Deployment Guide

Deploying the BIG-IP APM Optimized Solution for VMware Horizon View

This F5 deployment guide provides step-by-step instructions on configuring a first time deployment of F5 Access Policy Manager (APM) virtual edition and a first time VMware Horizon View software installation. While this guide has been tailored for customers who purchased one of the four Virtual Edition BIG-IP APM license SKUs, it is also a good place to start for customers who have never deployed VMware Horizon View with F5 BIG-IP Access Policy Manager. Customers should use this deployment guide as a starting point for preparing and installing their VMware View server farm and BIG-IP system virtual edition installation. The iApp and deployment guidance is tailored towards building the VMware Horizon View reference architecture highlighted on f5.com at *https://f5.com/partners/product-technology-alliances/vmware*.

Why F5?

F5 and VMware have a long-standing relationship that centers on technology integration and solution development. As a result, customers can benefit from leveraging the experience gained by peers from deploying proven, real-world solutions.

F5's products and solutions bring an improved level of reliability, scalability, and security to View deployments. For large View deployments requiring multiple pods or several data centers, F5's products provide the load balancing and traffic management needed to satisfy the requirements of customers around the world.

F5 and VMware continue to work together on providing customers best-of-breed solutions that allow for better and faster deployments as well as being ready for future needs, requirements, and growth of your organization.

Products and versions

Product	Versions
BIG-IP APM[3]	11.4 HF-5, 11.4.1, 11.5. 11.5.1, 11.6
VMware Horizon View	5.2, 5.3, 6.0[1], 6.1[1, 2]
iApp Template version	f5.vmware_view_optimized_solution.v1.2.1
Deployment Guide version	1.9.1 (see *Document Revision History on page 27*)

[1] BIG-IP APM v11.6 HF-3 and earlier does not support publishing and providing remote connectivity to the RDS hosted applications feature in Horizon View 6.0; however v11.6 HF-4 or later enables the View Remote App publishing feature.

[2] BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.

[3] BIG-IP APM does not support proxying the VMware View RDP protocol.

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/horizon-view-optimized-iapp-dg.pdf*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com.*

Contents

What is F5 iApp™? 3
Prerequisites and configuration notes 3

Downloading the software 4
Reference architecture diagram 5

Obtaining and installing the SSL certificate for your View environment 6
Configure MSSQL Database for View 8
Install View Composer (optional) 9
Install View Connection Servers 10
Build the virtual desktop pool 13

Configuring the BIG-IP system 15
Deploying the BIG-IP OVF 15
Performing the initial BIG-IP system configuration 16
Installing and configuring the iApp template 22

Next steps 25

Troubleshooting 26

Document Revision History 27

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for View acts as the single-point interface for building, managing, and monitoring View deployments.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- This guide assumes you have a Virtual infrastructure and Active Directory domain already in place. Configuring either is outside of the scope of this deployment guide.
- You must have the proper licenses for VMware Horizon View and BIG-IP Access Policy Manager. Please contact the appropriate sales representative for specific information on licensing.
- You must be using BIG-IP APM version 11.4 HF 5 or later.

Downloading the software

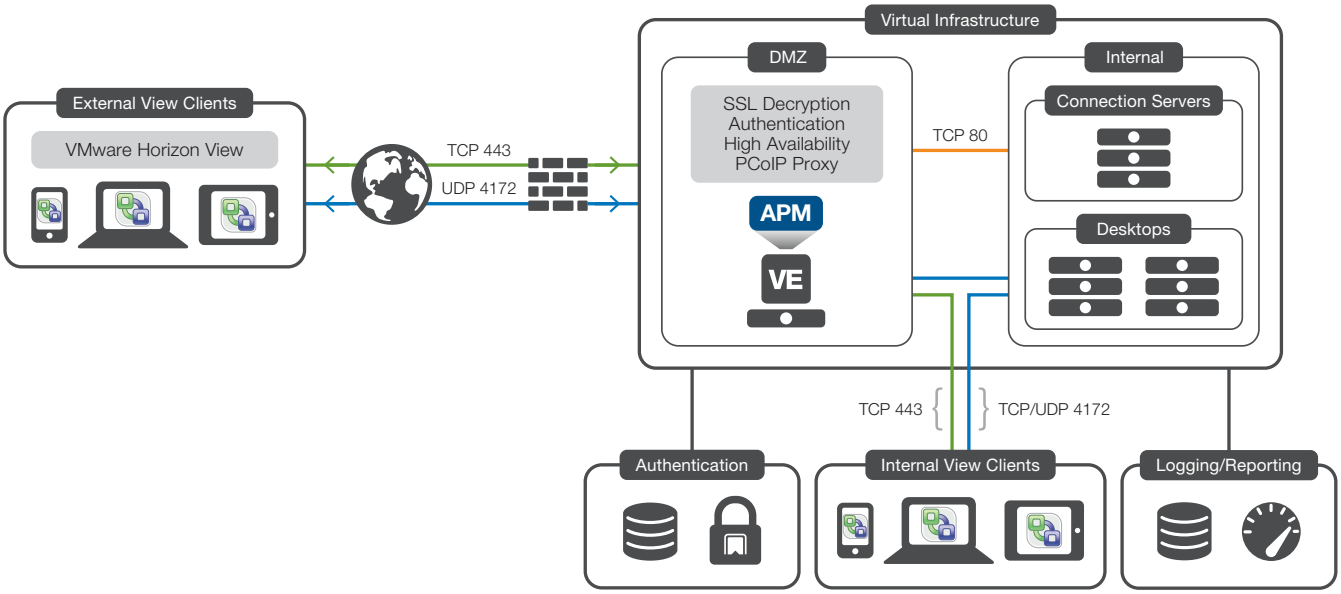
This section contains information on downloading the software required for this deployment. As noted, you must have the appropriate licenses in place.

1. ***Download the latest version of BIG-IP VE***
   a. Go to *https://downloads.f5.com/* and login using a registered account. If you do not have an account, you can create one by clicking **Register for an Account**.
   b. Click **Find a Download.**
   c. In the BIG-IP section, click the most recent Virtual Edition such as **BIG-IP v11.x/ Virtual Edition**.

      Important: *You must use BIG-IP version 11.4 HF-5 or later for this configuration. We recommend using version 11.5 if possible. If you need HF-5, download it before clicking Virtual Edition. See https://support.f5.com/kb/en-us/solutions/public/13000/100/sol13123 for information on installing the Hot Fix.*
   d. Click **Virtual-Edition**.
   e. Read the End User Software license agreement and then click **I Accept**.
   f. Select the OVA file for your hypervisor and save it to a location accessible from VMware vCenter.
2. ***Download the latest version of VMware Horizon View***
   a. Go to *https://www.vmware.com* and click **Login to My VMware** to login using a registered account. If you do not have an account, you can create one.
   b. On the Menu bar, select the **Downloads** Tab and then click **All Products**.
   c. From the drop-down list that defaults to *All Products*, select **Desktop & End-User Computing**.
   d. From the **VMware Horizon View** row, click **View Download Components**.
   e. From the Select Version list, select the latest version.
   f. From the **VMware Horizon View <version>** row, click **Go to Downloads**, and then download the following files:
      - Horizon View Connection Server
      - Horizon View Agent (32/64-bit)
      - Horizon View Composer
   g. Return to the previous page (Download VMware Horizon View), and from the **VMware Horizon View Feature Pack 1** row, click **Go to Downloads**. Download the following files:
      - Remote Experience Agent (32/64 bit)
      - HTML Access Web Portal installer
3. ***Download the latest iApp and deployment guide for f5.vmware_view_optimized_solution***
   a. Open a web browser and go to *downloads.f5.com*.
   b. Click **Find a Download**, and then click **BIG-IP v11.x / Virtual Edition**.
   c. If necessary, select a BIG-IP product version from the list, and then click **iApp-Templates**.
   d. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
   e. Extract (unzip) the **f5.vmware_view_optimized_solution.v1.2.1** file.

Reference architecture diagram

The following diagram represents the configuration described in this deployment guide.



The virtual inventory used to create our Horizon View Optimized solution with F5 reference architecture includes the following guests built on VMware ESXI hosts managed by VMware vCenter (as mentioned in the prerequisites, this guide assumes you have a Virtual infrastructure and Active directory Domain already in place):

- 4 Virtual Windows 2008 R2 servers
  - 2 Horizon View Connection Servers
  - 1 Horizon View Composer
  - 1 MSSQL server
- 2 BIG-IP Virtual Editions
  - HA configuration requires 2 or more BIG-IP systems
  - This guide sets up an active/passive HA configuration
  - For information on how to setup an N+1 active/active configuration see reference material found on Ask F5: *https://support.f5.com/kb/en-us/products/big-ip_apm.html*.
- Virtual Desktops
  - Supported Virtual Desktop Master image; such as Windows 7 or Windows 8.

Begin by building four Windows 2008 R2 servers, setting a static address on each server, binding each server to the appropriate Active Directory domain, and verifying the DNS of each server is correct within your DNS infrastructure. In our example, we use the domain **view.mycompany.com** and give the servers the following names:

Connection servers

- *con1.view.mycompany.com*
- *con2.view.mycompany.com*

MSSQL server

- *sql1.view.mycompany.com*

View Composer

- *com1.view.mycompany.com*

In our example we have Connection servers, View Composer server, and an MS SQL server on the same network to simplify server-to-server communication. Move onto the next section once you have verified all servers are bound to your Active Directory domain, are able to resolve to one another, and can reach supporting services (DNS, NTP, LDAP, and so on).

Obtaining and installing the SSL certificate for your View environment

Although there are many ways to obtain SSL certificates, the following section explains how to create a Certificate Signing Request (CSR) file which can then be used to obtain an SSL certificate from your internal or 3rd party certificate authority (CA).

The following example CSR uses **certreq** (available on 2008 R2 servers).

1. Build the **request.inf** file and save it onto *con1.view.mycompany.com* using the example below. Make sure to modify the example as described in the following. Required changes are in red text in the example.
    a. Replace **CN=remote.view.mycompany.com** with the FQDN used by clients to access your Horizon View environment. Note that in our reference architecture, we suggest using split DNS, which allows you to use the same FQDN for both remote (untrusted) and local (trusted) client connections.
    b. Fill in the appropriate information for OU=OU, O=Org, L=City, S=State, C=Country.
    c. Modify the Key Length value to the appropriate setting. We suggest using at least a length of 2048.

```
;----------------- request.inf -----------------

[Version]
Signature="$Windows NT$
[NewRequest]
Subject = "CN=remote.view.mycompany.com, OU=OU, O=Org, L=City, S=State, C=Country"
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

;-------------------------------------------------
```

2. Create a CSR using Certreq:
    a. On *con1.view.mycompany.com*, a Windows 2008 R2 server, open a command prompt as an administrator.
    b. Navigate to the directory where you saved your **request.inf** file, such as **cd c:\cert**.
    c. Type **`certreq -new request.inf viewcert.txt`**.
    d. Open **viewcert.txt** with Notepad and copy the contents.
3. Using the guidelines for your organization, submit the CSR to an internal or third party CA by pasting the copied contents when prompted for the CSR.
4. Copy the certificate that is returned onto *con1.view.mycompany.com* and save it as **view.cer**, using the same folder used to create the CSR. In some cases the certificate is returned in base 64 digital format rather than a file. Copy the returned ASCII characters into a file you create with the name **view.cer**.
5. Create and install the certificate and key onto *con1* using Certreq.
    a. Make sure both the CSR file and returned certificate are located in **c:\cert**.
    b. Use the following command: **`Certreq -accept view.cer`**
6. Open the Microsoft Management Console with the certificates snap-in using the following guidance.
    a. Click **Start**, **Run** and then type **mmc**. The Console opens.
        » Click **File**, and then **Add/Remove Snap-in**.
        » From the list of Snap-ins, select **Certificates** and then click **Add**.
        » When asked what type of certificates to manage, click **Computer account**.
        » When asked to select the computer you want the snap-in to manage, select **Local Computer**.
        » Click **Finish**.
        » Click **Ok**.
    b. View the locally installed certificates using the following guidance.
        » Under Console Root, expand **Certificates** and **Personal**, and then click **Certificates**
        You should now see a certificate with the FQDN you entered into your request.inf file. In our example we see a certificate named remote.view.mycompany.com.
        » Verify you see a key symbol in the upper left hand corner of the certificate. This indicates the Cert includes the private key.
    c. Add a friendly name to certificate.
        » Right-click the certificate and then click **Properties**.
        » In the **Friendly Name** field, type **vdm**.
        Vdm is used by View to indicate which certificate should be used in the View environment. Make sure you have only one certificate installed with a friendly name of **vdm**.
        » Click **Ok**.
    d. Export the Certificate and Key.
        » Right-click the certificate, and then from the **All tasks** menu, click **Export**. The Export Wizard opens.
        » On the Export Private Key page, select **Yes, export the private key**.
        » On the Export File Format page, check the **Include all certificates in the certificate path if possible** box.
        » On the Password page, type and then confirm a password.
        » On the File to Export page, specify the file name, and specify a secure location to save the exported certificate.
        » Click **Finish**.
    e. Add intermediate and root certificates.
    » Make sure the CA that issued your certificate is located as a root authority.
    Note: Root and/or intermediate certificates can be obtained from the Certificate Authority.
    » Under Console Root, expand **Certificates** and **Trusted Root Certification Authorities**, and then click **Certificates**.

- Import the Root server if not present
  - In the left panel, right-click **Certificates** and from the **All tasks** menu, click **Import**. The Import Wizard opens.
  - On the File to Import page, select the file you to import.
  - Walk through the rest of the wizard, and then click **Finish**.
- Import Intermediate Certificates if required.
  In some cases an intermediate CA is used rather than the root server to protect the identity of the CA root servers. If so, import intermediate CA certificate using import wizard.
  - Under Console Root, expand **Certificates** and **Intermediate Certification Authorities**, and then click **Certificates**.
  - Right-click **Certificates** and from the **All tasks** menu, click **Import**. The Import Wizard opens.
  - On the File to Import page, select the file you to import.
  - Walk through the rest of the wizard, and then click **Finish**.

7. Apply the exported certificate to all View servers. In our environment we import *remote.view.mycompany.com* to servers *con2* and *com1* using the import wizard in the MMC certificates snap-in. You also need to install root and intermediate server certificates if they are not present.
   a. Go to the server (*con2* in our example) and open MMC (see step 6a above on how to open MMC if necessary).
      - Click **File**, and then **Add/Remove Snap-in**.
      - From the list of Snap-ins, select **Certificates** and then click **Add**.
      - When asked what type of certificates to manage, click **Computer account**.
      - When asked to select the computer you want the snap-in to manage, select **Local Computer**.
      - Click **Finish**.
      - Click **Ok**.
   b. Import the certificates using the following guidance.
      - Under Console Root, expand **Certificates** and **Personal**, and then click **Certificates**
      - In the left panel, right-click **Certificates** and then from the **All tasks** menu, click **Import**. The Import Wizard opens.
      - On the File to Import page, select the certificate you previously exported.
      - Walk through the rest of the wizard, and then click **Finish**.
   c. Import root and intermediate certificates if necessary.
   d. Repeat on the other server (*com1.view.mycompany.com* in our example).

Configure MSSQL Database for View

While you can use other database software with View, in this example we use Microsoft SQL Server 2008 R2. The following section provides basic guidance for database setup required for supporting View Composer and View connection server logging (Events DB).

1. Open SQL Server Management Studio.
   a. Connect and authenticate to the appropriate server using server type **Database Engine**.
2. Create a database for Composer.
   a. Right-click **Databases** and then click **New Database**.
      - In the **Name** field, type a name for the Database. In our example we use **Composer**.
      - Click **Ok**.
3. Create a database for View Connection server logs.
   a. Right-click **Databases** and then click **New Database**.
      - In the **Name** field, type a name for the Database. In our example we use **Events**.
      - Click **Ok**.
4. Create a database user for the Composer database.

a. Select **Security**, and then click **Logins**.

b. Right-click **Login** and then click **New Login**.

- In the **Login** field, type the login name. In our example, we use **composer**.
- Select SQL Server authentication and provide password.
- Select appropriate password policies and enforcement.
- Select **Composer** (or the name you gave this database) as default database.
- Select **User Mapping** located in the left side of page.
  i). Click a check in **Map** next to composer database.
  ii). Highlight the Composer database and click a check next to the **db_owner** role located at the bottom of the page.
- Click **Ok**.

5. Create a database user for the Events database.

a. Select **Security**, and then **Logins**

b. Right-click **Login** and then click **New Login**.

- In the **Login** field, type the login name. In our example, we use **events**.
- Select SQL Server authentication and provide password
- Select appropriate password policies and enforcement
- Select **Events** (or the name you gave this database) as default database
- Select **User Mapping** located in the left side of page
  i). Click a check in **Map** next to composer database
  ii). Highlight the Events database and click a check next to the **db_owner** role located in the bottom of the page.
- Click **Ok**.

Install View Composer (optional)

Horizon View Composer is an optional service that you install only if you plan to deploy multiple linked-clone desktops from a single centralized base image. Linked-clone desktop images optimize the use of storage space. Administrators make changes to a master image, which View Composer applies to user desktops without affecting user settings, data, and applications. View Composer is a feature of View Connection Server, but its service operates directly on virtual machines managed by vCenter.

1. On the *com1* server, launch the ODBC Data Source Administrator.

a. From the Start menu, select **Administrative Tools**, and then click **Data Sources (ODBC)**.

2. Create a System DSN.

a. From the ODBC Data Source Administrator, click the DSN tab and then click **Add**.

b. From the Driver list, click **SQL Server,** and then click **Finished**. The Create a New Data Source to SQL Server wizard opens.

c. In the **Name** field, type a name for the system DSN. In our example, we use **composer**. You can optionally type a description.

d. In the **Server** field, type the FQDN of the SQL server (in our example, we use *com1.view.mycompany.com*) and then click **Next**.

e. On the next screen, click **With SQL Server authentication using a login ID and password entered by the user**.

- In the **Login ID** field, type the login you created for the Composer database.
- In the **Password** field, type the associated password and then click **Next**.

f. Check **Change the default database to:** and then select the Composer database. Click **Next**.

g. Click **Finish**.

h. Test the Data Source.
   - » Click **Test data source**
   - » You should see **Tests completed successfully**.

i. Click **Ok**.

j. Click **Ok** to leave the ODBC configuration.

3. Run View Composer as Administrator.
   a. Right-click the Horizon View Composer executable you downloaded in Step 2f on *page 4* and then select **Run as administrator**.
   b. When asked if you want to allow the program to make changes, click **Yes**.
   c. Click **Next** on the Welcome Page.
   d. Read and Accept license agreement.
   e. If necessary, change the destination folder, and then click **Next**.
   f. Add the System DSN you created (in our example, this is **composer**).
   g. Type user name and password created for the composer database. In our example the username is **composer**.
   h. Click **Next**.
   i. Select **Use an existing SSL certificate**.
   j. Select the SSL certificate you imported to *com1*. In our example the SSL certificate is *remote.view.mycompany.com*.
   k. Click **Next**.
   l. When asked to install Composer, click **Install**.
   m. Click **Finish** when installation has completed.
   n. Click **Yes** when asked to reboot the system.

Install View Connection Servers

In this section, we install Horizon View Connection server onto *con1*.

1. Install Horizon View Connection software onto the *con1* server
   a. Run the Connection server software as an administrator by right-clicking the Horizon View Connection Server executable you downloaded in Step 2f on *page 4* and then click **Run as administrator**.
   b. When asked if you want to allow the program to make changes, click **Yes**.
   c. Click **Next** on the Welcome Page.
   d. Read and Accept license agreement and then click **Next**.
   e. If necessary, modify default installation location and then click **Next**.
   f. Select **View Standard server** and then click **Next**.
   g. Type a data recovery password and a password reminder (optional) and then click **Next**.
   h. Make sure **Configure Windows Firewall automatically** is selected and then click **Next**.
   i. Select **Authorize a specific domain user or domain group**, and then type a user or group of users that are allowed to login to Horizon View Management Console
   j. Select an appropriate response to **User Experience Improvement Program** and then click **Next**.
   k. On the ready to install page, click **Install**.
   l. Select **Finish** on Installer Complete page.

2. (Optional – required to support HTML 5 client connections) Install the Horizon View HTML Access software onto *con1* server
    a. Run the HTML access software as an administrator by right-clicking the executable you downloaded in Step 2g on *page 4*, and then and selecting **Run as administrator.**
    b. When asked if you want to allow the program to make changes, click **Yes**.
    c. Run through the installation wizard accepting the defaults.
    d. Click **Finish** on the **Completed** page.

3. Logon to the View Administrator Console.
    a. From the Start menu, open the View Administrator console.
    b. Select **Continue to this website**.
        » Adobe Flash Player 10.1 or greater is required; install it if necessary from the Adobe.com.
    c. Login using appropriate credentials.

4. Add the Horizon View License.
    a. From the View Administrator console, click **Edit License**.
    b. Type your serial number, and then click **Ok**.
    You should now at least see View Composer and the Local Mode license enabled.

5. Add the vCenter server(s) to Horizon View Connection servers.
    a. On the View Configuration tab, click **Servers**.
    b. Highlight the vCenter Servers tab and then click **Add**.
    c. Enter the vCenter IP address, the appropriate credentials, a description (optional), and then click **Next**.
    d. Click **Standalone View Composer Server**, type the Composer IP address and the appropriate credentials.
        » Note, you will receive a message indicating your server URL does not match the server's certificate. Select **View Certificate** and you should see the certificate previously installed onto *com1*. Click **Accept**.
    e. Click **Add** to select the appropriate domain. In our example, we use *view.mycompany.com*.
        » Type the FQDN of the domain used for this Horizon View environment and appropriate credentials, and then click **Ok**.
    f. Click **Next**.
    g. Select the appropriate storage Acceleration settings and then click **Next**.
    h. Click **Finish**.
        » You can verify the settings by checking the system health status from the Dashboard tab. The vSphere components should have a *green* status. If it does not, check the information you entered in the previous steps.

6. Add the Events configuration.
    a. From the View Configuration tab, click **Event Configuration**.
    b. Under **Events Database**, click **Edit**.
        » Enter the database server and database name, the appropriate credentials, and a prefix (optional), and then click **Ok**. In our example, we use *sql1.view.mycompany.com* for the SQL server, **events** for database name, and **events** for username.

7. Install the Horizon View Connection software onto *con2* server.
    a. Run the Connection server software as an administrator by right-clicking the Horizon View Connection Server executable you downloaded in Step 2f on *page 4* and then click **Run as administrator**.
    b. When asked if you want to allow the program to make changes, click **Yes**.

c. Click **Next** on the Welcome Page.

d. Read and Accept license agreement and then click **Next**.

e. If necessary, modify default installation location and then click **Next**.

f. Select **View Replica server** and then click **Next**.

g. Type the FQDN or IP address for *con1* and then click **Next**.

h. Make sure **Configure Windows Firewall automatically** is selected and then click **Next**.

i. Select **Authorize a specific domain user or domain group**, and then type a user or group of users that are allowed to login to Horizon View Management Console.

j. On the Ready to Install page, click **Install**.

k. Select **Finish** on Installer Complete page.

8. (Optional – required to support HTML 5 client connections) Install Horizon View HTML Access software onto *con2* server

   a. Run the HTML access software as an administrator by right-clicking the executable you downloaded in Step 2g on *page 4*, and then and selecting **Run as administrator.**

   b. When asked if you want to allow the program to make changes, click **Yes**.

   c. Run through the installation wizard accepting the defaults.

   d. Click **Finish** on the **Completed** page.

9. Modify the Connection Server to use the remote FQDN supplied in the SSL certificate

   a. From the View Configuration tab, select **Servers**.

   b. Click **Connection Servers**.

   c. Highlight **CON20** and then click **Edit**.

   d. Modify the **HTTP External URL** and **BLAST External URL** to match the URL of your SSL certificates. In our example, we use *https://remote.view.mycompany.com:443*.

      » Clear the check from **Use Secure Tunnel connection to desktop** and **Use Blast Secure Gateway for HTML access to desktop** after modifying the External URLs.

   e. Click **OK**.

   f. Highlight **CON21** and then click **Edit**.

   g. Modify the **HTTP External URL** and **BLAST External URL** to match the URL of your SSL certificates. In our example, we use *https://remote.view.mycompany.com:443*.

      » Clear the check from **Use Secure Tunnel connection to desktop** and **Use Blast Secure Gateway for HTML access to desktop** after modifying the External URLs.

10. Verify the settings from the Dashboard tab.

    a. Click the Dashboard menu item.

    b. Review the Connection Server status to confirm the status has changed from *red* to *green*. If necessary, click refresh as status changes can take a couple of minutes to complete.

Allowing HTTP connections to intermediate servers (optional and requires server reboot)

When SSL is offloaded to an intermediate server, you can configure View Connection Server instances to allow HTTP connections from the client-facing BIG-IP system. The BIG-IP system must accept HTTPS for View Client connections.

To allow HTTP connections between View servers and BIG-IP system, you must configure the **locked.properties** file on each View Connection Server instance on which HTTP connections are allowed.

Even when HTTP connections between View servers and intermediate devices are allowed, you cannot disable SSL in View. View servers continue to accept HTTPS connections as well as HTTP connections.

To configure the locked.properties file

1. Create or edit the **locked.properties** file in the SSL gateway configuration folder on the View Connection Server host. For example: *install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties*
2. To configure the View server's protocol, add the **serverProtocol** property and set it to **http**. The value **http** must be typed in lower case.
3. *Optional*: Add properties to configure a non-default HTTP listening port and a network interface on the View server.
   - To change the HTTP listening port from 80, set **serverPortNonSSL** to another port number to which the intermediate device is configured to connect.
   - If the View server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set **serverHost** to the IP address of that network interface.
4. Save the **locked.properties** file.
5. Restart the View Connection Server service to make your changes take effect.

For example, the following locked.properties file allows non-SSL HTTP connections to a View server. The IP address of the View server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value http must be lower case.

```
serverProtocol=http

serverHost=10.20.30.40
```

Build the virtual desktop pool

The last step in for the Horizon View deployment is to build images and create pools for users. There are numerous ways to appropriately configure virtual desktop pools for your environment. The following example creates an automated pool and uses View Composer linked clones. An automated pool uses a vCenter Server template or virtual machine snapshot to generate new desktops. The desktops can be created when the pool is created or generated on demand based on pool usage. View Composer linked clones share the same base image and use less storage space than full virtual machines. The user profile for linked clones can be redirected to persistent disks that will be unaffected by OS updates and refreshes.

1. Open VMware Horizon View Administrator.
2. From the **Inventory** menu, select **Pools**, and then click **Add**.
   a. ***Type***: Verify **Automated Pool** is selected and then click **Next**.
   b. ***User Assignment***: Select **Appropriate User assignment** and then click **Next**.
   c. ***vCenter Server***: Select **View Composer linked clones** and then click **Next**.
   d. ***Pool Identification***: Enter the ID, Display Name, Appropriate View Folder, and Description (optional), and then click **Next**.
   e. ***Pool Settings***: Enter the appropriate pool settings based on your preferences and policies; make sure the **Default display protocol** is set to **PCoIP**, **Allow users to choose** set to **No**, **HTML Access** is enabled if supporting HTML 5 client connections, and then click **Next**.

      Note that BIG-IP APM only supports PCoIP connections, which is why the display protocol is set to PCoIP and Allow users to choose is set to No.
   f. ***Provisioning Settings***: Specify the appropriate provisioning settings based on your preferences and policies and then click **Next**.
   g. ***View Composer Disks***: Enter the appropriate Composer Disk settings based on preferences and policies and then click **Next**.

h. ***Storage Optimization***: Select the appropriate storage optimization based on preferences and policies and then click **Next**.

i. ***vCenter Settings***:

- *Parent VM*: Browse and select the parent VM, and then verify appropriate Horizon View software agent has been installed on it.
  If supporting HTML 5 client connections, verify the appropriate Remote Experience Agent software has been installed on the parent VM.
- *Snapshot*: Browse and select the appropriate snapshot of the parent VM.
- *VM folder location*: Browse and select appropriate folder location
- *Host or Cluster*: Browse and select appropriate cluster or individual host
- *Resource Pool*: Select appropriate resource pool
- *Datastores*: Select appropriate data store(s) and appropriate storage overcommit
- Click **Next**.

j. ***Advanced Storage Options***: Select appropriate Storage Options and then click **Next**.

k. ***Guest Customization***: Select the Domain for desktops to use, enter the Active Directory container to add desktops, optionally select QuickPrep or Sysprep options, and then click **Next**.

l. ***Ready to Complete***: Check the box next to Entitle users after this wizard finishes. Verify settings and then click **Finish**.

m. ***Entitlements***: Click **Add**.

- Enter the appropriate search and then click **Find**.
- Select the group or users to add as entitled to the pool.
- Repeat if necessary.
- Click **OK**.

Be sure to see *Allowing HTTP connections to intermediate servers (optional and requires server reboot) on page 12* if offloading SSL.

Configuring the BIG-IP system

Configuring the BIG-IP system is broken into three distinct sections:

- *Deploying the BIG-IP OVF on this page*
- *Performing the initial BIG-IP system configuration on page 16*
- *Installing and configuring the iApp template on page 22*

Deploying the BIG-IP OVF

Use this section to deploy the BIG-IP software onto a virtual machine.

1. Launch VMware vCenter and login.
2. From the **File** menu, click **Deploy OVF Template**. The Deploy OVF Template wizard opens. Complete the following.
   a. Click **Browse** and go to the location you saved the BIG-IP system OVF file you downloaded using the instructions on *page 4* (remember the BIG-IP version of the file you downloaded must be 11.4 or newer). Click **Open**, and then back on the Source Page, click **Next**.
   b. On the OVF Template Details page, review the details and then click **Next**.
   c. Read the End User Software License. When finished, click **Accept**, and then click **Next**.
   d. From the Name and Location page, in the **Name** box, type a unique name for this VM, and then select an inventory location. Click **Next**.
   e. On the Deployment Configuration page, select the appropriate number of CPUs and amount of RAM for this deployment and then click **Next**.
      » Use the appropriate settings based on your license. The VMware virtual machine guest environment for the BIG-IP Virtual Edition (VE), at minimum, must include:
      - 2 x virtual CPUs
      - 4 GB RAM
      - 1 x VMXNET3 virtual network adapter or Flexible virtual network adapter (for management)
      - 1 x virtual VMXNET3 virtual network adapter (three are configured in the default deployment for dataplane network access)
      - 1 x 100 GB SCSI disk, by default
      - 1 x 50 GB SCSI optional secondary disk, which might be required as a datastore for specific BIG-IP modules. For information about datastore requirements, refer to the BIG-IP module's documentation.

        Important: Not supplying at least the minimum virtual configuration limits will produce unexpected results.
   f. On the Host/Cluster page, select appropriate cluster and then click **Next**.
   g. On the Resource Pool page, select the appropriate pool and then click **Next**.
   h. On the Storage page, select the appropriate destination storage for the virtual machine and then click **Next**.
   i. On the Disk Format page, click **Next**.
   j. On the Network Mapping page, select the appropriate Destination Networks for each of the Source Networks. By default, the there are four source networks: Management, Internal, External, and HA.
      » Management is used specifically for managing this BIG-IP instance and is not used to pass production traffic.
      » Internal, for this View reference architecture, is used to reach your backend View Connection servers and Virtual Desktop networks. It is also used by internal trusted View clients.
      » External, for this View reference architecture, is used for remote untrusted View Client connections.
      » HA is used for communication to and from the secondary BIG-IP system.

      When you have mapped all of the networks, click **Next**.

k. On the Ready to Complete page, review the deployment settings. Use the **Back** button to make any changes. If the settings are correct, check **Power on after deployment** and then click **Finish**.

l. After vCenter deploys and powers on the BIG-IP system, click the Summary tab of the new virtual machine and then click **Open Console**.

m. At the localhost login prompt, type **root**. At the password prompt, type **default**.

n. At the prompt, type **config** and press Enter to start the Configuration Utility.

- Press Enter to start the Configuration Utility.
- On the Configure IP Address page, use the Tab key to select **No** and then press Enter.
- On the IP Address page, type the IP address for management and then select **OK**.
- On the Subnet mask page, type the appropriate subnet mask for the management network and the select **OK**.
- On the Management Route page, if you do not need to supply a gateway (default route), select **No** and then continue with the next step.
  If you need to supply a gateway, select **Yes**, and then enter the gateway address for the management network on the next page. Select **OK** to continue.
- On the Confirm Configuration page, review the settings and select **Yes** to continue.

o. At the prompt, type **exit** and then press Enter. You return to the login page. You may now close the console session.

3. Return to step 1 and repeat this entire process for the second BIG-IP system.

Performing the initial BIG-IP system configuration

In this section we walk through using the Setup Utility wizard to deploy an internal, external, and high availability network. In our example we name the first BIG-IP system, *bigip1.mycompany.com*, and the second BIG-IP system, *bigip2.mycompany.com*.

Configuring the first BIG-IP system

1. Open *https://bigip1.mycompany.com* using your preferred web browser. If you have not yet configured *bigip1.mycompany.com* to resolve to the appropriate IP address, use the management IP address for the BIG-IP system. Ignore any warnings about untrusted connections at this point.
2. For both the **Username** and **Password** fields, type **admin**. The BIG-IP Configuration utility opens to the Setup Utility page.
3. License the system using the following guidance:
   a. On the Welcome page, click **Next**. The License page opens.
   b. On the License page, click the **Activate** button to Activate your F5 license. The way you license the device depends on whether the BIG-IP system has outbound internet connectivity (the automatic option) or not (the manual option).
      - Automatic (the BIG-IP must have access to the Internet):
        i). In the **Base Registration Key** field, type (or copy/paste) the base registration key you received from F5.
        ii). In the **Activation Method** row, make sure **Automatic** is selected.
        iii). In the **Outbound Interface** row, make sure **mgmt** is selected.
        iv). Click **Next**.
        v). Read the End User Software License and then click **Accept**.
        vi). Wait while the system verifies the license and then click **Log in**. Continue with #4.
      - Manual (does not require outbound internet access):
        i). In the **Base Registration Key** field, type (or copy/paste) the base registration key you received from F5.
        ii). In the **Activation Method** row, make sure **Manual** is selected, and then click **Next**.

iii). In the **Dossier** row, copy the dossier. You can alternatively click the **Download/Upload File** option.

iv). On a device that has Internet access, open a browser and go to *https://secure.f5.com/*.

v). Under Activate, click the first **Activate License** link.

vi). Paste the contents of the dossier into the box. If you chose to download the dossier file, click **Choose File** and browse to the dossier. Click **Next**.

vii). Read the End User Software License and then click **Accept**.

viii). Copy the license text (or click **Download license**).

ix). Return to the BIG-IP system and paste the license into the **License** box. If you chose to download the license file, click **Choose File** and browse to the license. Click **Next**.

x). Wait while the system verifies the license and then click **Log in**.

4. Provision the Access Policy Manager (APM) and deprovision the Local Traffic Manager (LTM) using the following guidance:
   a. From the Module table, find the **Local Traffic (LTM)** row, and clear the box to deprovision LTM.
   b. In the **Access Policy (APM)** row, check the box to provision APM. Ensure **Nominal** is selected.
   c. Click the **Next** button.
   d. When the reprovisioning warning displays asking if you want to proceed, click **OK**. The system loads and verifies the new configuration.
5. Configure the Device certificates using the following guidance.
   Note that the Certificate subject needs to match the FQDN host name of the BIG-IP system. See *Obtaining and installing the SSL certificate for your View environment on page 6* for more information on creating a CSR for each BIG-IP system.
   a. On the Device Certificates page, click the **Import** button.
   b. From the **Import type** list, select **PKCS 12 (IIS)**.
   c. From the **Certificate Source** row, click Choose File and then select the appropriate file.
   d. In the **Password** field, type the associated password.
   e. Click **Import**.
   f. Select the correct certificate subject and then click **Next**.
6. Configure the Platform options using the following guidance.
   a. In the **Host Name** field, type a host name. In our example, we use *bigip1.mydomain.com*.
   b. From the **Time Zone** list, select the correct time zone.
   c. In the **Root Account** row, type and confirm a password for the root account in the associated fields.
   d. In the **Admin Account** row, type and confirm a password for the admin account in the associated fields.
   e. Optional: If you want to restrict SSH access that are allowed to access this system to a specific range of IP addresses, from the **SSH IP Allow** list, select **Specify Range** and then type a range of IP addresses.
   f. Click **Next**.
   g. When the updated password warning displays, click **OK**. You are logged out. Log in again with your new credentials.
7. Configure the Network options using the following guidance:
   a. Under **Standard Network Configuration**, click the **Next** button.
   b. In the **Config Sync** row, make sure the **Display configuration synchronization options** box is checked.
   c. In the **High Availability** row, make sure the **Display failover and mirroring options** box is checked and the Failover Method is set to **Network**.
   d. Click **Next**.

e. Complete the Internal Network Configuration using the following guidance:
   - In the **Self IP** row, in the **Address** box, type an IP address that is part of the trusted network you configured during the BIG-IP OVF installation.
   - In the **Netmask** box, type the associated mask.
   - In the **Floating IP** row, in the **Address** box, type an IP address that is part of the trusted network set you during the BIG-IP OVF installation. This is the address that both units in a redundant system share, and must be different than the Self IP address.

f. Complete the Internal VLAN Configuration using the following guidance
   - In the **VLAN Tag ID** field, type an ID if the VLAN associated with the internal network is configured to use tagging.
   - In the **VLAN interfaces** row, from the Available list, select interface **1.1** and click the Add button to move it to either **Untagged** or **Tagged**.

g. Click **Next**.

h. Complete the External Network Configuration using the following guidance:
   - In the **Self IP** row, in the **Address** box, type an IP address that is part of the untrusted network you configured during the BIG-IP OVF installation.
   - In the **Netmask** box, type the associated mask.
   - In the **Default Gateway** field, type the default gateway for the system.
   - In the **Floating IP** row, in the **Address** box, type an IP address that is part of the untrusted network you set during the BIG-IP OVF installation. This is the address that both units in a redundant system share, and must be different that the Self IP address.

i. Complete the External VLAN Configuration using the following guidance
   - In the **VLAN Tag ID** field, type an ID if the VLAN associated with the external network is configured to use tagging.
   - In the **VLAN interfaces** row, from the Available list, select interface **1.2** and click the Add button to move it to either **Untagged** or **Tagged**.
   - Click **Next**.

j. Complete the High Availability Network Configuration using the following guidance:
   - In the **Self IP** row, in the **Address** box, type an IP address that is part of the trusted HA network you configured during the BIG-IP OVF installation.
   - In the **Netmask** box, type the associated mask.

k. Complete the High Availability VLAN Configuration using the following guidance
   - In the **VLAN Tag ID** field, type an ID if the VLAN associated with the HA network is configured to use tagging.
   - In the **VLAN interfaces** row, from the Available list, select interface **1.3** and click the Add button to move it to either **Untagged** or **Tagged**.
   - Click **Next**.

l. On the Config Sync Configuration page, from the **Local Address** list, select the IP address on the **HA** VLAN to use for configuration synchronization and then click **Next**.

m. Complete the Failover configuration using the following guidance:
   - In the Failover Unicast Configuration section, click the **Add** button.
   - From the **Address** list, select the address on the **internal** VLAN, and then click **Repeat**.
   - From the **Address** list, select the address on the **external** VLAN, and then click **Finish**.
   - In the Failover Unicast Configuration table, check the box for the addresses on the Management Address and HA VLANs, and then click **Delete**. Click **OK** to confirm.

Note: *The internal and external local addresses will be monitored for availability by the second BIG-IP system. If the second BIG-IP device is unable to reach either address, system automatically fails over.*

» Click **Next**.

n. Complete the Mirroring configuration using the following guidance. Mirroring (or Connection mirroring) on the BIG-IP system is the mechanism by which connections on one system are essentially replicated on another system. Configuring mirroring helps ensure that in-process connections are not dropped when failover occurs. You enable mirroring on each relevant device. To set up mirroring, you specify, on the local device, the primary and secondary IP addresses that you want the system to use for mirroring. These are typically self IP addresses.

» From the Primary Local Mirror Address list, select the **HA** IP address.

» Optional: From the Secondary Local Mirror Address list, select another local IP address to mirror connections.

» Click **Next**.

o. Complete the Active/Standby Pair configuration using the following guidance:

» Under **Standard Pair Configuration**, click the **Next** button.

» Under **Configure Peer Device**, click the **Finished** button.

This completes the configuration for the first BIG-IP system.

Configuring the second BIG-IP system

1. Open *https://bigip2.mycompany.com* using your preferred web browser. If you have not yet configured your DNS settings, use the management IP address for the BIG-IP system. Ignore any warnings about untrusted connections at this point.
2. For both the **Username** and **Password** fields, type **admin**. The BIG-IP Configuration Utility opens to the Setup Utility page.
3. License the system using the following guidance:
   a. On the Welcome page, click **Next**. The License page opens.
   b. On the License page, click the **Activate** button to Activate your F5 license. The way you license the device depends on whether the BIG-IP system has outbound internet connectivity (the automatic option) or not (the manual option).
      » Automatic (the BIG-IP must have access to the Internet):
         i). In the **Base Registration Key** field, type (or copy/paste) the base registration key you received from F5.
         ii). In the **Activation Method** row, make sure **Automatic** is selected.
         iii). In the **Outbound Interface** row, make sure **mgmt** is selected.
         iv). Click **Next**.
         v). Read the End User Software License and then click **Accept**.
         vi). Wait while the system verifies the license and then click **Log in**. Continue with #4.

      » Manual (does not require outbound internet access):
         i). In the **Base Registration Key** field, type (or copy/paste) the base registration key you received from F5.
         ii). In the **Activation Method** row, make sure **Manual** is selected, and then click **Next**.
         iii). In the **Dossier** row, copy the dossier. You can alternatively click the **Download/Upload File** option.
         iv). On a device that has Internet access, open a browser and go to *https://secure.f5.com/*.
         v). Under Activate, click the first **Activate License** link.
         vi). Paste the contents of the dossier into the box. If you chose to download the dossier file, click **Choose File** and browse to the dossier. Click **Next**.
         vii). Read the End User Software License and then click **Accept**.
         viii). Copy the license text (or click **Download license**).

ix). Return to the BIG-IP system and paste the license into the **License** box. If you chose to download the license file, click **Choose File** and browse to the license. Click **Next**.

x). Wait while the system verifies the license and then click **Log in**.

4. Provision the Access Policy Manager (APM) and deprovision the Local Traffic Manager (LTM) using the following guidance:
   a. From the Module table, find the **Local Traffic (LTM)** row, and clear the box to deprovision LTM.
   b. In the **Access Policy (APM)** row, check the box to provision APM. Ensure **Nominal** is selected.
   c. Click the **Next** button.
   d. When the reprovisioning warning displays asking if you want to proceed, click **OK**. The system loads and verifies the new configuration.

5. Configure the Device certificates using the following guidance.
   Note that the Certificate subject needs to match the FQDN host name of the BIG-IP system.
   a. On the Device Certificates page, click the **Import** button.
   b. From the **Import type** list, select **PKCS 12 (IIS)**.
   c. From the **Certificate Source** row, click Choose File and then select the appropriate file.
   d. In the **Password** field, type the associated password.
   e. Click **Import**.
   f. Select the correct certificate subject and then click **Next**.

6. Configure the Platform options using the following guidance.
   a. In the **Host Name** field, type a host name. In our example, we use *bigip2.mydomain.com*.
   b. From the **Time Zone** list, select the correct time zone.
   c. In the **Root Account** row, type and confirm a password for the root account in the associated fields.
   d. In the **Admin Account** row, type and confirm a password for the admin account in the associated fields.
   e. Optional: If you want to restrict SSH access that are allowed to access this system to a specific range of IP addresses, from the **SSH IP Allow** list, select **Specify Range** and then type a range of IP addresses.
   f. Click **Next**.
   g. When the updated password warning displays, click **OK**. You are logged out. Log in again with your new credentials.

7. Configure the Network options using the following guidance:
   a. Under **Standard Network Configuration**, click the **Next** button.
   b. In the **Config Sync** row, make sure the **Display configuration synchronization options** box is checked.
   c. In the **High Availability** row, make sure the **Display failover and mirroring options** box is checked and the Failover Method is set to **Network**.
   d. Click **Next**.
   e. Complete the Internal Network Configuration using the following guidance:
      » In the **Self IP** row, in the **Address** box, type an IP address that is part of the trusted network you configured during the BIG-IP OVF installation.
      » In the **Netmask** box, type the associated mask.
      » In the **Floating IP** row, in the **Address** box, type the same IP address you used on the first BIG-IP system in step 7e.
   f. Complete the Internal VLAN Configuration using the following guidance

- » In the **VLAN Tag ID** field, type an ID if the VLAN associated with the internal network is configured to use tagging.
- » In the **VLAN interfaces** row, from the Available list, select interface **1.1** and click the Add button to move it to either **Untagged** or **Tagged**.

g. Click **Next**.

h. Complete the External Network Configuration using the following guidance:

- » In the **Self IP** row, in the **Address** box, type an IP address that is part of the untrusted network you configured during the BIG-IP OVF installation.
- » In the **Netmask** box, type the associated mask.
- » In the **Default Gateway** field, type the default gateway for the system.
- » In the **Floating IP** row, in the **Address** box, type the same IP address you used on the first BIG-IP system in step 7h.

i. Complete the External VLAN Configuration using the following guidance

- » In the **VLAN Tag ID** field, type an ID if the VLAN associated with the external network is configured to use tagging.
- » In the **VLAN interfaces** row, from the Available list, select interface **1.2** and click the Add button to move it to either **Untagged** or **Tagged**.
- » Click **Next**.

j. Complete the High Availability Network Configuration using the following guidance:

- » In the **Self IP** row, in the **Address** box, type an IP address that is part of the trusted HA network you configured during the BIG-IP OVF installation.
- » In the **Netmask** box, type the associated mask.

k. Complete the High Availability VLAN Configuration using the following guidance

- » In the **VLAN Tag ID** field, type an ID if the VLAN associated with the HA network is configured to use tagging.
- » In the **VLAN interfaces** row, from the Available list, select interface **1.3** and click the Add button to move it to either **Untagged** or **Tagged**.
- » Click **Next**.

l. On the Config Sync Configuration page, from the **Local Address** list, select the IP address on the **HA** VLAN to use for configuration synchronization and then click **Next**.

m. Complete the Failover configuration using the following guidance:

- » In the Failover Unicast Configuration section, click the **Add** button.
- » From the **Address** list, select the address on the **internal** VLAN, and then click **Repeat**.
- » From the **Address** list, select the address on the **external** VLAN, and then click **Finish**.
- » In the Failover Unicast Configuration table, check the box for the addresses on the Management Address and HA VLANs, and then click **Delete**. Click **OK** to confirm.

  Note: *The internal and external local addresses will be monitored for availability by the first BIG-IP system. If the first BIG-IP device is unable to reach either address, system automatically fails over.*
- » Click **Next**.

n. Complete the Mirroring configuration using the following guidance.
Mirroring (or Connection mirroring) on the BIG-IP system is the mechanism by which connections on one system are essentially replicated on another system. Configuring mirroring helps ensure that in-process connections are not dropped when failover occurs. You enable mirroring on each relevant device. To set up mirroring, you specify, on the local device, the primary and secondary IP addresses that you want the system to use for mirroring. These are typically self IP addresses.

- » From the Primary Local Mirror Address list, select the **HA** IP address.
- » Optional: From the Secondary Local Mirror Address list, select another local IP address to mirror connections.

» Click **Next**.

o. Complete the Active/Standby Pair configuration using the following guidance:

» Under **Standard Pair Configuration**, click the **Next** button.

» Under **Discover Configured Peer Device**, click the **Next** button.

» Under **Remote Device Credentials**, specify the **Management IP address**, **Administrator Username**, and **Administrator Password** for the first BIG-IP system.

» Click **Retrieve Device Information**.

» Click **Finished** after the peer device information has been retrieved.

» Click **Awaiting Initial Sync**.

» Select **bigip2.mycompany.com (Self)**.

» Verify **Sync Device to Group** is selected.

» Select **Sync.** Sync status should now read In Sync

p. If a reboot is required:

» If you have a message indicating the system needs to reboot for some changes to take effect do the following:

» Right-click the BIG-IP virtual machine, select **Power**, and then click **Restart Guest**. Alternatively, you can reboot the system using the BIG-IP GUI by going to **System > Configuration > Device >** and then clicking **Reboot**.

Installing and configuring the iApp template

Use the following procedure to import the SSL certificate and key, as well as the iApp template, onto the BIG-IP system, and then configure the iApp template for Horizon View.

1. Login to the active BIG-IP system and import the Horizon View server SSL certificate and key you created in *Obtaining and installing the SSL certificate for your View environment on page 6* using the following guidance. The certificate and key must be in a location accessible by the BIG-IP system.
   a. On the Main tab, click **System** > **File Management** > **SSL Certificate List** > **Import**.
   b. From the Import Type list, select **PKCS 12 (IIS)**.
   c. In the **Certificate Name** field, type a name. In our example, we use **remote**.
   d. In the **Certificate Source** row, click **Choose File** and browse to the PCKS file you created on page 5.
   e. In the **Password** field, type the password you assigned.
   f. Click **Import**. The system imports the certificate and key.

2. Import the View optimized iApp template onto the BIG-IP system.
   a. On the Main tab, click **iApps** > **Templates**.
   b. Click the **Import** button on the right.
   c. Click the **Choose File** button and then browse to the location where you downloaded the iApp template. If you have not yet downloaded the iApp template, see Step 3 on page 4.
   d. Click **Upload**.

3. Create a new iApp Application service using the following guidance
   a. On the Main tab, click **iApps** > **Application Services**.
   b. Click the **Create** button.
   c. In the **Name** field, type a name for this application service. In our example, we use **view**.

d. From the Template list, select the **f5.vmware_view_optimized_solution.vx.x.x** template, where the x.x.x corresponds to the version of the iApp template, such as v1.2.1.

e. Read the welcome information and prerequisites.

4. Configuring the iApp template for Horizon View
Use the following guidance to help configure the iApp template. Each sub-step corresponds to a section of the iApp.

a. Configure the **Template Options** section

» *Inline Help*: We recommend leaving inline help set to **Show inline help text** unless you are already very familiar with this iApp template.

» *DNS Servers*: Specify the IP address of at least one DNS server unless you have already configured DNS services on the BIG-IP system outside of the iApp template. Some services, such as authentication, require server-to-IP resolution or IP-to-host name lookups to work properly. The BIG-IP system uses the list of servers you enter to resolve hosts to IP addresses or reverse lookup IP to hosts when required.

» *NTP Servers*: Specify the IP address of at least one NTP server unless you have already configured NTP on the BIG-IP system outside of the iApp template. You can specify the FQDN of a NTP server farm, or individual NTP server IP address(es).

b. Configure the **BIG-IP Access Policy Manager**

» *NAT address*: This is optional. If your remote clients use a network translated address to connect to the View environment, specify this IP address. Only enter a value if the remote IP address is translated on another device ***prior*** to communicating with the BIG-IP system.

» *NetBIOS domain*: Enter the NetBIOS domain(s) used for this Horizon View installation. In our domain example (view.mycompany.com), we use **view**.

» *AAA Server object*: The AAA Server performs user name look ups against Active Directory. If you already created an AAA server object outside of this iApp template, you select it from the list, otherwise, complete the following:

i). *Active Directory Servers*: Specify each of your Active Directory domain controllers, both FQDN and associated IP address, used for this View environment. Click the **Add** button for additional rows.

ii). *Active Directory domain name*: Specify the fully qualified domain name (FQDN) used for this View environment.

iii). *Anonymous binding*: Select whether anonymous binding is allowed in your Active Directory environment. If it is not allowed, specify an Active Directory user with administrative permissions in the fields that appear.

iv). *Health monitor*: Unless you have already created an Active Directory health monitor on this BIG-IP system, we recommend you allow the iApp template to create a new monitor. You can choose between no monitor, a simple ICMP ping monitor, or a more sophisticated Active Directory monitor. The Active Directory monitor requires a valid user account which it uses to login to each server as part of the health check.

If you choose the Active Directory monitor, we recommend creating a user account specifically for this health monitor that is set to never expire. Specify the user name and password in the appropriate fields, as well as the LDAP tree for the account. In the final monitor question, specify whether your Active Directory domain requires a secure protocol.

c. Configure **SSL Encryption**

» *Encrypted traffic*: There are two ways the BIG-IP system can handle encrypted traffic:

- SSL Offload: With SSL offload, traffic is encrypted to and from the client to the BIG-IP system. The BIG-IP system decrypts the traffic for processing, and then communicates with the View servers unencrypted. This offloads the task of processing SSL from the View servers, saving resources.

Important

To use SSL offload, you must configure your View servers to support unencrypted communication. See the instructions on page 14.

- SSL Bridging: With SSL bridging, traffic is encrypted to and from the client to the BIG-IP system. The BIG-IP system decrypts the traffic for processing, and then re-encrypts the traffic before sending it on to the View servers. Use this option if your View servers must receive encrypted traffic.

» *SSL Certificate*: No matter which method you choose, you must select the SSL Certificate you imported using the guidance in #1 on *page 22 .*

» *SSL key:* Select the associated key you imported.

d. Configure the **Virtual Servers and Pools**

» *Public IP address*: Specify the IP address your remote, untrusted clients will use to access the View servers.

» *Private IP address*: (Optional): Specify the IP address the local, trusted clients will use to access the View servers.

» *Port:* Specify the associated service port, if different than 443.

» *FQDN*: Specify the FQDN clients use to resolve to the remote and internal addresses. This solution uses a split DNS architecture where internal clients use local DNS which points the FQDN to the local trusted virtual server address, and remote clients use external DNS which points the same FQDN to the remote untrusted virtual server address.

» *Server IP addresses*: Specify the IP addresses of the View servers. In our example, we type the IP addresses for *con1.view.mycompany.com* and *con2.view.mycompany.com*.

e. Configure **Client optimization**

» *HTTP compression profile*: Select whether you want the system to compress HTTP responses. If you want the system to use compression, you can specify a compression profile you have already created, or use the F5 recommended compression profile.

f. Configure **Application Health**

» *Health Monitor*: Unless you have created a health monitor specifically for this implementation, leave the default: **Create a new health monitor**.

» *Interval:* Specify the interval at which the BIG-IP system should monitor the View servers. We recommend the default of 30 seconds.

5. Final steps

a. Synchronize the configuration of the BIG-IP systems.

» In the upper left corner of the BIG-IP system, click **Changes Pending**.

» Select the BIG-IP system with a status of **Changes Pending**.

» Click **Sync**.

» Verify the iApp configuration exists on the other BIG-IP system. Login to the system, and on the Main tab, click **iApp** > **Application Services**. You should see the application service you created.

b. High level review of objects iApp created

» On the Main tab, click **iApp** > **Application Services**. Click the application services you just created and you enter the Components view. On the right you see object type, and on the left you see the object name.

- There are five virtual servers:

1). <iApp_name>**_proxy_https**: Remote untrusted clients initiate connections to this virtual server. Note the BIG-IP APM Access Policy has been attached to this virtual server.

2). <iApp_name>**_apm_redirect**: If remote clients attempt to connect via HTTP, this virtual server automatically redirects them to HTTPS.
3). <iApp_name>**_pcoip_udp**: A PCoIP connection (UDP 4172) is initiated to this virtual server after the remote client successfully authenticates and makes a pool selection. BIG-IP APM translates the PCoIP connection back to the correct virtual desktop.
4). (Optional) <iApp_name>**_internal_https**: Local trusted clients initiate connections to this virtual server. Note internal connections are simply load balanced and authenticated by the individual View server to which they connect.

   Because APM is not proxying PCoIP connections, internal clients need to have route with appropriate port access to virtual desktop resources.

5). (Optional) <iApp_name>**_internal_redirect**: If internal clients attempt to connect via HTTP, this virtual server automatically redirects them to HTTPS.

- There is one Access Policy (policy enforcement for remote users): The <iApp_name>**_apm_access** policy has two branches
  1). If the BIG-IP APM detects the client is a View client, the user is directed down the first branch, where:
     » The user is authenticated via Active Directory.
     » If authentication is successful, the user is assigned a Connection server pool member and entitled View desktop pools are displayed to the user.
     » The View client behaves as though it had directly connected to the Connection server.

  2). If the BIG-IP APM detects the client is a browser, the user is directed down the second branch, where:
     » The user is presented a standard logon page
     » The credentials are sent to Active Directory for authentication
     » If authentication is successful, the user is assigned a Connection server pool member and entitled virtual desktop pools are displayed to the users via the F5 Dynamic Webtop.
     » When HTML Access has been enabled on selected pool, after the user selects an available pool they are presented with 3 possible options:
       - An option to launch the View Client and connect to selected pool
       - An option to connect using the HTML 5 client
       - An option to cancel
     » If HTML access has not been enabled for the selected pool, the View Client is launched and the user is directed to the selected virtual desktop pool.

Next steps

Once you have completed the entire configuration, verify the environment is working properly by creating client connections to the remote and local virtual servers. Verify the split DNS is properly, there are no SSL certificate warnings, and the Virtual Desktops display properly.

Troubleshooting

Q: *Why are available pool members being marked down after deploying the advanced health monitors?*

A: The advanced monitor created by the iApp template is unable to respond to disclaimer messages generated from Connection servers, which causes the monitor to mark servers down.

The next release of the iApp template will correct this behavior. Until that time, if you have disclaimer messages generated from Connection servers, you must either use the simple monitor option in the template (re-enter the template, and then from the "Create a new health monitor or use an existing one?" question, select "Create a Simple Monitor.") or use the BIG-IP APM to generate the disclaimer message and remove the disclaimer message from the Connection servers. See *ii). Should the BIG-IP system show a message to View users during logon? on page 15.*

Q: *Why are users getting multiple authentication prompts using the View Client?*
Why are the View desktop resources failing to render when connecting using a browser-based View connection?

A: These issues occur if you have a pre-authentication message configured on your VMware Connection servers. Because BIG-IP APM displays a login prompt for the client, you must disable the **Display a pre-login message** setting on the VMware Horizon View server (see *https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-third-party-integration-implementations-11-6-0/7.html* for more required settings for VMware Horizon View).

If you are experiencing this issue, you can disable the pre-authentication message on the View Connection servers. If you require a pre-authentication message, we recommending using the full View iApp template: *https://support.f5.com/kb/en-us/solutions/public/15000/000/sol15041.html*, and the associated deployment guide: *http://www.f5.com/pdf/deployment-guides/vmware-view5-iapp-dg.pdf*.

Document Revision History

Version	Description	Date
RC-1	New deployment guide	04-01-2014
RC-1a	Added support for Horizon View 6.0, with a note that BIG-IP APM currently does not support publishing and providing remote connectivity to the RDS hosted applications feature in Horizon View 6.0.	07-14-2014
1.0	Updated the guide for the fully supported iApp f5.vmware_view.optimized.solution.v1.1.1 available on downloads.f5.com.	07-16-2014
1.1	- Added support for BIG-IP v11.6. - Added the section *Modifying the iApp configuration if using BIG-IP v11.6* with a required change to the iApp configuration if using 11.6.0.	09-03-2014
1.2	- Updated the guide for iApp version f5.vmware_view.optimized.solution.v1.2.0rc1. - Removed the section *Modifying the iApp configuration if using BIG-IP v11.6* as the issue is fixed in v1.2.0rc1 of the iApp - Marked the private IP address setting as optional. The iApp now gives the optional ability to configure a virtual server for internal, trusted clients.	09-23-2014
1.3	- Updated this guide to reference iApp version f5.vmware_view.optimized.solution.v1.2.0rc2 available on downloads.f5.com in the RELEASE-CANDIDATE folder. All changes are contained in the release candidates described above.	10-06-2014
1.4	- Modified the Product and version footnote on page 1 to mention an engineering hotfix is available from F5 technical support for BIG-IP v11.6 which enables the View Remote App publishing feature.	12-08-2014
1.5	Updated this guide for the fully supported iApp f5.vmware_view.optimized.solution.v1.2.0 available on downloads.f5.com. All changes were contained in the Release Candidate iApps.	12-16-2014
1.6	Added a new a new section, *Troubleshooting on page 26*, with an entry concerning pool members being unavailable after deploying advanced health monitors.	02-11-2015
1.7	Updated this guide for the fully supported iApp f5.vmware_view.optimized.solution.v1.2.1 available on downloads.f5.com. There were no new features in this release, only the following fixes: - The iApp now correctly uses Source IP persistence when an internal virtual server is used - The iApp now allows using advanced monitors when BIG-IP APM is not used, by asking an additional question about the NetBIOS name. Previously, the iApp would display a script error. - The iApp no longer displays a script error when in LTM only mode. Previously, the iApp would display an error when BIG-IP APM was not provisioned. - Modified the note in the Product version table on page 1 to state that support for the View Remote App publishing feature is available in BIG-IP v11.6 HF-4 and later.	04-09-2015
1.8	Added support for VMware Horizon View 6.1, with the exception that BIG-IP APM currently does not support the Horizon View HTML5 client in Horizon View 6.1.	04-30-2015
1.9	- Added a footnote to the Product and Version table page 1 to mention that BIG-IP APM does not support proxying the VMware View RDP protocol.	05-20-2015
1.9.1	Added a new a new entry to *Troubleshooting on page 26*, concerning possible issues when using APM with pre-authentication messages configured on the View Connection servers.	06-22-2015

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com