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

Version 11.3
# Table of Contents

Legal Notices.....................................................................................................................................5

Chapter 1: Getting Started with BIG-IP Virtual Edition...............................................7  
   What is BIG-IP Virtual Edition?................................................................................................8  
   About BIG-IP VE compatibility with VMware hypervisor products.................................8  
   About the hypervisor guest definition requirements...............................................................8

Chapter 2: Deploying BIG-IP Virtual Edition......................................................11  
   About BIG-IP VE VMware deployment...................................................................................12  
   Host machine requirements and recommendations...............................................................12  
   Deploying the BIG-IP VE virtual machine...........................................................................12  
   Powering on the BIG-IP VE virtual machine.....................................................................13  
   Assigning a management IP address to a BIG-IP VE virtual machine............................14

Chapter 3: Updating a BIG-IP VE Virtual Machine.............................................15  
   About updates to the BIG-IP VE virtual machine...............................................................16  
   Downloading or importing a BIG-IP VE update.................................................................16  
   Installing a BIG-IP VE update...............................................................................................16  
   Rebooting after a BIG-IP VE update.....................................................................................17  
   Upgrading BIG-IP VE from version 10.x to 11.x.................................................................17

Appendix A: Deployment Best Practices...........................................................21  
   Best practices for deploying BIG-IP VE on VMware.........................................................22

Appendix B: Troubleshooting BIG-IP Virtual Edition........................................23  
   About troubleshooting BIG-IP Virtual Edition.................................................................24
Table of Contents
Legal Notices

Publication Date
This document was published on January 17, 2013.

Publication Number
MAN-0347-02

Copyright
Copyright © 2012-2013, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

All other product and company names herein may be trademarks of their respective owners.

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 January 17, 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

Topics:

• What is 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 in specifically-supported hypervisors. 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.

About BIG-IP VE compatibility with VMware hypervisor products

Each time there is a new release of BIG-IP® Virtual Edition (VE) software, it includes support for additional hypervisor management products. The Virtual Edition and Supported Hypervisors Matrix on the AskF5™ website, http://support.f5.com, details which hypervisors are supported for each release.

Important: Hypervisors other than those identified in the matrix are not supported with this BIG-IP version; installation attempts on unsupported platforms might not be successful.

About the hypervisor guest definition requirements

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.

For production licenses, F5 Networks suggests using the maximum configuration limits for the BIG-IP VE system. Reservations can be less for lab editions. For each virtual machine, the VMware virtual machine guest environment permits a maximum of 10 virtual Network Adapters (either 10 VMXNET3 with 1 management + 9 dataplane or 1 Flexible management + 9 VMXNET3 dataplane).

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.
• To achieve licensing performance limits, all allocated RAM must be reserved.
• For production environments, virtual disks should be deployed Thick (allocated up front). Thin deployments are acceptable for lab environments.

⚠️ **Important:** There is no longer any limitation on the maximum amount of RAM supported on the hypervisor guest.
Chapter 2

Deploying BIG-IP Virtual Edition

Topics:

- About BIG-IP VE VMware deployment
About BIG-IP VE VMware deployment

To deploy the BIG-IP® Virtual Edition (VE) system on a VMware ESXi®, you need to perform these tasks:

• Verify the host machine requirements.
• Deploy an instance of the BIG-IP system as a virtual machine 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

To successfully deploy and run the BIG-IP® VE system, the host system must satisfy minimum requirements.

The host system must include:

• VMware ESX 4.0 or 4.1, or ESXi 4.0 or 4.1 update 1, or ESXi 5.0 or 5.1
• 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
• must have support for virtualization (AMD-V™ or Intel® VT-x) 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 step in deploying BIG-IP® Virtual Edition (VE) is to download the OVA file to your local system. Next, you can run the Deploy OVF Template wizard from within the VMware vSphere™ client. 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.
3. Start your vSphere Client and log in.
4. From the vSphere Client File menu, choose Deploy OVF Template.
   The Deploy OVF Template wizard starts.
5. In the Source pane, click **Deploy from file or URL**, and, using the **Browse** button, locate the OVA file, open it, and then click **Next**.
   For example: \MyDocuments\Work\Virtualization\<BIG-IP_OVA_filename>
The OVF Template Details pane opens.
6. Verify that the OVF template details are correct, and click **Next**.
   This displays the End-User License Agreement (EULA).
7. Read and accept the license agreement, and click **Next**.
   The Name and Location pane opens.
8. In the **Name** field, type a name for the BIG-IP VE virtual machine, such as: smith_big-ip_ve.
9. In the Inventory Location area, select a folder name and click **Next**.
10. From the **Configuration** list, select the number of CPUs and disks required for your system, and then 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. In the **Datastore** field, type the name of data source your system will use, in the **Available space** field, type in the amount of space your system needs (in Gigabytes), and then click **Next**.
   The Network Mapping dialog box opens.
13. Map the Source Networks for Management, External, Internal, and HA to the Destination Networks in your inventory.
   a) Map the source network **Management** to the name of the appropriate external network in your inventory.
      An example of a destination external network is **Management**.
   b) Map the source network **Internal** to the name of a destination non-management network in your inventory.
      An example of a destination internal network is **Private Access**.
   c) Map the source network **External** to the name of the appropriate external network in your inventory.
      An example of a destination external network is **Public Access**.
   d) Map the source network **HA** to the name of a high-availability network in your inventory.
      An example of a destination internal network is **HA**.
   e) When you have all four destination networks correctly mapped, click **Next**.
      The Ready to Complete screen opens.
14. 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 before you can begin 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 virtual machine is on. Note that BIG-IP VE will not process traffic until you configure the BIG-IP VE virtual machine 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 needs an IP address assigned to its virtual management port.

Tip: The default configuration for new deployments and installations is for DHCP to acquire the management port IP address.

1. From the main vSphere client screen, click the Administration menu.
2. At the <username> login prompt, type root.
3. At the password prompt, type default.
4. Type config and press Enter.
   The F5 Management Port Setup screen opens.
5. Click OK.
6. 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.

When assigned, the management IP address appears 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

Topics:

• About updates to the BIG-IP VE virtual machine
• Upgrading BIG-IP VE from version 10.x to 11.x
About updates to the BIG-IP VE virtual machine

BIG-IP® VE updates within the same major version 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, 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 or importing a BIG-IP VE update

To install an update, BIG-IP software needs access to the ISO file. You can either download the ISO file using a script or the command line; or, you can import the file with the user interface.

1. In a browser, open the F5 Downloads page (https://downloads.f5.com).
2. Download the version's base ISO file, such as 11.1, and its associated MD5 checksum file.

   **Important:** If you are installing a hotfix, you must import the ISO for the base version of the hotfix before you can successfully import and install a hotfix update. For installation, you select only the hotfix image, but the base version of the hotfix must be in place before the hotfix can be applied to BIG-IP VE.

3. Download the update ISO file, such as Hotfix-BIGIP-11.1.1-511.0-HF3.iso, and its associated MD5 checksum file.

   **Attention:** Before you perform the installation, F5 recommends testing 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.

4. On the Main tab, click **System > Software Management**.
   The Software Management Image List screen opens.
5. At the right side of the screen, click **Import**.
   The New Image screen opens.
6. Click **Browse** to navigate to the downloaded installation file.
7. 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, click **System > Software Management**. The Software Management Image List 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 is installed.

**Rebooting after a BIG-IP VE update**

When the installation operation is complete, you can safely reboot into the newly installed volume or partition.

1. On the Main tab of the navigation pane, click **System > Software Management**. The Software Management Image List screen opens.

2. On the menu bar, click **Boot Locations**. The Boot Locations screen opens.

3. In the Boot Location 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.

**Upgrading BIG-IP VE from version 10.x to 11.x**

When a new version is available, you can upgrade from BIG-IP® VE version 10.x to the BIG-IP VE version 11.x that is available for your hypervisor.

**Note:** The BIG-IP VE commands in this procedure are run using the BIG-IP command-line interface within the hypervisor.

1. Download the base ISO files and MD5 files for versions 10.2.x and version 11 from the F5 Downloads page (https://downloads.f5.com), and verify the downloaded ISO files against their corresponding MD5 files.
Important: If you are installing a hotfix, you must import the ISO for the base version of the hotfix before you can successfully import and install a hotfix update. For installation, you select only the hotfix image, but the base version of the hotfix must be in place before the hotfix can be applied to BIG-IP VE.

2. Save a UCS file offline for the BIG-IP VE system you are upgrading.

   Important: An SCF will not suffice for this procedure.

3. Make sure to note the host name for UCS restoration.
   The command string `tmsh list sys global-settings hostname` will show you the active host name.

4. In the VMware vSphere™ client, power off (shut down) the BIG-IP VE virtual machine.
5. Take a snapshot and back up the BIG-IP VE virtual machine.
6. Add a CD/DVD drive to the virtual machine using either a physical device or ISO file as appropriate.
7. Configure the target virtual machine to boot from the 10.2.x ISO image as the virtual device default node.
   The virtual device node should be IDE, where (0:0) or (1:0) is bootable. The Connect at power on setting should remain selected.
8. Remove the existing virtual disk labeled Hard disk 1.
   Important: Select Remove from virtual machine so that the disk is available for recovery purposes.

9. Add a hard disk.
   a) Select Create a new virtual disk and make the disk size 100 GB.
      Caution: Other sizes are not supported, and unexpected problems can occur if a size other than 100 GB is used.
   b) Select the Provision type.
      For production nodes, a Flat Disk/Thick Provision is preferred to a Thin Provision. For lab editions, a Thin Provision can be used.
   c) Select Create a new virtual disk.
      Use SCSI (0:0) for the Virtual Device node.
   d) After the Summary screen, click Finish.
      At this point:
      • A CD/DVD drive has been configured to attach when powering on the BIG-IP VE 10.2.x ISO image.
      • The legacy 40 GB disk has been removed.
      • A new 100 GB disk has been created.

10. Select BIG-IP VE from the inventory panel and power it on.
11. At the [VT100] prompt, press Enter.
12. You are prompted for an unattended default installation; press Enter to continue.
   BIG-IP VE version 10.2.2 and later 10.x versions should proceed normally. Versions 10.2.0 and 10.2.1 will return the message: No configuration provided for hardware type Z100. For these
versions, use the command `diskinit --style volumes` to format the volume, and then use the
command `image2disk --nosaveconfig --instslot HD1.1` to install the image.

This will prepare the disk and automatically install the 10.2.x system onto boot volume HD1.1.

13. When the installation is complete for version 10.2.2 and later, the system prompt shows this message:
   Remove media, then press [Enter] to reboot. Press Enter to reboot the machine. For versions
   10.2.0 and 10.2.1, type `reboot` and press Enter.

14. Boot into the 10.2.x BIG-IP VE system.

15. Log in to the console and run `config` to configure the management port’s IP address.

16. Copy the 10.2.x and 11 ISO files to `/shared/images`.

17. If a hotfix was installed, copy the hotfix ISO file to `/shared/images`, and then perform a live installation
   of the hotfix onto the system’s HD1.2. When finished, reboot into the hotfix image before restoring the
   UCS.

18. Copy the UCS to `/var/local/ucs/` on the BIG-IP VE.

19. Run the command `tmsh modify sys global-settings hostname xxx.xxx`, where `xxx.xxx` is
   the previously collected host name.

20. Restore the UCS. For example, if the UCS is named `webfarm1.ucs` and is stored in `/var/local/ucs`,
    then the restoration command is `tmsh load sys ucs webfarm1`.
    At this point, the system is active with the 10.2.x configuration restored.

21. Perform a live installation of BIG-IP VE 11 on the system.

22. When the live installation is complete, halt and power off the BIG-IP VE virtual machine.

23. Within the hypervisor, open the guest settings for the BIG-IP VE.

24. Remove the previously added CD/DVD drive.

25. Adjust the memory reservation from 2 GB to 4 GB to match the memory configuration.

   **Important:** BIG-IP VE version 11 includes new high-availability features. You should consider
adding another VMXNET3 network interface at this point in order to avoid a reboot at a later
   time.

The BIG-IP VE virtual machine will boot into version 11.
Updating a BIG-IP VE Virtual Machine
Appendix

A

Deployment Best Practices

Topics:

- Best practices for deploying BIG-IP VE on VMware
Best practices for deploying BIG-IP VE on VMware

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant system configuration</td>
<td>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.</td>
</tr>
<tr>
<td>Live migration of BIG-IP VE virtual machines</td>
<td>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.</td>
</tr>
<tr>
<td>VMware DRS environments</td>
<td>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 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.</td>
</tr>
<tr>
<td>Resource reservations</td>
<td>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.</td>
</tr>
<tr>
<td>Disable hyper-threading on older processors</td>
<td>F5 Networks recommends turning off Hyper-Threading Technology when using host machines with Intel® Pentium® 4 era processors. Doing so will prevent possible timing issues with BIG-IP VE.</td>
</tr>
</tbody>
</table>

**Important:** Production licenses are not supported on Pentium 4 processors.
Appendix B

Troubleshooting BIG-IP Virtual Edition

Topics:

- About troubleshooting BIG-IP Virtual Edition
About 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 (ID 324968; CR 134473)
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 (CR 135980)
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.

Link speed of management interface (ID 224507; CR 136578)
The management port might not correctly reflect the uplink port speed of the vSwitch that it is connected to. This should have no adverse affects on actual management port traffic.

Incorrect status of VMware Tools in vSphere (CR 136980)
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 (CR 137014)
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 (CR 137596)
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 ESXi® Configuration Guide.

Use of Single Configuration File (SCF) feature (CR 137597)
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 additional interfaces (CR 137616; CR 137621)
When a BIG-IP VE system is configured with more than four interfaces (one management interface and more than three TMM interfaces), the interface numbering might appear out of order. To view the actual
portgroup interface mapping, compare the MAC addresses of the interfaces displayed in the BIG-IP Configuration utility to those displayed in the hypervisor client. If you change the number of virtual interfaces on the BIG-IP VE system after a binary MCPD database is 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 (CR 138676)

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 (CR 138798)

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 (CR 126854-1)

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 (CR 133194)

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 (CR 138498)

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 (CR 137905)

Setting the source OID for RMON alarm, event, and history tables generates an error message.

Media speed messages in log file (CR 137973)

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 (ID 358996)

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

802.1q headers and QoS field, troubleshooting 24

A
active/standby configuration 22
auto-licensing, troubleshooting 24

B
best practices
  for deployment 22
  for redundant system configuration 22
BIG-IP import command, troubleshooting 24
BIG-IP Virtual Edition
  and VMware ESXi host machine requirements 12
  updating 16

C
configuration, editing virtual 24
Configuration of additional interfaces, troubleshooting 24
CPU
  and best practices for 22
  and guest definition 8
  and host machine requirements 12

default route for virtual management port 14
deployment overview 12
downloads
  and importing update 16, 17
  of ISO base file 16, 17
  of ISO update file 16, 17

E
environment, for guest 8

G
guest environment 8

H
HA events due to BIG-IP VE inactivity, troubleshooting 24
host machine, CPU requirements 12
hypervisor, See guest environment.
  hypervisor guest definition 8

I
import command, troubleshooting bigpipe import errors 24
installation
  rebooting after 17
  installation operation 16
insufficient video RAM event message, troubleshooting 24
IP address, management port 14
iRule, troubleshooting sessionid command for SSL 24
ISO file
  and location on virtual machine 16
  downloading 16, 17
  downloading base 17
  downloading base ISO file 16
  downloading update 17
  downloading update ISO file 16

L
Layer 2, troubleshooting 24
license for BIG-IP system, troubleshooting 24
log file
  and location 16, 24
  and media speed messages 16, 24
log in
  after updating 17
  assigning management IP address 14

M
management link speed, troubleshooting 24
management port IP address, assigning 14
maximum allowed throughput rate 8
media speed messages in log file, troubleshooting 24
MOS bash prompt exiting shell, troubleshooting 24

N
NTP time synchronization, troubleshooting 24

O
OVA file, location 12

P
power-on procedure, virtual machine 13
product license 8
progress indicator, for update 16
protocols
  troubleshooting 24
Q
QoS, troubleshooting 24

R
reboot after configuring additional interfaces, troubleshooting 24
reboot operation
  after updating 17
redundant system configuration
  and host machine requirements 12
  and NTP requirement 12
  deploying 22
resource reservations 22
RMON tables and SNMP OID, troubleshooting 24

S
Setup utility 12
Single Configuration File (SCF) feature, troubleshooting 24
SNMP OID for RMON tables, troubleshooting 24
SSL, troubleshooting sessionid command in iRule 24
system reboot, See reboot operation.
system update procedure 16

T
task list
  for deploying on virtual machine 12
  for deploying on VMware 12
  for updating on virtual machine 16
  for updating on VMware 16
troubleshooting 24

U
UCS importing from BIG-IP Virtual Edition Trial, troubleshooting 24
update
  BIG-IP VE version 10.x to 11.x 17
  downloading and importing 16
  installing 16
update progress indicator 16
user configuration sets for licensing BIG-IP system, troubleshooting 24

V
virtual configuration, and hypervisor guest definition 8
virtual guest configuration, editing, troubleshooting 24
virtual machine, powering-on 13
virtual machine settings 8
virtual management port 14
virtual network interface status, troubleshooting 24
VLAN groups, troubleshooting 24
VMware
  and compatible versions 8
VMware Tools status, troubleshooting 24
VMware Tools troubleshooting
time synchronization 24
VMware virtual machine
  creating 12
VMXNET3 unavailability, troubleshooting 24
vSwitch promiscuous mode, troubleshooting 24