**Prerequisites**

Make sure you have the following prerequisites completed:

- Determine what the FQDN will be and what virtual IP Address will be used.
- Add the FQDN and virtual IP into your company's DNS.
- Create and/or import the certificate chain (Root/Intermediate CA and SSL server certificate with private key) that will be used for securing App Volumes network traffic.

**Note:** These instructions *do not* cover creating, importing, and/or chaining certificates for App Volumes Manager servers.

Certificates – things to consider:

- The certificate should contain the FQDN that will be used for load balancing App Volumes agents and manager access.
- You can leave the default certificates on the App Volumes Manager servers - BIG-IP handles all the server-side SSL translations, even with the self-signed certificates created on the App Volumes servers.
- A standard, 2048-bit Web Server SSL Certificate (with private key) will work well with the BIG-IP.
- Make sure you import the entire certificate chain to the BIG-IP - including the Root CA and Intermediate CA Certificates and the web server certificate with the private key.

**Creating Profiles**

Before creating the Virtual Server, we will create specific profiles to control any specific settings needed for load balancing App Volumes Agent and Manager traffic.

These instructions will focus on creating the following:

- SSL Client profile
- SSL Server profile
- Cookie Persistence profile
- HTTP Profile

**Note:** F5’s OneConnect (connection pooling) will not be covered in this document. In most cases, the App Volume agent and manager connections are short-lived and infrequent (service startup/shutdown and logon/logoff events) and may not benefit from OneConnect.
Creating the App Volumes Cookie Persistence Profile


2. Click Create.

3. Complete the following:
   - Type the name of the persistence profile (this example – name is APPVOL-PERSIST).
   - Select Cookie as the Persistence Type.
   - Select Cooke (lower case) as the parent persistence profile that will be used.
   - Leave all remaining values as default.
   - Click Finish when completed.
Creating the App Volumes SSL Client Profile

Note: Prior to completing this step – the SSL Certificate (and Intermediate/Root CA’s) must be imported.


2. Click Create.

3. Complete the following:
   - Type the name of the SSL Client profile (this example – name is APPVOL-CLIENT-SSL).
   - Select “clientssl” as the parent profile.
   - Change the configuration to “Advanced”.
   - On the right side of the screen, check the “Custom” box in the Certificate Key Chain section.

   - Select the Certificate, Key and Certificate Authority/Intermediate Certificate Chain that was previously imported to the BIG-IP and will be used for App Volumes.
• Once the Certificate, Key and Chain are selected, click the Add button. You will see the certificate information appear in the box below the Add button. (Note in our example we are using a wildcard SSL certificate and an Entrust intermediate certificate as the chain certificate.

• Leave the remaining options using the default/existing settings.

4. Click Finish.

Creating the App Volumes SSL Server Profile

Note: Prior to completing this step – the SSL Certificate (and Intermediate/Root CA’s) must be imported.


2. Click Create.
3. Complete the following:

- Type the name of the SSL Server profile (this example – name is APPVOL-SERVER-SSL).
- Select “serverssl” as the parent profile.
- Leave the remaining options using the default/existing settings.

4. Scroll down to the bottom, and then click Finish.

**Creating the App Volumes HTTP Profile**


2. Ensure you are on the Local Traffic: Profiles: Services: HTTP Screen. Click Create.

3. Complete the following:
   - Type the name of the HTTP profile (this example – name is APPVOL-HTTP-PROFILE).
• Select “http” as the parent profile.
• Select “Reverse” as the proxy mode.

• On the right side of the screen, check the “Custom” box in the X-Forwarded-For section.
• On the left side of the screen, change the setting to Enabled.

4. Scroll down to the bottom, then click Finish

Creating the Health Monitor

Creating the health monitor provides intelligent health checks of the server, beyond simply whether the service is listening or the server is pingable. This monitor will initially cover checking the web page for specific content.

NOTE: An enhanced monitor will be developed to simulate a user login to the App Volumes manager in the future.

1. On the BIG-IP - click Local Traffic, Monitors.

2. Click Create
3. Complete the following:

- Type the name of the Monitor profile (this example – name is APPVOL-HTTPS-MON).
- Select “https” as the type of monitor.
- Select 30 seconds for the Interval.
- Select 15 seconds for the Timeout.
- For the Send String, type in the following (replacing fqdn-for-appvolumes with the actual FQDN that will be used):

  GET /login HTTP/1.1
  Host: fqdn-for-appvolumes
  Connection: Close

- For the Receive String, type in the following:

  App Volumes Manager Login

- Accept the remaining default settings.

4. Scroll down to the bottom, then click Finish

**Creating Virtual Server and Pool**

2. Click Create.

3. Complete the following (setting up a VIP with SSL Termination (Bridging):

- Provide a name for the Virtual Server – this example uses APPVOL-HTTPS.
- Set the Type to Standard.
- Provide an IP Address for the Virtual Server under Destination Address.
- Set the Service Port to 443
- Set the Protocol to TCP
- Set the Protocol Profile (Client) to tcp-wan-optimized and the Protocol Profile (Server) to tcp-lan-optimized.

- Set the HTTP Profile to the HTTP Profile that was created earlier.
- Choose the SSL Profiles (both Client and Server) that were created earlier.
• Set the Source Address Translation accordingly (refer to the product documentation for more information on SNAT). For this example, the default gateways for the App Volume servers are not the F5 – the Source Address Translation will be set to Auto Map.

• Next to Default Pool, click the “+” sign (in this example, we will assume the pool for the App Volume servers has NOT been created).

• Set the configuration to Advanced.
• Type in a name for the App Volumes Pool (this example uses APPVOL-POOL).
• Select the App Volumes health monitor that was created earlier.

• Change the Load Balancing Method to Least Connections (member).
• Type in the Node Name (optional) and IP address for each server (required); set the Service Port to HTTPS (443)
• Click Add
• Repeat the previous two (2) steps for each App Volumes Manager server.

• Click Finish - this will create the App Volumes pool.

• Validate the new pool that was just created appears under Default Pool.
• Set the Default Persistence Profile to the App Volumes Persistent Profile created earlier.

4. Click Finish.
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.