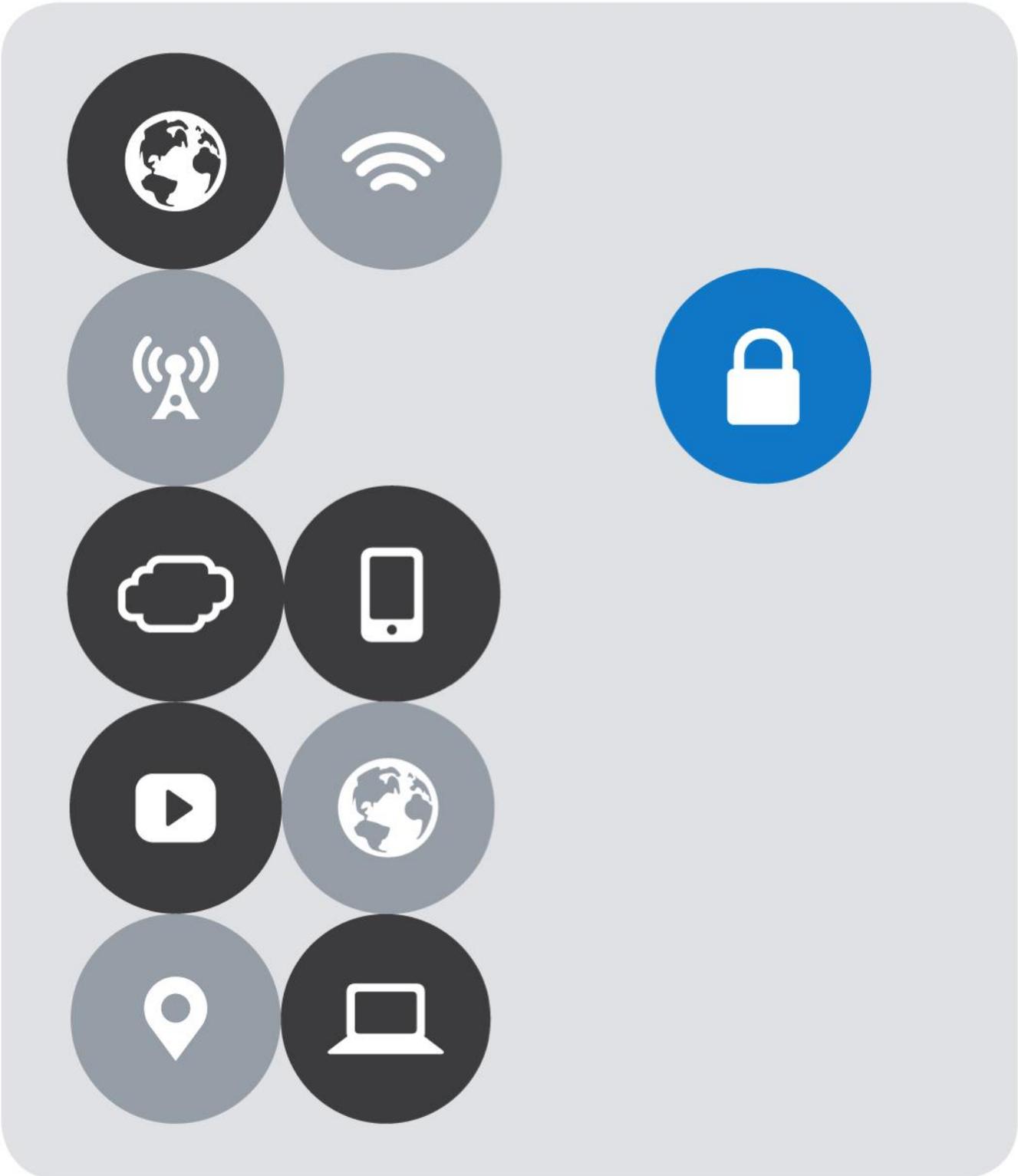




INTEGRATION GUIDE

vmware®

# Load Balancing VMware App Volumes





# Version History

Date	Version	Author	Description	Compatible Versions
Dec 2020	3.0	Matt Mabis	Documentation Update and Persistence Method Changed	VMware App Volumes 2.x, 3.x, 4.x
May 2018	2.1	Matt Mabis	Documentation Update and Monitor Changed.	VMware App Volumes 2.x (1)
Oct 2017	2.0	Matt Mabis	Updated/Revised Documentation	VMware App Volumes 2.x (1)
Feb 2015	1.0	Justin Venezia	Initial Document with How-To Configure F5 LTM with VMware App Volumes	VMware App Volumes 2.x

NOTES:

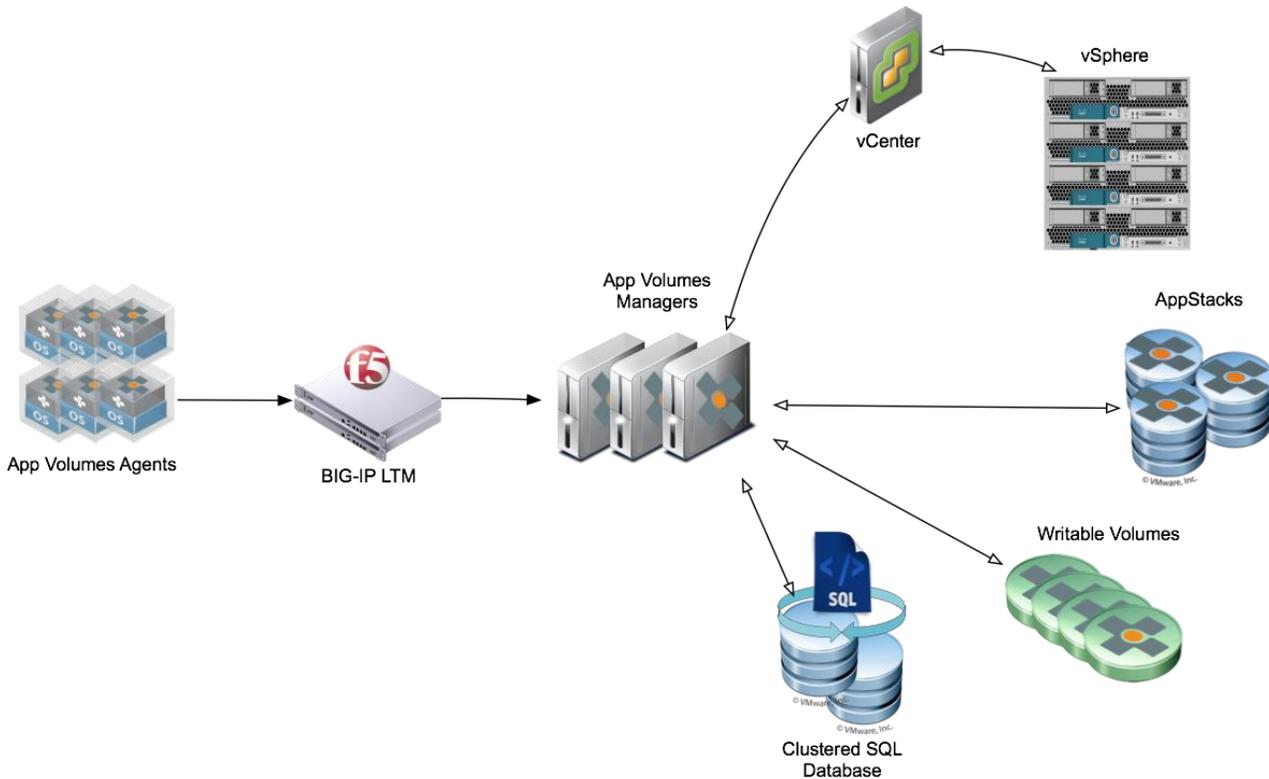
- (1) This Document by default utilized a source address affinity persistence which was recommended until App Volumes 2.14.



# Contents

Version History .....	2
Overview .....	4
Prerequisites .....	5
Create a Client SSL Profile.....	6
SSL Client Profile Configuration .....	7
Create a Server SSL Profile.....	8
SSL Server Profile Configuration .....	9
Create HTTP Profile.....	10
HTTP Profile Configuration .....	11
Create Persistence Profile .....	12
Persistence Profile Configuration (Cookie).....	13
Alternative - Persistence Profile Configuration (Source_Addr) .....	14
Create Monitor .....	15
Monitor Configuration.....	16
Create Pool .....	17
Pool Configuration .....	18
Create a Port 443 Virtual Server.....	19
Create a Port 80 Redirect Virtual Server (Optional) .....	23
Testing and Validation .....	27
References .....	27

# Overview



VMware App Volumes is a system that delivers applications to desktops and remote hosted applications via virtual disks. Applications are containerized and bundled in “AppStacks” then delivered by attaching a portable standard disk system (Such as VMDK or VHD) file to a virtual machine. App Volumes Manager provides the IT administrator a way for centrally managing and deploying applications without having to modify the specific desktops or individual applications. Applications delivered using App Volumes will provide a native feeling and upgrades/updates can be done with AppStacks in Real-time providing a seamless operation without disrupting users.

All Applications are delivered/provisioned during login time and from the user's perspective have a persistent desktop experience. Users can also be provided a Writable Volume to allow for extended persistence options where users can install their own applications and have them persisted across sessions. In upcoming editions App Volumes will have Computer and User based AppStack assignments which allows for further flexibility.

This document provides step-by-step instructions for setting up the App Volumes Manager(s) within an LTM configuration. It is highly recommended to follow VMware Best Practices for deploying out Multiple App Volumes Managers for Scalability and Redundancy.

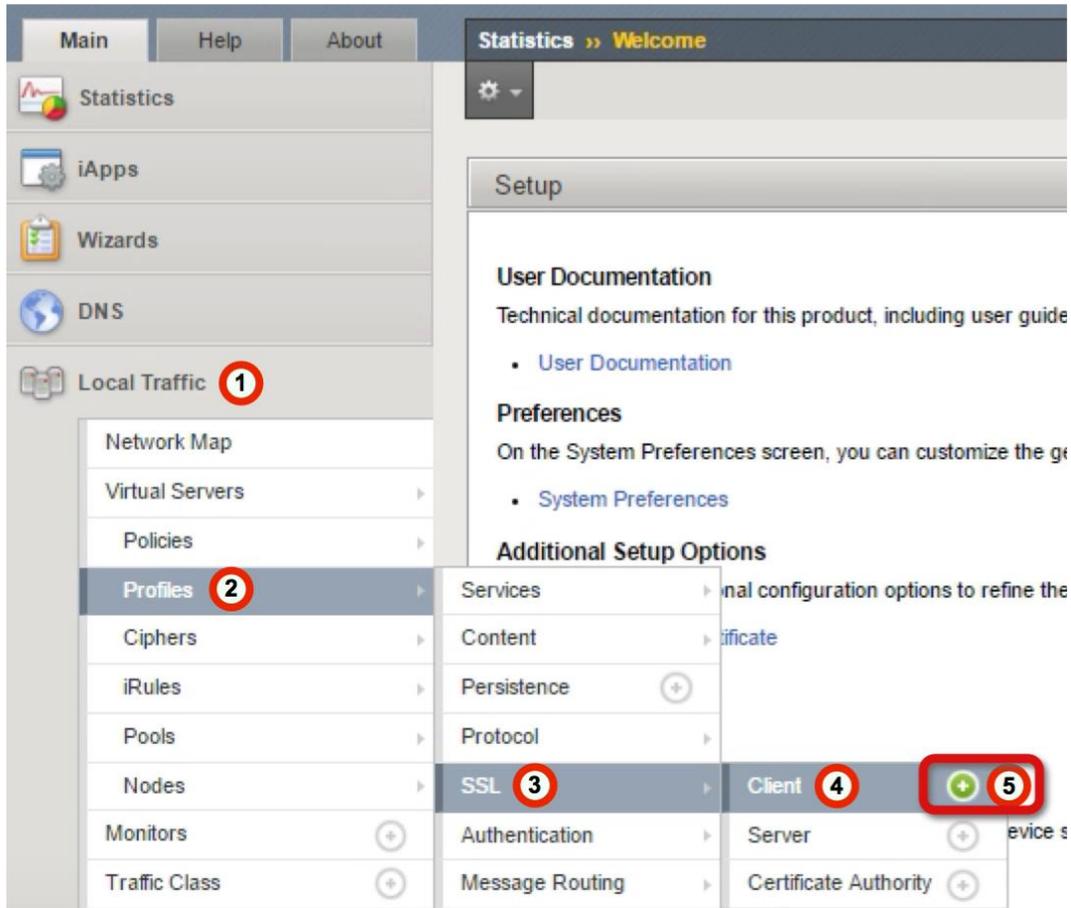
# Prerequisites

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](http://support.f5.com) for specific instructions.

1. Create/import an SSL Certificate that contains the load balanced FQDN that will be used for VMware App Volumes
2. Upload the following to the BIG-IP system:
  - The SSL Certificate must be uploaded to the BIG-IP.
  - 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 App Volumes Manager Servers 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 App Volumes Servers.
4. You must have deployed at least a single instance of App Volumes Manager.

# Create a Client SSL Profile

From the BIG-IP Configuration utility, use the following guidance to create a Client SSL profile.



1. Click **Local Traffic**.
2. Hover over **Profiles** to open the Profiles menu.
3. Hover over **SSL**.
4. Hover over **Client**.
5. Click the Add button (+) to the right of Client to create a new SSL Client Profile.

## SSL Client Profile Configuration

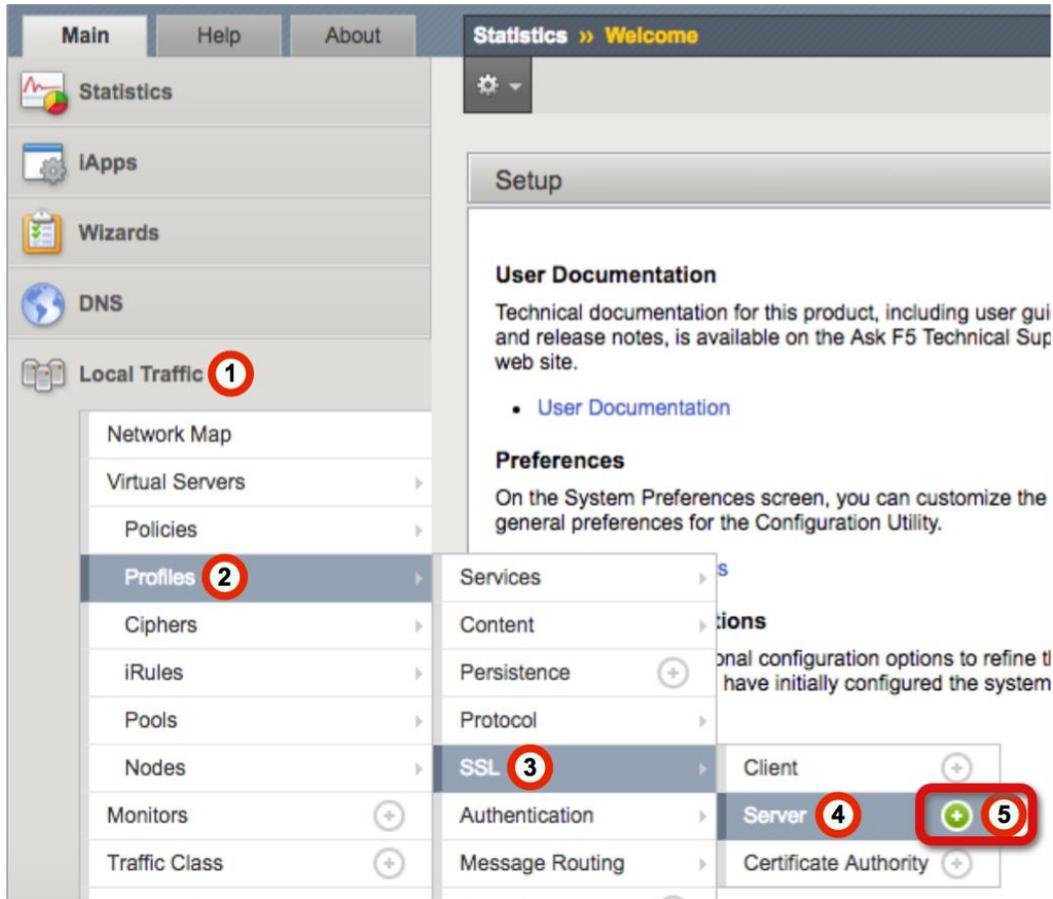
Use the following guidance to create a new SSL Client profile.

1. In the **Name** field, type a unique name, such as **AppVolumes-ClientSSL**.
2. From the **Parent Profile** list, ensure **clientssl** is selected.
3. In the Certificate Key Chain area, click the **Custom** check box.
4. Click the **Add** button. The Add SSL Certificate to Key Chain dialog box opens.

5. From the **Certificate** list, select the certificate with the FQDN that you uploaded to the BIG-IP as specified in the prerequisites.
6. From the **Key** list, select the certificate key that corresponds with the certificate you selected.
7. From the **Chain** list, select the primary or root CA/certificate chain that corresponds with the certificate you uploaded to the BIG-IP.
8. Click the **Add** button to add the certificate key chain to the SSL profile.
9. Click **Finished**.

# Create a Server SSL Profile

From the BIG-IP Configuration utility, use the following guidance to create a Server SSL profile.



1. Click **Local Traffic**.
2. Hover over **Profiles** to open the Profiles menu.
3. Hover over **SSL**.
4. Hover over **Server**.
5. Click the Add button (+) to the right of Client to create a new SSL Server Profile.

## SSL Server Profile Configuration

Use the following guidance to create a new SSL Server profile.

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

**General Properties**

Name	1	AppVolumes-ServerSSL
Parent Profile	2	serverssl

Configuration: Basic

Certificate	None
Key	None
SSL Forward Proxy	Disabled
SSL Forward Proxy Bypass	Disabled
Bypass on Handshake Alert	Disabled
Bypass on Client Cert Failure	Disabled
Proxy SSL	<input type="checkbox"/>
Proxy SSL Passthrough	<input type="checkbox"/>

**Server Authentication**

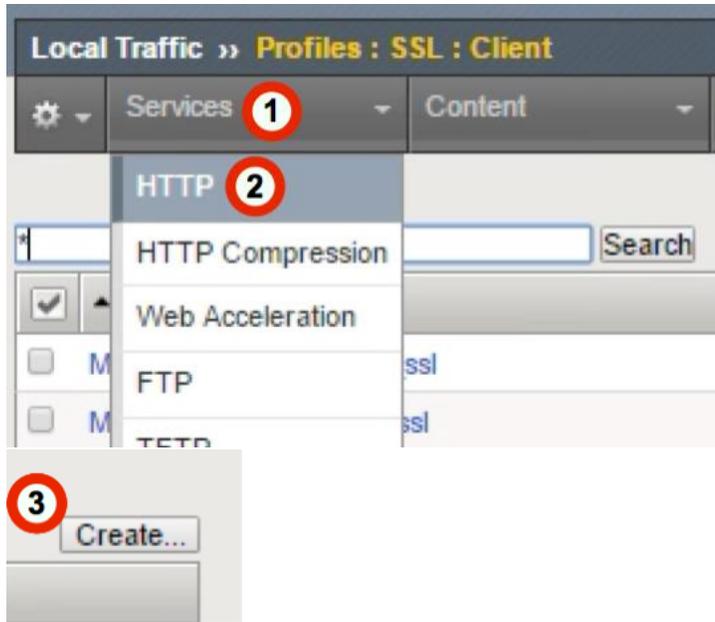
Server Certificate	ignore
Expire Certificate Response Control	drop
Untrusted Certificate Response Control	drop
Frequency	once
Retain Certificate	<input checked="" type="checkbox"/> Enabled
Certificate Chain Traversal Depth	9
Authenticate Name	
Trusted Certificate Authorities	None
Certificate Revocation List (CRL)	None
Allow Expired CRL	<input type="checkbox"/>

Cancel Repeat Finished 3

1. In the **Name** field, type a unique name, such as **AppVolumes-ServerSSL**.
2. From the **Parent Profile** list, ensure **serverssl** is selected.
3. Click **Finished**.

# Create HTTP Profile

The next task is to create an HTTP Profile, use the following guidance.



1. From the **Menu** bar, click **Services** (you may need to click **Local Traffic > Profiles** first).
2. Click **HTTP** from the list.
3. Click the **Create** button in the upper right-hand corner of the HTTP Profiles table.

# HTTP Profile Configuration

Create a new HTTP Profile with the following settings.

**Local Traffic » Profiles : Services : HTTP » New HTTP Profile...**

**General Properties**

Name	AppVolumes-HTTPF
Proxy Mode	Reverse
Parent Profile	http

**Settings** Custom

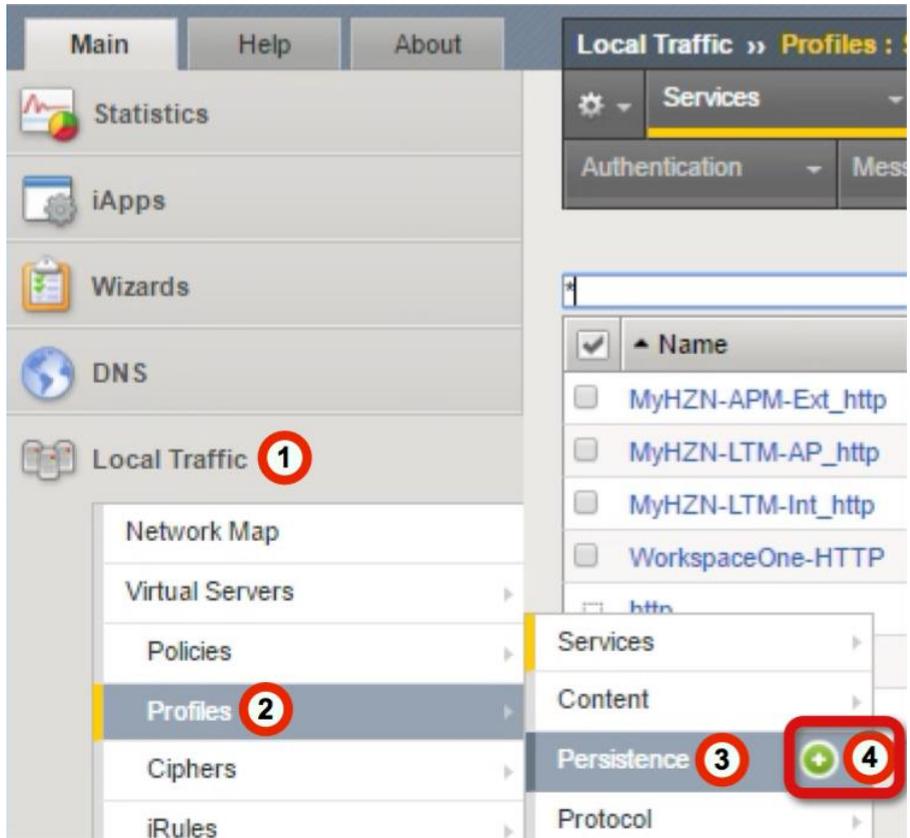
Basic Auth Realm		<input type="checkbox"/>
Fallback Host		<input type="checkbox"/>
Fallback on Error Codes		<input type="checkbox"/>
Request Header Erase		<input type="checkbox"/>
Request Header Insert		<input type="checkbox"/>
Response Headers Allowed		<input type="checkbox"/>
Request Chunking	Preserve	<input type="checkbox"/>
Response Chunking	Selective	<input type="checkbox"/>
OneConnect Transformations	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Redirect Rewrite	None	<input 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"/>

1. In the **Name** field, type a unique name, such as **AppVolumes-HTTPF**.
2. In the Insert X-Forwarded-For row, click the **Custom** checkbox.
3. From the **Insert X-Forward-For** list, select **Enabled**.
4. Click **Finished**.

**\*\* Important \*\*** You must enable X-Forwarded-For headers on your BIG-IP system.

# Create Persistence Profile

Use the following guidance to create a Persistence profile.



1. Click **Local Traffic**.
2. Hover over **Profiles**.
3. Hover over **Persistence**.
4. Click the Add button (+) to the right of Persistence to create a new Persistence Profile.

## Persistence Profile Configuration (Cookie)

After App Volumes version 2.14 Cookie is the recommended persistence method for connecting App Volumes Agents and Servers.

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

**General Properties**

Name	AppVolumes-Persi
Persistence Type	Cookie
Parent Profile	cookie

**Configuration** Custom

Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>
Cookie Name		<input type="checkbox"/>
HTTPOnly Attribute	Enabled	<input type="checkbox"/>
Secure Attribute	Enabled	<input type="checkbox"/>
Always Send Cookie	<input type="checkbox"/>	<input type="checkbox"/>
Default Cookie Encrypt Pool-Name	<input type="checkbox"/>	<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie	<input type="checkbox"/>
Cookie Encryption Use Policy	disabled	<input type="checkbox"/>
Encryption Passphrase		<input type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Repeat Finished

1. From the **Name** field, type a unique name such as **AppVolumes-Persistence**.
2. From the **Persistence Type** list, select **Cookie**.
3. Leave the rest of the **defaults** and Click **Finished**.

## Alternative - Persistence Profile Configuration (Source\_Addr)

Prior to App Volumes 2.14 Source Address Affinity is the preferred persistence method for connecting App Volumes Agents and Servers. This method can also be used in version 2.14+ instead of cookie persistence.

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

**General Properties**

Name	AppVolumes-Persi:	1
Persistence Type	Source Address Affinity	2
Parent Profile	source_addr	

**Configuration** Custom

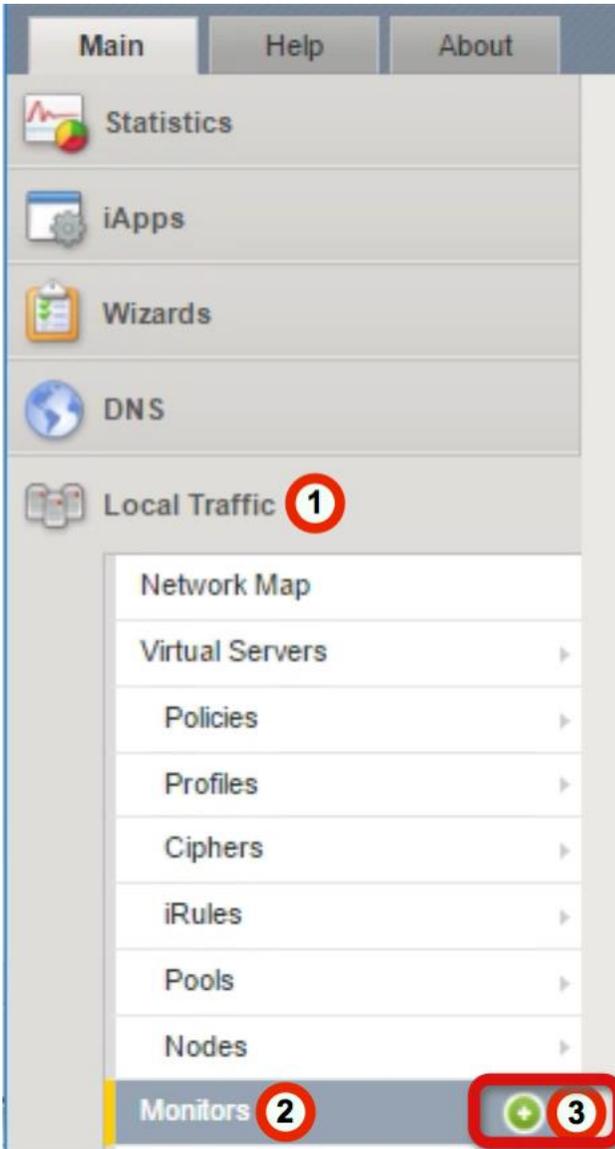
Mirror Persistence	<input checked="" type="checkbox"/>	3	<input checked="" type="checkbox"/>
Match Across Services	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	5	<input checked="" type="checkbox"/>
Match Across Pools	<input type="checkbox"/>		<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 7

1. From the **Name** field, type a unique name such as **AppVolumes-Persistence**.
2. From the **Persistence Type** list, select **Source Address Affinity**.
3. Check the **Custom** checkbox for **Mirror Persistence**
4. Check the **Custom** checkbox for **Match Across Services**
5. Check the **Custom** checkbox for **Match Across Virtual Servers**
6. Check the **Enable** checkbox for **Mirror Persistence**
7. Click **Finished**.

# Create Monitor

The next task is to create the Monitor for the BIG-IP Appliance to validate when the webserver is available. Use the following guidance to create a health monitor on the BIG-IP system.



1. Click **Local Traffic**.
2. Hover over **Monitors**.
3. Click the Add button (+) to the right of Monitors to create a new health monitor.

## Monitor Configuration

Create a Monitor with the following settings. In previous guides the monitor configuration used the /login page VMware recommends now using the /health\_check page to validate server availability.

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

**General Properties**

Name	1 AppVolumes-Monitor
Description	
Type	2 HTTPS
Parent Monitor	https

**Configuration:** Basic

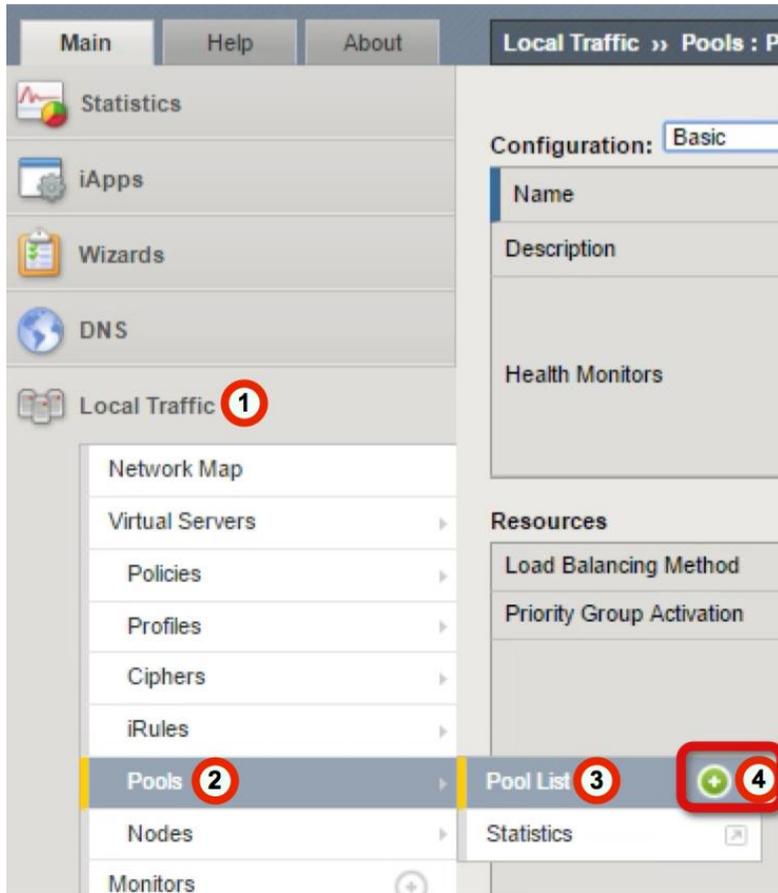
Interval	3 30 seconds
Timeout	4 15 seconds
Send String	5 GET /health_check HTTP/1.1\r\nHost: appvolumes.dsc-services.local\r\nConnection: Close\r\n\r\n
Receive String	6 200 OK
Receive Disable String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<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 7

1. In the **Name** field, type a unique name such as AppVolumes-Monitor.
2. From the **Type** list, select **HTTPS**.
3. Set the **Interval** to **30** Seconds
4. Set the **Timeout** to **15** Seconds
5. In the **Send String** field, type (Change the FQDN-For-App-Volumes to your FQDN)  
GET /health\_check HTTP/1.1\r\nHost: FQDN-FOR-AppVolumes\r\nConnection: Close\r\n\r\n
6. In the **Receive String** field, type  
200 OK
7. Click **Finished**.

# Create Pool

The next task is to create the App Volumes Managers load balancing pool for the BIG-IP Appliance to monitor.



1. Click **Local Traffic**.
2. Hover over **Pools**.
3. Hover over **Pool List**.
4. Click the Add button (+) to the right of Pool List to create a new Pool.

## Pool Configuration

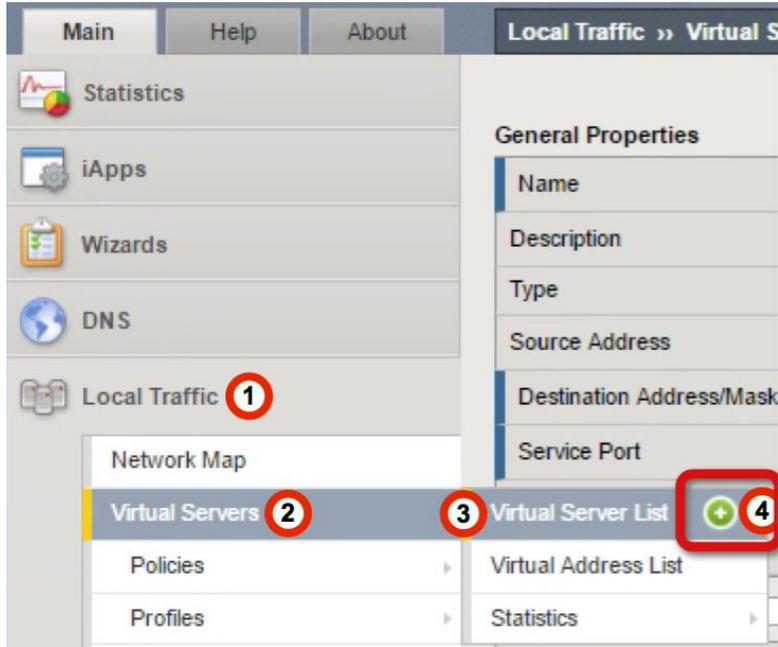
Create a Pool with the following settings.

The screenshot shows the 'New Pool...' configuration window. The 'Name' field is set to 'AppVolumes-Pool'. In the 'Health Monitors' section, 'AppVolumes-Monitor' is moved from the 'Available' list to the 'Active' list. The 'Load Balancing Method' is set to 'Least Connections (member)'. In the 'New Members' section, the 'New Node' radio button is selected. The 'Node Name' is 'AV-MGR-03.bd.f5.com', the 'Address' is '10.105.169.202', and the 'Service Port' is '443' with 'HTTPS' selected. The 'Finished' button is highlighted with a red circle and the number 5.

1. In the **Name** field, type a unique name such as **AppVolumes-Pool**.
2. In the **Health Monitors** area, use the Add (<<) button to move the monitor you created (AppVolumes-Monitor in our example) to the **Active** list.
3. From the **Load Balancing Method** list, select **Least Connections (node)**.
4. In the **New Members** area, complete the following for each App Volumes Manager node
  - In the **Node Name** field, type a unique name such as **AV-MGR-01.bd.f5.com**.
  - In the **Address** field, type IP address of the First AppVolumes Manager Node (Node 1).
  - In the **Service Port** field, type **443** or select **HTTPS** from the list.
  - Click the **Add** button.
  - **Repeat this step for each additional App Volumes Manager nodes**
5. Click the **Finished** button.

# Create a Port 443 Virtual Server

The next task is to create a Virtual Server.



1. Click **Local Traffic**.
2. Hover over **Virtual Servers**.
3. Hover over **Virtual Server List**.
4. Click the Add button (+) to the right of Virtual Server List to create a new Virtual Server.

### Virtual Server General Properties Section

Use the following guidance to configure the General Properties of the virtual server.

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

General Properties	
Name	1 AppVolumes-VS
Description	
Type	Standard
Source Address	
Destination Address/Mask	2 10.105.169.100
Service Port	3 443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

1. In the **Name** field, type a unique name such as **AppVolumes-VS**.
2. In the **Destination Address/Mask** field, type the IP Address you want to use for the virtual server.
3. In the **Service Port** field, type 443 or select **HTTPS** from the list.

### Virtual Server Configuration Section

Use the following guidance to configure the Configuration section of the virtual server.

Configuration: Basic					
Protocol	TCP				
Protocol Profile (Client) <b>1</b>	tcp-wan-optimized				
Protocol Profile (Server) <b>2</b>	tcp-lan-optimized				
HTTP Profile <b>3</b>	AppVolumes-HTTP				
HTTP Proxy Connect Profile	None				
Traffic Acceleration Profile	None				
FTP Profile	None				
RTSP Profile	None				
SSL Profile (Client) <b>4</b>	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>/Common AppVolumes-ClientSSL</td> <td>/Common AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL clientssl clientssl insecure compatible</td> </tr> </tbody> </table>	Selected	Available	/Common AppVolumes-ClientSSL	/Common AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL clientssl clientssl insecure compatible
Selected	Available				
/Common AppVolumes-ClientSSL	/Common AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL clientssl clientssl insecure compatible				
SSL Profile (Server) <b>5</b>	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>/Common AppVolumes-ServerSSL</td> <td>/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl splitsession-default-serverssl</td> </tr> </tbody> </table>	Selected	Available	/Common AppVolumes-ServerSSL	/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl splitsession-default-serverssl
Selected	Available				
/Common AppVolumes-ServerSSL	/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl splitsession-default-serverssl				
SMTSP Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map <b>6</b>				

1. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
2. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
3. From the **HTTP Profile** list, select the HTTP profile you created (**AppVolumes-HTTP** in our example).
4. From the **SSL Profile (Client)** list, select the Client SSL profile you created (**AppVolumes-ClientSSL** in our example).
5. From the **SSL Profile (Server)** list, select the Server SSL profile you created (**AppVolumes-ServerSSL** in our example).
6. From the **Source Address Translation** list, select **Auto Map**.

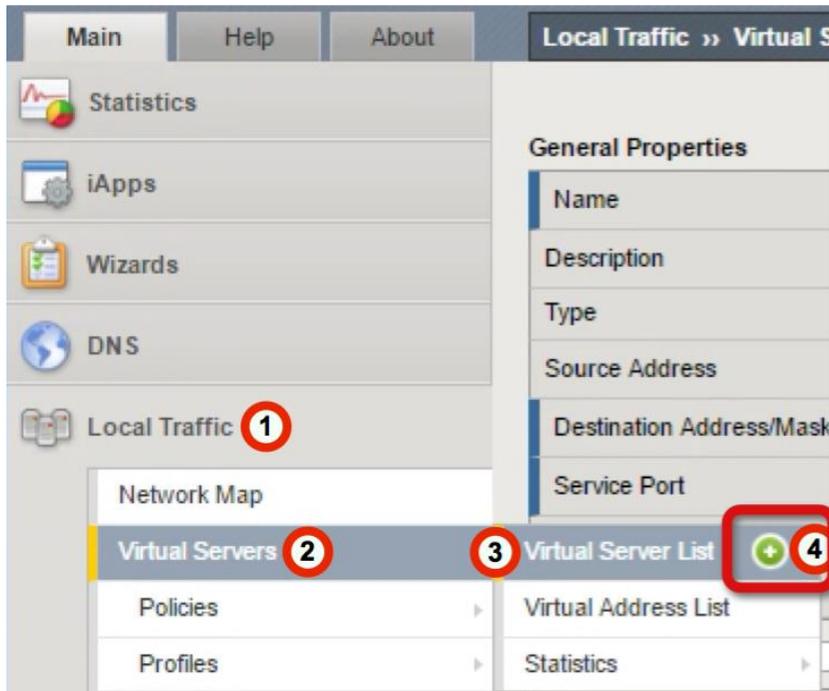
### Virtual Server Resources Section

Use the following guidance to configure the Resource properties of the virtual server.

1. From the **Default Pool** list, select the pool you created (**AppVolumes-Pool** in our example).
2. From the **Default Persistence Profile** list, select the persistence profile you created (**AppVolumes-Persistence** in our example).
3. After you have completed all three sections, click the **Finished** button.

# Create a Port 80 Redirect Virtual Server (Optional)

After you configure the Port 443 virtual server, you can create another virtual server that redirects any port 80 traffic to the newly created Port 443 virtual server. App Volumes Manager can run on Port 80 as well as 443 but any production deployment should only use a secured port.



1. Click **Local Traffic**.
2. Hover over **Virtual Servers**.
3. Hover over **Virtual Server List**.
4. Click the Add button (+) to the right of Virtual Server List to create a new Virtual Server.

### Virtual Server General Properties Section

Use the following guidance to configure the General Properties of the virtual server.

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

#### General Properties

Name	1	AppVolumes-VS-Redirect
Description		
Type		Standard
Source Address		
Destination Address/Mask	2	10.106.169.100
Service Port	3	80 HTTP
Notify Status to Virtual Address		<input checked="" type="checkbox"/>
State		Enabled

1. In the **Name** field, type a unique name such as **AppVolumes-VS-Redirect**.
2. In the **Destination Address/Mask** field, type the same IP Address you used for the HTTPS (port 443) virtual server.
3. In the **Service Port** field, type 80 or select **HTTP** from the list.

### Virtual Server Configuration Section

Use the following guidance to configure the Configuration section of the virtual server.

Configuration: Basic					
Protocol	TCP				
Protocol Profile (Client) <b>1</b>	tcp-wan-optimized				
Protocol Profile (Server) <b>2</b>	tcp-lan-optimized				
HTTP Profile <b>3</b>	AppVolumes-HTTP				
HTTP Proxy Connect Profile	None				
Traffic Acceleration Profile	None				
FTP Profile	None				
RTSP Profile	None				
SSL Profile (Client)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> <b>/Common</b>                      AppVolumes-ClientSSL                      AppVolumes-SSL                      VPN-ClientSSL                      Wildcard-ClientSSL                 </td> </tr> </tbody> </table>	Selected	Available		<b>/Common</b> AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL
Selected	Available				
	<b>/Common</b> AppVolumes-ClientSSL AppVolumes-SSL VPN-ClientSSL Wildcard-ClientSSL				
SSL Profile (Server)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> <b>/Common</b>                      AppVolumes-ServerSSL                      apm-default-serverssl                      crypto-client-default-serverssl                      pcoip-default-serverssl                 </td> </tr> </tbody> </table>	Selected	Available		<b>/Common</b> AppVolumes-ServerSSL apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl
Selected	Available				
	<b>/Common</b> AppVolumes-ServerSSL apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl				
SMTSPS Profile	None				
Client LDAP Profile	None				
Server LDAP Profile	None				
VLAN and Tunnel Traffic	All VLANs and Tunnels				
Source Address Translation	Auto Map <b>4</b>				

1. From the **Protocol Profile (Client)** list, select **tcp-wan-optimized**.
2. From the **Protocol Profile (Server)** list, select **tcp-lan-optimized**.
3. From the **HTTP Profile** list, select the HTTP profile you created (**AppVolumes-HTTP** in our example).
4. From the **Source Address Translation** list, select **Auto Map**.

### Virtual Server Resources Section

Under the Resource properties of the Virtual Server, enter the following settings.

The screenshot shows the 'Resources' configuration window. It is divided into three main sections: iRules, Policies, and Default Pool. The iRules section has a red circle '1' next to it. It contains two lists: 'Enabled' and 'Available'. The 'Enabled' list contains '/Common' and '\_sys\_https\_redirect'. The 'Available' list contains '\_sys\_auth\_radius', '\_sys\_auth\_ssl\_cc\_idap', '\_sys\_auth\_ssl\_crdp', '\_sys\_auth\_ssl\_ocsp', and '\_sys\_auth\_tacacs'. There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list. The Policies section has two empty lists for 'Enabled' and 'Available' with '<<' and '>>' buttons between them. The Default Pool section has a dropdown menu set to 'None'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons, with a red circle '2' next to the 'Finished' button.

1. In the **iRules** area, use the Add (<<) button to move the redirect iRule (**\_sys\_https\_redirect**) to the **Active** list.
2. After you have completed all three sections, click the **Finished** button.

## Testing and Validation

Conduct testing by accessing the App Volumes Manager through its web interface as well as testing App Volumes Agent connectivity.

- App Volumes-enabled desktops will have applications provisioned and de-provisioned on login/logoff, as well as computer startup and shut down.
- App Volumes Manager access through the web interface should be accessible.
- Check the BIG-IP pool member statistics to ensure the App Volume Manager and Agent sessions are being equally distributed between the App Volume pool members.

## References

Jeremy Wheeler – Consulting Architect at VMware

Justin Venezia – Senior Architect, End User Computing Office of the CTO at VMware