

BIG-IQ™ Systems and Amazon® EC2®: Setup

Version 4.2



Table of Contents

Legal Notices.....5

Acknowledgments.....7

Chapter 1: Getting Started with BIG-IQ Virtual Edition.....13

 What is BIG-IQ Virtual Edition?.....14

 About BIG-IQ VE compatibility with EC2 hypervisor products.....14

 About the hypervisor guest definition requirements.....14

Chapter 2: Deploying BIG-IQ Virtual Edition.....15

 About VE EC2 deployment.....16

 Task summary for BIG-IQ VE EC2 deployment.....16

Legal Notices

Publication Date

This document was published on December 20, 2013.

Publication Number

MAN-0512-00

Copyright

Copyright © 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

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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

Patents

This product may be protected by one or more patents indicated at:

<http://www.f5.com/about/guidelines-policies/patents>

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, <http://www.and.com>.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at <http://www.perl.com>.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (<http://www.rrdtool.com/index.html>) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (<http://www.nominum.com>).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software developed by Oracle America, Inc. Copyright ©2012.

1. Java Technology Restrictions. Licensee shall not create, modify, change the behavior of, or authorize licensees of licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developer.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icon including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at <http://www.oracle.com/html/3party.html>; (b) not do anything harmful to or inconsistent with Oracle's

rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.

3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portion of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.
5. Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table I-I (Commercial Features In Java SE Product Editions) of the Software documentation accessible at <http://www.oracle.com/technetwork/java/javase/documentation/index.html>.

This product includes software developed by members of the CentOS Project under the GNU Public License, copyright ©2004-2011 by the CentOS Project.

This product includes software developed by members of the OpenJDK Project under the GNU Public License Version 2, copyright ©2012 by Oracle Corporation.

This product includes software developed by The VMWare Guest Components Team under the GNU Public License Version 2, copyright ©1999-2011 by VMWare, Inc.

This product includes software developed by The Netty Project under the Apache Public License Version 2, copyright ©2008-2012 by The Netty Project.

This product includes software developed by Stephen Colebourne under the Apache Public License Version 2, copyright ©2001-2011 Joda.org.

This product includes software developed by the GlassFish Community under the GNU Public License Version 2 with classpath exception, copyright ©2012 Oracle Corporation.

This product includes software developed by the Mort Bay Consulting under the Apache Public License Version 2, copyright ©1995-2012 Mort Bay Consulting.

This product contains software developed by members of the Jackson Project under the GNU Lesser General Public License Version 2.1, ©2007 – 2012 by the Jackson Project”.

This product contains software developed by QOS.ch under the MIT License, ©2004 – 2011 by QOS.ch.

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This software incorporates JFreeChart, ©2000-2007 by Object Refinery Limited and Contributors, which is protected under the GNU Lesser General Public License (LGPL).

This product contains software developed by the Mojarra project. Source code for the Mojarra software may be obtained at <https://jaserverfaces.dev.java.net/>.

This product includes JZlib software, Copyright © 2000-2011 ymnk, JCraft, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes Apache Lucene software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes Apache MINA software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes OData4J software, distributed under the Apache License version 2.0.

This product includes software developed by the Visigoth Software Society (<http://www.visigoths.org/>).

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes software developed by Addy Osmani, and distributed under the MIT license. Copyright © 2012 Addy Osmani.

This product includes software developed by Charles Davison, and distributed under the MIT license. Copyright © 2013 Charles Davison.

This product includes software developed by The Dojo Foundation, and distributed under the MIT license. Copyright © 2010-2011, The Dojo Foundation.

This product includes google-gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes ec2-tools software, copyright © 2008, Amazon Web Services, and licensed under the Amazon Software License. A copy of the License is located at <http://aws.amazon.com/asl/>.

This product includes Apache Ant software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes isc-dhcp software. Copyright © 2004-2013 by Internet Systems Consortium, Inc. ("ISC"); Copyright © 1995-2003 by Internet Software Consortium.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

This product includes jQuery Sparklines software, developed by Gareth Watts, and distributed under the new BSD license.

This product includes jsdiff software, developed by Chas Emerick, and distributed under the BSD license.

This product includes winston software, copyright © 2010, by Charlie Robbins.

This product includes Q software developed by Kristopher Michael Kowal, and distributed under the MIT license. Copyright © 2009-2013 Kristopher Michael Kowal.

This product includes SlickGrid software developed by Michael Liebman, and distributed under the MIT license.

Chapter

1

Getting Started with BIG-IQ Virtual Edition

- *What is BIG-IQ Virtual Edition?*
-

What is BIG-IQ Virtual Edition?

BIG-IQ™ Virtual Edition (VE) is a version of the BIG-IQ system that runs as a guest in specifically-supported hypervisors. BIG-IQ VE emulates a hardware-based BIG-IQ system running a VE-compatible version of BIG-IQ™ software.

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

About BIG-IQ VE compatibility with EC2 hypervisor products

BIG-IQ™ VE is compatible with the Amazon Web Services (AWS) EC2 hypervisors. This guide documents the AWS interface as it exists just prior to the version 11.3.0 BIG-IP software release.

Important: *Hypervisors other than those identified in this guide are not supported with this BIG-IQ version; any installation attempts on unsupported platforms might not be successful.*

About the hypervisor guest definition requirements

The EC2 virtual machine guest environment for the BIG-IQ™ Virtual Edition (VE), at minimum, must include:

- a 64 bit EC2 instance with at least 2 virtual cores (up to 16 are supported in this release)
- at least 4 GB RAM (64GB has been tested, F5® Networks recommends at least 2GB per virtual core)
- 2 x virtual network adapter cards (NICs) (up to 9 are supported)

Important: *F5® Networks recommends three or more network adapters for most topologies, but the minimum requirement is two (one for management and one for traffic).*

Important: *To support multiple NICs on an Amazon Web Services you must create a virtual private cloud (VPC).*

- 1 x virtual private cloud (VPC).

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

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

Note: *Currently, these requirements map to what Amazon designates as an M1 Large instance. Refer to <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/instance-types.html#AvailableIpPerENI> for their most current definition.*

Chapter

2

Deploying BIG-IQ Virtual Edition

- *About VE EC2 deployment*

About VE EC2 deployment

To deploy the BIG-IQ™ Virtual Edition (VE) system on EC2, you perform these tasks:

- Verify the host machine requirements.
- Deploy a BIG-IQ™ system as a virtual machine.
- Deploy a BIG-IP® system.
- After you have deployed the virtual machines, log in to the BIG-IQ VE system and run the Setup utility. Using the Setup utility, you perform basic network configuration tasks, such as assigning VLANs to interfaces.
- Configure secure communication between the BIG-IQ system and the BIG-IP device.

Task summary for BIG-IQ VE EC2 deployment

To deploy BIG-IQ™ Cloud you perform a series of tasks using Amazon Web Services (AWS) to create an elastic compute cloud (EC2) that runs a public cloud virtual machine management service.

When you complete these tasks, your cloud environment will be similar to the basic cloud topology depicted here.

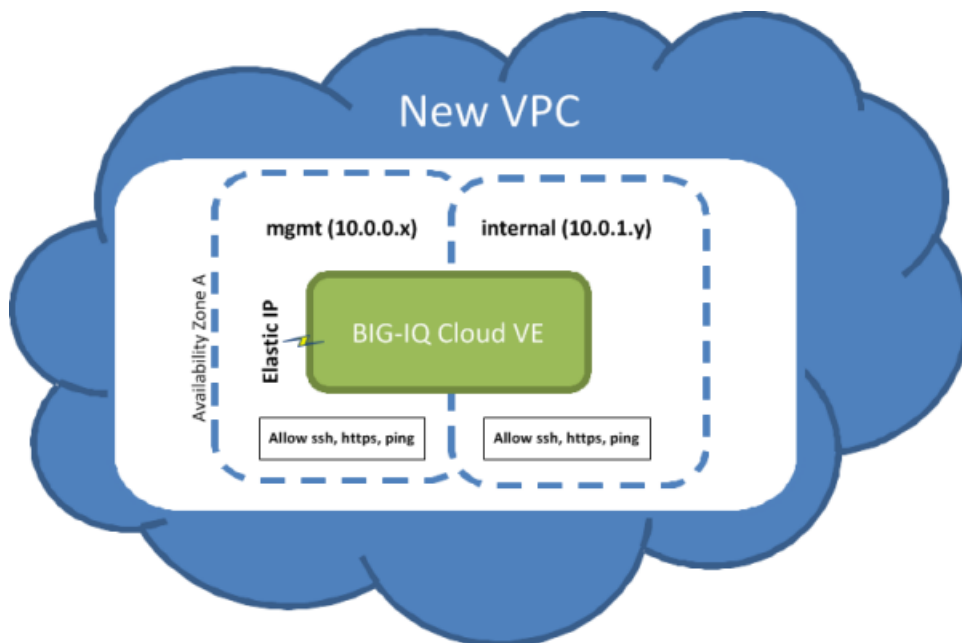


Figure 1: Basic Cloud Topology

Task list

Acknowledgments

Creating a new IAM user account

Creating a new IAM user account

Creating a key pair

Creating a new virtual private cloud

Adding an additional subnet

Creating new security groups

[Adding a route for external subnet accessibility](#)
[Launching a new virtual machine](#)
[Adding a third network interface](#)
[Making the virtual machine management port accessible](#)
[Logging in and setting the Admin password](#)

Creating a new IAM user account

An Amazon Identity Access Management (IAM) user account provides access to specific AWS resources. Creating IAM user access provides you with more granular control of the AWS resources that your users can access.

Tip: This task is optional; you can create a virtual machine without creating an IAM user account to control access, but using IAM is considered to be best practice.

Tip: When you manually deploy a virtual machine on AWS EC2, you need to create an administrator password in addition to the IAM access keys. If you use the automated process to deploy a VM, only the access keys are required.

For the most current instructions for creating a new IAM user, refer to the Amazon Virtual Private Cloud (VPC) Documentation web site, <http://aws.amazon.com/documentation/iam/>.

When you complete this task, you will have created a new IAM user and downloaded the credentials (an access key ID and secret access key) that provide access to AWS resources for that new user.

Creating a key pair

Before you can deploy a virtual machine on Amazon Web Services (AWS) Elastic Cloud Computing, you need an AWS account.

To create a virtual private cloud (VPC) on which you can deploy the BIG-IQ™ system, you need a (private-public encryption) key pair to authenticate your sessions. Key pairs are reusable, so if you have a key pair, you do not need to repeat this task.

For the most current instructions for creating a key pair, refer to the Amazon Virtual Private Cloud (VPC) Documentation web site, <http://aws.amazon.com/documentation/vpc/>.

Important: It is crucial to your success that you be consistent in the region that you choose throughout the configuration process. Objects configured in one region are not visible within other regions, so they cannot function together. There are a number of factors that determine which region will best suit your requirements. Refer to Amazon user documentation for additional details.

The file that downloads from Amazon Web Services uses the extension `.pem`. If you plan to use this key pair with the PuTTY terminal emulator application, you will need to convert the key pair from a `.pem` to a `.ppk` file. At the time of this release, PuTTY does not support the extension `.pem`. PuTTY does have a tool (called PuTTYgen) that converts your key pair to the required PuTTY format.

Creating a new virtual private cloud

You need a virtual private cloud (VPC) to deploy the BIG-IQ™ Cloud system because Amazon Web Services (AWS) only provides multiple network interface card (NIC) support for EC2 instances that reside within a VPC.

For the most current instructions for creating a Virtual Private Cloud, refer to the Amazon Virtual Private Cloud (VPC) Documentation web site, <http://aws.amazon.com/documentation/vpc/>.

Important: *It is crucial to your success that you be consistent in the availability zone that you choose throughout the configuration process. Objects configured in one zone are not visible within other zones, so they cannot function together.*

Important: *The first choice you have when creating a VPC is to select a VPC configuration. Choose the VPC with **Public and Private Subnets** option.*

Adding an additional subnet

When you create a VPC, Amazon Web Services creates two subnets for it. The first subnet is the management subnet (10.0.0.0/24) and the second subnet is external (10.0.1.0/24). Many network topologies require three or more subnets (Management, External, and Internal). You can use this task to create an internal subnet (10.0.2.0/24).

For the most current instructions for creating an internal subnet, refer to the Amazon Virtual Private Cloud (VPC) Documentation web site <http://aws.amazon.com/documentation/vpc/>.

If you are following a typical deployment strategy, when you finish adding the Internal subnet, your VPC will have three subnets.

- a Management subnet on 10.0.0.0/24
- an External subnet on 10.0.1.0/24
- an Internal subnet on 10.0.2.0/24

Creating new security groups

To use your virtual private cloud (VPC) to deploy your virtual machine, the VPC needs two security groups; each with its own set of rules that govern the security behavior for the traffic that routes through it. The table details the rules required for each group to function properly.

Group Name	Group Description	Rule Name	Source	Rule Type
allow-only-ssh-https-ping	Allow only SSH HTTPS or PING	Inbound SSH	0.0.0.0/0	
		Inbound HTTPS	0.0.0.0/0	
		Inbound Custom ICMP	0.0.0.0/0	Echo Request
		Outbound Custom ICMP	0.0.0.0/0	Echo Request
		Outbound Custom ICMP	0.0.0.0/0	Echo Reply

Group Name	Group Description	Rule Name	Source	Rule Type
allow-all-traffic	Allow all traffic	Inbound All Traffic	0.0.0.0/0	
		Outbound All Traffic	0.0.0.0/0	

1. Create two security groups, one named `allow-only-ssh-https-ping` and the other named `allow-all traffic`.

Tip: For the most current instructions for creating security groups, refer to the Amazon Virtual Private Cloud (VPC) Documentation web site <http://aws.amazon.com/documentation/vpc/>.

Important: The `allow-all-traffic` security group is critically important for successful operation of the BIG-IP® VE on Amazon EC2.

2. For each security group, create the rules described in the preceding table. For each rule, define the Group Description, Rule Name, Source, and Rule Type as shown in the table.

Important: No punctuation is permitted in the text of the Group Description that you type in.

When you finish adding the two groups and their associated rules, your VPC should be ready to go with three subnets and two security groups.

It is a good idea to test connectivity before proceeding. You should be able to communicate with your VPC NAT server at this point.

F5 Networks recommends enhancing your security by using the security group source fields to restrict the subnets to allow only management access; however, we recognize that this does not complete your security solution. For enhanced security, you may want to deploy a topology with limited management network access.

Adding a route for external subnet accessibility

Most network topologies require an Amazon Web Services route to the virtual private cloud (VPC) that makes the external subnet used by the virtual machine accessible to the Internet.

1. From the Services tab at the top of the Amazon Web Services Management Console screen, select **VPC**.
2. In the navigation pane, select **Route Tables**.
The Route Tables screen opens.
3. Select the routing table with one subnet.
4. Click the Associations tab at the bottom of the window.
5. From the **Select a subnet** list, select the **10.0.1.0/24** subnet.
6. Click **Associate**.
The Associate Route Table dialog box opens.
7. Click **Yes, Associate**.

Launching a new virtual machine

Before you can complete this task, you need to know the name of your key pair and the Availability Zone from which it was created.

You launch an EC2 Amazon Machine Image (AMI) so that you can deploy the virtual machine.

Important: At publication, this task illustrates the Amazon web interface. However, F5 recommends that you refer to Amazon user documentation for the latest documentation.

1. Log in to your account on Amazon Web Services (AWS) marketplace.
2. In the Search AWS Marketplace bar, type **F5 BIG-IQ** and then click **GO**.
The F5 BIG-IQ Virtual Edition for AWS option is displayed.
3. Click **F5 BIG-IQ Virtual Edition for AWS** and then click **CONTINUE**.

Tip: You might want to take a moment here to browse the pricing details to confirm that the region in which you created your security key pair provides the resources you require. If you determine that the resources you need are provided in a region other than the one in which you created your key pair, create a new key pair in the correct region before proceeding.

The Launch on EC2 page is displayed.

4. Click the **Launch with EC2 Console** tab.

Important: At the time this was written, the virtual machine must be launched in a VPC so that NICs can be attached. This configuration is supported from the **Launch with EC2 Console** option, but not the **1-Click Launch** option.

Launching Options for your EC2 AMI are displayed.

5. Select the software version appropriate for your installation, and then click the **Launch with EC2** button that corresponds to the Region that provides the resources you plan to use.

Important: The first time you perform this task, you need to accept the terms of the end user license agreement before you can proceed, so the **Launch with EC2** button reads **Accept Terms and Launch with EC2**.

Important: There are a number factors that determine which region will best suit your requirements. Refer to Amazon user documentation for additional detail. Bear in mind that the region you choose must match the region in which you created your security key pair.

The Request Instances Wizard opens.

6. Select an **Instance Type** appropriate for your use.
7. From the **Launch Instances** list, select **EC2-VPC**.
8. From the **Subnet** list, select the **10.0.0.0/24** subnet and click **CONTINUE**.
The Advanced Instance Options view of the wizard opens.
9. From the **Number of Network Interfaces** list, select **2**.
10. Click the horizontal **eth1** tab to set values for the second network interface adapter, and then from the **Subnet** list, select the **10.0.1.0/24** subnet and click **CONTINUE**.
The Storage Device Configuration view of the wizard opens.
11. In the **Value** field, type in an intuitive name that identifies this AMI and click **CONTINUE** (for example, **BIG-IQ VE <version>**).
The Create Key Pair view of the wizard opens.
12. From **Your existing Key Pairs**, select the key pair you created for this AMI and click **CONTINUE**.
The Configure Firewall view of the wizard opens.
13. Under Choose one or more of your existing Security Groups, select the **allow-all-traffic** security group, and then click **CONTINUE**.
The Review view of the wizard opens.
14. Confirm that all settings are correct, and then click **Launch**.

The Launch Instance Wizard displays a message to let you know your instance is launching.

15. Click **Close.**

Your new instance appears in the list of instances when it is fully launched.

Adding a third network interface

When you first create a virtual private cloud (VPC), there are typically only two network interfaces associated with it. F5 Networks recommends adding a third network interface to the VPC before you use it to deploy the virtual machine.

1. From the Services tab at the top of the Amazon Web Services (AWS) Management Console screen, select **EC2**.
2. In the navigation pane, select **Network Interfaces**.
The Network Interfaces screen opens.
3. Click the **Create Network Interface** button (at top left).
The Create Network Interface dialog box opens.
4. In the **Description** field, type `Internal 10.0.2.0-24` (or a similarly mnemonic name).
5. In the **Subnet** field, select **10.0.2.0/24**.
6. From the **Security Groups** list, select **allow-all-traffic**.
7. Click **Yes, Create**
AWS adds your network interface to the list.
8. Right-click the new network interface, and then select **Attach**.
The Attach Network Interface dialog box opens.
9. From the **Instance** list, select the VE AMI that you created.

Making the virtual machine management port accessible

The management port for your virtual machine may require accessibility over the Internet. However, there are alternative topologies that do not require exposing the management port to the Internet.

F5 Networks recommends, at a minimum, adding restrictions to your source addresses in the `allow-only-ssh-https-ping` security group.

Alternatively, you may find the Amazon Web Services EC2 VPN sufficiently effective so that you do not need to associate an Internet-accessible Elastic IP with the management port.

1. From the Services tab at the top of the Amazon Web Services Management Console screen, select **EC2**.
2. In the navigation pane, select **Elastic IPs**.
The Addresses screen opens.
3. Click **Allocate New Address**.
The Allocate New Address dialog box opens.
4. From the **EIP used in** list, select **VPC**.
5. Click **Yes, Allocate**.
6. In the Address column, right-click the newly created Elastic IP and select **Associate** from the popup menu.
The Associate Address dialog box opens.
7. From the **Instance** list, select the VE AMI that you created as an EC2 hypervisor.
8. From the **Private IP Address** list, select **10.0.0.0/24** (the Management subnet).
9. Click **Yes, Associate**.

Logging in and setting the Admin password

To perform this task, you must have completed the following tasks:

- Created a key pair
- Created and configured a VPC
- Instantiated and launched a BIG-IQ™ Virtual Edition (VE) AMI
- Made the virtual machine management port accessible through the Internet

To maintain security, the first time you log in to your EC2 AMI, you should log in as root, and change the Admin password.

1. Log in to the new AMI that you just launched.

Use the name of the key pair (.pem file), and the elastic IP address of your EC2 instance. `$ ssh -i <username>-aws-keypair.pem root@<elastic IP address of EC2 instance>`

Tip: You can also use a terminal emulator such as PuTTY to test your connectivity. At publication, PuTTY does not support the extension .pem, so remember that you will also need to convert the key pair .pem file to a .ppk file before you can use it with PuTTY.

2. At the command prompt, type `tmsh modify auth password admin`.

Warning: Because this login is visible externally, make sure to use a strong, secure password.

The terminal window displays the message: `changing password for admin`, and then prompts: `new password`.

3. Type in your new password and then press **Enter**.
The terminal window displays the message: `confirm password`.
4. Re-type the new password and then press **Enter**.
5. To ensure that the system retains the password change, type `tmsh save sys config`, and then press **Enter**.

Important: Without your security key pair, you cannot access this AMI. Once you log in with your key pair, you could create a root password. However, if you decide to do this, choose the root password wisely, bearing in mind that depending on your Security Group policies, this login may provide external SSH access.

The Admin password is now changed.

Tip: If at some point you determine you want to restore your virtual machine to its default state, use the following `tmsh` command: `tmsh load sys config default; bigstart restart dhclient` Using a less explicit `tmsh` command has been shown to produce undesirable results.

Index

A

Admin password
 changing [22](#)
 setting [22](#)
 AMI
 launching new [19](#)
 authentication [17](#)

C

CPU
 and guest definition [14](#)

D

deployment
 for EC2 [16](#)
 deployment overview [16](#)

E

EC2 AMI
 launching [19](#)
 EC2 VPC
 creating [18](#)
 Elastic Compute Cloud
 and compatible versions [14](#)
 environment, for guest [14](#)
 external subnet
 adding route for accessibility [19](#)

G

guest environment [14](#)

H

hypervisor, See guest environment.
 hypervisor guest definition [14](#)

I

IAM
 creating user account [17](#)

K

key pairs
 creating [17](#)

M

management port
 making it accessible [21](#)
 maximum allowed throughput rate [14](#)

N

network interface
 adding [21](#)

P

password
 changing Admin [22](#)
 setting Admin [22](#)
 product license [14](#)

R

route
 adding for external subnet [19](#)

S

security groups
 creating [18](#)
 Setup utility [16](#)
 subnet
 adding additional [18](#)
 adding route for external [19](#)

T

task list
 for deploying on EC2 [16](#)
 for deploying on virtual machine [16](#)

V

virtual configuration, and hypervisor guest definition [14](#)
 virtual machine
 launching new [19](#)
 virtual machine settings [14](#)
 virtual private cloud
 creating [18](#)

