

1. VMware NSX AVI Loadbalancer Integration with VMware Horizon

To deploy AVI LoadBalancer, there are two main components involved:

AVI Controller:

The Avi Controller is a centralized brain that spans data centers and clouds. The Avi Controller has full visibility across the environments and automates the deployment and management of the load balancing endpoints, which we call Service Engines.

We need one AVI Controller to manage the Service Engine across the site if all the network configurations are in-place. In Our Lab, Avi Controller is pre-deployed in Site-2 which will manage both the Service Engines

Service Engine:

Service Engine is a Load Balancer Component which runs on each datacenter. Service Engine(SE) is managed by AVI Controller. In the lab we will see how SEs are configured as a Load Balancer to full-fill the request from Applications.

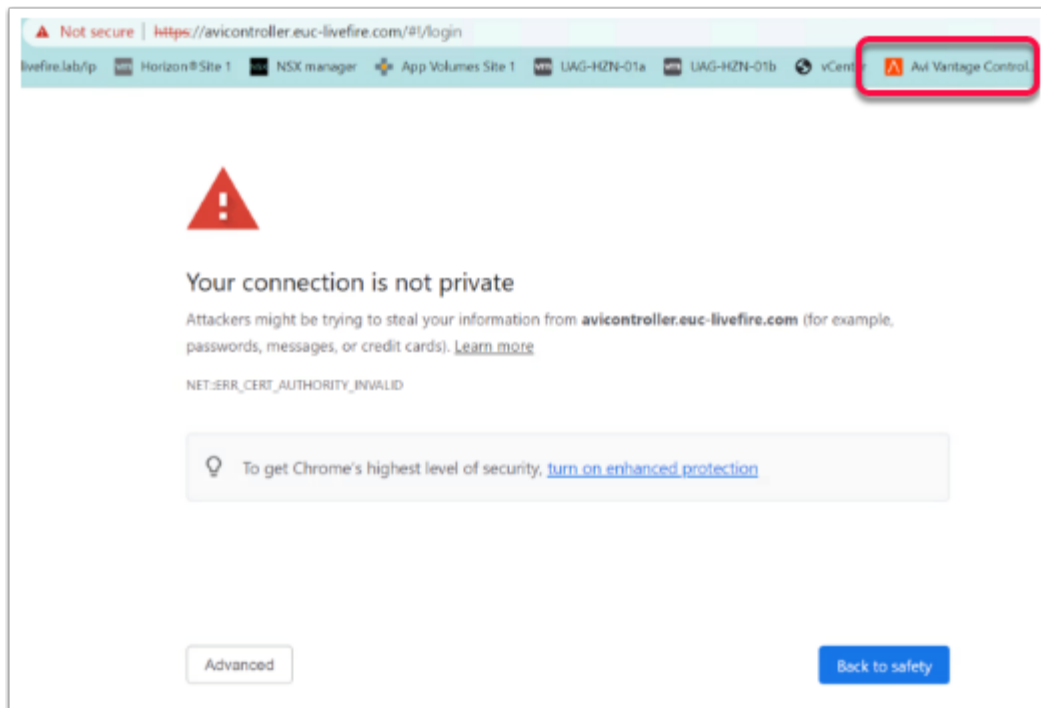
In Our case Applications are UAGs across both Site-1 and Site-2

Configure Backend server groups

Part 1 - AVI Integration with UAG Servers Site-1

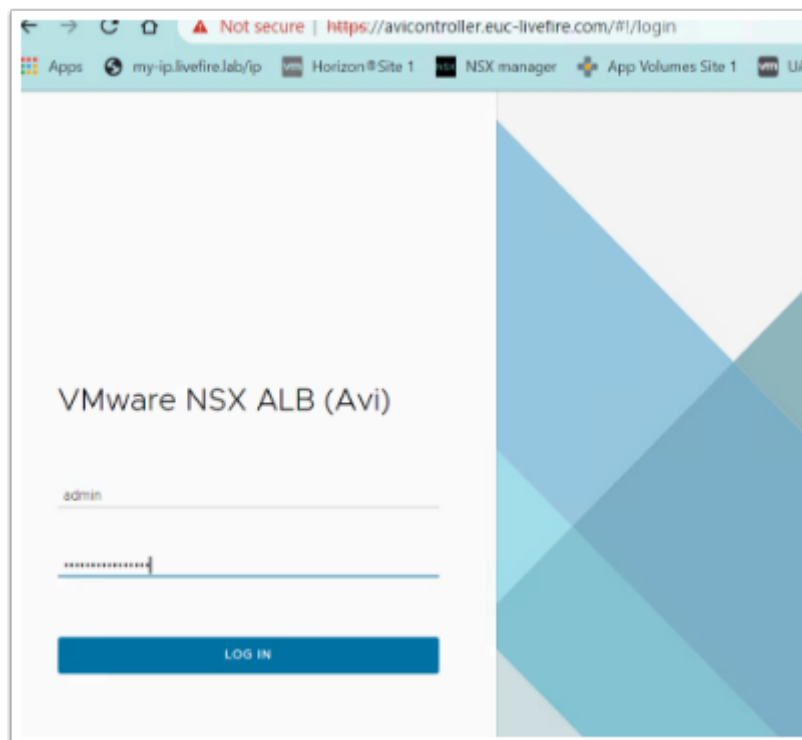
Section 1 - AVI Integration with UAG Servers in Site1

FQDN	Entity Description	Real IP
uag-hzn-avi01.euc-livfire.com	FQDN of Avi LB VIP Site-1	172.16.20.100
uag-hzn-01a.euc-livfire.com	FQDN of UAG server 1 on site 1	172.16.20.10
uag-hzn-01b.euc-livfire.com	FQDN of uag server 2 on site 1	172.16.20.11



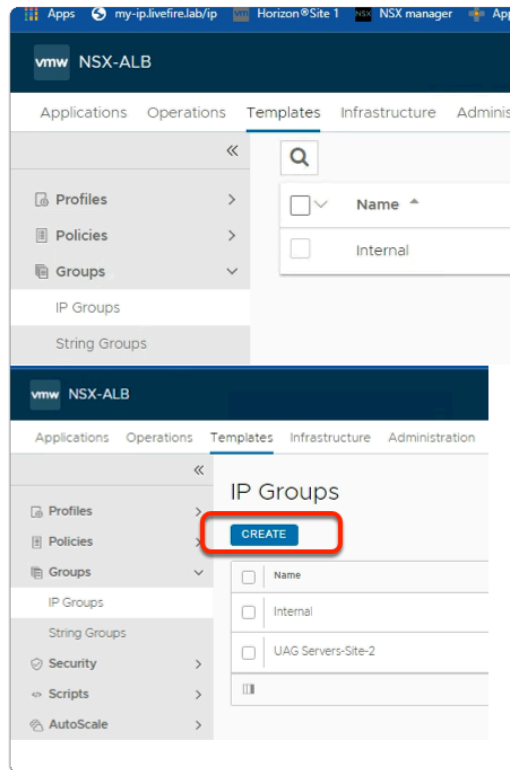
1. On your ControlCenter Server

- Open your **Chrome Browser for Site-1**
 - In the **Address bar**, Enter and browse to **avicontroller.euc-livewire.com**
 - In the **Your Connection is not private** window
 - Select **Advanced**
 - Select **Proceed to avicontroller.euc-livewire.com**

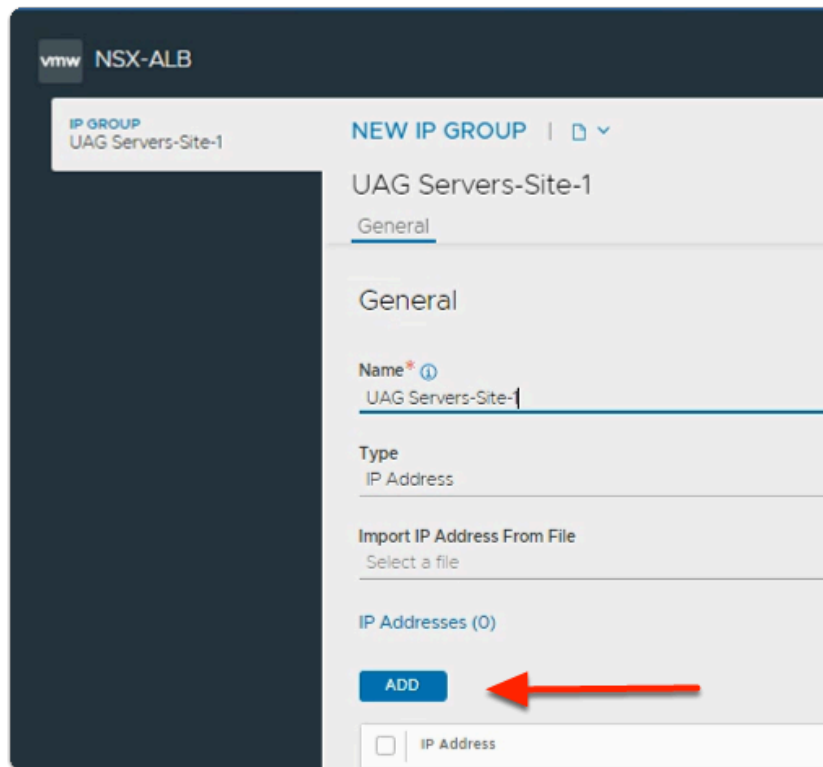


2. In the **VMware NSX ALB (Avi)** page

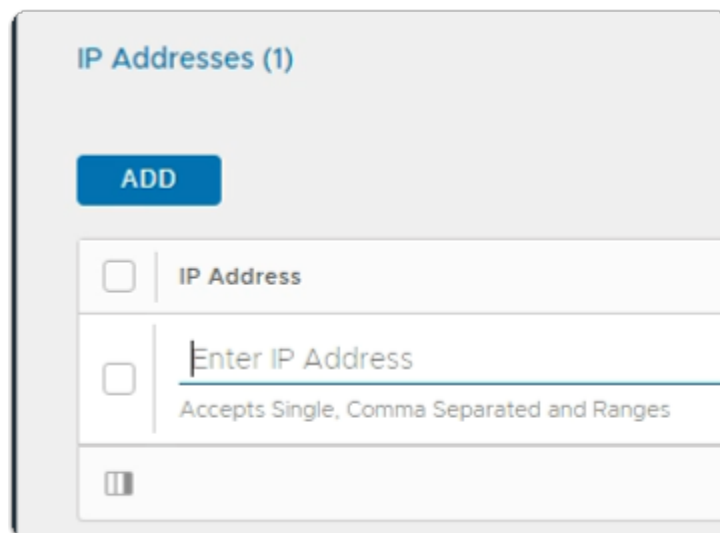
- Under Username, enter **admin** and **VMware1!VMware1!** as the password



3. From the **NSX-ALB** console,
 - Navigate to **Templates** > **Groups**.
 - Select **IP Groups**
 - In the **IP Groups** area
 - Select **CREATE**



4. In the **NEW IP Group:** window
 - In the **General** area
 - Under **Name***
 - Type **UAG Servers-Site-1**
 - Under **IP Addresses** area
 - Select **ADD**



5. In the **IP Addresses (1)** area
 - Under **IP Address**
 - In the **Enter IP Address** area
 - Type **172.16.20.10**

IP Addresses (1)

ADD

<input type="checkbox"/>	IP Address
<input type="checkbox"/>	172.16.20.10 Accepts Single, Comma Separated
<input type="checkbox"/>	

6. In the **IP Addresses (1)** area

- Select **ADD**

IP Addresses (2)

ADD

<input type="checkbox"/>	IP Address
<input type="checkbox"/>	172.16.20.10 X Accepts Single, Comma Separated and Ranges
<input type="checkbox"/>	Enter IP Address Accepts Single, Comma Separated and Ranges


7. In the **IP Addresses (2)** area

- Under **IP Address**
 - In the **Enter IP Address** area
 - Type **172.16.20.11**

8. In the **IP Addresses (2)** area
 - In the bottom right hand corner
 - Select **Save**

Verify Custom Health Monitor Profile

Part 2: Verify Custom Health Monitor Profile

-  The next step is to validate the custom Health Monitor Profile.
Note:- This is pre-created

Name	Type	Federated	Send Interval	Receive Timeout	Successful Checks	Failed Checks
Horizon-HTTPS	HTTPS	No	30 Seconds	10 Seconds	2	2
System-DNS	DNS	No	6 Seconds	4 Seconds	2	2
System-HTTP	HTTP	No	10 Seconds	4 Seconds	3	3

1. From the **NSX-ALB** console,
 - Navigate to **Templates > Profiles**
 - Under **Profiles**
 - Select **Health Monitors > Horizon-HTTPS**

- Click on the **pencil** icon to the right of **Horizon-HTTPS**

Form fields and values:

- Name: Horizon-HTTPS
- Type: HTTPS
- Description: (empty)
- Successful Checks: 2
- Failed Checks: 2
- Send Interval: 30 sec
- Receive Timeout: 10 sec
- Is Federated: ☐

- On the **New Health Monitor** page,
 - Validate the following configuration
 - **Name: Horizon-HTTPS**
 - **Type : HTTPS**
 - **Send Interval 30**
 - **Receive Timeout 10**

Page title: Edit Health Monitor: Horizon-HTTPS

Section: • HTTPS Settings •

Health Monitor Port: Use Server Port

Authentication Type: Authentication Type

Client Request Header	CONVERTED
USER INPUT	
GET /favicon.ico HTTP/1.0	GET /favicon.ico

- On the **Edit Health Monitor: Horizon-HTTPS** page,
 - Scroll down to the **HTTPS Settings** section
 - Under **Client Request Header: GET /favicon.ico HTTP/1.0**

This screenshot shows a configuration panel with the following fields:

- Response Code***: A dropdown menu currently showing '2XX' with a close icon (X) and a help icon (?).
- SSL Attributes**: A checkbox that is checked, with a help icon (?).
- TLS SNI Server Name**: A text input field containing 'Host Header' and a help icon (?).
- SSL Profile***: A dropdown menu showing 'System-Standard' with a close icon (X) and an edit icon (pencil).
- PKI Profile**: A dropdown menu showing 'Select PKI Profile' with a help icon (?) and a close icon (X).

4. On the **New Health Monitor: Horizon-HTTPS** page,
 - Scroll down until you locate **Response Code***
 - **Response Code*** : 2XX
 - **Next to SSL Attributes:** Checkbox is selected
 - **SSL Profile*** : System-Standard.

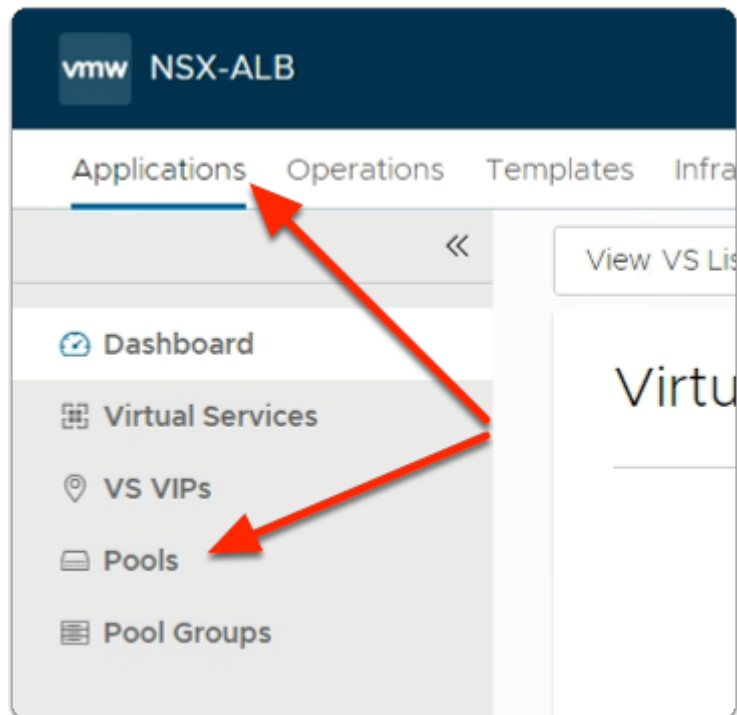
This screenshot shows the 'New Health Monitor: Horizon-HTTPS' page. The 'Maintenance Response Code' field is visible and contains the value '503'. Below this field is an 'ADD' button. At the bottom of the page, there is a 'Save' button and a pagination control showing 'Items per page 10'.

5. On the **New Health Monitor: Horizon-HTTPS** page,
 - **Scroll down** until you locate **Maintenance Response Code***

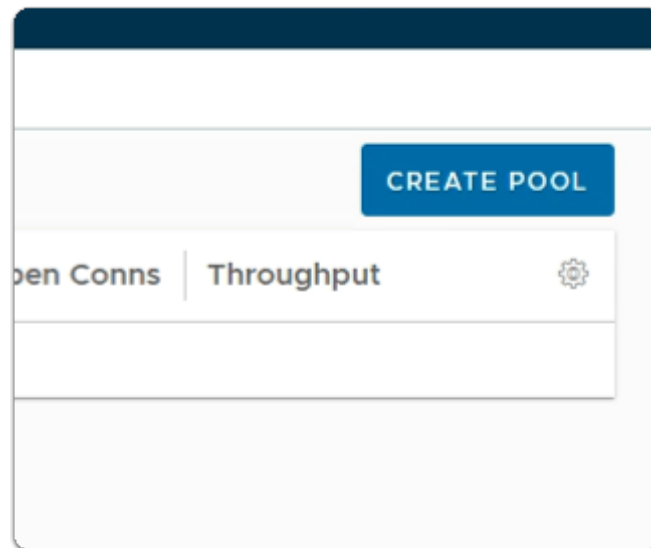
- **Maintenance Response Code :503**
- Close the **Edit Health Monitor: Horizon-HTTPS**
- **Do Not make any changes**

i We will now create L7 Pools for Site-1

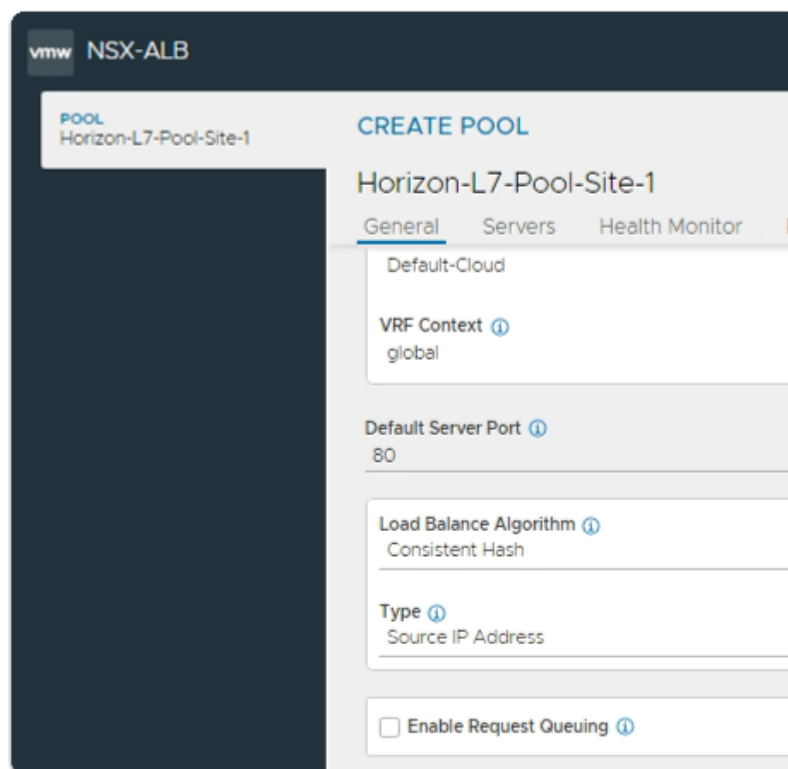
Part 3: Creating Layer 7 Pools For Site-1



1. From the NSX-ALB console
 - Navigate to **Applications > Pools**.

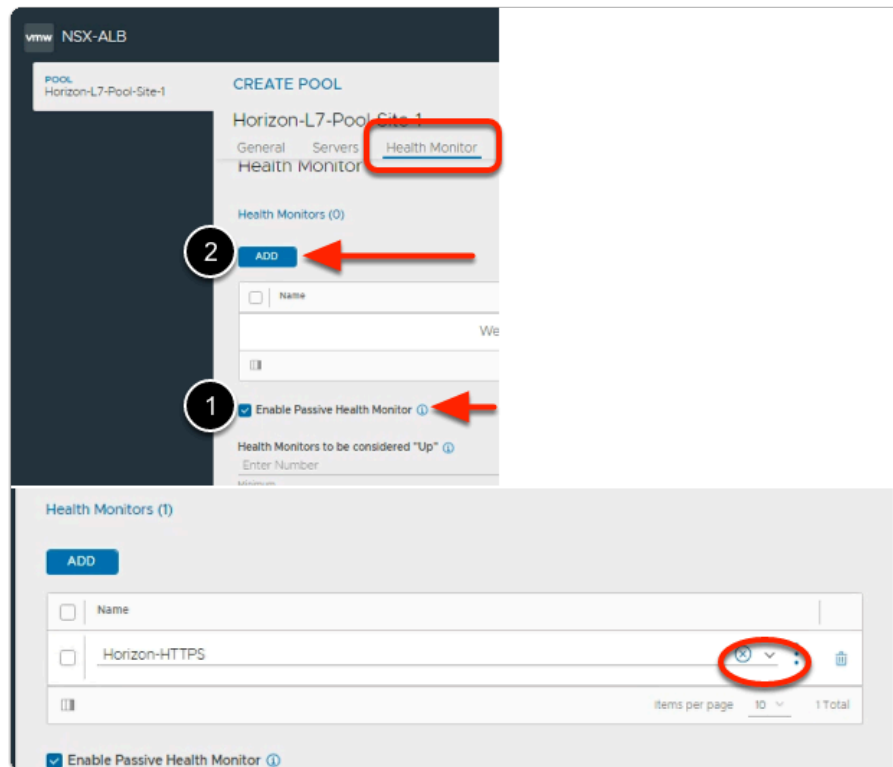


2. In the **Pools** area
 - To the right of the pane
 - Select **CREATE POOL**



3. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - **Step 1: Settings**
 - Enter the required information:
 - Under **Name***:
 - Type **Horizon-L7-Pool-Site-1**
 - Under **Default Server Port**
 - Type **443**

- Under **Load Balance Algorithm**:
 - From the drop down
 - Select **Consistent Hash**
 - with **Source IP Address** as the hash key.



4. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - In the **Health Monitor** tab
 1. Make sure the **checkbox** next to:
 - **Enable Passive Health Monitor** is **checked**
 2. Select **ADD**.
 - Above **+ Add Active Monitor**.
 - From the dropdown,
 - select is **Horizon-HTTPS**
 - This is the health monitor that you validated earlier

Graceful Deactivate Timeout ⓘ

1

Minutes

☐ Enable HTTP2 ⓘ

☐ Lookup Server by Name ⓘ

☐ Rewrite Host Header to Server Name ⓘ

Append Port To Host Name ⓘ

☒ Never ☐ Always ☐ Non Default (80, 443)

☐ Deactivate Port Translation ⓘ

☐ Use Service SSL Mode ⓘ

5. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - To the right of the **Health Monitors** area
 - Scroll Down
 - below **Append Port To Host Name**
 - next to **Never**
 - select the **radio button**

CREATE POOL

Horizon-L7-Pool-Site-1

General Servers Health Monitor Profiles/Policies **SSL** Fail Action

SSL

SSL Profile ⓘ
System-Standard

Server SSL Certificate Validation PKI Profile ⓘ
Select Profile

Service Engine Client Certificate ⓘ
Select Certificate

☐ Enable Common Name Check ⓘ

☒ Enable TLS SNI ⓘ

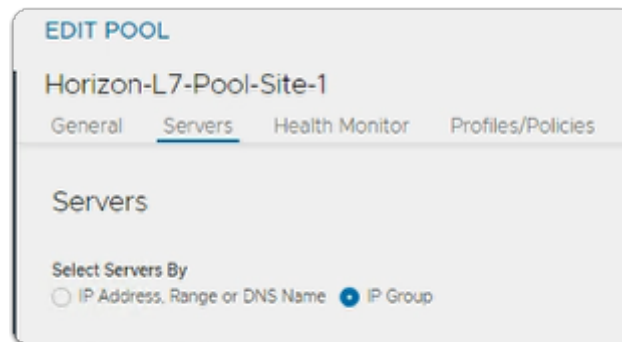
TLS SNI Server Name ⓘ
Enter Server Name
Host header will be used by default

☐ Rewrite Host Header to SNI Name ⓘ

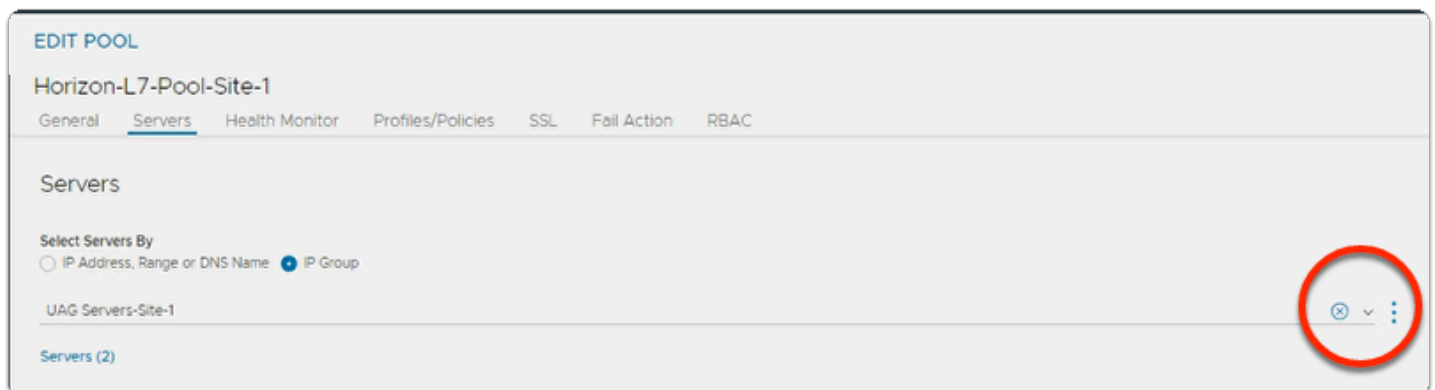
SAVE

6. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - **Scroll down**
 - below the **SSL section**
 - under **SSL Profile**
 - select **System-Standard.**

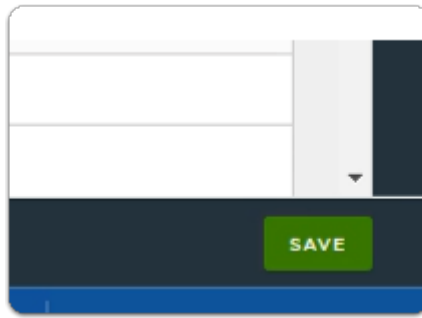
- next to the **Enable TLS SNI**
 - ensure this box is **Checked**
 - Leave all the remaining settings as defaults



8. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - **In the top of the interface**
 - select the **Servers** tab
 - under **Servers**
 - next to **IP Group**
 - ensure the **radio button** is select



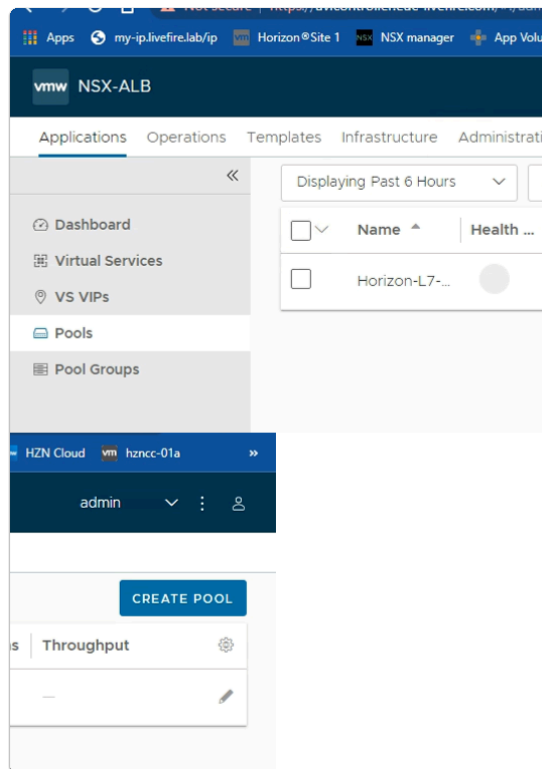
9. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - **Servers tab**
 - **IP Group** area
 - From the **dropdown**,
 - select **UAG Servers-Site-1**
 - You created this earlier
 - Leave all the other settings as default



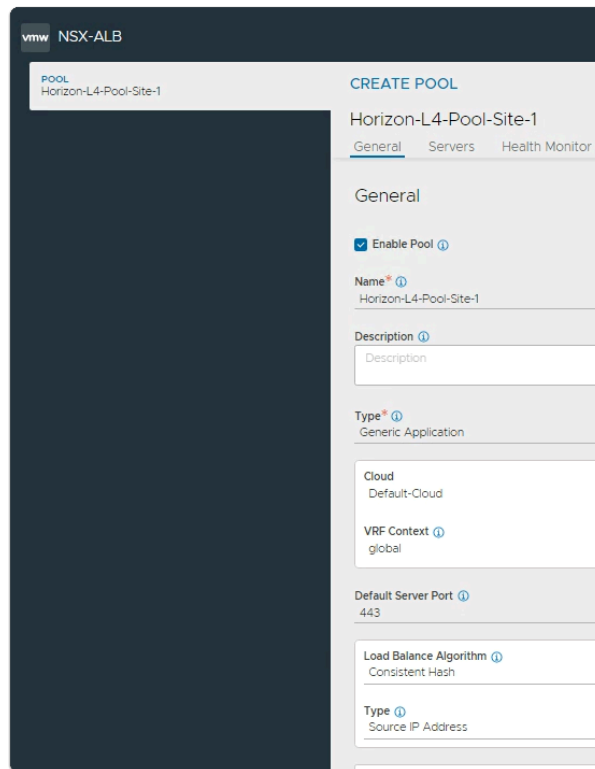
11. In the CREATE POOL: **Horizon-L7-Pool-Site-1** window,
 - In the bottom right corner
 - select **SAVE**

Creating the UAG L4 Pool For Site-1

Part 4: Creating Layer 4 Pools For Site-1

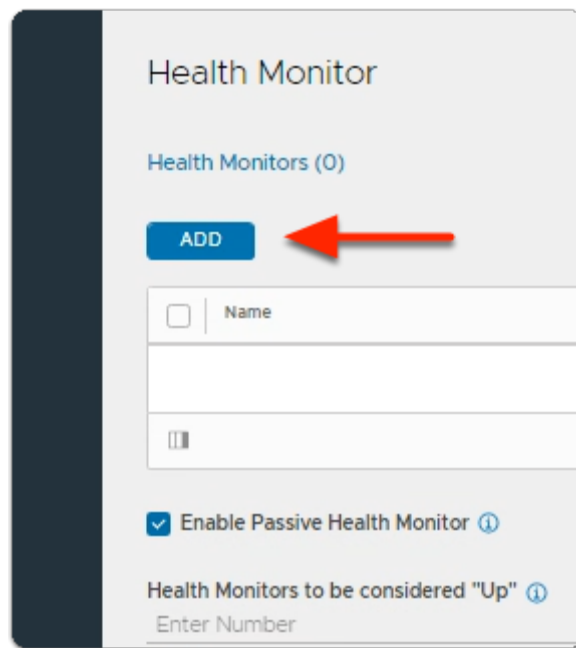


1. In the NSX-ALB admin console
 - In the **Applications > Pools** area
 - Select **CREATE POOL**

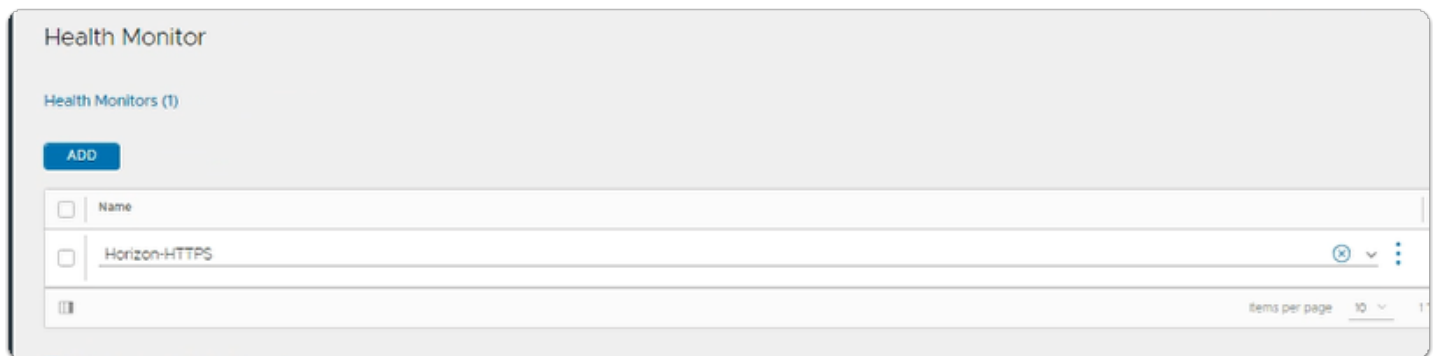


2. In the **CREATE POOL:** window

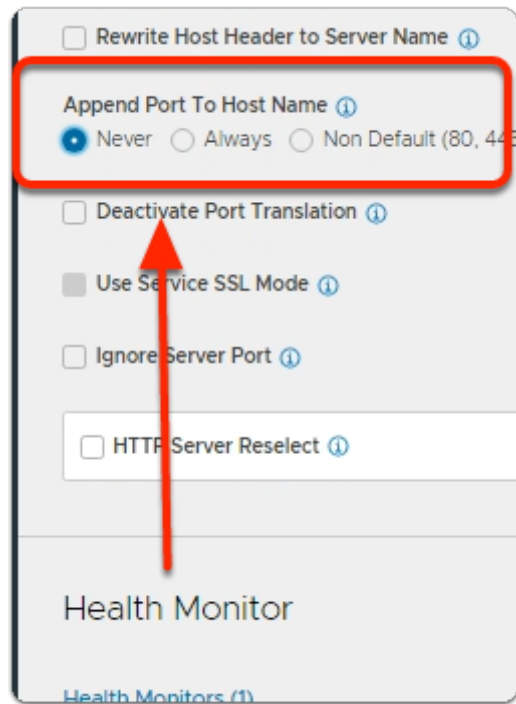
- **General** tab
 - Enter the following under:-
 - Under **Name***
 - type: **Horizon-L4-Pool-Site-1**
 - Under **Default Server Port**
 - Type: **443**
 - Under **Load Balance Algorithm:**
 - Select **Consistent Hash**
 - with **Source IP Address** as the Type
 - select the **Health Monitor** tab



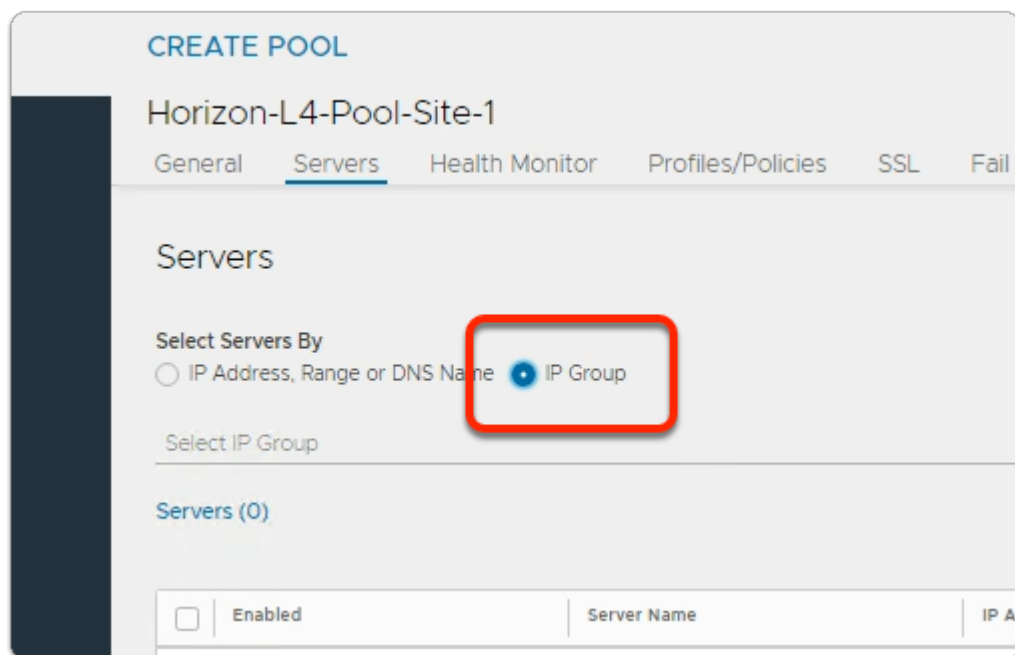
3. In the **CREATE POOL:** window
 - **Health Monitor** tab
 - enable the following under:-
 - ensure **Enable Passive Health Monitor** is checked
 - under **Health Monitors**
 - select **ADD**



4. In the **CREATE POOL:** window
 - **General** tab
 - under **Health Monitors**
 - from the dropdown.
 - select **Horizon-HTTPS**



5. In the **CREATE POOL:** window
 - **Health Monitor** tab
 - Just **above** the **Health Monitor** section
 - below **Append Port To Host Name:**
 - next to **Never**
 - select the **Radio button**



6. In the **CREATE POOL:** window
 - select the **Servers** tab

- under **Select Servers By**
 - select the **IP Group radio button**

CREATE POOL

Horizon-L4-Pool-Site-1

General Servers Health Monitor Profiles/Policies SSL Fail Action RBAC

Servers

Select Servers By

☐ IP Address, Range or DNS Name ☒ IP Group

UAG Servers-Site-1

Servers (2)

Enabled	IP Add
<input type="checkbox"/>	172.16

- In the **CREATE POOL:** window
 - **Servers** tab
 - below **Select Servers By**
 - from the **dropdown**
 - select **UAG Servers-Site-1**
 - leave all the rest of the settings default

10 1 Total

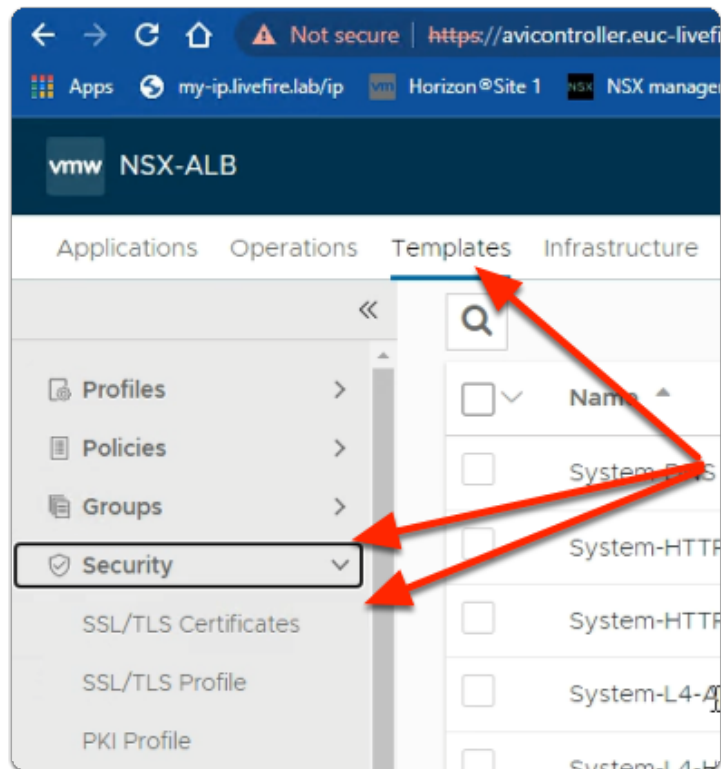
SAVE

- In the **CREATE POOL:** window
 - bottom right corner
 - Select **SAVE**



Validate the SSL certificate Required for L7 VIP is pre-configured

Part 5: Verify SSL Certificate required for Layer 7 VIP is present.



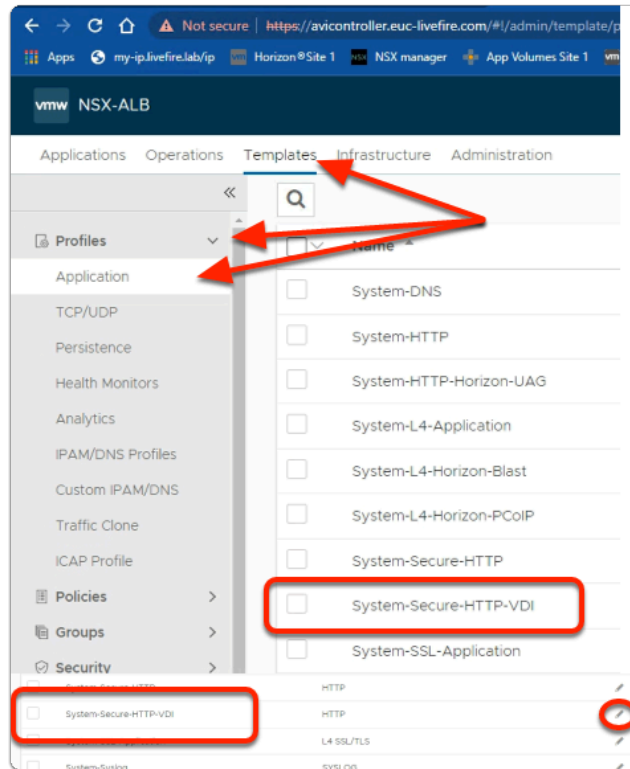
1. From the **NSX-ALB** Admin console
 - Navigate to **Templates** > **Security** > **SSL/TLS Certificates**



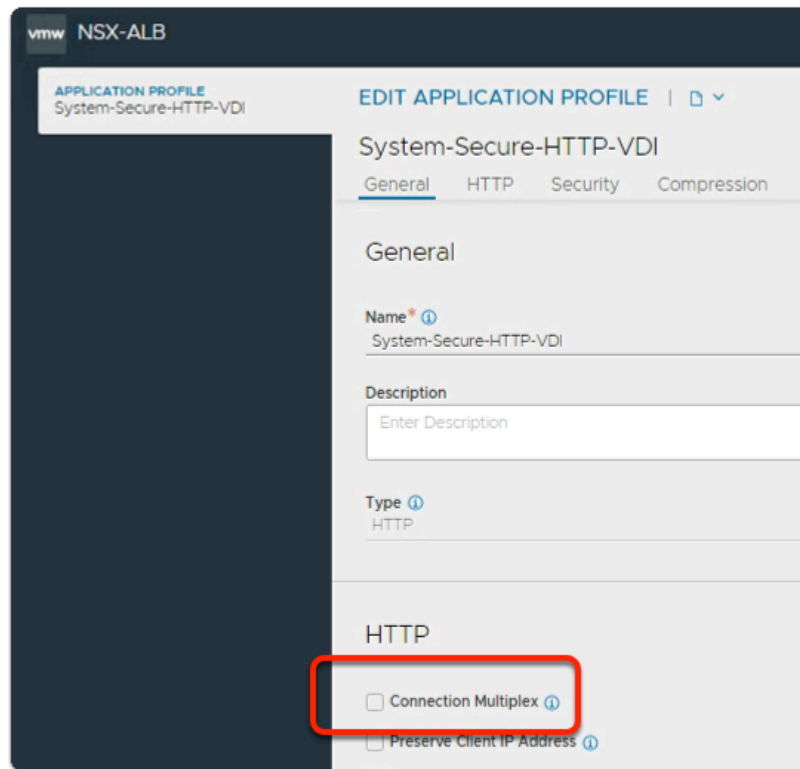
2. In the **SSL/TLS Certificate** Window
 - Verify the **HZNCert2023** shows status **green**

i Validating that Connection Multiplexing is disabled

Part 6: Validating that Connection Multiplexing is disabled



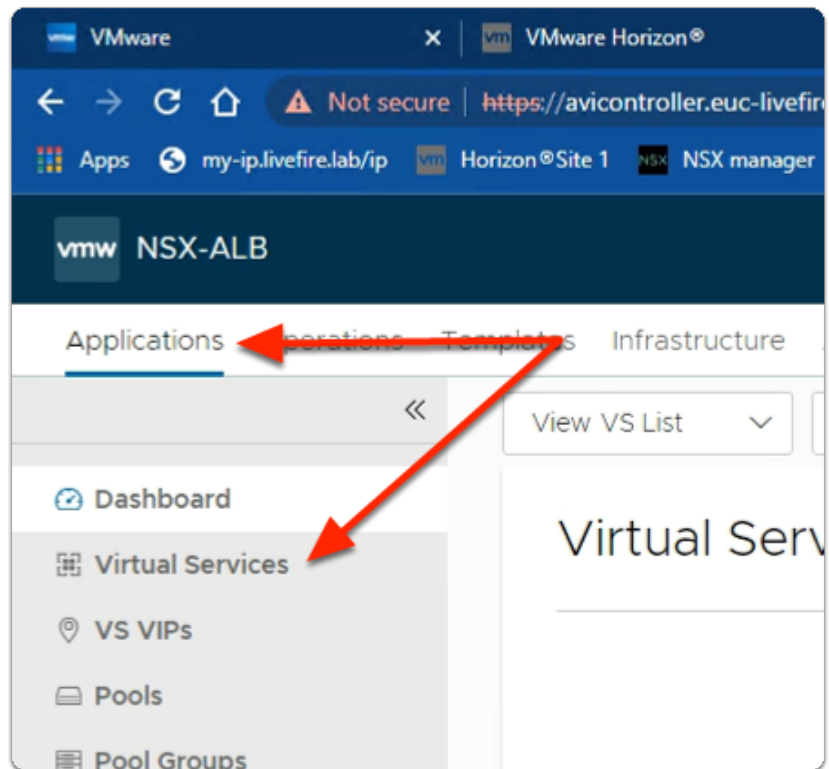
1. In the **NSX-ALB** console
 - Navigate to **Templates** > **Profiles** > **Application**
 - In the **Application** area
 - select **System-Secure-HTTP-VDI**.
 - To the right of **System-Secure-HTTP-VDI**
 - Select the **edit** icon.



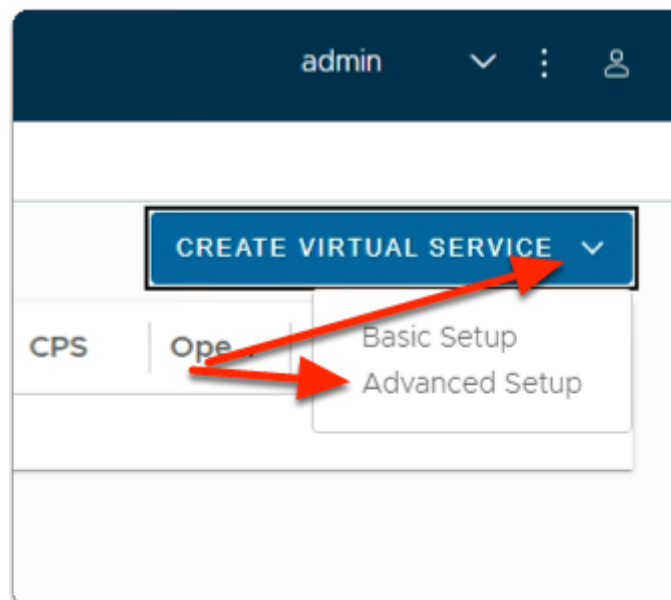
2. In **Edit Application Profile: System-Secure-HTTP-VDI** window
 - Ensure the **checkbox** next to **Connection Multiplexing** is **NOT selected**
 - Select **Cancel**
 - to close the **Edit Application Profile: System-Secure-HTTP-VDI** window

Creating the L7 Virtual Service for Site-1

Part 7: Creating the Layer 7 Virtual Service for Site-1



1. In the **NSX-ALB** Console
 - Navigate to **Applications** > **Virtual Services**



2. In the **Virtual Services** area
 - To the top right, select **CREATE VIRTUAL SERVICE**
 - Select **Advanced Setup**.

Step 1: Settings

Name* ?
Horizon-UAG-L7-Site-1

Enabled ?
✓

• VIP Address •

VS VIP* ?
Select VS VIP

3. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - enter the following under:
 - **Name***
 - type **Horizon-UAG-L7-Site-1**
 - **VS VIP ***
 - select the **dropdown**,
 - notice a **Create VS VIP Green box** appears

• VIP Address •

VS VIP* ?
Select VS VIP

Search

-- no valid entries --

Create VS VIP

4. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - In the **VIP Address** area
 - select **Create VS VIP**

Create VS VIP: VIP-H

General RBAC

General

Name* ⓘ
VIP-Horizon-UAG-Site1

Cloud
Default-Cloud

VRF Context ⓘ
global

VIPs (0)* ⓘ

ADD

5. In the **Create VS VIP:** page
 - In the **General** tab,
 - under **Name**
 - type: **VIP-Horizon-UAG-Site1**
 - Select **ADD**

Edit VIP: 1

General

General

☒ Enable VIP ⓘ

Private IP ⓘ

IPv4 Address* ⓘ
172.16.20.100

IPv6 Address ⓘ
Enter IPv6 Address

SAVE

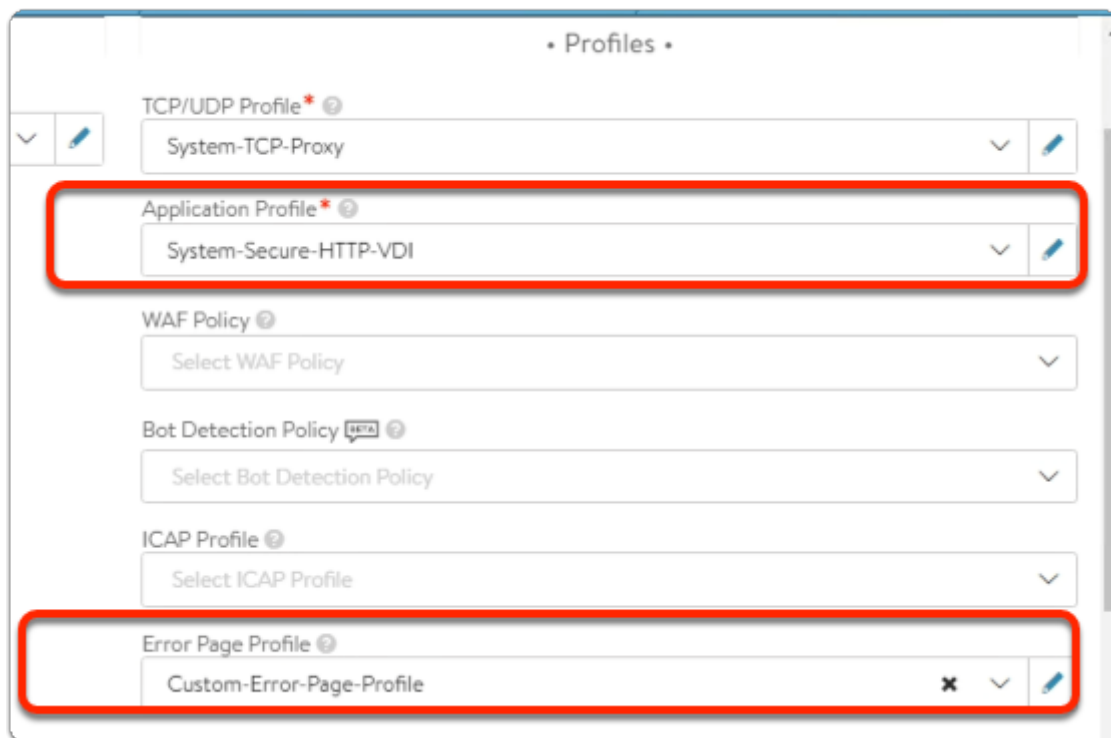
6. In the **Edit VIP: 1** page
- Under **IPv4 Address***
 - type **172.16.20.100**
 - Select **SAVE**

The screenshot shows the 'Create VS VIP: VIP-Horizon-UAG-Site1' window with the 'RBAC' tab selected. The 'General' tab is also visible. The 'Enabled' checkbox is checked. The 'VIP ID' is 1, 'IP Address' is 172.16.20.100, and 'IPv6 Address' is -. The 'BGP Peer Labels' section is collapsed. The 'Role-Based Access Control (RBAC)' section is expanded, showing a table with columns 'Key' and 'Value(s)'. The table is empty, and a message 'We couldn't find any objects!' is displayed. The 'ADD' button is visible. The 'CANCEL' and 'SAVE' buttons are at the bottom.

7. In the **Create VS VIP: VIP-Horizon-UAG-Site1** window
- Select **SAVE**

The screenshot shows the 'New Virtual Service: Horizon-UAG-L7-Site-1' window. The 'Step 1: Settings' tab is active, and the 'Step 2: Policies' tab is also visible. The 'Service Port' section is expanded, showing a table with columns 'Services' and 'Protocol'. The 'Services' column contains the value '443'. The 'Protocol' column has two options: 'HTTP2' (unchecked) and 'SSL' (checked). The 'SSL' option is highlighted with a red box. The 'Switch' button is visible on the right.

8. In the **New Virtual Service** wizard
- **Step 1: Settings** area
 - **Scroll down** to the **Service Port** area
 - under **Services**
 - Enable the **checkbox** next to **SSL**



9. In the **New Virtual Service** wizard
- **Step 1: Settings** area
 - In the **Profiles** sub-area
 - Below **Application Profile***:
 - From the **dropdown**
 - Select **System-Secure-HTTP-VDI**
 - Below **Error Page Profile**:
 - From the **dropdown**
 - Select **Custom-Error-Page-Profile**

• Pool •

☒ Pool
 ☐ Pool Group

Pool ⓘ

Horizon-L7-Pool-Site-1 ✕ ▼ ✎

☐ Ignore network reachability constraints for the server pool ⓘ

• SSL Settings •

SSL Profile* ⓘ

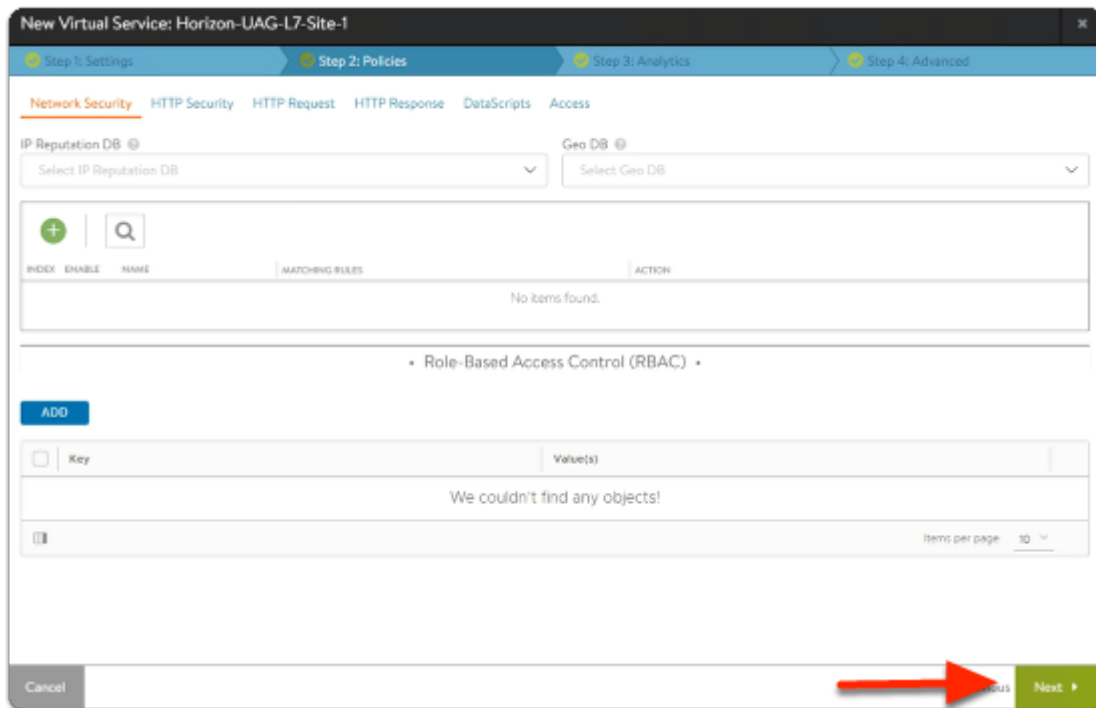
System-Standard ▼ ✎

SSL Certificate* ⓘ

HZNcert2023 ✕ ▼ ✎

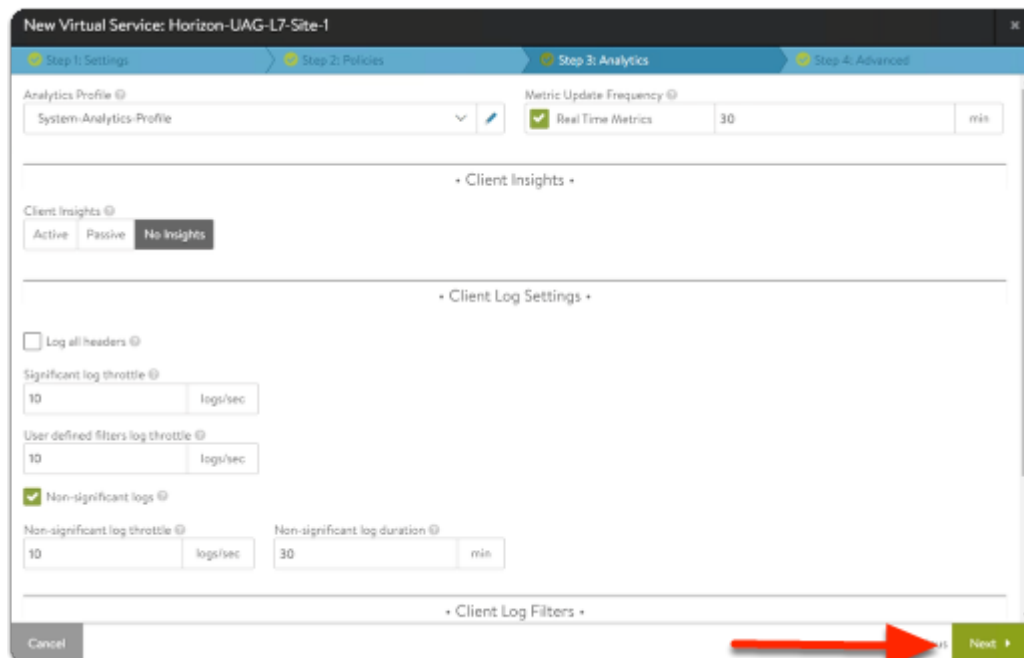
10. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - In the ***Pool*** sub-area
 - Under **Pool**
 - Select the **dropdown**
 - Select: **Horizon-L7-Pool-Site-1**
 - In the ***SSL Settings*** sub-area
 - Under **SSL Profile***
 - Select the **dropdown**
 - Select: **System-Standard**
 - Under **SSL Certificate:**
 - Select the **dropdown**
 - Select **HZNcert2023**
 - **Remove** the **System-Default-Cert**
 - Leave all other settings as default
- In the bottom right corner
 - Select **Next**



11. In the **New Virtual Service** wizard

- **Step 2: Policies** area
 - (Leave everything as default)
- Select **Next**



12. In the **New Virtual Service** wizard

- **Step 3: Analytics** area
 - (Leave everything as default)
- Select **Next**

- **Step 4: Advanced** tab,
 - (Leave everything as default)
 - Select **Save**

The screenshot shows the 'New Virtual Service: Horizon-UAG-L7-Site-1' wizard, Step 4: Advanced. The interface includes the following sections:

- Performance Limit Settings:** A checkbox for 'Performance Limits' is present.
- Quality of Service:** Includes a 'Weight' field set to '1' and 'Fairness' options with 'Throughput And Delay Fairness' and 'Throughput Fairness' tabs.
- Other Settings:**
 - Checkboxes for 'Auto Gateway', 'Use VIP as SNAT', 'Advertise VIP via BGP', and 'Advertise SNAT via BGP'.
 - Fields for 'Host Name Translation' (set to 'sub.com') and 'Service Engine Group' (set to 'Service Engine Group').
 - Fields for 'SNAT IP Address' (set to '1.1.1.1, 200::1') and 'Traffic Clone Profile' (set to 'Select Traffic Clone Profile').
 - Checkboxes for 'Remove Listening Port when VS Down' and 'Scale out ECMP'.
- Role-Based Access Control (RBAC):** A section header at the bottom.

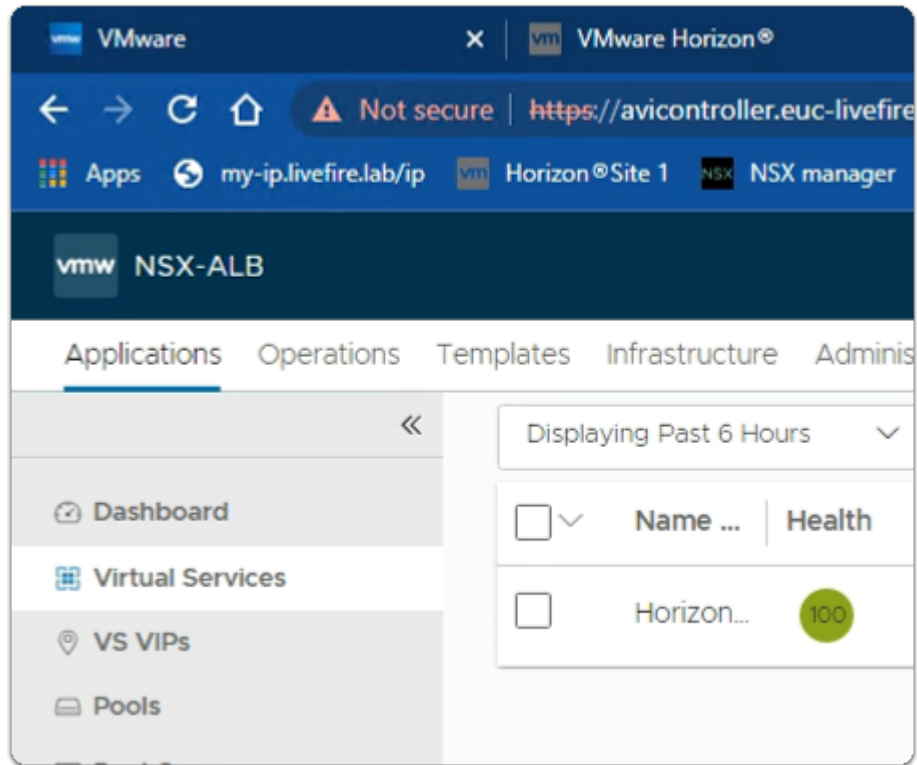
At the bottom of the wizard, there are 'Cancel', 'Previous', and 'Save' buttons. A red arrow points to the 'Save' button.

13. In the **New Virtual Service** wizard

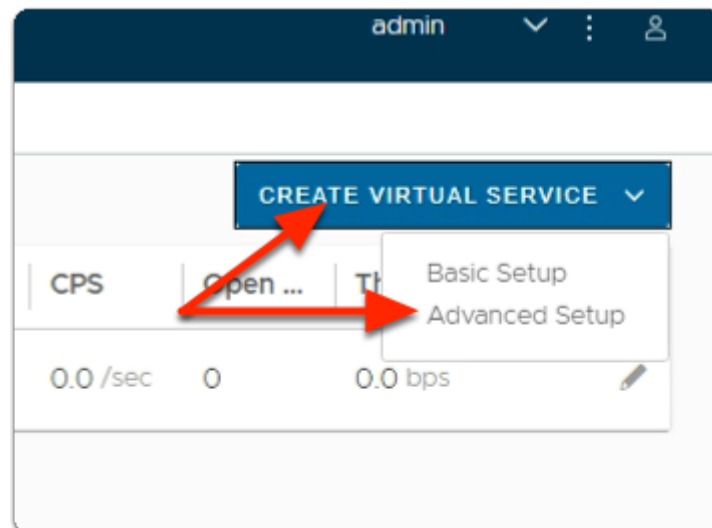
- **Step 4: Advanced** area
 - (Leave everything as default)
- Select **Save**

Creating L4 Virtual Service for Site-1

Part 8: Creating the Layer 4 Virtual Service for Site-1



1. From the NSX-ALB admin console
 - Navigate to **Applications** > **Virtual Services**



2. In the **Virtual Services** window
 - In the top right corner,
 - Select **CREATE VIRTUAL SERVICE**
 - Select **Advanced Setup**.

New Virtual Service: Horizon-UAG-L4-Site-1

Step 1: Settings | Step 2: Policies

Name* ? Enabled ? ☒

• VIP Address •

VS VIP* ? ▼

3. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - configure the following under:
 - **Name***
 - type **Horizon-UAG-L4-Site-1**
 - **VS VIP ***
 - select the **dropdown**,
 - select **VIP-Horizon-UAG-Site1**

• Profiles •

TCP/UDP Profile* ? ▼

Application Profile* ? ▼

4. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - ***Profiles*** sub area
 - Under **Application Profile***
 - from the **dropdown**
 - Select: **System-L4-Application**

• Service Port •

Services ⓘ

80

+ Add Port

Switch to Advanced

5. In the **New Virtual Service** wizard
 - **Step 1: Settings** area
 - ***Service Port*** sub area
 - Select **Switch to Advanced**.

New Virtual Service: Horizon-UAG-L4-Site-1

Step 1: Settings Step 2: Policies

VIP-Horizon-UAG-Site1

• Service Port •

Services ⓘ

443 TO 443

☐ Use as Horizon Primary/Tunnel Protocol Ports ⓘ

Override Application Profile ⓘ

Override TCP/UDP ☒

+ Add Port

6. In the **New Virtual Service** wizard
 - **Step 1: Settings** area
 - ***Service Port*** sub area
 - Under **Services**
 - Replace port **80** with port **443**
 - **Port Min** and **Port Max** areas to **443**
 - Select the **Checkbox** next to **Override TCP/UDP**

New Virtual Service: Horizon-UAG-L4

Step 1: Settings Step 2: Policies

• Service Port •

Services ?

443 TO 443

☐ Use as Horizon Primary/Tunnel Protocol Ports ?

Override Application Profile ?

Select Application Profile

☒ Override TCP/UDP

System-UDP-Fast-Path-VDI

+ Add Port

7. In the **New Virtual Service** wizard

- **Step 1: Settings** area
 - Below the checkbox enabled **Override TCP/UDP**
 - Select the **dropdown**
 - Select **System-UDP-Fast-Path-VDI**
 - Select **+ Add Port**

The screenshot displays the 'Service Port' configuration window in VMware NSX AVI. It contains three service port entries, each with the following fields:

- Port Min:** 443 (for the first entry) and 8443 (for the second and third entries).
- Port Max:** 443 (for the first entry) and 8443 (for the second and third entries).
- Use as Horizon Primary/Tunnel Protocol Ports:** Unchecked for all entries.
- Override Application Profile:** A dropdown menu with 'Select Application Profile' as the current selection.
- Override TCP/UDP:** Checked (green checkmark) for the first and third entries, and unchecked for the second entry.
- System-UDP-Fast-Path-VDI:** A dropdown menu with 'System-UDP-Fast-Path-VDI' as the current selection.

A '+ Add Port' button is located at the bottom left of the configuration area.

8. In the **New Virtual Service** wizard

- **Step 1: Settings:** continued
 - Type **8443** in Port Min and **8443** to Port Max
 - **Note:** You will notice Port Max will change automatically to 8443.
- **Uncheck** **Override TCP/UDP** box if selected
- Select **+ Add Port** again.
- Type **8443** in Port Min and **8443** to Port Max
- **Check** the box **Override TCP/UDP**
- Under **Select Dropdown**
 - Select **System-UDP-Fast-Path-VDI**
 - **Note:** Ensure all the **Service Port** details matches as per the screenshot above.
- Select **+ Add Port** again

System-UDP-Fast-Path-VDI

4172 TO 4172

☐ Use as Horizon Primary/Tunnel Protocol Ports ?

Override Application Profile ?

Select Application Profile

☐ Override TCP/UDP

4172 TO 4172

☐ Use as Horizon Primary/Tunnel Protocol Ports ?

Override Application Profile ?

Select Application Profile

☒ Override TCP/UDP

System-UDP-Fast-Path-VDI

+ Add Port

9. In the **New Virtual Service** wizard

- **Step 1: Settings:** continued
 - Type **4172** in Port Min and **4172** to Port Max
 - **Uncheck** **Override TCP/UDP** box if selected.
 - Select **+ Add Port** again
 - Type **4172** in Port Min and **4172** to Port Max
 - **Check** the box **Override TCP/UDP**
 - Under **Select Dropdown**
 - Select **System-UDP-Fast-Path-VDI**
 - **Note:** Ensure all the **Service Port** details matches as per the screenshot above.

• Pool •

☒ Pool ☐ Pool Group

Pool ?

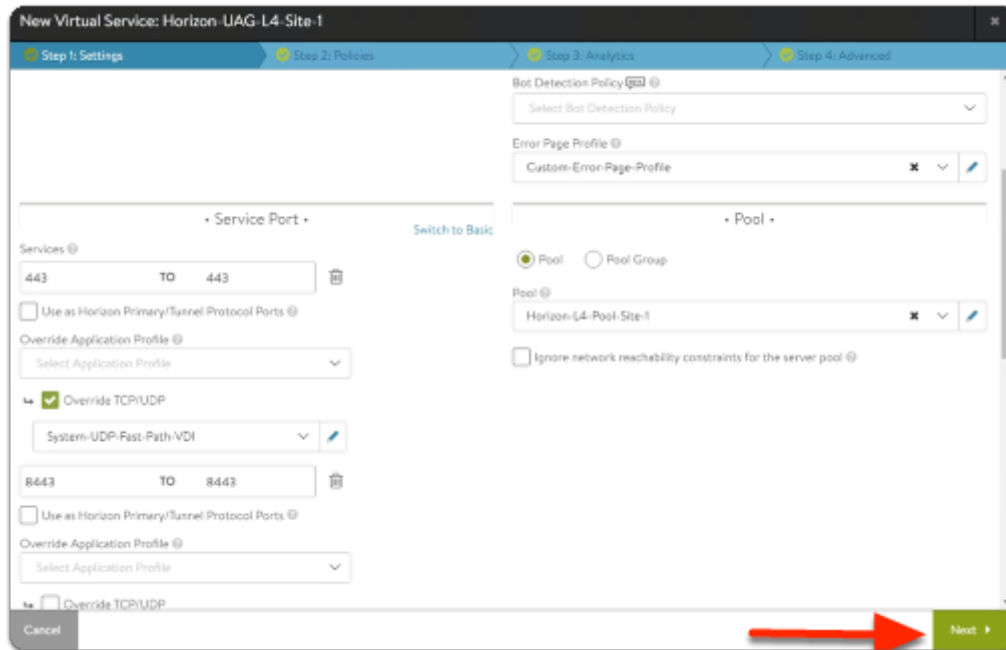
Horizon-L4-Pool-Site-1

☐ Ignore network reachability constraints for the server pool ?

10. In the **New Virtual Service** wizard

- **Step 1: Settings** area

- To the right of ***Service Port***
 - You will see the ***Pool*** area
 - Under **Pool**
 - From the **dropdown**
 - Select **Horizon-L4-Pool-Site-1**
- Select **Next**

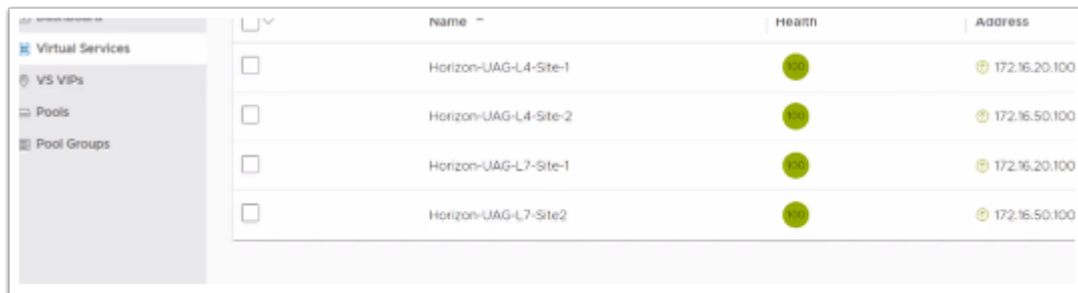


11. In the **New Virtual Service** wizard
- **Step 2: Policies** area
 - Leave everything as default
 - Select **Next**

12. In the **New Virtual Service** wizard
- **Step 3: Analytics** area
 - Leave everything as default
 - Select **Next**

13. In the **New Virtual Service** wizard
- **Step 4: Advanced** area
 - Leave everything as default

- Select **Save**



	Name	Health	Address
<input type="checkbox"/>	Horizon-UAG-L4-Site-1	●	● 172.16.20.100
<input type="checkbox"/>	Horizon-UAG-L4-Site-2	●	● 172.16.50.100
<input type="checkbox"/>	Horizon-UAG-L7-Site-1	●	● 172.16.20.100
<input type="checkbox"/>	Horizon-UAG-L7-Site2	●	● 172.16.50.100

14. In the **NSX-ALB admin** console

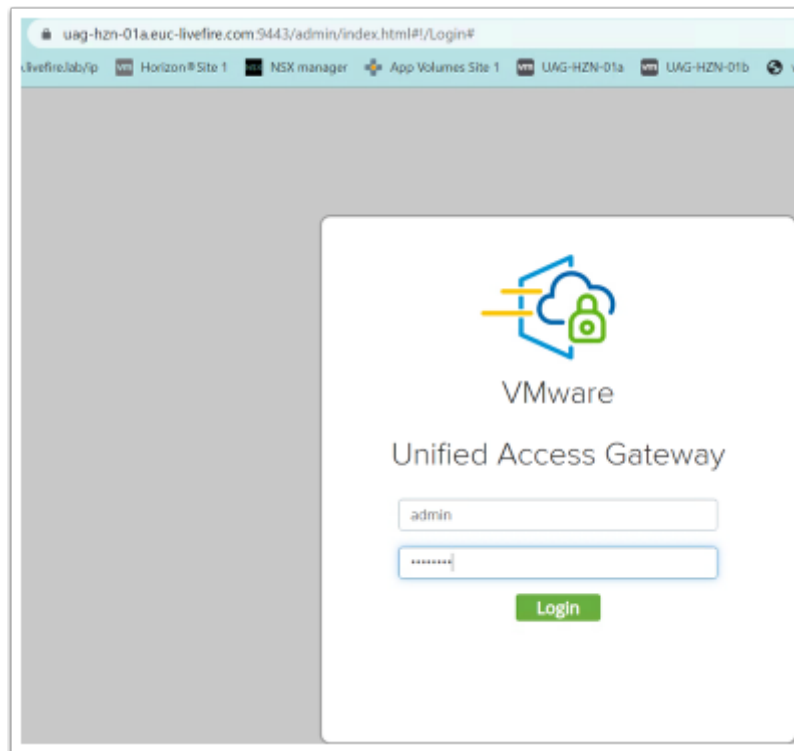
- Select **Applications**
 - Select **Virtual Services**
- In the right pane your configurations should look like the image above.

i Testing LTM Configuration for both Site1 and Site2

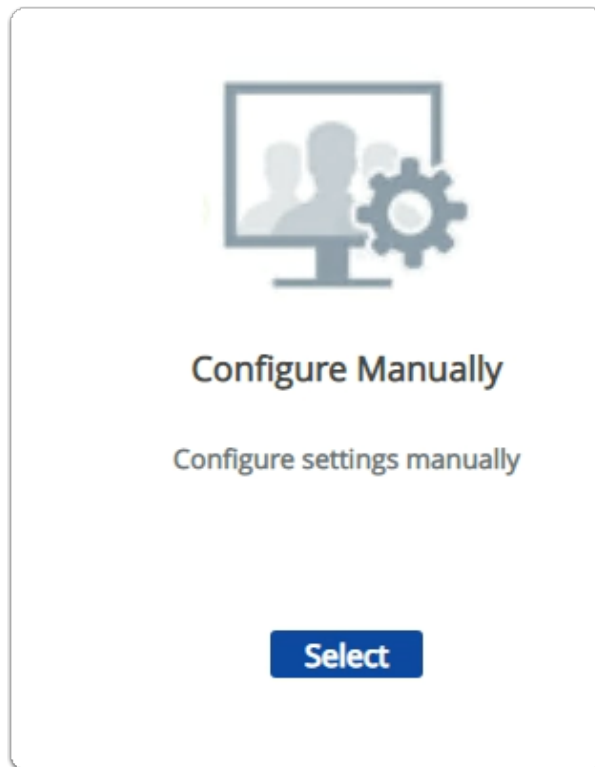
Part 9: Configuring the Unified Access Gateway for Site 1

Section 1. Configuring UAG-HZN-01a for AVI Integration

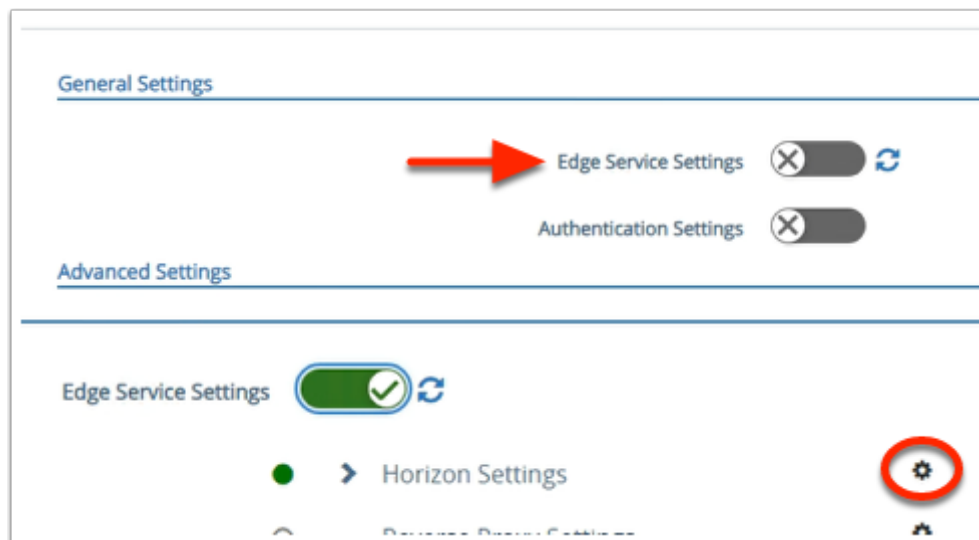
Section 1. Configuring UAG-HZN-01a for AVI Integration



1. On your **ControlCenter** Server
 - Open your **Chrome Browser for Site-1**
 - In the **Address bar**, browse to <https://uag-hzn-01a.euc-livefire.com:9443/admin/index.html>
 - Login username: **admin**
 - Login password: **VMware1!**



2. In the **UAG Admin Console**
 - Under **Configure Manually**
 - Click **Select**



3. In the UAG Admin Console
 - **Scroll** back-up to **General Settings**
 - Next to **Edge Service Settings**,
 - Move the **TOGGLE** to the right
 - Next to **Horizon Settings**
 - Select the **GEAR icon**

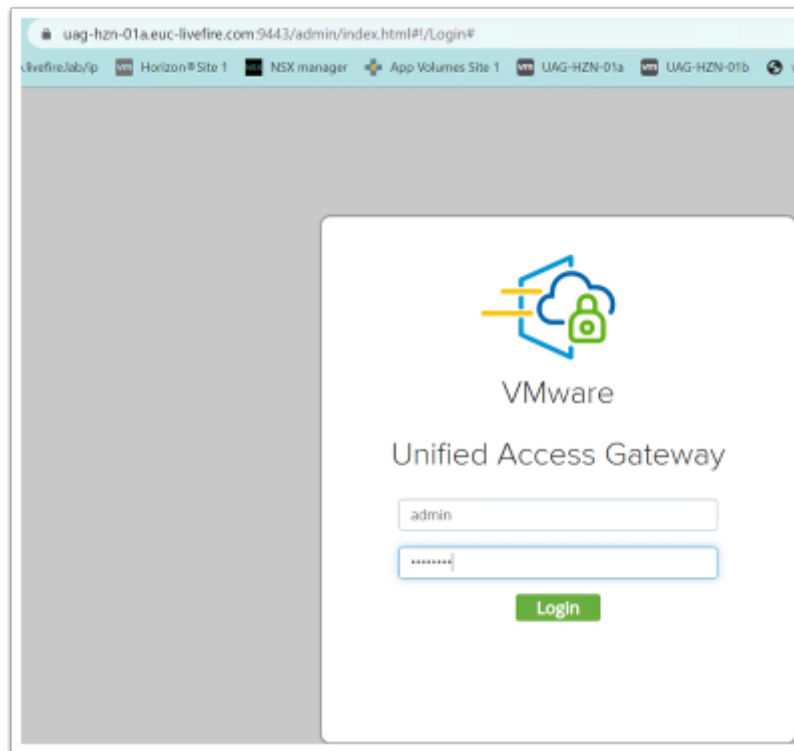


4. Next to **Host Port Redirect Mappings**,
 - In the **Source Host Port** area
 - enter **uag-hzn-avi01.euc-liveware.com**
 - In the **Redirect Host Port** area
 - enter **uag-hzn-01a.euc-liveware.com**
 - Once the **Host Redirect Mappings** are filled,
 - click on **+** symbol to add the entries.
 - **Note:** It should match the screenshot above
 - To Close the **Horizon settings** page
 - Select **Save**



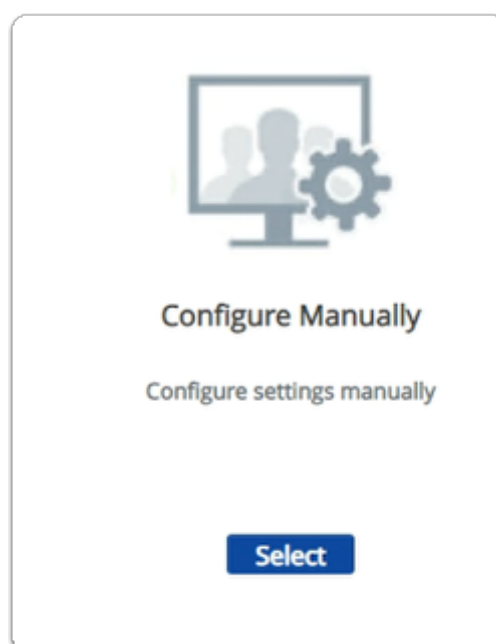
Section 2: Configuring **UAG-HZN-01B** in Site1 for AVI Integration

Section 2. Configuring UAG-HZN-01B for AVI Integration

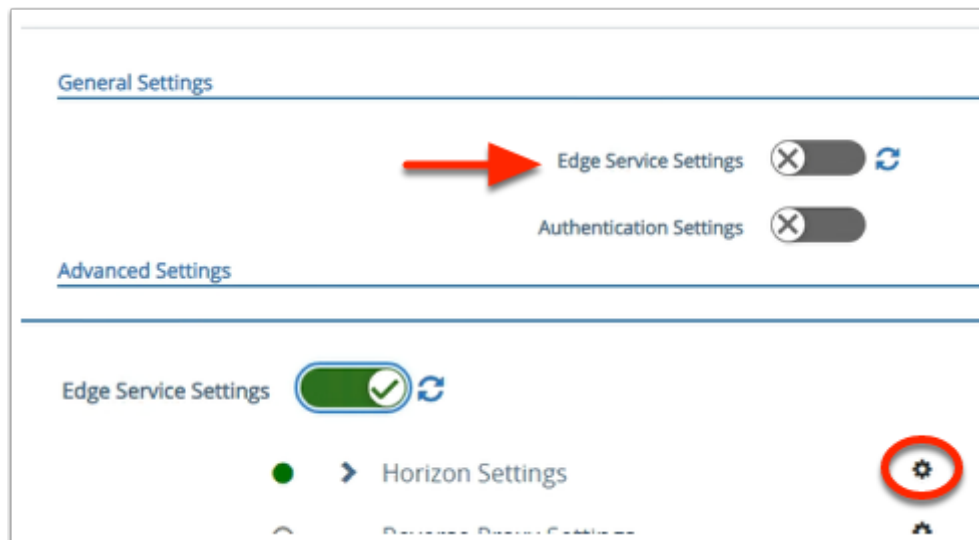


1. On your **ControlCenter** Server

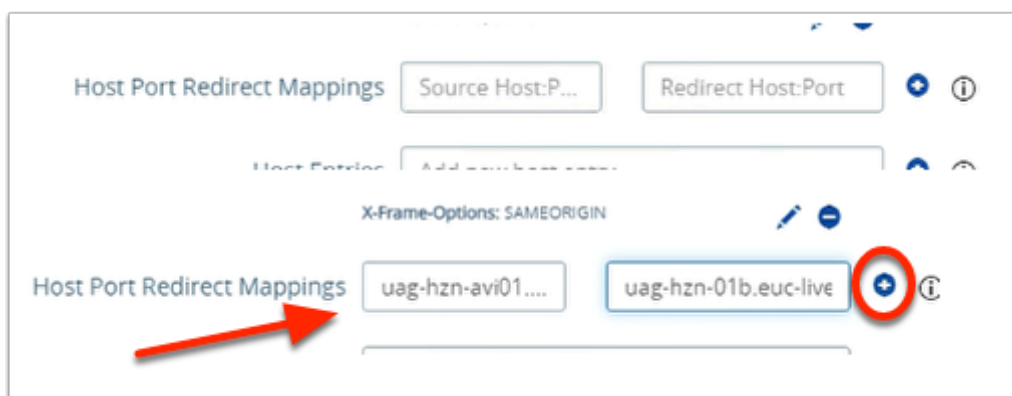
- Open your **Chrome Browser for Site-1**
- In the **Address bar**, browse to <https://uag-hzn-01b.euc-livewire.com:9443/admin/index.html>
- Login username: **admin**
- Login password: **VMware1!**



2. In the **UAG Admin Console**
 - Under **Configure Manually**
 - Click **Select**



3. In the UAG Admin Console
 - In the **General Settings** area
 - Next to **Edge Service Settings**,
 - Move the **TOGGLE** to the right
 - Next to **Horizon Settings**
 - Select the **GEAR** icon

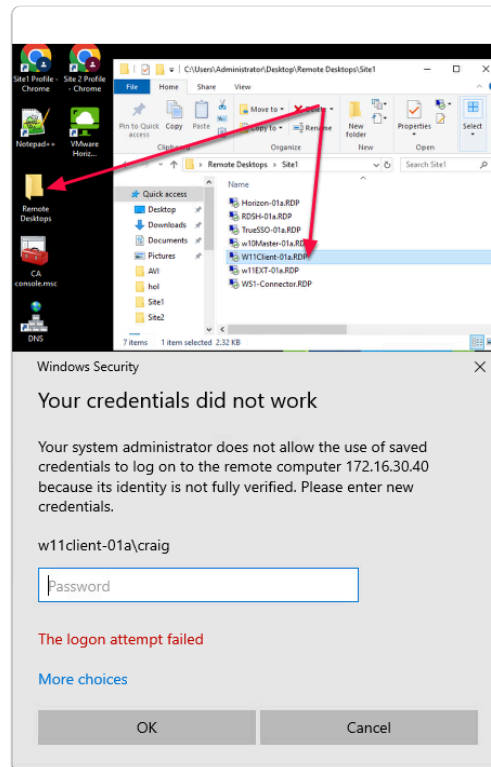


4. Next to **Host Redirect Mappings**,
 - In the **Source Host Port** area
 - enter **uag-hzn-avi01.euc-livefire.com**
 - In the **Redirect Host Port** area
 - enter **uag-hzn-01b.euc-livefire.com**
 - Once the **Host Redirect Mappings** are filled,
 - click on **(+)** symbol to add the entries.
 - **Note:** It should match the screenshot above

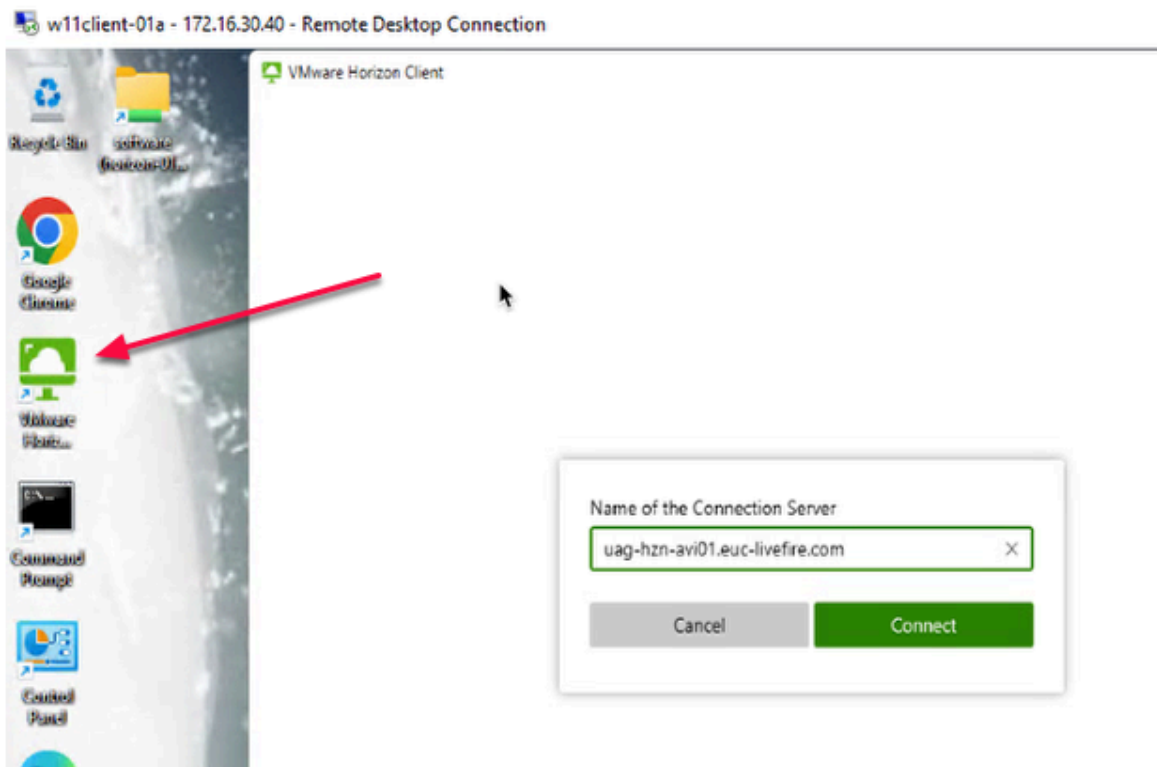
- To Close the **Horizon settings** page
 - Select **Save**

Part 10: Testing LTM Configuration

Part 9 Section 1: Testing Site1 LTM

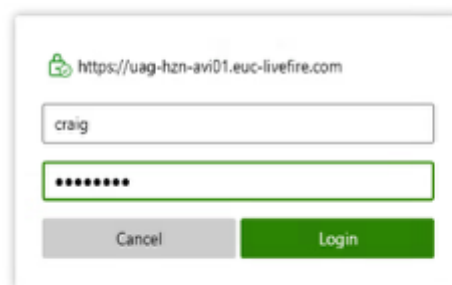


1. On your **ControlCenter** server
 - On the Desktop
 - Open the **Remote Desktops** Folder
 - Open **Site1**
 - Launch **W11Client-01a.rdp**
 - Login as **craig**
 - With the password **VMware1!**



2. In **W11Client-01a**

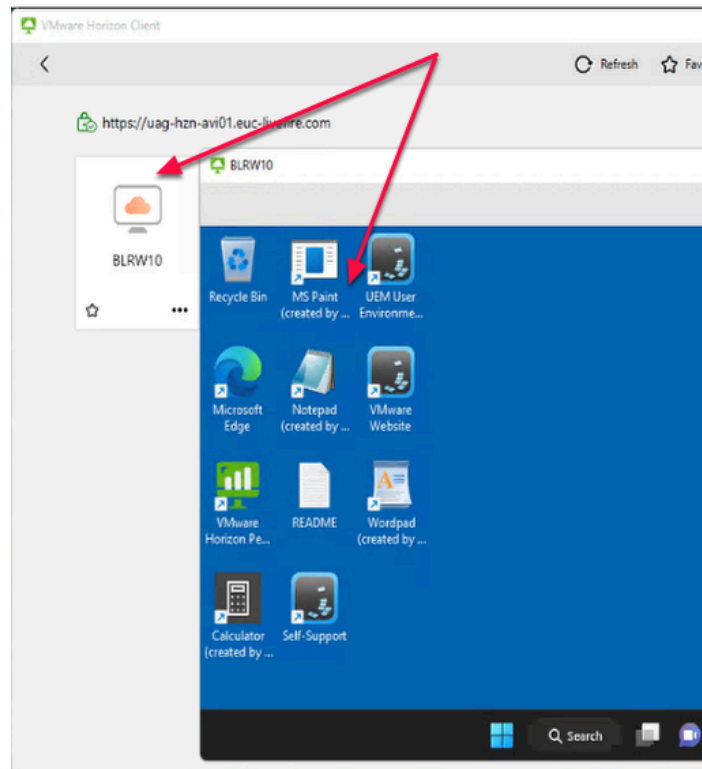
- Open **Horizon Client** from desktop
 - In the Horizon Client,
- Click on **Add Server** Button
 - In the **Name of the Connection Sever** textbox,
 - Type
 - **uag-hzn-avi01.euc-liveware.com**
 - Click **Connect**



3. In the Horizon Client textbox

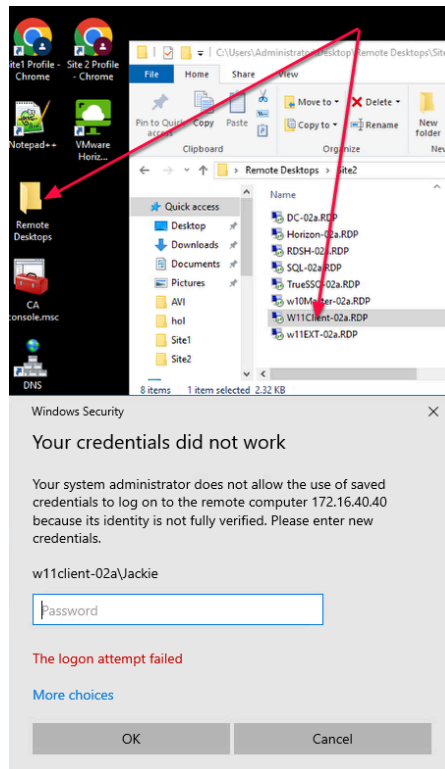
- **Username**
 - **craig**

- Password
 - **VMware1!**
- Click **login**

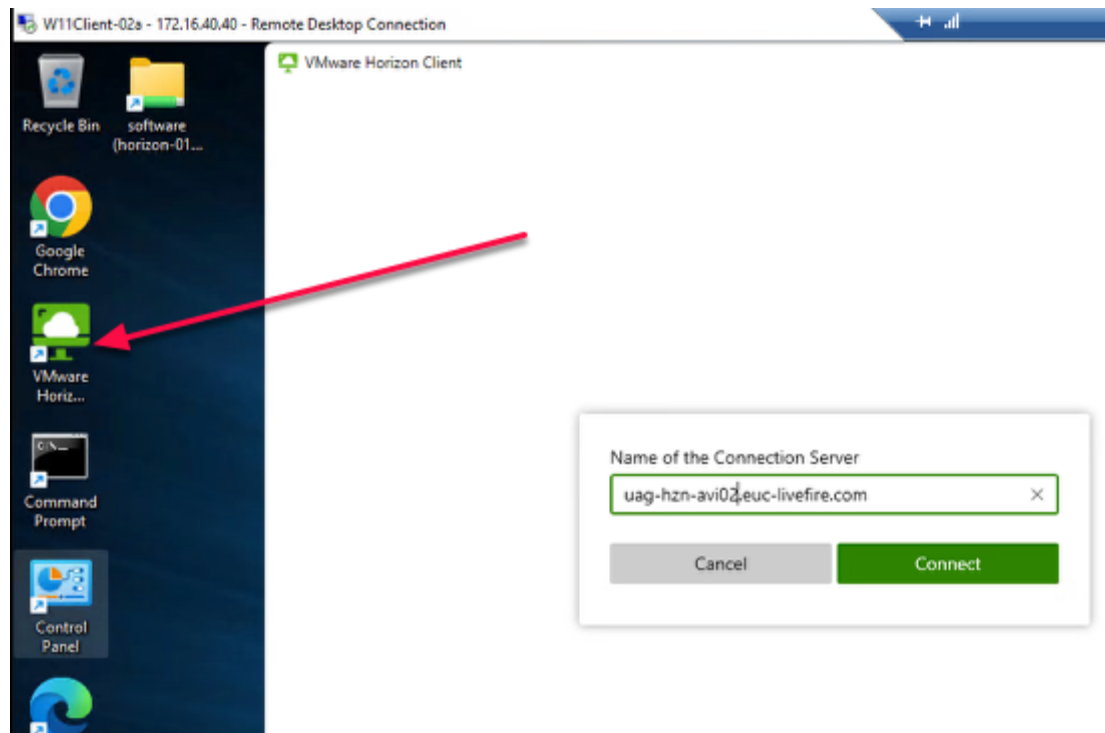


4. In the Horizon Client
 - Double Click **BLRW10** Pool
 - You will be presented with the desktop
 - This validates our testing and configuration

Part 9 Section 2: Testing Site2 LTM

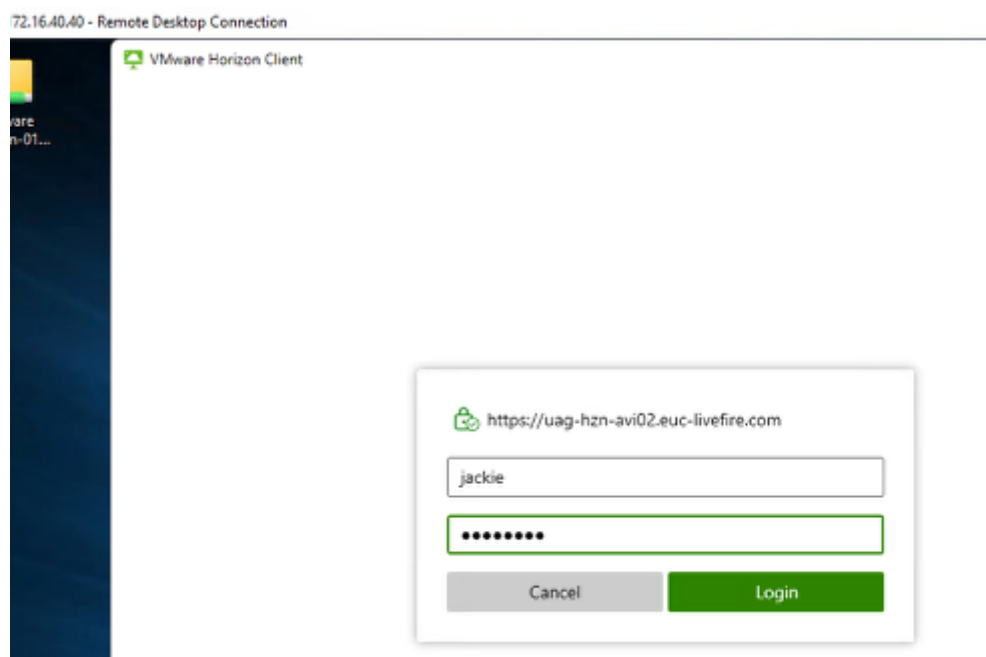


1. On your **ControlCenter** server
 - On the Desktop
 - Open the **Remote Desktops** Folder
 - Open **Site 2**
 - Launch **W11Client-02a.RDP**
 - Login as **jackie**
 - With the password **VMware1!**



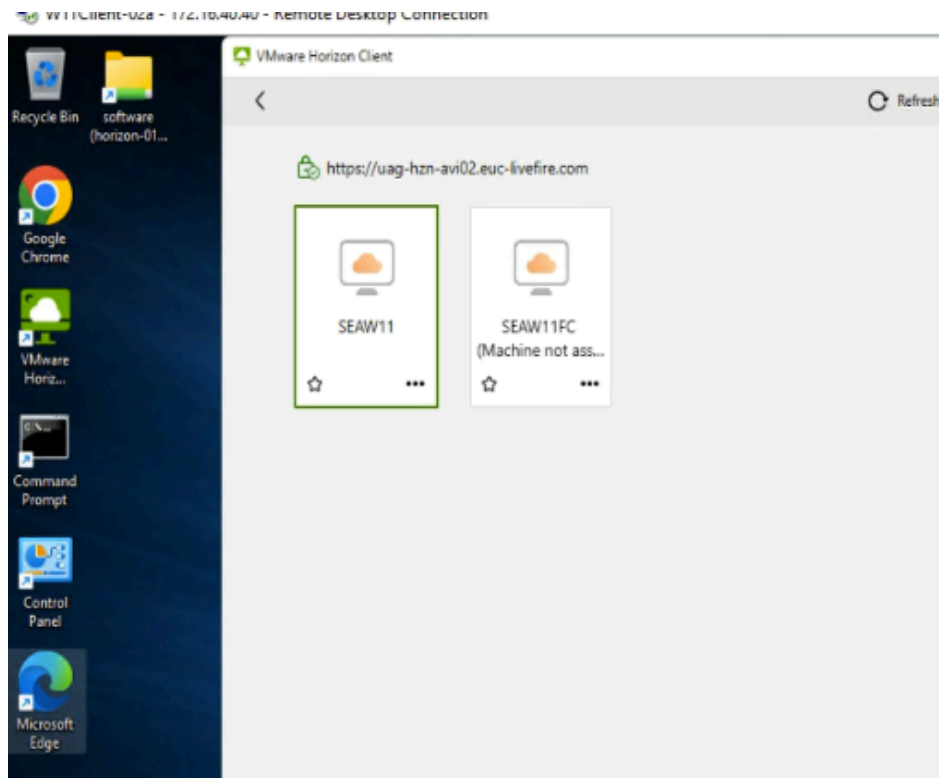
2. In **W11Client-02a**

- Open **Horizon Client** from desktop
 - In the Horizon Client,
 - Click on **Add Server** Button
 - In the **Name of the Connection Sever** textbox,
 - Type
 - uag-hzn-avi02.euc-liveware.com
 - Click **Connect**



3. In the Horizon Client textbox

- **Username**
 - **jackie**
- **Password**
 - **VMware1!**
- Click **login**



4. In the Horizon Client

- Double Click **SEAW11** Pool
 - You will be presented with the desktop
 - This validates our testing and configuration

i Once the testing complete, this brings to the end of LTM configuration. Move to the next lab of GSLB configuration lab