BIG-IQ® Device: Device Management

Version 4.4

Table of Contents

Legal Notices

Publication Date

This document was published on June 30, 2015.

Publication Number

MAN-0498-02

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

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.

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 (eay@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.oraclc.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 tile 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 jQuery Foundation and other contributors, distributed under the MIT License. Copyright ©2014 jQuery Foundation and other contributors (http://jquery.com/).

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://javaserverfaces.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.

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.

All code not authored by the Depressed Press is attributed (where possible) to its rightful owners/authors, used with permission and should be assumed to be under copyright restrictions as well.

This product includes Angular software developed by Google, Inc., http://angularjs.org, copyright © 2010-2012 Google, Inc., and distributed under the MIT license.

This product includes node.js software, copyright © Joyent, Inc. and other Node contributors. All rights reserved.

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 product includes the epoxy.js library for backbone, copyright © 2012-2013 Greg MacWilliam. (http://epoxyjs.org)

This product includes Javamail software, copyright ©1997-2013 Oracle and/or its affiliates, all rights reserved; and copyright © 2009-2013 Jason Mehrens, all rights reserved. This software is distributed under the GPLv2 license.

This product includes underscore software, copyright © 2009-2014 Jeremy Ashkenas, DocumentCloud, and Investigative Reporters & Editors.

This product includes node-static software, copyright © 2010-2014 Alexis Sellier.

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opencsv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

This product includes cookies software, copyright © 2014, Jed Schmidt, http://jed.is/, and distributed under the MIT license.

This product includes node-fastcgi software, copyright © 2013, Fabio Massaioli, and distributed under the MIT license.

This product includes socket.io software, copyright © 2013, Guillermo Rauch, and distributed under the MIT license.

This product includes node-querystring software, copyright © 2012. Irakli Gozalishvili. All rights reserved.

Chapter 1

BIG-IQ Device: Device Management Overview

About BIG-IQ Device

BIG-IQ® Device offers you the flexibility to deploy software images, and configurations, and monitor and distribute licenses and license pools for managed BIG-IP ®devices. BIG-IQ Device also provides you with an inventory management tool so that you can easily view and export detailed information about every device you are managing. This centralized device management saves you time because you can perform multiple deployments to a number of BIG-IP devices, without having to log in to each of them individually. The inventory management functionality keeps you apprised of every detail about your managed devices, helping you to better manage your assets.

About the BIG-IQ system user interface

The BIG-IQ® system interface is composed of panels. Each panel contains objects that correspond with a BIG-IQ system feature. Depending on the number of panels and the resolution of your screen, some panels are collapsed on either side of the screen. You can cursor over the collapsed panels to locate the one you want, and click the panel to open. To associate items from different panels, click on an object, and drag and drop it onto the object to which you want to associate it.

Filtering for associated objects

The BIG-IQ system helps you easily see an object's relationship to another object, even if the objects are in different panels.

1. Hover on the object on which you want to filter, click the gear icon, and then click **Show Only Related Objects**.
   The screen refreshes to display only associated objects in each panel.
2. To remove a filter, click **x** icon next to the filtered object in a panel.

Customizing panel order

You can customize the BIG-IQ system interface by reordering the panels.

1. Click the header of a panel and drag it to a new location, then release the mouse button.
   The panel displays in the new location.
2. Repeat step 1 until you are satisfied with the order of the panels.

Filtering on multiple objects

The BIG-IQ system interface makes it easy to search for a specific object. This can be especially helpful as the number of objects increase when you add more users, applications, servers, and so forth.

1. In a panel, click the object on which you want to filter.
   The selected object name displays in the Filter field, and the screen refreshes to display unassociated objects as unavailable.
2. To display only those objects associated with the object you selected, click the **Apply** button.
   The screen refreshes and the objects previously displayed in a gray font do not appear. Only objects associated with the object you click display, and the object you selected displays below the Filter field.
3. To remove a filter, click the **x** icon next to the object that you want to remove, below the Filter field.

Additional resources and documentation for BIG-IQ systems

You can access all of the following BIG-IQ® system documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`.

Document	Description
BIG-IQ® Virtual Edition Setup	BIG-IQ Virtual Edition (VE) runs as a guest in a virtual environment using supported hypervisors. Each of these guides is specific to one of the hypervisor environments supported for the BIG-IQ system.
BIG-IQ® Systems: Licensing and Initial Configuration	This guide provides the network administrator with basic BIG-IQ system concepts and describes the tasks required to license and set up the BIG-IQ system in their network.
BIG-IQ® Device: Device Management	This guide provides details about how to deploy software images, licenses, and configurations to managed BIG-IP devices.
BIG-IQ® Cloud: Cloud Administration	This guide contains information to help a cloud administrator manage cloud resources, devices, applications, and tenants (users).
BIG-IQ® Cloud: Tenant User Guide	This guide contains information to help tenants manage applications.
BIG-IQ® Security Administration	This guide contains information used to centrally manage BIG-IP® firewalls, policies, rule lists (as well as other shared objects), and users.
Platform Guide: BIG-IQ® 7000 Series	This guide provides information about setting up and managing the BIG-IQ 7000 hardware platform.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

Chapter 2

Required BIG-IQ System Components

Installing required BIG-IQ system components

Installing BIG-IQ® system components on a BIG-IP® device requires a licensed BIG-IP device running version 11.3 or later.

You must install and keep up-to-date certain BIG-IQ system components on all BIG-IP devices that are to be brought under central management. Otherwise, device discovery will fail. These required components provide a REST framework required for the BIG-IQ platform. To install these components manually, run the commands from the command line.

Important: *When running this installation script, the traffic management interface (TMM) on each BIG-IP device restarts. Therefore, before running this script, verify that no critical network traffic is targeted to the BIG-IP devices.*

---

1. Log in to the BIG-IQ system command line as the root user.
2. Establish SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-copy-id root@<BIG-IP Management IP Address>`

   This step is optional. However, if you do not establish trust, you will be required to provide the BIG-IP system's root password multiple times.
3. Navigate to the folder in which the required files reside:
   `cd /usr/lib/dco/packages/upd-adc`
4. Run the installation script:

   `./update_bigip.sh –a admin –p <password> <BIG-IP Management IP Address>`

   Where *<password>* is the administrator password for the BIG-IP device.
5. Revoke SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-keygen –R <BIG-IP Management IP address>`

   This step is not required if you did not establish trust in step 2.

Installing these BIG-IQ components results in a REST framework that supports the required Java-based management services.

Chapter 3

Device Resource Management

About device discovery and management

You use BIG-IQ® Device to centrally manage resources located on BIG-IP® devices in your local network, in a public cloud like Amazon EC2, or in a combination of both.

The first step to managing devices is making BIG-IQ Device aware of them through the discovery process. To discover a device, you provide BIG-IQ Device the device IP address, user name, and password. Alternatively, you can upload a CSV file to discover a large number of devices. When you discover a device you place it into a group. These groups help you organize devices with similar features, like those in a particular department or running a certain software version.

After you discover devices, you can view and export inventory details about those devices for easy asset management.

Discovering devices

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

Discovering BIG-IP devices is the first step to managing them.

1. Log in to BIG-IQ Device with the administrator user name and password.
2. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**.
3. For devices on the same subnet as the BIG-IQ system, in the **IP Address** field, specify the IP address of the device:
   - For devices in your local network, or located on an OpenStack or VMware cloud device, type the device's internal self IP address.
   - For devices located on Amazon EC2 cloud, type the device's external self IP address.

   You cannot discover a BIG-IP device using its management IP address.
4. In the **Admin User Name** and **Admin Password** fields, type the administrator user name and password for the managed device.
5. Select the **Auto Update Framework** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.

   For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework. If you do not select the **Auto Update Framework** check box before you click the **Add** button, a message displays prompting you do update the framework or cancel the task.
6. Click the **Add** button.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

Discovering a large group of devices

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you

want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

Before you discover a large group of devices, you must save the information in a `.csv` file in one of the following formats:

- `[address],[userName],[password],[automaticFrameworkUpdate?],[rootUser],[rootPassword]`, for example: `192.168.2.xxx,admin,password,true,root,password` Use this option if you want BIG-IQ Device to automatically update the framework required to manage the devices.
- `[address],[userName],[password]`, for example: `192.168.2.xxx,admin,password`

If you have a large number of devices to discover, discovering them in a group saves you a significant amount of time, because you are not required to provide the device identification details for each individual device. Instead, you can upload a CSV file that contains the IP address, user name, and password for the devices you want to discover.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Devices header, and when the + icon appears, select **Import Devices**.
4. From the **Group Name** list select the group to which you want to add the imported devices.
5. Click the **Choose File** button and select the CSV file to which you exported the device list.

   Alternatively, you can navigate to the CSV file on your computer and drag and drop it to the Import Devices screen.
6. Click the **Discover** button to complete the discovery process.

   If there was a format error for the data in the .csv file, discovery fails and BIG-IQ Device returns an error.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

Discovering and upgrading legacy devices

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

Discovering BIG-IP devices is the first step to managing them. Use this procedure to discover and upgrade BIG-IP devices running a version prior to 11.5.

1. Log in to BIG-IQ Device with the administrator user name and password.
2. Hover over the Devices header, click the + icon when it appears, and then select **Upgrade Legacy Device**.
3. For devices on the same subnet as the BIG-IQ system, in the **IP Address** field, specify the IP address of the device:

   - For devices in your local network, or located on an OpenStack or VMware cloud device, type the device's internal self IP address.
   - For devices located on Amazon EC2 cloud, type the device's external self IP address.

   You cannot discover a BIG-IP device using its management IP address.
4. In the **Admin User Name** and **Admin Password** fields, type the administrator user name and password for the managed device.

5. From the **Software Version** list, select the software version to which you want to upgrade and click the **Upgrade** button.

BIG-IQ System populates the properties of the device that you upgraded, and displays the device in the Devices panel.

Viewing and exporting device inventory details

You can view detailed data about the managed devices in your network. Information includes associated IP addresses, platform type, license details, software version, and so forth. In addition to viewing this information, you can also export it to a CSV file and edit the data as required to create reports for asset management.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. In the Devices panel, click the gear icon next to the device group you want to view, and then click **Inventory**.
   The panel expands to display device details.
4. To export the data to a CSV file, click the **Export** button.
   You can modify the report as required in Microsoft Excel.

About static and dynamic device groups

To help you manage a large number of BIG-IP® devices, you can organize them into groups. You can create two different types of device groups:

- Static group
- Dynamic group

A *static group* contains a specific set of devices. You may want to create a static group for devices hosting certain applications, in a certain geographical location, or running specific version of BIG-IP software. In contrast, a *dynamic group* is essentially a saved query on against a static group. For example, if you create a static group that contained all of your managed BIG-IP devices and you wanted to view only those devices running a specific version of software, you would create a dynamic group with that parameter.

If you delete a managed BIG-IP device from the static group, that change reflects in the dynamic group when you view it.

Creating static group of managed devices

You must license and discover devices before you can place BIG-IP® devices into a group.

To help you manage a large number of devices, you can organize them into groups. For example, you could group devices by applications, geographical location, or department.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Devices header, click the + icon when it appears, and then click **New Group**.
4. In the **Group Name** field, type a name for the BIG-IQ system to identify this group.

You cannot change this identifier once you create this group. The name must contain only alphanumerics, underscores, and dashes. Do not include a space in the group name.

5. In the **Display Name** field, type the name you want to use to identify this group.

   This name is displayed in the Devices panel. You can change this name at any time, after you save this group.

6. In the **Description** field, type a description for this group.

   For example, `BIG-IP devices located in Seattle`. You can change this name at any time, after you save this group.

7. For the **Group Type** setting, select **Static Group**.
8. From the **Parent Group** list, select the source for the group you are creating.
9. Click the **Save** button.

The associated managed devices now display in the Device panel, within the group you created. If you a saved filter on specific devices within this group, you can create a dynamic group.

Creating a dynamic group of managed devices

You must license, discover devices, and create a static group before you can create a dynamic group.

To filter a static group on specific parameters, you can create a dynamic group. For example, if you have a static group for all devices located in a particular city, you might want to view only those running a specific version of software.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Hover over the Devices header, click the + icon when it appears, and then click **New Group**.
4. In the **Group Name** field, type a name for the BIG-IQ system to identify this group.

   You cannot change this identifier once you create this group. The name must contain only alphanumerics, underscores, and dashes. Do not include a space in the group name.

5. In the **Display Name** field, type the name you want to use to identify this group.

   This name is displayed in the Devices panel. You can change this name at any time, after you save this group.

6. In the **Description** field, type a description for this group.

   For example, `BIG-IP devices located in Seattle`. You can change this name at any time, after you save this group.

7. For the **Group Type** setting, select **Dynamic Group**.
8. For the **Source Group** setting, select the static group on which you want to query for results.
9. In the **Search Filter** field, type a term on which you want to filter the group.

   You can filter on a single term or, if you want to filter on more than one parameter, use the standard Open Data Protocol (OData) format.

10. Click the **Save** button.

This dynamic group displays in the Device panel as a child of the associated static group.

Chapter 4

Software Upgrades for Managed Devices

About upgrading software for managed devices

A key feature of BIG-IQ® Device is the ability to centrally upgrade your managed BIG-IP® devices using the Upgrade Advisor.

Upgrades are installed to a new volume, retaining the existing configuration so that if the upgrade does not go as planned, you can boot to the current volume and restore the current configuration.

Upgrading a device

Before you can upgrade a device, you must first download the software image from the F5 Downloads site, `https://downloads.f5.com` to the Images panel.

Use the Upgrade Advisor to upgrade the software version of your managed BIG-IP device from version 11.4.1 or later.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Click the arrow next to the device group that contains the device that you want to upgrade to expand the group.
4. Click the gear icon next to the device you want to upgrade, and then click **Upgrade Software**.
5. Type the admin and root user names and passwords in the appropriate fields.
6. From the **Software Version** list, select the software image to which you want to upgrade this device.
7. Click the **Check** button.

   This initiates a check to ensure that the device is available for upgrade by verifying connectivity.
8. Click the **Upgrade** button to upgrade the device.

Upgrading a legacy device

Before you can upgrade a device, you must first download the software image from the F5 Downloads site, `https://downloads.f5.com` to the Images panel.

Legacy devices are BIG-IP® devices running software version 10.2.0 and later. For this process, you use the legacy Upgrade Advisor. This process confirms that the device has a valid configuration, and rolls that configuration forward to the upgraded software version.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover on the Devices panel header, click the + sign when it appears, and then click **Upgrade Legacy Device**.
4. In the **IP Address** field, type the IP address for the legacy device that you want to upgrade from version 10.2.0 or earlier.
5. Type the admin and root user names and passwords in the appropriate fields.
6. From the **Software Version** list, select the software image to which you want to upgrade this device.
7. Click the **Check** button.

   This initiates a check to ensure that the device is available for upgrade by verifying connectivity.

8. Click the **Upgrade** button to upgrade the device.

Chapter 5

Backing up and Restoring UCS Files

About UCS files

The configuration details of managed devices (including BIG-IQ® Device itself) are contained in a compressed user configuration set (UCS) file. The UCS file contains all of the information required to restore a device's configuration, such as:

- System-specific configuration files
- License
- User account and password information
- SSL certificates and keys

The tasks detailed in this chapter describe operations you may want to perform. Except where noted they are not presented as a required sequence.

Creating a backup UCS file

It is best practice to create a backup of the UCS file for each device in your network, including the BIG-IQ system itself) on a regular basis and before performing a software upgrade. The UCS file backup provides your network with added stability in the event that a system needs to be restored.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Backups header, and click the + icon when it appears.
4. In the **Name** and **Description** fields, type a file name and description to identify this UCS backup file.
   The file name you define in the **Name** field must include the extension `.ucs`.
5. From the **Device** list, select the device for which you want to create the UCS file backup.
6. If you want to include the SSL private keys in the backup file, select the **Include Private Keys** check box.
7. To encrypt the backup file, select the **Encrypt Backup Files** check box.
8. Click the **Create** button
9. To view the status of the backup or change its description, click the gear icon.

This UCS backup file is now available for restoration.

Restoring a UCS file backup

You must create a backup of a device's UCS file before you can restore it.

In the event of a system failure or a requirement to roll back to a previous configuration, you can easily restore a backed up UCS file without having to recreate all of a device’s content.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. In the Backups panel, click the gear icon next to the backup that you want to restore.
4. To change the target device, click the **Change Device** button and select a device from the **Device** list.

5. Click the **Restore** button.

The BIG-IQ system restores the saved UCS backup file to the associated device.

Chapter 6

SSL Certificate Monitoring

About SSL certificate monitoring

When you manage BIG-IP® devices that load balance SSL traffic, you must monitor both their SSL traffic and SSL system certificates. *Traffic certificates* are server certificates that a device uses for traffic management tasks. *System certificates* are the web certificates that allow client systems to log in to the BIG-IP Configuration utility.

BIG-IQ® Device populates the Certificates panel with details about each certificate on every managed BIG-IP device you discover. This makes it easy to monitor the expiration dates all of your devices' SSL certificates from one location.

Monitoring SSL certificate expiration dates

You must discover at least one device for the Certificates panel to display a device's SSL certificate properties before you can monitor the certificates.

SSL certificates have a set expiry date, and do not automatically renew. For this reason, it is important to monitor the SSL certificate's expiration dates for your managed devices.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Configuration**.
3. Review the Certificates panel.

   A yellow icon appears next to any SSL certificates that are either within 30 days of expiring, or have already expired.
4. Click the gear icon next to an SSL certificate to view its properties.

If an SSL certificate is about to expire, or has expired, immediately contact the owner of the device.

Chapter 7

Users, User Groups, and Roles

About users, user groups, and roles

A *user* is an individual to whom you provide resources. You provide access to users for specific BIG-IQ® system functionality through authentication. You can associate a user with a specific role, or associate a user with a user group and then associate the group with a role. A *role* is defined by its specific privileges. A *user group* is a group of individuals that have access to the same resources. When you associate a role with a user or user group, that user or user group is granted all of the role's corresponding privileges.

Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system automatically create the administrator user.

After you initially license and configure the BIG-IQ system, it is important to change the password for the administrator password user from the default password, `admin`.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, click the properties gear for **Admin User**.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click the **Add** button.

Changing the default password for the root user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system automatically create the root user.

After you initially license and configure the BIG-IQ system, it is important to change the password for the root user from the default password, `default`.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, click the gear icon for the **root** user.
4. In the **Old Password** field, type the password.
5. In the **Password** and **Confirm Password** fields, type a new password.
6. Click the **Save** button.

Creating a BIG-IQ system user

You create a user so you can then associate that user with a particular role to define access to specific BIG-IQ® system resources.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. Hover over the Users header, and click the + icon when it appears.
   The panel expands to display the User properties.
4. From the **Auth Provider** list, select the provider that supplies the credentials required for authentication.
5. In the **Full Name** field, type a name to identify this user.
   The full name can contain a combination of symbols, letters, numbers and spaces.
6. In the **Password** and **Confirm Password** fields, type the password for the new user.
7. Click the **Add** button.

You can now associate this user with a role.

Associating a user or user group with a role

Before you can associate a user or user group with a role, you must create a user or user group.

When you associate a user or user group with a role, you define the resources users can view and modify.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users or User Groups panel, click the name you want to associate with a role, and drag and drop it on a role in the Roles panel.
   A confirmation pop-up screen opens.
4. Click the **Confirm** button to assign the user or user group to the selected role.

This user or user group now has access to the resources associated with the role you specified.

Disassociating a user from a role

Use this procedure to disassociate a user from an assigned role.

1. Log in to BIG-IQ System with your administrator user name and password.
2. At the top of the screen, click **System >Users**.
3. Click the name of the user you want to edit.
4. For the User Roles property, delete the user role that you want to disassociate from this user.
5. Click the **Save** button to save your changes.

This user no longer has the privileges associated with the role you deleted.

Chapter 8

Deploying Software Images

About deploying software images and configuration files

Using BIG-IQ® Device to centrally manage the devices in your network means that you can deploy software images and configurations without having to log in to each individual BIG-IP® device. Software image files can contain new software, upgrades, or hot fixes. You can choose to deploy a software installation job immediately, or you can save the job for later deployment. While the software installation job runs, you can continue to perform other administrative tasks.

Installing software images

You must first discover and license a device before you can install a software image.

You can centrally deploy software images for new installations, upgrades, or hot fixes to managed physical and virtual devices with just a few clicks.

1. Browse to the F5 Downloads site, `https://downloads.f5.com`, and locate the image you want to download.
2. Using a file transfer program, such as FTP, download the `.iso` file to the BIG-IQ® Device shared images directory (`/shared/images`).
3. Log in to BIG-IQ Device with the administrator user name and password.
4. At the top of the screen, click **Provisioning**.
5. Hover over the Deployment panel and click the (+) icon.
6. In the **Name** field, type a name for this deployment job.
7. From the **Type of Job** list, select **Install a Software Image**.
8. For the **Options** setting, select the check box next to the action(s) you want the BIG-IQ system to perform after the image is installed.
9. From the **Software Image** list, select the image you want to install on the specified device.
10. From the **Install Location** list, select the location you want to install the software image.
11. Click the **Deploy** button to immediately initiate the job, or click the **Save** button for later deployment.
12. Monitor the job by viewing the status in the Deployment panel.
    - If the **Pending** list shows the status of the job as **Validation Failed**, modify the details as required.
    - Once the job displays as **Runnable**, click the gear icon, and then click the **Deploy** button.

When deployment is complete, the job displays in the Deployment panel's **Complete** list until you delete it.

Chapter 9

Configuring BIG-IQ High Availability

About a high availability active-active cluster

You can ensure that you always have access to managed BIG-IP® devices by installing two or more BIG-IQ® systems in an active-active, high availability (HA) configuration. Any configuration change that occurs on one BIG-IQ system is immediately synchronized with its peer devices. If a BIG-IQ® system in an active-active HA configuration fails, a peer BIG-IQ system takes over the device management.

Configuring BIG-IQ System in an active-active high availability cluster

You must activate a license on two or more BIG-IQ® systems before you can configure a high availability cluster.

Configuring a high availability cluster ensures that if one BIG-IQ system goes offline, another BIG-IQ system can continue managing your devices without interruption.

1. Log in to BIG-IQ System with your administrator user name and password.
2. Hover over the BIG-IQ Systems banner and click the + sign when it appears.
3. In the **Peer IP Address** field, type the self IP address (on the internal VLAN) of the peer system.
   Do not use the management IP address of the peer system.
4. In the **User name** and **Password** fields, type the administrative user name and password for the system.
5. From the **Group** list, select the group to which you want to add this BIG-IQ system.

If discovery of the newly configured BIG-IQ system fails, a **Delete** button displays. Verify the correct self IP address and credentials. Then click the **Delete** button to remove the incorrect information, and re-type the self IP address, user name, and password.

Chapter 10

License Pools

About pool and utility licenses

When you purchase and activate a license pool, you can assign licenses to BIG-IP® virtual edition (VE). This keeps operating costs fixed and allows for flexible provisioning options. There are two types of license pools: pool licenses and utility licenses.

Pool licenses are purchased for a fixed number of devices, but are not permanently tied to a specific device. As resource demands change, you can revoke and grant those licenses to other resources as required.

Utility licenses are not limited to a set number of devices. You can create any number of licenses as needed, selecting the frequency in which you are billed.

About pool licenses

Pool licenses are purchased for a fixed number of devices, but are not permanently tied to a specific device. As resource demands change, you can revoke and grant those licenses to other resources as required.

Automatically activating a pool license

You must have a base registration key before you can activate the license pool.

If the resources you are licensing are connected to the public internet, you can automatically activate the license pool.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses panel, click the + sign when it appears, and then click **Add New Pool License**. The panel expands to display New License properties.
4. In the **License Name** field, type a name for this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. In the **Add-on Keys** field, paste any additional license key you have.
7. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button. The End User License Agreement (EULA) displays.
8. To accept the EULA, click the **Accept** button.

You can now assign this license to a BIG-IP® device.

Manually activating a pool license

You must have a base registration key before you can activate the pool license.

If the BIG-IQ® Device you are licensing is not connected to the public internet, you can still activate the pool license manually.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses panel, click the + sign when it appears, and then click **Add New Pool License**. The panel expands to display New License properties.

4. In the **License Name** field, type a name for this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. In the **Add-on Keys** field, paste any additional license key you have.
7. For the **Activation** method setting, select **Manual** and click the **Generate Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
8. Copy the text displayed in the Device Dossier field, and click the **Access F5 manual activation web portal** link.

   Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
9. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
   The Accept User Legal Agreement displays.
10. To accept the EULA, click the **Accept** button.
11. Copy the license file from the F5 license activation portal to BIG-IQ Device.

You can now assign this license to a BIG-IP® device.

Assigning a pool license to a BIG-IP VE

Before you can assign a license pool to a BIG-IP® VE device, you must activate the license pool on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign a pool license.

Using a pool license for a BIG-IP VE device provides you with the flexibility to easily manage resources and operating costs.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Deployment panel, click the + sign when it appears, and click **New Deployment Job**.
4. In the **Name** field, type a name for this license deployment.
5. From the **Device** list, select the device you want to license.
6. From the **Licensing** list, select **Use a Pool License**.
7. From the **License Pool** list, select the pool license you want to use for this device.
8. Click the **Deploy** button.
9. To confirm that the license was successfully deployed, click the **License Pool** from which you deployed the license, and click the **Assignments** tab.
   The device you licensed displays with the license status and the last contact from BIG-IQ Device.

Revoking a utility license from a managed device

Before you revoke a utility pool license, you must assign a pool license to a BIG-IP® device.

When fewer devices are required for your applications, you can revoke licenses to reassign them to other resources as needed.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Deployment panel, click the + sign when it appears, and click **New Deployment Job**.
4. In the **Name** field, type a name for this license revocation.
5. From the **Type of Job** list, select **Modify a Virtual Device**.

6. From the **Device** list, select the device from which you want to revoke a license.
7. From the **Licensing** list, select **Revoke a License**.
8. From the **Utility License** list, select the utility license you want to revoke.
9. Click the **Deploy** button.

You can now assign this license to a BIG-IP® device.

About utility licenses

Utility licenses are based on metered usage and you are charged only for the duration that the license is activated. When a resource is no longer required, you revoke its license and are no longer charged for that instance.

Each utility license is associated with a specific set of F5 offerings (for example, BIG-IP LTM 25M, BIG-IP LTM 200G, and BIG-IP LTM 1G). You can activate any number of seat licenses (or license grants) for the selected offering. You create seat licenses when you need them, and specify the unit of measure (an hour, a day, a month, or a year) for which you want to be billed for each license. BIG-IQ® Device tracks usage consumed in each billing period, which you send that data directly to F5.

Automatically activating a utility license

You must have a base registration key before you can activate the utility license.

If the resources you are licensing are connected to the public internet, you can automatically activate the utility license.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses panel, click the + sign when it appears, and then click **Add New Utility License**.
4. In the **License Name** field, type a name for this license.
5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. For the **Activation Method** setting, select **Automatic**, and click the **Activate** button.
   The End User License Agreement (EULA) displays.
7. To accept the EULA, click the **Accept** button.

You can now assign this utility license to a BIG-IP device.

Manually adding and activating a utility license

You must have a base registration key before you can activate the utility license.

If the resources you are licensing are not connected to the public internet, you can still activate the utility license manually.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Licenses panel, click the + sign when it appears, and then click **Add New Utility License**.
4. In the **License Name** field, type a name for this license.

5. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
6. For the **Activation** method setting, select **Manual** and click the **Generate Dossier** button.
   The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
7. Copy the text displayed in the Device Dossier field, and click the **Access F5 manual activation web portal** link.

   Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
8. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
   The Accept User Legal Agreement displays.
9. Select the check box to agree to the license terms, and then click the **Next** button.
   The license key displays
10. Copy the license key.
11. On the BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Add** button.
    The unactivated utility license displays in the Licenses panel.
13. Click the arrow next to the utility license you created to expand the list of licenses.
14. Click the utility license you want to activate.
15. Copy the license key.
16. On the BIG-IQ Device, into the **License Text** field, paste the license key.
17. Click the **Apply** button.

    If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the utility license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this utility license to a BIG-IP VE device.

Assigning a utility license to a BIG-IP device

Before you can assign a utility pool to a BIG-IP® VE device, you must activate the utility license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign a pool license.

Using a utility license for a BIG-IP VE device provides you with the flexibility to easily manage resources and operating costs by choosing a specific billing term for licenses.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Deployment panel, click the + sign when it appears, and click **New Deployment Job**.
4. In the **Name** field, type a name for this license deployment.
5. From the **Type of Job** list, select **Modify a Virtual Device**.
6. From the **Device** list, select the device you want to license.
7. From the **Licensing** list, select **Use a Utility License**.
8. From the **License Pool** list, select the pool license you want to use for this device.
9. Click the **Deploy** button.
10. To confirm that the license was successfully deployed, in the Licenses panel, click the license you deployed and review the License Assignment section.
    The device you licensed displays with the license status, the associated device, and the billing terms for the license.

Revoking a utility license from a managed device

Before you revoke a utility pool license, you must assign a pool license to a BIG-IP® device.

When fewer devices are required for your applications, you can revoke licenses to reassign them to other resources as needed.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. Hover over the Deployment panel, click the + sign when it appears, and click **New Deployment Job**.
4. In the **Name** field, type a name for this license revocation.
5. From the **Type of Job** list, select **Modify a Virtual Device**.
6. From the **Device** list, select the device from which you want to revoke a license.
7. From the **Licensing** list, select **Revoke a License**.
8. From the **Utility License** list, select the utility license you want to revoke.
9. Click the **Deploy** button.

You can now assign this license to a BIG-IP® device.

Automatically submitting a utility license usage report to F5

You must assign a utility license to a device before you can submit and save a usage report.

You provide this report to F5 Networks for billing purposes, as per the terms and conditions of your contract.

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the gear icon for the utility license that you want to submit for billing, and then click **Create Usage Report**.
4. For the usage submission method, select **Automatically submit report to F5**.
5. Click the **Submit** button.
   BIG-IQ Device sends a report directly to F5, and saves a copy on BIG-IQ Device.

Downloading a utility license usage report

You must assign a utility license to a device before you can create a utility usage report for that license.

You can use this report to augment your internal licensing management and budget planning. You also have the option to submit this report manually to F5 for billing purposes.

Note: *If you would like to manually submit this report to F5 for billing purposes instead of automatically, contact F5 Support.*

---

1. Log in to BIG-IQ Device with your administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the gear icon for the utility license for which you want to download a usage report, and then click **Create Usage Report**.

4. For the **Period** setting, in the **From** and **To** fields, type the date range for the report. Alternatively, click the calendars and navigate to the dates.
5. Select a format option for the report.
6. Click the **Download** button and select an option to open the file, or save the file.

Chapter 11

Integrating Amazon Web Services

- *About Amazon Web Services (AWS) integration*
- *Network requirements for AWS integration communication*
- *Creating a Virtual Private Cloud*
- *Launching a virtual server with an Amazon Machine Image (AMI)*
- *Creating an Amazon Identity and Access Management (IAM) user account*
- *Creating a BIG-IP VE version 11.5 or later in the Amazon EC2 cloud*
- *Configuring an EC2 cloud connector*
- *Setting up tenant access using IAM*
- *Viewing activity for cloud resources*

About Amazon Web Services (AWS) integration

BIG-IQ® Cloud provides you with the tools to manage Amazon EC2 and CloudWatch resources required to perform application delivery. Management tasks include discovering and creating BIG-IP® VE virtual machines located in Amazon Virtual Private Cloud (VPC), application pool servers, and deploying applications. You can use these features to accommodate application traffic fluctuations by periodically adding and retracting devices and application servers, as needed. Additionally, you can provide tenants access to self-deployable iApps® through Amazon EC2 integration.

To provide access to these services for Amazon EC2 tenants, you configure communication between Amazon EC2 products, and BIG-IQ Cloud. Then, you associate a Amazon EC2 cloud connector with a device, and create a catalog entry for a corresponding Amazon EC2 service profile. The tenants to whom you give access to the catalog entry see it in their applications panel. From there, they can use it to self-deploy their own iApps.

Network requirements for AWS integration communication

BIG-IQ Cloud integrates with three different Amazon Web Services: Amazon EC2, Amazon CloudWatch, and BIG-IP Virtual Edition deployed in managed Amazon Virtual Private Cloud (VPC).

For proper communication to devices located in an Amazon web service, BIG-IQ® Cloud you must configure an outbound self IP address to DNS and NTP, and you must define a network route between the BIG-IQ Cloud internal VLAN and the public Internet, or the Amazon web services endpoint. For specific instructions, refer to *BIG-IQ® System: Licensing and Initial Setup* and your Amazon documentation .

Creating a Virtual Private Cloud

You need an Amazon Virtual Private Cloud (VPC) to deploy the BIG-IQ® Cloud system, because AWS provides only multiple network interface card (NIC) support for instances that reside within a VPC.

You create a virtual network topology according to your networking needs. The standard network topology used for BIG-IQ Cloud integration includes three subnets. These subnets provide virtual private address spaces used to interconnect your machines and applications. You can use elastic self IP addresses for public internet accessibility.

For the most current instructions for creating a VPC, refer to the VPC Documentation web site, `http://aws.amazon.com/documentation/vpc/`.

1. Navigate to `https://console.aws.amazon.com/vpc` and select the AWS Region in which you want to manage resources.

   For example, Oregon.

2. From the VPC Wizard's **VPC with Public and Private Subnets** option, set the IP CIDR Block to `10.0.0.0/16`.
3. Set the public subnet to `10.0.0.0/24`.

   This is the management network.

4. Select an availability zone.

For example, **us-west-2c**. It is crucial that you use this availability zone throughout the configuration process. Objects configured in one zone are not visible within other zones, so they cannot function together. This availability zone is required when you create a BIG-IQ Cloud connection.

5. Set the private subnet to `10.0.1.0/24`.

   This is the external data network.

6. Create subnet `10.0.2.0/24`.

   This is the internal network.

7. Create a security group named, `allow-all-traffic`, and associate it with the VPC you created.

   You must use this exact name.

8. Set the **Inbound Rules ALL Traffic Source** to `0.0.0.0/0`.
9. Set the **Outbound Rules ALL Traffic Destination** to `0.0.0.0/0`.
10. Create a Route Table for the external data network to reach the Internet.
11. Add a route to Destination **0.0.0.0/0** through Target `igw-<xxxx>`.

    `<xxxx>` is the Internet Gateway that the VPC Wizard created automatically.

12. Allocate two Elastic IP Addresses.

You now should create a BIG-IQ Cloud connector to associate with this VCP.

Launching a virtual server with an Amazon Machine Image (AMI)

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.

   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.

Creating an Amazon Identity and Access Management (IAM) user account

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

Important: *This task is optional; you can create a virtual machine without creating an IAM user account to control access, but it is best practice to use an IAM account. F5 recommends that you do not use the AWS root account and access keys. Instead, use IAM to create identities you can more easily manage and revoke in the case of a security breach.*

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

For this task, you must create a group and two IAM user accounts. For the most current instructions for performing these steps, refer to the IAM documentation web site, `http://aws.amazon.com/documentation/iam/`.

1. From `https://console.aws.amazon.com/iam`, create a group with aws-full-access (Administrator Access).
2. Create an AWS-Admin user and add that user to the **aws-full-access** group.
3. Create a BIG-IQ Connector user and add that user to the **aws-full-access** group.

   For this user, you must download or copy an access key that you use to connect BIG-IQ Cloud to your AWS account
4. From the AWS dashboard, set up an account alias.

   Note the IAM user login link. For example, `https://my-account-alias.signin.aws.amazon.com/console`
5. Log out of the AWS dashboard as the root user.
6. Navigate back to the user login link and sign in as the **AWS-Admin** user.

You can now create a new Virtual Private Cloud (VPC).

Creating a BIG-IP VE version 11.5 or later in the Amazon EC2 cloud

After you license and perform the initial configuration for the BIG-IQ system, you can create devices in the Amazon EC2 cloud. For proper communication, you must configure a route between each instance to the BIG-IQ system. If you do not specify the required network communication route between the devices, then creation fails.

Before you perform this task you must first open specific ports on your EC2 AMI BIG-IQ instance and on any associated EC2 BIG-IP instances. To open these ports, you need additional security group rules in your `allow-only-ssh-https-ping` security group, and you need to associate these rules with the management interface.

You need to create three rules: two outbound rules for the BIG-IQ instance, and one inbound rule for the BIG-IP instance.

Group Name	Group Description	Rule Name	Source	Port
allow-only-ssh-https-ping	Allow only SSH, HTTPS, or PING	Outbound SSH	0.0.0.0/0	22 (SSH)
		Outbound HTTPS	443 0.0.0.0/0	443 (HTTPS)
		Inbound HTTPS	0.0.0.0/0	443 (HTTPS)

To create a BIG-IP VE instance in Amazon EC2 cloud, you associate the EC2 Cloud connector you configured with that device.

1. Log in to BIG-IQ® Cloud with your administrator user name and password.
2. Hover over the Devices header, and click the + icon when it appears.
3. Select the **Create a Device** option.
4. From the Cloud Connector list, select the EC2 cloud connector you created.
5. From the **Device Image** list, select the AMI you created for this device.
6. Select the **Auto Update Framework** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.

For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework. If you do not select the **Auto Update Framework** check box before you click the **Add** button, a message displays prompting you do update the framework or cancel the task.

7. To prompt BIG-IQ Cloud to assign the default user admin and a randomly-selected password, select the **Use "admin"** check box.
8. To assign a specific user name and password, deselect the **Use "admin"** check box.
   The screen refreshes to display additional settings.
9. In the **User Name** and **Password** fields, type a user name and password for the user of this devices.
10. Click the **Add** button.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

Configuring an EC2 cloud connector

Before you can create an EC2 cloud connector, you must first discover devices in the Amazon EC2 cloud and create an Amazon Identity and Access Management (IAM) user account. If you want BIG-IQ Cloud to automatically provision additional BIG-IP VE servers and devices for your tenant when more resources are needed, you must also purchase and activate a license pool to associate with this connector.

To enable integration between a third-party cloud provider and the BIG-IQ device, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

1. Log in to BIG-IQ® Cloud with your administrator user name and password.
2. Hover over the Connectors header and click the + icon when it appears.
3. In the **Name** and **Description** fields, type a name and description.

   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
4. From the **Cloud Provider** list, select **Amazon EC2**.
5. In the **Region Endpoint** field, type the entry point URL.

   For example, `ec2.us-east-1.amazonaws.com` is the region end point for the Amazon EC2 US East (Northern Virginia) Region. Refer to the AWS documentation for a list of all regional end points at `http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region`
6. In the **Key ID** and **Secret Key** fields, type the credentials of the BIG-IQ-Connector IAM user.

   For security purposes, it is important to specify a user that has Amazon EC2 Full Control Access.
7. In the **Availability Zone** field, type the location of the region in which the instances are located.

   For example, type `us-west-2c` for the availability zone for Oregon state.
8. In the **Virtual Private Cloud** field, you may type the identification for the EC2 Virtual Private Cloud (VCP) network topology inside the Availability Zone.

   This step is optional. If you do not specify the identification for a VCP, BIG-IQ Cloud uses the first one it discovers in the Availability Zone.
9. Click the arrow next to **Device & Server Provisioning** to display associated options.
   The screen refreshes to display the options.
10. To prompt BIG-IQ Cloud to automatically provision additional BIG-IP VE devices when more resources are needed for application traffic, for the **Device Elasticity** setting, select **Enable**.

11. From the **Device License** list, select a rate at which you want Amazon to direct-bill for additional devices, or select a license pool from which to grant a license.

    You must activate a license pool before you can select it.
12. To automatically prompt BIG-IQ Cloud to provision additional servers when more resources are needed to manage an influx in application traffic, for the **Server Elasticity** setting, select **Enable**.
13. Review the network settings populated when you selected a connector, verifying that the proper CIDR blocks display for management, external, and internal.
14. Click the **Save** button.
15. If the system discovered devices, you must expand the device's properties panel, and provide the device's credentials to finalize the discovery process.
16. Review the network settings populated when you selected a connector, verifying that the proper CIDR blocks display for management, external, and internal.

You now create a device associated with this EC2 cloud connector.

Setting up tenant access using IAM

You might want your tenants to have access to all or part of the EC2 cloud you are provisioning so that they are able to configure resources required by their applications. You can provide full access by simply providing the account information (user name and password) that you created previously. More typically, you can provide more limited access by setting up separate user accounts for the tenant, and then configuring the access for those users as best suits your needs.

Important: *If you decide to grant full tenant access to the IAM account, bear in mind that restricting this account to a single tenant becomes even more prudent.*

The following step-sequence provides an outline of the tasks you perform using the AWS EC2 user interface. For the most current instructions for performing each of these tasks, refer to the Amazon Web Services EC2 Management Console web site `https://console.aws.amazon.com/ec2/v2/home`.

1. Log in to the AWS IAM console.
2. Create a user role to encapsulate relevant permissions for this tenant.

   If a user needs to create key pairs, make certain that they have sufficient permissions.
3. Configure password policies for this tenant.
4. Create user accounts and set passwords for this tenant.
5. Create the user(s).
6. Specify the IAM AWS Management URL that you will provide to your tenants so that they can log in to this IAM account and directly manage their resources.

Viewing activity for cloud resources

Before you can view dynamic cloud resource activity, you must have an EC2 cloud connector with the **Device Elasticity** setting enabled.

Viewing activity for dynamic cloud resources gives you insight into how cloud resources are expanding to address increased traffic to applications.

1. To view the resource associated with a particular activity, click the activity located on the Activities panel.
   The associated objects are highlighted in the relevant panels.
2. To view specific activity details, place your cursor on an activity.
   A popup window opens to display further details about the selected activity.

Chapter 12

Integrating OpenStack

About OpenStack integration

BIG-IQ® Cloud provides you with the tools to manage OpenStack versions 2013.1 (Grizzly) and 2013.2 (Havana) resources required to run applications. Management tasks include discovering BIG-IP® VE virtual machines and discovering, creating, starting, and stopping OpenStack application servers running in the private cloud. You can use this feature to accommodate seasonal traffic fluctuations by periodically adding and retracting devices and application servers as needed. Additionally, you can provide tenants access to self-deployable iApps® through OpenStack integration.

To provide access to these services for OpenStack tenants, you configure communication between OpenStack products, and BIG-IQ Cloud. Then, you associate an OpenStack cloud connector with a device, and create a catalog entry for a corresponding OpenStack service profile. The tenants to whom you give access to the catalog entry see it in their applications panel. From there, they can use it to self-deploy their own iApps.

Network requirements for communication with OpenStack cloud services

Before you can manage devices residing in an OpenStack private cloud, you must establish proper communication between the BIG-IQ® Cloud and the OpenStack controller node. Generally, this means defining a network route between the BIG-IQ Cloud internal VLAN and the public Internet, or the OpenStack private cloud endpoint.

The BIG-IQ Cloud connector for OpenStack parses the OpenStack cloud's network naming convention as follows:

- Any network that contains the name `mgmt`, `management`, `internal`, or `external` is assumed to indicate a network type (always-on management network, internal network, and external network, respectively). If there are multiple networks, BIG-IQ Cloud uses the first network it finds with those names to communicate with the OpenStack cloud.
- If there are no networks with those names, BIG-IQ Cloud assigns the network type based on the order in which the network was discovered. For example, if BIG-IQ Cloud discovers networks `10.10.10.0/24`, `20.20.20.0/24`, and `30.30.30/24`, it assigns them as follows:

- Management network `10.10.10.0/24`
- External network `20.20.20.0/24`
- Internal network `30.30.30.0/24`

This is important to know, because when you create a new application server in OpenStack through BIG-IQ Cloud, you are allowed to select the internal or external network, but not the management network.

Tip: *If you deploy a BIG-IP device in the OpenStack cloud and you want to discover it from BIG-IQ Cloud, you must have an external or interface route from BIG-IQ Cloud to the OpenStack cloud network. If BIG-IQ Cloud is not on same network as OpenStack, you might need to add a floating IP address to the interface to make it accessible. While either external or internal interfaces are acceptable, we recommend using the external interface.*

Important: *For specific instructions about how to configure your network for OpenStack, refer to the OpenStack documentation.*

OpenStack Compute edits required to use BIG-IP VE systems

Before you create BIG-IP VE systems in an OpenStack environment, you must edit a file on each OpenStack Compute node. If you do not edit this file, any BIG-IP VE system you configure fails to start.

1. Log in to the command line of each OpenStack Compute node and edit `/etc/nova/release` to read as follows:

```
[Nova]
vendor = Red Hat
product = Bochs
package = RHEL 6.3.0 PC
```

2. Restart the OpenStack Compute node services.

This edit provides the BIG-IP VE system required access to the OpenStack hypervisor. Any BIG-IP VE systems you create in the OpenStack environment can now properly start.

Discovering devices located in the OpenStack cloud

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

For devices located in a third-party cloud, you must know the internal self IP address (For OpenStack or VMware cloud) or the external self IP address for Amazon EC2. You also must configure BIG-IQ Cloud with DNS so it can resolve the endpoint by name. To access this setting, log in to BIG-IQ System, select the BIG-IQ system you want to modify, and click the gear icon.

1. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**.
2. In the IP Address field, type the device's external self IP address.

   You cannot discover a BIG-IP device using its management IP address.
3. When the BIG-IQ system and the BIG-IP device are on different subnets, you must create a route:
   a) Use SSH to log in to the BIG-IQ system's management IP address as the root user.
   b) Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

   Where `<route name>` is a user-provided name to identify the new route, and `<x.x.x.x>` is the IP address of the default gateway for the internal network.
4. In the **Admin User Name** and **Admin Password** fields, type the administrator user name and password for the managed device.
5. Select the **Auto Update Framework** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.

   For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework. If you do not select the **Auto Update Framework** check box before you click the **Add** button, a message displays prompting you do update the framework or cancel the task.
6. Click the **Add** button.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

You can now associate this device with an OpenStack cloud connector and allocate resources to tenants.

Associating an OpenStack connector with devices

BIG-IQ® Cloud must be able to collect statistics to provide server diagnostics to tenants. By default, most OpenStack deployments are configured to disallow diagnostics collection. For successful deployment, you must change this option by editing the Nova `policy.json` file (typically located in the `/etc/nova/` directory) and changing the following line: `compute_extension:server_diagnostics": "rule:admin_api` to `compute_extension:server_diagnostics": "rule:admin_or_owner"`.

To enable integration between a third-party cloud provider and the BIG-IQ device, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

1. Log in to BIG-IQ® Cloud with your administrator user name and password.
2. Hover over the Connectors header and click the + icon when it appears.
3. In the **Name** and **Description** fields, type a name and description.

   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
4. From the **Cloud Provider** list, select **OpenStack**.
5. In the **OpenStack Controller Node URI** field, type the URI for the OpenStack controller node.
6. In the **OpenStack User Name** field, type the user name for the OpenStack administrator.

   For example, `https://<IP address>:<Port>` or `http://<IP address>:<Port>`.

   Note that default port for `http` is `5000`.
7. In the **OpenStack Tenant Name** and **OpenStack Password** fields, type the tenant (also known as, project) name and password.
8. Click the **Save** button.

BIG-IQ Cloud discovers all associated OpenStack servers, and populates them in the Servers panel.

To complete discovery of BIG-IP® devices and populate the Devices panel, provide the administrator user name and password when requested. You can then associate tenants with the OpenStack connector.

Chapter 13

Integrating VMware

Overview: VMware integration

There are three VMware products that you can integrate with BIG-IQ® software.

- For VMware NSX version 6.1 (only), BIG-IQ Cloud provides you with the tools to manage VMware resources required to run applications. Management tasks include discovering, creating, starting, and stopping BIG-IP® VE devices running in the private cloud. You can use this feature to accommodate seasonal traffic fluctuations by periodically adding and retracting devices and application servers as needed. Additionally, you can provide tenants access to self-deployable iApps through VMware integration.
- For vCloud Director versions 1.5 and 5.1, the BIG-IQ software integration makes it possible for you to use the VCD interface with your cloud applications to manage the F5 cloud applications.
- For VMware vShield version 5.1 and 5.5 (also known as VCNS version 5.5), and VMware NSX 6.0, the BIG-IQ software integration provides you with the tools to provide tenants access to self-deployable iApps®.

To provide access to these services for VMware tenants, you configure communication between VMware products, and BIG-IQ Cloud. Then you associate a VMware cloud connector with a device, and create a catalog entry for a corresponding VMware service profile. The tenants to whom you give access to the catalog entry see it in their applications panel. From there, they can use it to self-deploy their own iApps.

Network requirements for communication with VMware cloud services

For proper communication, BIG-IQ® Cloud must have network access to the resources on which VMware software is installed. Before you can manage cloud resources, you must define a network route between the BIG-IQ Cloud device's internal VLAN and the management VLAN on the VMware.

Integrating VMware with your cloud applications

Integrating VMware with your cloud applications makes it possible for you to use the VMware interface to manage your F5 cloud applications.

1. Authenticate with the F5 Cloud REST API.

   Tip: *Refer to Authentication with the F5 REST API in the BIG-IQ Cloud Overview chapter of this guide for information about authentication strategies.*

   Tip: *Refer to the BIG-IQ® Cloud Service API Reference Guide for details about using the APIs required for this task.*

2. Discover at least one BIG-IP® system using the `Add a managed device` API.
   `/mgmt/cm/cloud/managed-devices POST`
3. Create a catalog of BIG-IQ® Cloud applications to publish into the VMware vendor template using the `Create provider iApp template` API.
   `/mgmt/cm/cloud/provider/templates/iapp POST`
4. Create new tenants for VMware using the `Create tenant` API.
   `/mgmt/cm/cloud/tenant POST`

5. Create a VMware cloud connector using the `Create VMware connection` API, specifying the IP address and appropriate credentials.
   `/mgmt/cm/cloud/connectors/vmware POST`
   The applications you included when you created the VMware vendor template are published to the VMware interface.

The tenants that you created and connected to VMware can now use the VMware interface to create applications. Fields that are tenant-editable are displayed in the VMware user interface.

Associating a VMware cloud connector with a device

To enable integration between a third-party cloud provider and the BIG-IQ device, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

1. Hover over the Connectors header and click the + icon when it appears.
2. In the **Name** and **Description** fields, type a name and description.
   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
3. From the **Cloud Provider** list, select **VMware Networking**.
4. From the **Devices** list, select the device you want to associate with this connector.
5. To select additional devices to associate with this connector, click the + icon at the right of the list. BIG-IQ system discovers application servers associated with this connector, and populates them in the Server panel. If the system discovers F5 devices, it populates the Device panel with them.
6. In the **VMware Networking Address** field, type the IP address of the VMware system.
   The VMware IP address must be fully accessible from the BIG-IQ device's internal VLAN.
7. In the **VMware Networking User Name** and **VMware Networking Password** fields, type the credentials for the VMware administrator.
8. From the **BIG-IQ User Name** list, select the BIG-IQ user the VMware administrator should contact and, in the **BIG-IQ Password** field, type the password for that user.
9. Click the **Save** button.

How vShield Manager processes tenant-editable values

There are a few complexities to be aware of when you create a service profile in the vShield interface to access the applications in your template.

Tenant Editable Field	Action
Tenant Name	Make a note of the tenant name you created. You need to enter it in the vShield interface. If you choose an incorrect tenant name or leave the tenant name blank, the VSM create service profile task fails.
Pool members	Enter values in the Service Attributes portion of the VSM interface.
Virtual IP addresses	Enter values in the Service Attributes portion of the VSM interface.

Tenant Editable Field	Action
Tabular data	There is additional complexity for API values represented in a table. Editable table columns appear in the VSM interface as an entry in the list of Vendor Attributes. To specify multiple values for an entry, you enter them in a comma-delimited list. Consider the following example.

```
{
"name": "pool__members",
"columns": [
{ "name": "addr",              "isRequired": false, "providerType": "NODE"},
{ "name": "port",              "isRequired": true, },
{ "name": "port_secure",       "isRequired": true, },
{ "name": "connection_limit", "isRequired": true, "provider": "10000" },
{ "name": "ratio",             "isRequired": true, "provider": "1" },
{ "name": "priority",          "isRequired": true, "provider": "0" }
],
"serverTier": "default"
}
```

For the table represented in this example, there are two editable columns, port and port_secure. In the VSM interface there are Vendor Attributes rows to represent these values. The port appears as pool__members.port and the secure port entry appears as pool__members.port_secure. Enter values for these in a comma-delimited list (for example, `pool__members.port_secure 443, 444`).

About VMware NSX version 6.1 integration

The tasks you perform to set up and configure BIG-IQ® devices to manage BIG-IP® system traffic in a VMware NSX version 6.1 network, use both the BIG-IQ software user interface and the VMware NSX user interface. There is also a task for which you can have greater control and flexibility using a REST API call to the NSX API. This optional task is included at the end of the task sequence.

In most production environments, data plane and control plane traffic are segregated for security reasons. To accommodate this requirement, traffic management functions are not permitted on the same network subnet with flowing network traffic. To accomplish this topology, this integration configures a total of four subnets. Two are used for BIG-IQ network management and the other two are for BIG-IP system traffic flow.

Task summary

Configuring VMware NSX 6.1 for BIG-IQ

You must have installed a BIG-IQ® system with two control plane subnets: one to be used for provisioning BIG-IP devices, and the other for BIG-IP® device discovery. These two subnets need to be interconnected.

Additionally, you must configure the following objects in VMware vSphere Web Client before you can perform this task.

- A Datacenter.
- A Datastore for your Datacenter.

Configuring the VMware objects described in this task makes it possible for a BIG-IQ system to configure and license a BIG-IP VE that you can manage with NSX as a load balancing service runtime. Your vCenter users can use this service runtime to deploy load-balanced virtual servers.

1. In the VMware vSphere Web Client, create four networks.

   Two networks must be control plane networks; the BIG-IQ system uses one for provisioning BIG-IQ systems and the other to discover BIG-IP devices. The other two networks are data plane; the BIG-IP device uses one to pass external traffic and the other to pass internal traffic.

2. In the VMware vSphere Web Client, create four IP Pools, one for each network. As you create each pool, you are prompted for a name. Make a note of the names you choose so that when you need to associate each pool to a network interface, you will know which is which.
   a) Define the provisioning network for the BIG-IP device. Use a typical IP address range to refer to the first management IP pool: `192.168.11.0/24`.
   b) Define the external data network. Use a typical IP address range to refer to the first data IP pool: `10.22.0.0/16`.
   c) Define the internal data network. Use a typical IP address range to refer to the second data IP pool: `10.33.0.0/16`.
   d) Define the discovery network for the BIG-IP device. Use a typical IP address range to refer to the second management IP pool: `192.168.44.0/24`.

3. In the VMware vSphere Web Client, set up a web server on one of the just-created management networks.

   The NSX Manager uses the URL of this web server to access the installation file (OVF) for the BIG-IP VE you intend to provision.

4. Copy the OVF file that the NSX Manager will use to create the BIG-IP VE to an accessible location on the just-created web server.
5. Create a new user using the `Create user` API.
   `/mgmt/shared/authz/users POST`

   Important: *BIG-IQ APIs use the name specified for this user to reference the BIG-IQ and NSX integration.*

6. Add the new user to the Administrator role using either the `Update a role` or `Modify a role` API.
   `/mgmt/shared/authz/users POST` or `/mgmt/shared/authz/users PATCH`

Next you must activate a pool license.

About activating a license pool

When you integrate with VMware NSX to create BIG-IP VEs, you can activate a pool license so that BIG-IQ software can use a license from that pool to license the BIG-IP VEs that it creates.

If you choose not to use a pool license, the BIG-IQ device still creates BIG-IP VEs, but you need to license them.

You initiate the license activation process with a base registration key. The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license. If the system has access to the internet, you select an option to automatically contact the F5 license server and activate the license. If the system is not connected to the internet, you must manually retrieve the activation key from a system that is connected to the internet, and then transfer it to the BIG-IQ system.

Note: *If you do not have a base registration key, contact your F5 Networks sales representative.*

Activating a license pool automatically

You need a base registration key to activate the license pool.

If the resources you are licensing are connected to the public internet, you can use this procedure to activate the license pool.

1. Authenticate with the F5 Cloud REST API.

   Tip: *Refer to Authentication with the F5 REST API in the BIG-IQ Cloud Overview chapter of this guide for information about authentication strategies.*

   Tip: *Refer to the BIG-IQ® Cloud Service API Reference Guide for details about using the APIs required for this task.*

2. Create a new license pool using the `Create a License Pool` API.
   `/mgmt/cm/shared/licensing/pools POST`
3. Get the text of the end user license agreement (EULA) using the `Get the EULA` API.
   `/mgmt/cm/shared/licensing/pools/[uuid] GET`
4. Agree to the EULA using the `Accept the EULA` API.
   `/mgmt/cm/shared/licensing/pools/[uuid] PATCH`

   The value of the `eulaText` parameter must match precisely the text returned in the previous step.

   Tip: *If a EULA has been previously accepted for this license, you might not need to perform this step.*

5. Add a device to the license pool and activate it using the `Activate a device` API.
   `/mgmt/cm/shared/licensing/pools/[uuid]/members POST`

Activating a license pool manually

You need a base registration key to activate the license pool.

If the resources you are licensing are not connected to the public internet, you can use this procedure to activate the license pool.

1. Authenticate with the F5 Cloud REST API.

   Tip: *Refer to Authentication with the F5 REST API in the BIG-IQ Cloud Overview chapter of this guide for information about authentication strategies.*

   Tip: *Refer to the BIG-IQ® Cloud Service API Reference Guide for details about using the APIs required for this task.*

2. Create a new license pool using the `Create a License Pool` API.
   `/mgmt/cm/shared/licensing/pools POST`
3. Get the license text for manual activation using the `Get the Dossier` API.
   `/mgmt/cm/shared/licensing/pools/[uuid] GET`
4. Submit the base registration key using the `Patch the License Text` API.
   `/mgmt/cm/shared/licensing/pools/[uuid] PATCH`

   The value of the `licenseText` parameter must match precisely the text returned in the previous step.

Tip: *If a EULA has been previously accepted for this license, you might not need to perform this step.*

5. Add a device to the license pool and activate it using the `Activate a device` API.
   `/mgmt/cm/shared/licensing/pools/[uuid]/members POST`

Create a connection between the BIG-IQ device and NSX

To enable integration between a third-party cloud provider and the BIG-IQ device, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

1. Log in to BIG-IQ® Cloud with your administrator user name and password.
2. Hover over the Connectors header and click the + icon when it appears.
3. In the **Name** and **Description** fields, type a name and description.

   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
4. From the **Cloud Provider** list, select **VMware NSX**.
5. In the **VMware NSX Address** field, type the IP address of the VMware system.

   The VMware IP address must be fully accessible from the BIG-IQ device's internal VLAN.
6. In the **VMware NSX User Name** and **VMware NSX Password** fields, type the credentials that the BIG-IQ device will use to authenticate to the NSX Manager REST API.
7. In the **VMware vCenter Server Address** field, type the IP address of the vCenter server.
8. In the **VMware vCenter Server User Name** and **VMware vCenter Server Password** fields, type the credentials that the BIG-IQ device will use to authenticate to the vCenter SOAP API.
9. In the **BIG-IQ User Name** and **BIG-IQ Password** fields, type the credentials that NSX Manager uses to authenticate to the BIG-IQ REST API.
10. If you plan to use a pool of licenses, in the **Device License** field, specify the pool of licenses to use when the NSX and BIG-IQ integration provisions a BIG-IP VE.

    If you skip this step, you'll need to specify a license each time you add a new device.
11. If you want to specify values for the remaining optional fields (**Timezone**, **NTP Server(s)**, **DNS Servers(s)**, and **DNS Suffix(s)**) so that the NSX and BIG-IQ system integration will use them when it provisions a BIG-IP VE, specify those values next.
12. Click the **Save** button.

Defining an NSX Runtime Deployment specification

VMware NSX uses a Runtime Deployment to specify parameters for BIG-IP virtual devices provisioned using a BIG-IQ software connection. Node templates simplify the task of specifying the parameters for the Runtime Deployment. This task uses the `Create node template` API to create a node template. The BIG-IQ and NSX integration uses this template when it provisions new BIG-IP virtual devices.

1. Authenticate with the F5 Cloud REST API.

Tip: *Refer to Authentication with the F5 REST API in the BIG-IQ Cloud Overview chapter of this guide for information about authentication strategies.*

Tip: *Refer to the BIG-IQ® Cloud Service API Reference Guide for details about using the APIs required for this task.*

2. Use the `Create node template` API to make a new template that specifies values needed for a deployment specification.
`/mgmt/cm/cloud/connectors/vmware-nsx/<connectorId>/nodes`

Option	Description
OvfUrl	The entry identifies the URL specified previously for the OVF file that the BIG-IQ device uses to create the BIG-IP VE.
BIG-IP	Setting this entry to true indicates that the template specifies provisioning details for a BIG-IP device.
NodeTemplateName	The entry identifies the name you want NSX users to specify when requesting deployment of this type of BIG-IP VE.

```
{
  "state": "TEMPLATE",
  "properties":[
    {
      "id": "BIG-IP",
      "provider": "true"
    },
    {
      "id": "NodeTemplateName",
      "value": "BIGIP-11.5.0.0.0.221.LTM_1SLOT-scsi.ovf"
    },
    {
      "id": "OvfUrl",
      "provider":
"http://server/ovfs/BIGIP-11.5.0.0.0.221.LTM_1SLOT-scsi/BIGIP-11.5.0.0.0.221-scsi.ovf"
    }
  ]
}
```

The API call registers the deployment specification received from the NSX API with the BIG-IQ software's NSX Partner Service. The REST API response includes the property ID `ImageId`. This value identifies the just-created deployment specification that confirms that the connection between the BIG-IQ system and the NSX device is established.

Make a note of the ImageId value. You will need it in the next task to identify which deployment specification you want to use to provision the BIG-IP VE.

Discovering devices located in the VMware cloud

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

For devices located in a third-party cloud, you must know the internal self IP address (For OpenStack or VMware cloud) or the external self IP address for Amazon EC2. You also must configure BIG-IQ Cloud with DNS so it can resolve the endpoint by name. To access this setting, log in to BIG-IQ System, select the BIG-IQ system you want to modify, and click the gear icon.

1. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**.
2. In the IP Address field, type the device's external self IP address.

   You cannot discover a BIG-IP device using its management IP address.
3. When the BIG-IQ system and the BIG-IP device are on different subnets, you must create a route:
   a) Use SSH to log in to the BIG-IQ system's management IP address as the root user.
   b) Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

   Where `<route name>` is a user-provided name to identify the new route, and `<x.x.x.x>` is the IP address of the default gateway for the internal network.
4. In the **Admin User Name** and **Admin Password** fields, type the administrator user name and password for the managed device.
5. Select the **Auto Update Framework** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.

   For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework. If you do not select the **Auto Update Framework** check box before you click the **Add** button, a message displays prompting you do update the framework or cancel the task.
6. Click the **Add** button.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

You can now associate this device with an VMware cloud connector and allocate resources to tenants.

About vCloud Director integration

Integrating vCloud Director (VCD) with your cloud applications makes it possible for you to use the VCD interface to manage the F5 cloud applications. The integration process involves tasks using the user interface in both the F5 BIG-IQ® Cloud and the VMware VCD.

After you integrate vCloud Director (VCD) with BIG-IQ Cloud, you can use VCD to manage your cloud applications. After integration, a catalog of BIG-IP® Cloud applications appears in the VCD user interface.

BIG-IQ Cloud refers to a service provider's customers as *tenants*. The VCD equivalent to a tenant is referred to as an *organization*. BIG-IQ Cloud identifies tenants using a tenant ID. One key to successfully integrating VCD with BIG-IQ Cloud is associating the tenant ID assigned to that catalog with a VCD organization.

To deploy an F5 application catalog in vShield Manager (VSM), you deploy a VSM service profile. While VSM service profiles do not currently recognize F5 tenants, they do recognize VCD organizations. So when your tenant’s ID is associated with a VCD organization, you can use VSM and VCD to administer and deploy the tenant’s application catalog.

When you create a tenant for VCD integration, make a note of the tenant ID so you can connect it to a VCD organization.

Task summary

When you are integrating vCloud Director (VCD) and BIG-IQ® Cloud, you must configure VCD, then BIG-IQ, then VCD again.

Before you begin vCloud Director integration

Before you integrate BIG-IQ® Cloud with your vCloud Director applications, make sure that you have completed the following prerequisites.

- Customize and store at least one provider template in the catalog.
- Create at least one tenant.

Determining an organization's globally unique identifier

The globally unique identifier (GUID) is the figurative glue that binds the BIG-IQ® Cloud connector to your vCloud Director (VCD) applications. You use the GUID when you create a tenant for a VCD connector.

1. Log in to your VCD system and complete the initial setup.
   Setup must include creating at least one VMware organization virtual data center (VDC).
2. In VCD, navigate to the list of organization VDCs.
3. In VCD, select the organization VDC that you are going to use to manage BIG-IQ applications.
   When you select the VDC, an alphanumeric string, known as the GUID appends to the end of the displayed URL. In the following example, the GUID is highlighted.

Make a note of the GUID; you will need it when you create a tenant for this connector.

Creating BIG-IQ Cloud integration objects

The BIG-IQ® Cloud integration objects you create in this task are available in your VMware vCloud Director (VCD) applications, so you can manage these objects using the VCD user interface.

1. Authenticate with the F5 Cloud REST API.

   Tip: *Refer to Authentication with the F5 REST API in the BIG-IQ Cloud Overview chapter of this guide for information about authentication strategies.*

   Tip: *Refer to the BIG-IQ® Cloud Service API Reference Guide for details about using the APIs required for this task.*

2. Discover at least one BIG-IP® system using the `Add a managed device` API.
   `/mgmt/cm/cloud/managed-devices POST`
3. Create a catalog of BIG-IQ Cloud applications to publish into the vShield Manager vendor template using the `Create provider iApp template` API.
   `/mgmt/cm/cloud/provider/templates/iapp POST`
4. Using the BIG-IQ Cloud APIs, create a VMware vShield Manager connector using the `Create VMware connection` API (`/mgmt/cm/cloud/connectors/vmware POST`), specifying the IP address and appropriate credentials.
5. Using the BIG-IQ Cloud APIs, create a new tenant using the `Create tenant` API.
   `/mgmt/cm/cloud/tenants POST`

Important: *You must use the organization's vCloud Director globally unique identifier (GUID) for the new tenant's name.*

Integrating vCloud Director with your cloud applications

You must create a VMware connector in BIG-IQ® Cloud before you can perform this task.

Connecting BIG-IQ integration objects to your vCloud Director (VCD) applications makes it possible for you to manage BIG-IQ applications using the VCD user interface.

1. In VCD, enable the cloud connector you just created for the Organization VDC that corresponds to the tenant you created for VCD.
2. In VCD, create an edge gateway for the organization VDC that corresponds to the tenant.
3. In VCD, create an edge gateway service for the edge gateway you just created.

   As part of creating the service, you need to first specify a pool, and then a virtual machine.

The tenants that you created and connected to VCD can now use the VCD interfaces to create and manage applications. The VCD user interface displays the fields that are tenant-editable.

Chapter 14

Local Cloud Integration

About using a local cloud source

In addition to providing self-service resources to tenants remotely in a third party cloud, you can also provide them resources to local F5 devices in your network.

Discovering BIG-IP devices in your network

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.3 or later. For proper communication, you must configure each F5 device you want to manage with a route to the BIG-IQ system. If you do not specify the required network communication route between the devices, then device discovery fails.

You can discover a device by providing the BIG-IQ system with the device's IP address, user name, and password.

1. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**.
2. For devices on the same subnet as the BIG-IQ system, in the **IP Address** field, type the IP address of the device.

   You cannot discover a BIG-IP device using its management IP address.
3. When the BIG-IQ system and the BIG-IP device are on different subnets, you must create a route:
   a) Use SSH to log in to the BIG-IQ system's management IP address as the root user.
   b) Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

   Where `<route name>` is a user-provided name to identify the new route, and `<x.x.x.x>` is the IP address of the default gateway for the internal network.
4. To change the root user name, type a new name in the **Root User Name** field.
5. Type a password for the root user in the **Root Password** field.
6. In the **Admin User Name** and **Admin Password** fields, type the administrator user name and password for the managed device.
7. Select the **Auto Update Framework** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.

   For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework. If you do not select the **Auto Update Framework** check box before you click the **Add** button, a message displays prompting you do update the framework or cancel the task.
8. Click the **Add** button.

BIG-IQ System populates the properties of the device that you added, and displays the device in the Devices panel.

Associating a local cloud connector with a device

Before you associate a local cloud connector with a device, you must discover one or more devices.

To enable integration between a third-party cloud provider and the BIG-IQ device, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

1. Hover over the Connectors header and click the + icon when it appears.
2. In the **Name** and **Description** fields, type a name and description.

   You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.
3. From the **Cloud Provider** list, select **Local Cloud**.
4. From the **Devices** list, select the device you want to associate with this connector.
5. To select additional devices to associate with this connector, click the + icon at the right of the list. BIG-IQ system discovers application servers associated with this connector, and populates them in the Server panel. If the system discovers F5 devices, it populates the Device panel with them.
6. Click the **Save** button.

Chapter 15

Glossary

BIG-IQ Cloud terminology

Before you manage cloud resources, it is important that you understand some common terms as they are defined within the context of the BIG-IQ® Cloud.

Term	Definition
application templates	An application template is a collection of parameters (in the form of F5 iApps® templates) that a cloud administrator defines to create a customized configuration for tenants. Cloud administrators add the configured application to a catalog from which a tenant can self-deploy it.
BIG-IQ Cloud	The BIG-IQ® Cloud system is a tool that streamlines management and access for tenants to services and applications hosted by local and/or cloud-based servers.
cloud administrator	Cloud administrators create application templates for tenants to centrally manage access to specific web-based applications and resources. Cloud administrators might also be referred to as cloud providers.
cloud bursting	Cloud bursting is a seamless way to manage an anticipated increase in application traffic by directing some traffic to another cloud resource. When demand falls back into normal parameters, traffic can be directed back to the original cloud resource. This elasticity enables efficient management of resources during periods of increased or decreased traffic to applications.
cloud connector	A cloud connector is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.
resources	A resource is any managed object, including devices, web applications, virtual servers, servers, cloud connectors, and so forth.
roles	A role defines specific privileges to which you can associate one or more users. There are two default roles for BIG-IQ Cloud: cloud administrator and cloud tenant.
tenant	A tenant is an entity that can consist of one or more users accessing resources provided by a cloud administrator.
user	A user is an individual who has been granted access to specific tenant resources.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V