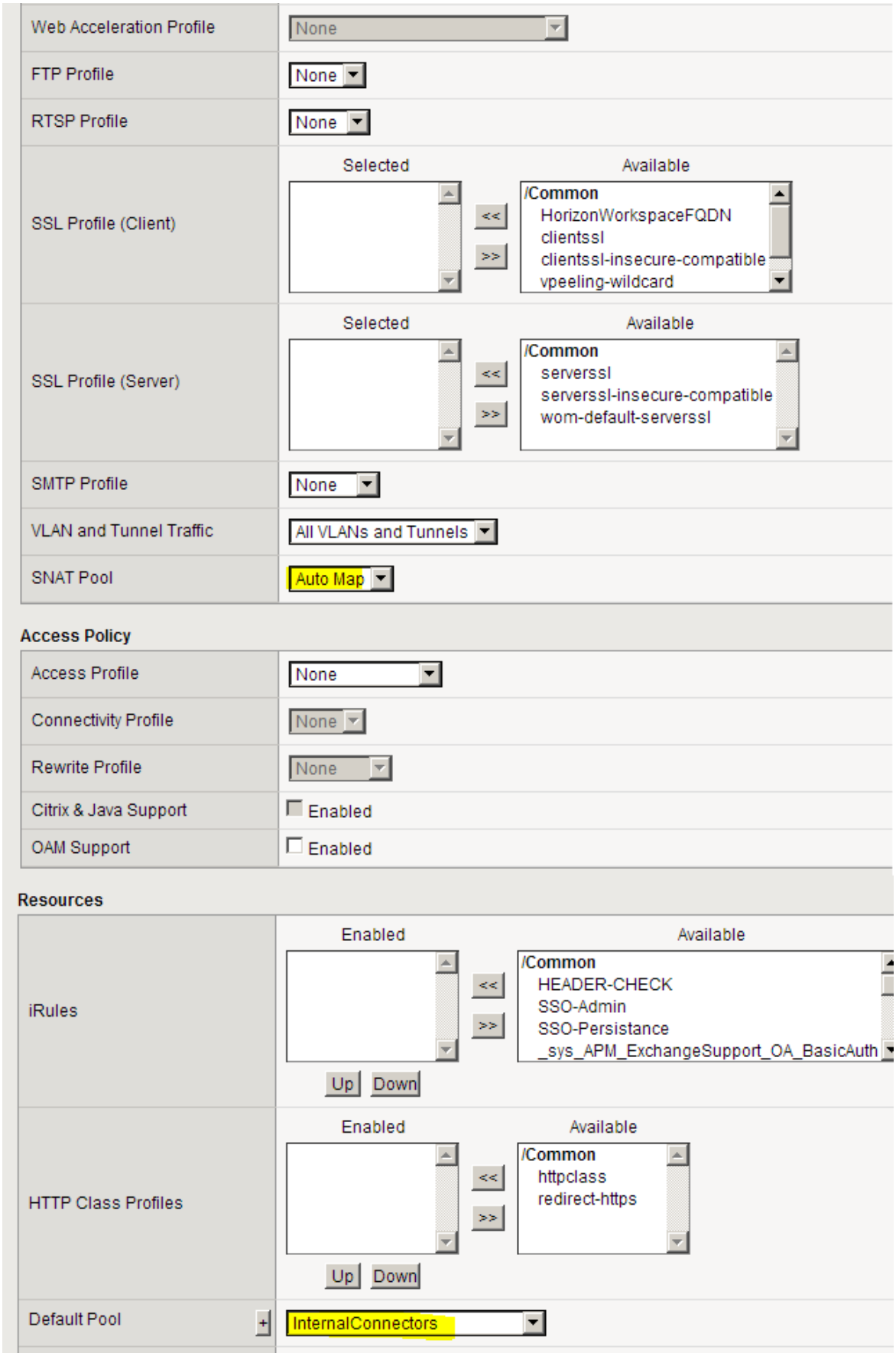


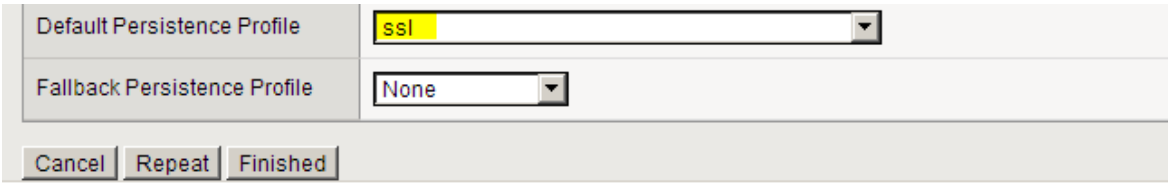
Scroll to the bottom and click "Finished"

Create Virtual Server on F5 LTM

Go to Local Traffic ›› Virtual Servers : Virtual Server List and click "Create".
Configure as detailed on the picture below and make sure that the "Default Pool" is set to the pool created in the above step and "Default Persistence Profile" is set to ssl.




Web Acceleration Profile
None
FTP Profile
None
RTSP Profile
None
SSL Profile (Client)
Selected
Available
/Common
HorizonWorkspaceFQDN
clientssl
clientssl-insecure-compatible
vpeeling-wildcard
SSL Profile (Server)
Selected
Available
/Common
serverssl
serverssl-insecure-compatible
wom-default-serverssl
SMTP Profile
None
VLAN and Tunnel Traffic
All VLANs and Tunnels
SNAT Pool
Auto Map
Access Policy
Access Profile
None
Connectivity Profile
None
Rewrite Profile
None
Citrix & Java Support
Enabled
OAM Support
Enabled
Resources
iRules
Enabled
Available
/Common
HEADER-CHECK
SSO-Admin
SSO-Persistance
_sys_APM_ExchangeSupport_OA_BasicAuth
Up
Down
HTTP Class Profiles
Enabled
Available
/Common
httpclass
redirect-https
Up
Down
Default Pool
InternalConnectors



Scroll to the bottom and click "Finished"

Validate that the Horizon Workspace FQDN is accessible and that all member nodes shows up as being accessible (green mark) in the F5 admin interface

---

Change certificates on the connectors

For Windows Authentication (Kerberos, SSO) to fully work the clients needs to trust the certificates on the connector. It is possible to import the existing self-signed certificate that comes with the connector-VA but this tech-note assumes the requirement for use of proper CA signed certificates.

Login to the connectors admin webinterface which is running on HTTPS port 8443 (eg. https://connector01.corp.local:8443/) and go to "SSL Certificate".
Paste in the certificate to be used as well as the corresponding private key and click "Save"
Do the above for all participating connectors.

Once the certificate has been changed on the connectors it is required to restart the *tcserver-c2* service on the connector.
To do this login to the connector-VA using SSH as the user sshuser. Afterwards change user to root. Run the following command to restart the service:

```
service tcserver-c2 restart
```

Once the service has been restart go back to the admin interface of the connectors (eg. https://connector01.corp.local:8443/) and validate that the certificate has been changed that it validates in the browser session.

NOTE: The above steps needs to be done on all participating connector VAs.

Stay logged in to the admin interface as well as the SSH session.

Establish certificate trust on the connectors

Before it is possible to change the idP Hostname of the connectors to point to the new F5

Virtual Server FQDN so they can be actively load balanced the certificates used on the connectors needs to be trusted by the connectors itself.
When changing the idP Hostname the tc-server checks the FQDN entered and expects a proper HTTP OK (Code 200) response. If using a certificate on the connectors that are not already trusted by the tc-server an error will be displayed when trying to change the idP Hostname.
To solve this issue the root certificate and any intermeddiate/subordanating/issuing used to sign the certificate used on the connectors needs to be added to the cacerts keystore.

NOTE: The entire certificate chain is required to establish the trust

Upload the entire certificate chain (root/subordinate/issuing etc.) in PEM format to the connector VAs. Eg. */tmp/mycerts.cer*
An example of the correct listing is provided below.

```
-----BEGIN CERTIFICATE-----
intermediate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
root certificate
-----END CERTIFICATE-----
```

Log into the connector VAs as sshuser and switch user to root. Run the following command:

```
/usr/java/jre-vmware/bin/keytool -import -trustcacerts -file /tmp/mycerts.c
-alias <your-alias> -keystore /usr/java/jre-vmware/lib/security/cacerts
```

Replacing */tmp/mycerts.cer* with the location of where the certificate chain PEM file was placed as well as replacing <your-alias> with a name for the certificate(s) excluding the "<>"

Once prompted for the password for the cacerts keystore enter: *changeit*

When it asks to trust the certificate and add it to the store answer by typing: *yes*

Finish the configuration by restarting the tc-service on the connector:

```
service tcserver-c2 restart
```

NOTE: The above steps needs to be done on all participating connector VAs.

Change idP Hostname of the connectors

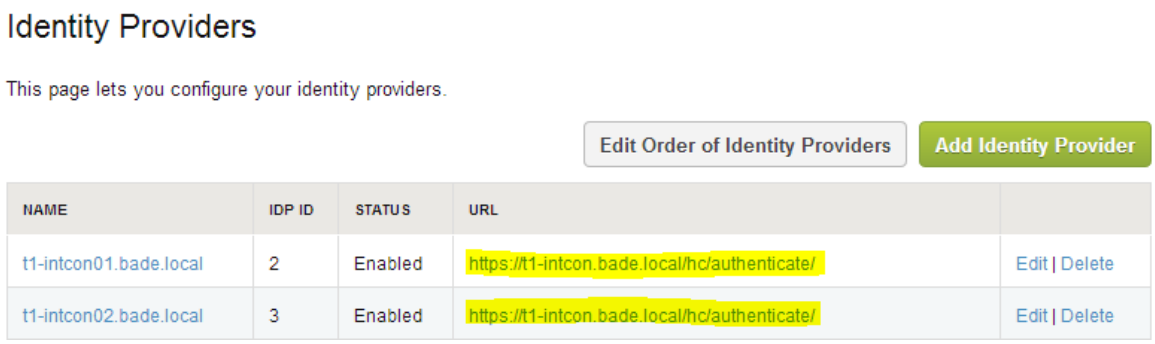
Once the certificates has been replaced on the connector VAs and the tc-server trusts the root certificate the idP Hostname can be changed from the admin interface of the individual connectors.

Log into the web admin of the connector VAs and go to "Identify Provider"

Change the "idP Hostname" to be the FQDN of the F5 LTM Virtual Server as created in the step above (eg. connectors.corp.local) and press save.
This should result in a message saying the idP Hostname was successfully changes. If it responds with an error it is typically due to a lack of trust for the certificates or the FQDN entered does not result to the correct Virtual Server (VIP) on the F5 LTM.

NOTE: The above steps needs to be run on all participating connector VAs.

Once the above changes has been made log into the Horizon Workspace Admin interface and go to "Identity Providers" under the "Settings" tab.
The "URL" of the connectors used for Windows Authentication should now show up with the same URL as shown on the picture below:



TROUBLESHOOTING

Troubleshooting section for the various configurations detailed above.

Finding the F5 BIG IP address

If setting the X-Forwarded-For options in the above steps does not work its possible that the wrong IP for the F5 BIG IP was entered.

If that is the case it is possible to disable the IP checks completely. This allows for accessing the Audit report even with an Load Balancer in front of the Gateway-VAs.

NOTE: The F5 BIG IP LTM will typically identify itself with the IP configured on the 'Private'

interface.

Edit the following file using vi or any other preferred editor:

/opt/vmware/nginx/conf/location-443.conf

Search for /AUDIT (If using vi just enter /AUDIT and press enter)

Comment out the following lines so they look like the below:

```
#allow 127.0.0.1;
#include gen/all.allow;
#deny all;
```

Commit the changes (if using VI type *:wq!*) and restart the nginx and memcached services:

```
service nginx restart
service memcached restart
```

Now when accessing the Audit Report in Horizon Workpace the IP address used by F5 BIG IP will show up in the logs.

Once this change has been made validate access to the Audit Reports by following the information in the section below.
As this step is for troubleshooting purposes with an incorrect X-Forwarded-For configuration the "sourceIp" field should now show you the IP adress that the F5 uses for communication with the Horizon Workspace solution. Note down this IP and ues it in the X-Forwarded-For configuration steps above.

For more information on these configuration changes go to the Installing Horizon Workspace 1.0 guide on page 56.
NEEDS UPDATE TO 1.5 DOCS

Validate login and AUDIT

Login to the Horizon Workspace URL as an admin and verify that you can successfully access the Audit Report

Click on one of the "LOGIN" event types and verify that the correct client IP shows up in the logs. There will be 2 entries for every login; One with information on which gateway-VA was used and the other containing client IP information. An example is provided below:

```
{
  "baseType" : "Action",
  "objectType" : "LOGIN",
  "values" : {
    "success" : "true"
  },
  "actorId" : 7,
  "actorUserName" : "administrator",
  "clientId" : null,
  "deviceId" : null,
  "sourceIp" : "192.168.0.12",
  "objectId" : null,
  "timestamp" : 1366270172165,
  "uuid" : "64fc70ec-417e-4e2a-9fb0-2f11025db9c9",
  "organizationId" : 1
}
```


Validate that the LOGIN response in the Audit report actually returns the proper IP address of the client. The IP address of the client logging in is shown in the "sourceIp" field.
If the "sourceIp" is not the IP of the client performing the login the X-Forwarded-For is not configured correctly.

Miscellaneous configuration options

This section details optional configuration options that can be performed to tighten security, provide additional features etc.

Redirecting HTTP to HTTPS for the Horizon Workspace URL

The default option for a Horizon Workspace gateway-va is to forward HTTP (80) to HTTPS (443) to avoid an error if https:// was not explicitly specified by the user accessing the Horizon Workspace service.
It is possible to achieve the same HTTP > HTTPS forward with F5 BIG IP by creating a new Virtual Server with the same VIP as used for HTTPS and then associating it with the same Pool as used by the VIP serving HTTPS.
To get the HTTPS redirect associate the *_sys_https_redirect* iRule with the newly created Virtual Server. This will forward HTTP > HTTPS so a user will automatically get transfered to the HTTPS VIP for proper Horizon Workspace access.

Deny access to the Horizon Workspace admin interface using iRule

It is possible to deny access to the admin interface of Horizon Workspace when exposing the service externally. This allows for a more secure implementation where the admin interface cannot be accessed from the VIP providing the external access.
This is achieved by using an iRule on the externally facing Virtual Server that drops any request for the admin URL.

Enter the following into a new iRule and afterwards associate it with the Virtual Server being used for providing external access to Horizon Workspace.

```
when HTTP_REQUEST {
        switch -glob [string tolower [HTTP::uri]] {
              "/admin*" {
        # Block Access to Admin URL From External
        log local0. "Access Blocked For URI- [HTTP::uri]"
        HTTP::respond 403 content {<html>Page Not Found</html>}
        return
        }
        default {
        # Do Nothing
        }
    }
}
```

External resources / links

- VMware Horizon Workspace Documentation
- F5 BIG-IP LTM / VE 11.3.0 Documentation

Changelog

Version 0.1

- Initial version including overview and general configuration procedure for load balancing gateway-VA(s) and load-balancing kerberos enabled connector-VA(s)

Version 0.2

- Added information on that the full certificate chain is required for establishing trust on

Kerberos Connector-VAs (Thanks to Rob Orr)

- Added pre-reqs for load balancing Gateway-VAs: ICMP required against F5 BIG IP from Gateway-VAs (Thanks to Matthew Mabis)