BIG-IP® Virtual Edition Setup Guide for VMware ESX® or ESXi®

Version 11.0

Table of Contents

Legal Notices

Publication Date

This document was published on August 2, 2013.

Publication Number

MAN-0347-01

Copyright

Trademarks

Patents

This product may be protected by U.S. Patents 6,374,300; 6,473,802; 6,970,733; 7,197,661; 7,287,084; 7,975,025; 7,996,886; 8,004,971; 8,010,668; 8,024,483; 8,103,770; 8,108,554; 8,150,957. This list is believed to be current as of August 2, 2013.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Chapter 1

Getting Started with BIG-IP Virtual Edition

What is BIG-IP Virtual Edition?

BIG-IP® Virtual Edition (VE) is a version of the BIG-IP system that runs as a virtual machine (VM) in specifically-supported hypervisors (VMware ESX® or ESXi® for this guide). BIG-IP VE emulates a hardware-based BIG-IP system running a VE-compatible version of BIG-IP® software.

Note: *The BIG-IP VE product license determines the maximum allowed throughput rate. To view this rate limit, you can display the BIG-IP VE licensing page within the BIG-IP Configuration utility. Lab editions have no guarantee of throughput rate and are not supported for production environments.*

BIG-IP Virtual Edition compatibility with VMware hypervisor products

BIG-IP® Virtual Edition (VE) is compatible with VMware ESX® 4.0 and 4.1, and VMware ESXi® 4.0 and 4.1 update 1 hosts.

Important: *BIG-IP® Virtual Edition (VE) does not support hypervisors other than those identified in this guide, and installation attempts on these platforms might be unsuccessful.*

Hypervisor guest definition

The VMware virtual machine guest environment for the BIG-IP® VE, at minimum, must include the following:

- 2 x virtual CPUs (reserve 2 GHz)
- 4 GB RAM with a 2-core CPU
- 8 GB RAM with a 4-core CPU
- 2 GB RAM with 2-core CPU (upgrade path from version 10.2.x)
- 1 x virtual Flexible (PCnet32 LANCE) network adapter (for management)
- 3 x virtual VMXNET3 network adapters
- 1 x 100 GB SCSI disk, by default
- 1 x 50 GB SCSI disk, as an extra disk option

A secondary disk is recommended and might be required for certain BIG-IP® modules.

When upgrading from version 10.2.x, change the configuration to at least 4 GB of RAM.

Important: *Not supplying at least the minimum virtual configuration limits will produce unexpected results.*

For production licenses, F5 Networks suggests using the maximum configuration limits for the BIG-IP® VE system. Reservations can be less for lab editions.

There are also some maximum configuration limits to consider for deploying a BIG-IP VE virtual machine, such as:

- CPU reservation can be up to 100 percent of the defined virtual machine hardware. For example, if the hypervisor has a 3 GHz core speed, the reservation of a virtual machine with 2 CPUs can be only 6 GHz or less.
- RAM reservation can be only 2, 4, or 8 GB.
- For production environments, virtual disks should be deployed Thick (allocated up front). Thin deployments are acceptable for lab environments.

Chapter 2

Deploying BIG-IP Virtual Edition

Deployment of BIG-IP VE on VMware

To deploy the BIG-IP® VE system on a VMware ESX® or ESXi®, you need to perform these tasks:

- Verify the host machine requirements.
- Deploy an instance of the BIG-IP system as a virtual machine (VM) on a host system.
- Power on the BIG-IP VE virtual machine.
- Assign a management IP address to the BIG-IP VE virtual machine.

After you complete these tasks, you can log in to the BIG-IP VE system and run the Setup utility. Using the Setup utility, you can perform basic network configuration tasks, such as assigning VLANs to interfaces.

Host machine requirements and recommendations

There are specific requirements for the host system to run successfully on the BIG-IP® VE system.

To successfully deploy and run the BIG-IP VE system, the host system requires:

- VMware ESX 4.0 or 4.1, or ESXi 4.0 or 4.1 with update 1
- VMware vSphere™ Client
- Connection to a common NTP source (this is especially important for each host in a redundant system configuration)

Important: *The hypervisor CPU must meet the following requirements:*

- use 64 bit architecture
- support for virtualization (AMD-V™ or Intel® VT-x) must be enabled
- support a one-to-one thread-to-defined virtual CPU ratio, or (on single-threading architectures) support at least one core per defined virtual CPU
- Intel processors must be from the Core (or newer) workstation or server family of CPUs

Deploying the BIG-IP VE virtual machine

The first steps in deploying BIG-IP® Virtual Edition (VE) are to download and extract the Zip file to your local system. Next, you can run the Deploy OVF Template wizard from within the VMware vSsphere™ Client. Note that the Zip file contains a virtual disk image based on an Open Virtual Format (OVF) template. Follow the steps in this procedure to create an instance of the BIG-IP system that runs as a virtual machine on the host system.

Important: *Do not modify the configuration of the VMware guest environment with settings less powerful than the ones recommended in this document. This includes the settings for the CPU, RAM, and network adapters. Doing so might produce unexpected results.*

1. In a browser, open the F5 Downloads page (`https://downloads.f5.com`).
2. Download the BIG-IP VE file package ending with `scsi.ova.zip`.
3. Extract the files from the Zip archive.
4. From the File menu, choose Deploy OVF Template.
   The Deploy OVF Template wizard starts.
5. In the Source pane, click **Deploy from file**, and, using the **Browse** button, locate the OVA file.

For example: `\MyDocuments\Work\Virtualization\<BIG-IP_OVA_filename>`

6. Click **Next**.
   The OVF Template Details pane opens.
7. Verify that the OVF template details are correct, and click **Next**.
   This displays the End-User License Agreement (EULA).
8. Read and accept the license agreement, and click **Next**.
   The Name and Location pane opens.
9. In the **Name** field, type a name for the BIG-IP virtual machine, such as: `smith_10.2.2.1-45`.
10. In the Inventory Location pane, select a folder name. Click **Next**.
11. If the host system is controlled by VMware vCenter, the Host Cluster screen opens. Choose the preferred host and click **Next**. Otherwise, proceed to the next step.
12. Map the source network **Management Network** to the name of a destination management network in your inventory. An example of a destination management network is **Management**.
13. Map the source network **Internal Network** to the name of a destination non-management network in your inventory. An example of a destination internal network is **Private Access**.
14. Map the source network **External Network** to the name of an external network in your inventory. An example of a destination external network is **Public Access**.
15. Map the source network **HA** to the name of a high-availability network in your inventory. An example of a destination high-availability network is **HA**.
16. Click **Next**.
    The Ready to Complete screen opens.
17. Verify that all deployment settings are correct, and click **Finish**.

Powering on the BIG-IP VE virtual machine

You must power on the BIG-IP® VE virtual machine (VM) before you can move on to assigning IP addresses.

1. In the main vSphere™ Client window, click the Administration menu.
2. Select the virtual machine that you want to power on.
3. Click the Summary tab, and in the Commands area, click **Power On**.
   The BIG-IP VE status icon changes to indicate that the VM is on. Note that the BIG-IP VE will not process traffic until you start the BIG-IP VE from its command line or through its web interface.

Assigning a management IP address to a BIG-IP VE virtual machine

The BIG-IP® VE virtual machine (VM) needs an IP address assigned to its virtual management port.

1. After a few seconds, a login prompt appears.
2. At the password prompt, type `default`.
3. Type `config` and press Enter.
   The F5 Management Port Setup screen appears.
4. Click **OK**.
5. If you want DHCP to automatically assign an address for the management port, select **Yes**. Otherwise, select **No** and follow the instructions for manually assigning an IP address and netmask for the management port.

6. When assigned, the management IP address will appear in the Summary tab of the vSphere™ Client. Alternatively, a hypervisor generic statement can be used, such as `tmsh list sys management-ip`.

Tip: *F5 Networks highly recommends that you specify a default route for the virtual management port, but it is not required for operation of the BIG-IP VE virtual machine.*

Chapter 3

Updating a BIG-IP VE Virtual Machine

Updating a BIG-IP VE virtual machine

BIG-IP® VE updates are installed in the same manner as updates to BIG-IP software already installed on BIG-IP hardware. You do not need to reinstall BIG-IP VE in the hypervisor guest environment to upgrade your system. To update a BIG-IP VE virtual machine (VM), you can use the Software Management tool in the Configuration utility, or you can upgrade the software from the command line. The update procedure described in this guide uses the Software Management tool.

Downloading and importing a BIG-IP VE update

1. In a browser, open the F5 Downloads page (`https://downloads.f5.com`).
2. Download the version's base ISO file, such as `10.2.1`, and its associated MD5 checksum file.

   Important: *The BIG-IP VE base ISO file for the associated hotfix version must be in the* `/shared/images` *directory of the BIG-IP VE virtual machine before any updates can apply.*

3. Download the update ISO file, such as `Hotfix-BIGIP-10.2.1-511.0-HF3.iso`, and its associated MD5 checksum file.
4. Save the four files to the BIG-IP® VE virtual machine in the `/shared/images` directory.

   Attention: *Before you perform the installation, F5 recommends that you test the integrity of the ISO files to verify that you have downloaded clean copies. Use an MD5 verification program to ensure that the downloaded ISO files checksums match the values in their corresponding MD5 files.*

5. On the Main tab, expand **System**, and click **Software Management**.
   The Software Management screen opens.
6. At the right-side of the screen, click **Import**.
   The Import Software Image screen opens.
7. Click **Browse** to navigate to the downloaded installation file.
8. When the image name appears in the **Software Image** field, click **Import** to begin the operation.

   Important: *If you navigate away from this screen before the operation completes, the system might not import the image successfully. Therefore, F5 recommends that you wait for the operation to complete before continuing with any other work on the BIG-IP VE system.*

   The system presents a progress indicator during the operation.

Installing a BIG-IP VE update

After you download the software installation image and import the software image to the `/shared/images` directory on the BIG-IP® VE system, you can initiate the installation operation. The destination you specify for installation must represent a hard drive volume or partition on the BIG-IP system.

1. On the Main tab of the navigation pane, expand **System**, and click **Software Management**.
   The Software Management screen opens.
2. From the Available Images table, select the software image you want to install.
   The image properties screen opens.

3. Click **Install**.
   The Install Software screen opens.
4. Select the disk you want to install the image on, and type or select a volume name and click **Install**.
   The upgrade process installs the software on the inactive disk location that you specify. This process usually takes between three and ten minutes.

   Tip: *If there is a problem during installation, you can use log messages to troubleshoot a solution. The system stores the installation log file as* `/var/log/liveinstall.log`.

   The software image will be installed.

Rebooting after a BIG-IP VE update

When the installation operation is complete, the system removes the refresh options. When that occurs, you can safely reboot into the newly installed volume or partition.

1. On the Main tab of the navigation pane, expand **System**, and click **Software Management**.
   The Software Management screen opens.
2. On the menu bar, click **Boot Locations**.
   The Boot Locations screen opens.
3. In the Boot Partition column, click the link representing the boot location you want to activate.
   The properties screen for the boot location opens.
4. Click **Activate**.
   A confirmation screen opens.
5. Click **OK** to initiate the reboot operation.
   The system presents progress messages during the restart operation.

When the BIG-IP® VE system reboot is complete, the system presents the login screen. To configure the system, log in using an account that has administrative permissions.

Appendix
A

Deployment Best Practices

Best practices for deploying BIG-IP VE on VMware

When deploying BIG-IP® Virtual Edition (VE) on a VMware host, use these best practices.

Issue	Recommendation
Redundant system configuration	Run the two units of an active/standby pair on separate physical hosts. You can accomplish this in two ways: either manually create a virtual machine peer on each host, or, if you are using VMware Dynamic Resource Scheduler (DRS), create a DRS rule with the option **Separate Virtual Machine** that includes each unit of the BIG-IP® VE redundant pair.
Live migration of BIG-IP VE virtual machines	Perform live migration of BIG-IP VE virtual machines on idle BIG-IP VE virtual machines only. Live migration of BIG-IP VE while the virtual machine is processing traffic could produce unexpected results.
VMware DRS environments	In DRS environments, perform live migration of BIG-IP VE virtual machines (using VMware vMotion™) on idle BIG-IP VE virtual machines only. Live migration of BIG-IP VE while the virtual machine (VM) is processing traffic could produce unexpected results. Disable automatic migrations by adjusting the DRS Automation Level to **Partially Automated**, **Manual**, or **Disabled** on a per BIG-IP VE basis.
Resource reservations	By default, BIG-IP VE is deployed with a 2000 or 4000 MHz CPU and 2, 4, or 8 GB of memory reservation. Together, these reservations typically prevent system instability on heavily loaded hosts and are considered minimal. The CPU reservation can be up to 100 percent of the defined virtual machine hardware. For example, if the hypervisor has a 3 GHz core speed, the reservation of a virtual machine with 2 CPUs can be only 6 GHz or less.

Appendix
B

Unsupported BIG-IP Features

- *BIG-IP VE unsupported features*

BIG-IP VE unsupported features

BIG-IP® Virtual Edition (VE) does not support specific BIG-IP system or VMware features.

These BIG-IP system features are not supported by BIG-IP Virtual Edition (VE).

- Optional BIG-IP system modules, such as:
  - Link Controller™ (LC™)
- Advanced SSL functions
- Bridging protocols, such as:
  - Spanning Tree Protocol (STP)
  - Rapid Spanning Tree Protocol (RSTP)
  - Multiple Spanning Tree Protocol (MSTP)
- Link Aggregation Control Protocol (LACP)
- Hard-wired failover
- Federal Information Processing Standards (FIPS) 140-2

These VMware features are not supported by BIG-IP VE:

- VMware Fault Tolerance technology
- `vmmemctl` memory balloon driver
- Memory snapshots

Appendix
C

Troubleshooting BIG-IP Virtual Edition

Troubleshooting BIG-IP Virtual Edition

If you have followed the setup procedures as described in this guide, BIG-IP® VE should be working correctly with the hypervisor. However, because BIG-IP VE emulates BIG-IP hardware running in a virtual environment, you might encounter some issues as you try new configurations for BIG-IP VE that are outside the scope of this setup guide, or unsupported in BIG-IP VE with certain hypervisor environments. Use this troubleshooting information to solve problems and address limitations that you might encounter with BIG-IP VE.

Event log reports insufficient video RAM

On VMware ESXi systems only, the following event message is logged:
The maximum resolution of the virtual machine will be limited to 1176x885 at 16 bits per pixel. To use the configured maximum resolution of 2360x1770 at 16 bits per pixel, increase the amount of video RAM allocated to this virtual machine by setting svga.vramSize="16708800" in the virtual machine's configuration file.
You can ignore this message or follow the recommended action without adverse effects.

Time synchronization using VMware Tools or NTP protocol

If you want to use VMware Tools to enable time synchronization, you must select the **Synchronize guest time with host** check box within vSphere Client. If you want to use network time protocol (NTP) instead, you must first disable time synchronization in VMware Tools by clearing the check box within vSphere Client. For more information, see the VMware vSphere™ Client documentation. Note that the two units of a BIG-IP VE redundant system configuration must share the same time synchronization source.

Incorrect status of VMware Tools in vSphere

VMware vSphere incorrectly shows the status of VMware Tools as **Not Installed**. You can verify that VMware Tools are installed by viewing the **IP Address** and **DNS Name** fields on the vSphere screen. Note that if you migrate the virtual machine or start a snapshot or cloned image of the virtual machine, the status correctly shows as **Unmanaged**.

Lack of VMXNET3 availability

The VMXNET3 driver can become unavailable after you suspend and resume BIG-IP VE. Resetting the BIG-IP VE will resolve the problem.

Use of VLAN groups

Use of VLAN groups with BIG-IP VE requires proper configuration of the VMware vSwitch. To use the VLAN group feature, you must configure security policies on the vSwitch. The properties of the security policy that you need to configure are **Promiscuous Mode** and **Forged Transmits**. For any transparency mode, you must configure these properties to accept (rather than reject) the security policy exceptions on the vSwitch. For information about how to configure these options, see the *VMware ESX® or ESXi® Configuration Guide*.

Use of Single Configuration File (SCF) feature

Copying an SCF from a VMware host system to an F5 hardware platform causes an error related to interface mismatching. Edit the SCF and remove speed and duplex media statements from the network interface statements before importing.

Configuration of an OVF with additional interfaces

When you deploy an OVF with more than five interfaces (one management interface and more than four TMM interfaces), the interface numbering might appear out of order. To view the actual TMM-to-vSwitch portgroup interface mapping, compare the MAC addresses of the interfaces displayed in the BIG-IP Configuration utility to those displayed in the vSphere Client.

If you change the number of virtual interfaces on the BIG-IP VE system after a binary MCPD database has been created, the system does not detect the change when subsequently rebooted. To ensure that the system properly detects the new or removed interfaces, type the command `rm /var/db/mcpd*` at the BIG-IP VE command prompt, and reboot the system.

HA events due to BIG-IP VE inactivity

If the VMware hypervisor runs the BIG-IP VE software for fewer than four minutes continuously (for example, due to a manual suspension or the timeout of network disk I/O), high-availability failure events occur. The system might note a failure and restart key system processes and trigger failover if within a high-availability (HA) group. This is intended system behavior.

VMware vSwitch Promiscuous Mode

When the VMware vSwitch **Promiscuous Mode** is set to **Reject**, the VLAN group transparency mode, **Opaque**, will not be able to pass packets.

Virtual network interface status is wrong

The BIG-IP VE system reports the status of host-only network interfaces as UNINITIALIZED, even though the interface is functioning normally.

Auto-licensing and the default management route

If you have not defined a default route to the management port, the default interface `1.1` is used, which does not work. To prevent this from occurring, verify that you have defined a default route for the management port before attempting to activate a license.

BIG-IP licensing and User Configuration Sets

When you import a User Configuration Set (UCS) from another BIG-IP system or BIG-IP VE system, the system overwrites the local license with the license contained in the UCS. To work around this issue, you can re-license the local system after importing the UCS by accessing a backup copy of the license file, located in `/config/bigip.license.bak`. Also, when importing a UCS, ensure that the host names of the two systems differ. When the host names differ, the system correctly imports only the configuration data that is common to both the originating platform and the target platform. If the host names match, the system attempts to import all of the UCS configuration data, which can cause the import process to fail.

Use of SNMP OID for RMON tables

Setting the source OID for RMON alarm, event, and history tables generates an error message. This OID will be disabled in future releases.

Media speed messages in log file

When starting the BIG-IP VE system or when removing an interface from a VLAN, the system logs media-related messages to the file `/var/log/ltm`. You can ignore these messages.

The virtual switch clears the QoS field in 802.1q headers

A hypervisor's Layer 2 bridging device might remove quality of service (QoS) classification from packets.

Index

Q

R

S

T

U

V