Deployment Guide

Document Version: 1.0

What's inside:

2 Configuration example

4 Securing the iSession deployment

6 Downloading and importing the new iApp

6 Configuring the BIG-IP systems using the Cloud Connector iApp

7 Configuring the remote data center LTM VE

10 Configuring the local data center BIG-IP LTM

12 Next steps

13 Document Revision History

Configuring a single-tenant BIG-IP Virtual Edition in the Cloud

Welcome to the F5 deployment guide for Cloud Connector with BIG-IP v11.3.0. This guide shows how to configure the BIG-IP Virtual Edition (VE) running the WAN Optimization Manager (WOM) in a cloud connector deployment.

This document provides guidance for using a BIG-IP iApp Template to quickly and accurately configure BIG-IP networking objects and WAN optimization for a single tenant BIG-IP VE launched in the cloud. You can also use the template to configure WAN optimization alone.

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

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

Products and versions tested

Product	Version
BIG-IP LTM	v11.3

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.

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:

- For this deployment guide, the BIG-IP LTM system must be running version 11.3 or later

- If the two BIG-IP LTM systems have a firewall between them, then port 443 must be open in both directions for the WAN Optimization to work.
- The Cloud Connector iApp requires SSL encryption to secure the endpoints of the iSession connection. To secure the endpoints, you must import a WOM-specific root certificate from a trusted certifying authority. See *Securing the iSession deployment on page 4.*
- The WAN Optimization configuration supports TCP only. For that reason, you can use only NFSv4 (not v2 or v3)
- When configuring the local BIG-IP system using the iApp, you must have a fully-configured LTM, including VLANs and Self IP addresses, as well as at least one virtual server with an associated load balancing pool.
- Using an iApp to configure shared networking configuration (such as VLANs, Self IPs, default routes, and WAN Optimization) is generally not recommended. This iApp was developed for the special case of a single tenant VE LTM in the cloud where this iApp is used for initial setup and is not deleted. Thus, additional applications can use the resources configured by the iApp.
- This deployment guide shows how to configure the BIG-IP WOM devices using the iApp template. For manual configuration instructions, refer to the BIG-IP WOM documentation, available on Ask F5: *http://support.f5.com/kb/en-us/products/wan_optimization.html*.

Configuration example

The following is a logical diagram example of the configuration of a BIG-IP LTM system configured for Cloud Connector.

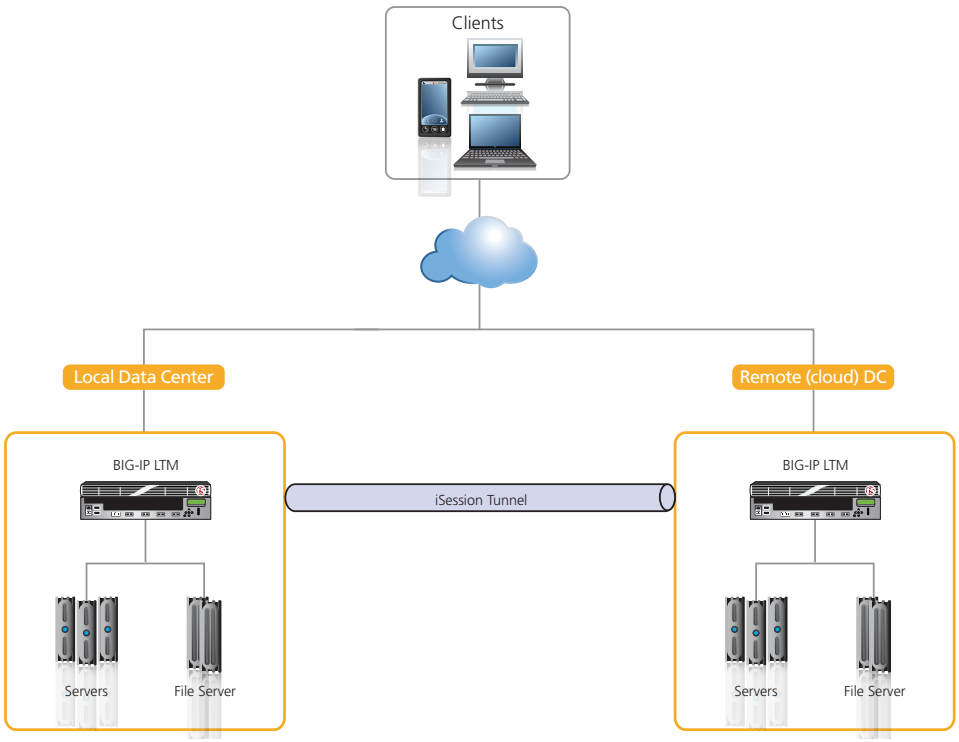

Figure 1: *Logical configuration example*

Preparation Worksheet

To prepare to use the iApp for Cloud Connector, you need to gather some information, such as the interfaces for internal and external VLAN on the LTM VE and IP addresses. Use the following worksheets to record the information but do not enter it until requested to do so by the procedures.

For more information on these objects, see the online help or the BIG-IP WOM documentation.

BIG-IP object	Primary Data Center	Remote/Cloud Data Center
VLAN (Internal) name		
- Interface		
- Self IP address		
VLAN (External) name		
- Interface		
- Self IP address		
Remote Endpoint IP Address		
Local Endpoint IP Address		
Advertised Routes		
VLAN (LAN facing) name		
Inbound SSL certificate for iSession		
Outbound SSL certificate for iSession		

Securing the iSession deployment

As mentioned in the prerequisites, the Cloud Connector iApp requires a secure iSession™ deployment; you must use SSL encryption to secure the endpoints of the iSession connection. To secure the endpoints while configuring the iApp, you must first import SSL a WOM-specific root certificate from a trusted certifying authority, and then use that certificate to create an SSL profile.

The process of securing a WAN optimization deployment using SSL includes importing a certificate for each endpoint, and then specifying this certificate (along with its associated key) in WOM-related profiles and settings on the system.

The following tasks are manual steps that must be performed before you can run the iApp.

Generating and importing SSL certificates for a secure iSession connection

In the following procedure, you generate and import SSL certificates on both systems.

To generate and import SSL certificates

1. Generate a root certificate using external CA software such as the freeware program SimpleCA or OpenSSL.
2. Import the generated root certificate into both BIG-IP WOM systems.
3. On one of the BIG-IP systems, complete the following steps:
   a. On the Main tab, expand **System** and then click **File Management > SSL Certificate List > Import**.
   b. From the **Import Type** list, select **Certificate**.
   c. For **Certificate Name**, click **Create New** and then type **wom-root-ca**.
   d. For **Certificate Source**, either click **Upload File** and provide a file name by typing or browsing to the file, or click **Paste Text**, and paste text copied from another source into the text box.
   e. Click **Import**.
   f. Repeat these steps on the other BIG-IP system.
4. Create a certificate and key on one of the BIG-IP systems.
   a. On the Main tab, expand **System** and then click **File Management > SSL Certificate List**.
   b. Click the **Create** button.
   c. For Name, type **wom-endpoint-ca**.
   d. From the **Issuer** list, select **Certificate Authority**.
   e. For **Common Name**, type the **wom-endpoint-ca**.
   f. Provide any additional information required by your organization.
   g. Click **Finished**. The Certificate Signing Request screen opens.
   h. On the Certificate Signing Request screen, copy or download the certificate signing request for the certificate created in the previous step and use it to generate a signed certificate using your external CA and the CA certificate generated in step 1.
5. Import the generated certificate into the BIG-IP WOM system.

a. On the Main tab, expand **System** and then click **File Management > SSL Certificate List**.
b. Click **wom-endpoint-ca** (the certificate created in step 4).
c. Select the file **wom-endpoint.crt**.
d. Click **Import**.

6. Repeat steps 4 and 5 on the other BIG-IP system.

Customizing SSL profiles for a secure iSession connection

In the following procedure, you create custom server and client SSL profiles to use in securing iSession connections. Perform the procedure on both the local and the remote BIG-IP LTM systems.

To create a customized Server SSL profile

1. On the Main tab, expand **Local Traffic** and then click **Profiles > SSL > Server**.
2. Click the **Create** button.
3. In the **Name** box, type **wom-endpoint-serverssl**.
4. From the **Configuration** list, select **Advanced**, and then click the **Custom** check box on the right.
5. From the **Certificate** list, select **wom-endpoint-ca**.
6. From the **Key** list, select **wom-endpoint-ca**.
7. In the Server Authentication section click the **Custom** check box.
8. From the **Server Certificate** list, select **require**.
9. From the **Trusted Certificates Authorities** list, select **wom-root-ca**.
10. Click **Finished**.

To create a customized Client SSL profile.

1. On the Main tab, expand **Local Traffic** and then click **Profiles > SSL > Client**.
2. Click the **Create** button.
3. In the **Name** box, type **wom-endpoint-clientssl**.
4. From the **Configuration** list, select **Advanced**, and then click the **Custom** check box on the right.
5. From the **Certificate** list, select **wom-endpoint-ca**.
6. From the **Key** list, select **wom-endpoint-ca**.
7. In the Server Authentication section click the **Custom** check box.
8. From the **Server Certificate** list, select **require**.
9. From the **Trusted Certificates Authorities** list, select **wom-root-ca**.
10. Click **Finished**.

Downloading and importing the new iApp

The first task is to download and import the Cloud Connector iApp template.

To download and import the iApp

1. Open a web browser and enter the following URL (you may be required to login or complete a free registration):
   https://devcentral.f5.com/wiki/iApp.Codeshare.ashx#_FF_Contributed_iApp_Templates__2
2. In the F5 Contributed iApp Templates section, click **Cloud Connector**.
3. Download the Cloud Connector iApp to a location accessible from your BIG-IP system.
4. Extract (unzip) the **Cloud Connector** zip file.
5. Log on to the BIG-IP system web-based Configuration utility, and then perform the following:
   a. On the Main tab, expand **iApp**, and then click **Templates**.
   b. Click the **Import** button on the right side of the screen.
   c. Click the **Browse** button, and then browse to the location you saved the iApp file.
   d. Click the **Upload** button.
6. Perform step 6 on the other BIG-IP system.

The iApp is now available for use.

Configuring the BIG-IP systems using the Cloud Connector iApp

The Cloud Connector template operates in two modes: local and remote.

- In remote mode, the template sets up all networking (VLANs, Self IPs, routes, and a WOM endpoint) for a remote data center (single-tenant LTM VE).
  See *Configuring the remote data center BIG-IP VE system on page 7*
- In local mode, the template configures WAN optimization and the WOM iSession and WOM virtual sessions in the local data center where the networking is already configured.
  See *Configuring the local data center BIG-IP system on page 10.*

Configuring the remote data center BIG-IP VE system

Use this section to configure the BIG-IP system in the remote data center.

To configure the remote data center BIG-IP VE

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name.
5. From the **Template** list, select **f5.cloud_connector**.
   The Cloud Connector template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list, you see Device and Traffic Group options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Networking configuration

This main section of the template asks questions about your networking configuration.

1. ***Is this the local data center?***
   Select **No**. In this section, we are configuring the remote data center BIG-IP system.
2. ***Configure an internal Self IP?***
   Select **Yes** to configure the internal Self IP. Answer the following:
   a. **Do you want to create a new VLAN or use an existing one?**
      » Create new VLAN
      Unless you have already created a VLAN for the internal self IP, select **Create New VLAN**.
      - *On which interface is the internal VLAN?*
        From the list, select the appropriate interface.
      - *Is this a tagged interface?*
        From the list, select **Yes** or **No**, depending on your network.
        If you select Yes, specify the tag value in the box that appears.

» Use VLAN
If you have already created a VLAN for the internal Self IP, select **Use VLAN**.

- *Which VLAN is the internal VLAN?*
  From the list, select the internal VLAN.

b. **What is the internal Self IP address?**
Type the internal Self IP address in the box.

c. **What is the mask for the internal Self IP address?**
If necessary, type the mask for the internal Self IP address. The default is **255.255.255.0**.

3. ***Configure an External Self IP?***
Select **Yes** to configure the External Self IP. Answer the following:

a. **Do you want to create a new VLAN or use an existing one?**

» Create new VLAN
Unless you have already created a VLAN for the external self IP, select **Create New VLAN**.

- *On which interface is the external VLAN?*
  From the list, select the appropriate interface.
- *Is this a tagged interface?*
  From the list, select **Yes** or **No**, depending on your network.
  If you select Yes, specify the tag value in the box that appears.

» Use VLAN
If you have already created a VLAN for the external Self IP, select **Use VLAN**.

- *Which VLAN is the external VLAN?*
  From the list, select the external VLAN.

b. **What is the external Self IP address?**
Type the external Self IP address in the box.

c. **What is the mask for the external Self IP address?**
If necessary, type the mask for the external Self IP address. The default is **255.255.255.0**.

4. ***Configure a default gateway?***
Select whether you want the iApp to configure a default gateway. If you have already configured a default gateway on the BIG-IP system, you must select No.

Important →

There can only be one default gateway per BIG-IP system. This is generally a shared resource, and should only be configured with this template if ownership by this iApp will not affect other applications

If you do not want the iApp to configure the default gateway, continue with #5.

a. **What is the default gateway IP address?**
Type the IP address of the default gateway.

5. ***What is the WOM endpoint address?***
Specify the endpoint address for this BIG-IP WOM device. This should be the same IP address as the Internal Self IP address you configured in #2b.

Important

There can only be one WOM endpoint and one remote WOM endpoint per BIG-IP system. These are generally shared resources and should only be configured with this template if ownership by this iApp will not affect other applications.

6. ***What is the remote WOM endpoint address?***
   Specify the endpoint address for the other BIG-IP WOM device.

7. ***What is the WOM advertised route?***
   Type the IP address for the advertised route. An advertised route is a subnet that can be reached through the local endpoint.

8. ***What is the mask for the WOM advertised route?***
   If necessary, type the mask for the advertised route. The default is **255.255.255.0**.

9. ***What is the outbound iSession to WAN?***
   From the list, select the Server SSL profile you created for this BIG-IP system in *To create a customized Server SSL profile on page 5*. In our example, this is **wom-endpoint-serverssl**.

10. ***What is the inbound iSession from WAN?***
    From the list, select the Client SSL profile you created for this BIG-IP system in *To create a customized Client SSL profile. on page 5*. In our example, this is **wom-endpoint-clientssl**.

Finished

Review your answers to the questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Creating virtual services on the BIG-IP system

The next task is to create Application services on the BIG-IP system, using the appropriate F5 iApp template for your application.

To create virtual services

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click **Create**.
3. In the **Name** box, type a unique name for the application service.
4. From the **Template** list, select the appropriate template.

For more information about creating application services, see the online help or the deployment guide associated with the application (*www.f5.com/products/documentation/deployment-guides/*).

Configuring the local data center BIG-IP system

Use this section to configure BIG-IP WAN optimization on the BIG-IP system in the local data center.

As mentioned in the prerequisites, you must have an existing BIG-IP system configuration including VLANs and Self IP addresses, as well as at least one virtual server with an associated load balancing pool.

To configure the local data center LTM VE

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name.
5. From the **Template** list, select **f5.cloud_connector**.
   The Cloud Connector template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list, you see Device and Traffic Group options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Networking configuration

This main section of the template asks questions about your networking configuration.

1. ***Is this the local data center?***
   Select **Yes**. In this section, we are configuring the local data center BIG-IP system.
2. ***What is the WOM endpoint address?***
   Specify the endpoint address for this BIG-IP WOM device.

   Important →

   There can only be one WOM endpoint and one remote WOM endpoint per BIG-IP system. These are generally shared resources and should only be configured with this template if ownership by this iApp will not affect other applications.
3. ***What is the remote WOM endpoint address?***
   Specify the endpoint address for the other (remote) BIG-IP WOM device.

4. ***What is the WOM advertised route?***
   Type the IP address for the advertised route. An advertised route is a subnet that can be reached through the local endpoint.

5. ***What is the mask for the WOM advertised route?***
   If necessary, type the mask for the advertised route. The default is **255.255.255.0**.

6. ***Which VLAN do you want to use for LAN traffic?***
   Select the name of the internal VLAN.

7. ***What is the outbound iSession to WAN?***
   From the list, select the Server SSL profile you created for this BIG-IP system in *To create a customized Server SSL profile on page 5*. In our example, this is **wom-endpoint-serverssl**.

8. ***What is the inbound iSession from WAN?***
   From the list, select the Client SSL profile you created for this BIG-IP system in *To create a customized Client SSL profile. on page 5*. In our example, this is **wom-endpoint-clientssl**.

Finished

Review your answers to the questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the service you just created. To see the list of all the configuration objects created to support this configuration, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying the iApp configuration

If you find it necessary to make changes to the configuration, you can modify the iApp application service quickly and easily. F5 has implemented a Strict Updates feature that prevents direct modification of a generated configuration. With Strict Updates, the only way to update the configuration is by using the iApp Application Service.

Important → *You can disable Strict Updates, but use extreme caution in doing so. Results can be unpredictable.*

iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Cloud Connector Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the configuration objects created by the iApp template.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics, see the online help or product documentation.

Document Revision History

Version	Description	Date
1.0	New document	12-17-2012

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