BIG-IP® Virtual Edition Setup Guide for Linux® Community Xen®

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0472-00

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 May 15, 2013.

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 in specifically-supported hypervisors. BIG-IP VE virtualizes 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 Community Xen 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 Community Xen virtual machine guest environment for the BIG-IP® Virtual Edition (VE), at minimum, must include:

- 2 x virtual CPUs
- 4 GB RAM
- 3 x virtual network adapters (minimum); more if configured with the high availability option

  Important: *The number of virtual network adapters per virtual machine definition is determined by the hypervisor.*

- 1 x 100 GB Virtio disk

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 Community Xen virtual machine guest environment permits a maximum of 10 network adapters. You can either deploy these as a management port and 9 dataplane ports or a management port, 8 dataplane ports, and an HA port.

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.*

About TCP Segmentation Offloading support

If you want to disable support for TCP Segmentation Offloading (TSO), you must submit a `tmsh` command, because the TSO feature is enabled by default. Note that enabling TSO support also enables support for large receive offload (LRO) and Jumbo Frames.

Configuring a hypervisor for TSO support

You must have the Admin user role to enable or disable TSO support for a hypervisor.

Using the `tmsh` command `sys db`, you can turn TSO support on, off, or check to see whether support is currently enabled.

1. To determine whether TSO support is currently enabled, use the `tmsh list` command.
   `list sys db` *`tm.tcpsegmentationoffload`*
2. To enable support for TSO, use the `tmsh enable` command.
   `sys db` *`tm.tcpsegmentationoffload`* `enable`
3. To disable support for TSO, use the `tmsh disable` command.
   `sys db` *`tm.tcpsegmentationoffload`* `disable`

About SR-IOV support

If you want support for SR-IOV, in addition to using the correct hardware and BIOS settings, you must configure hypervisor settings before you set up the guests.

You must have an SR-IOV-compatible network interface card (NIC) installed, and the SR-IOV BIOS enabled before you can configure SR-IOV support.

Refer to the documentation included with your hypervisor operating system for information on support and configuration for SR-IOV.

Chapter 2

Deploying BIG-IP Virtual Edition

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:

- CentOS 5.9 or Fedora 18 (for SR-IOV support)
- Ubuntu 12.04 with the Community Xen package (if SR-IOV support is not required)
- Virtual Machine Manager®
- Connection to a common NTP source (this is especially important for each host in a redundant system configuration)

If SR-IOV support is required, additional drivers and configuration steps are required, consult your Community Xen documentation for detail.

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

---

About BIG-IP VE Community Xen deployment

To deploy the BIG-IP® Virtual Edition (VE) system on Linux® Community Xen®, 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.

Deploying the BIG-IP VE virtual machine

The primary task in deploying BIG-IP® VE on the open source Community Xen environment is creating and executing a configuration file that sets up most of what you need to get up and running.

Important: *Do not modify the configuration of the Community Xen 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 `qcow2.zip`.

3. Extract the file from the Zip archive and save it where your `qcow2` files reside on the Community Xen server.
4. Use VNC to access the Community Xen server, and then convert the qcow2 image to the raw format necessary for Community Xen. You can use the following syntax to convert the image.
   `# qemu-img convert <qcow_file_name>.qcow2 <raw_file_name>.raw`
5. Generate a MAC address for the network interface card associated with the management interface.

   Important: *Be sure that the MAC address you create starts with the prefix `00:16:3e:`.*

   You can use a tool such as MAC Address Generator (`http://www.miniwebtool.com/mac-address-generator/`) to create this address.
6. Use an editor to create a BIG-IP VM definition file that specifies the required parameters for your VM.

   Attention: *The sample configuration file provided here serves only as an example of the kinds of parameters you need to specify for your virtual machine. The actual file that you create will likely contain different parameters and settings.*

```
# vi /etc/xen/<config_file_name>
```

```
                    name = <config_file_name>
                    maxmem = 4096
                    memory = 4096
                    vcpus = 2
                    builder = "hvm"
                    boot = "c"
                    pae = 1
                    acpi = 1
                    apic = 1
                    hpet = 1
                    localtime = 0
                    on_poweroff = "destroy"
                    on_reboot = "restart"
                    on_crash = "restart"
                    sdl = 0
                    vnc = 1
                    vncunused = 1
                    keymap = "en-us"
                    disk = [
"file:/mnt/xen-bender/bigip/<raw_file_name.raw>,hda,w" ]
                    vif = [
"mac=00:16:<mgmt_interface_mac>,bridge=mgmtbr,script=vif-bridge",

"mac=00:16:3e:<external_interface_mac>,bridge=ext_bridge,script=vif-bridge",


"mac=00:16:3e:<internal_interface_mac>,bridge=int_bridge,script=vif-bridge",]

                    parallel = "none"
                    serial = "pty"
                    #pci = [ '05:10.0', '05:10.1' ]
```

   Important: *The last line of the example configuration file contains an optional entry that specifies the IDs for PCI external and internal network interface cards (NIC). This optional entry is required for SR-IOV support. Naturally, if you use this entry, you would omit the external and internal bridges specified in the `vif` section.*

   Once you have perfected and saved your configuration file you are ready to create the BIG-IP VM,
7. Run the configuration file using an open source tool such as `xm`.

```
xm create /etc/xen/<config_file_name>
```
The console should indicate a successful start up by displaying something similar to: `Started domain <config_file_name>(id=444)`

8. Allow some time for the boot-up process; then, you should be able to connect to the BIG-IP console.
```
# xm console <config_file_name>
```

Powering on the virtual machine

You must power on the virtual machine before you can begin assigning IP addresses.

Assigning a management IP address to a virtual machine

The 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. At the password prompt, type `default`.
2. Type `config` and press Enter.
   The F5 Management Port Setup screen opens.
3. Click **OK**.
4. 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 virtual machine.*

Index