BIG-IQ™ Device: Device Management

Version 4.3

Table of Contents

Legal Notices

Publication Date

This document was published on March 6, 2014.

Publication Number

MAN-0498-01

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 Leaflet software, copyright © 2010-2014, Vladimir Agafonkin, and copyright © 2010-2011, CloudMade; all rights reserved. This software is distributed under the BSD license.

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

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.

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™ Network Security Administration	This guide contains information used to manage BIG-IP® firewalls, policies, rule lists (and other shared objects), and users.
BIG-IQ™ Web Application Security Administration	This guide contains information used to manage all policies in an enterprise by bringing under central management all the BIG-IP® devices where those policies reside.
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.

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. 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 further filter the objects displayed, you can type one additional object in the Filter field, and click the **Apply** button.
3. 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.
4. To remove a filter, click the **x** icon next to the object that you want to remove, below the Filter field.

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.

Chapter 2

Device Resource Management

About device discovery and inventory 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.

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

Using a script to install required BIG-IQ components on managed BIG-IP devices

You can perform this task only after you have licensed and installed the BIG-IQ™ system and at least one BIG-IP® device running version 11.3 or later.

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)

Installing requisite BIG-IQ components onto your managed BIG-IP devices results in a REST framework that supports the required Java-based management services. You must perform this installation task on each device before you can discover it.

Important: *When you perform this task, the traffic management interface (TMM) on each BIG-IP device restarts. Before you perform this task, verify that no critical network traffic is targeted to the BIG-IP devices.*

1. Log in to the BIG-IQ system terminal 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. 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 files reside.
   `cd /usr/lib/dco/packages/upd-adc`
4. Run the installation script.
   - For devices installed in an Amazon EC2 environment: `./update_bigip.sh -a admin -p <password> -i /<path_to_PEM_file> <BIG-IP Management IP Address>`

- For devices installed in any other environment: `./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 root@<big-ip addr> 'cat /var/ssh/root/authorized_keys' | grep -v -F -f
/root/.ssh/identity.pub | ssh root@<big-ip addr> 'cat -
>/var/ssh/root/authorized_keys.tmp && mv /var/ssh/root/authorized_keys.tmp
/var/ssh/root/authorized_keys'
```
This step is not required if you did not establish trust in step 2.

Important: *Before you begin using this BIG-IQ system in a production capacity, depending on your security policies, you will likely want to stop using the security group rules that you added as prerequisite to this task.*

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, device discovery will fail.

Important: *Before you can discover a device, you must first install the required BIG-IQ components on that device.*

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

1. Log in to BIG-IQ Device with your administrator user name and password.
2. Hover on the Devices header, and click the + icon when it appears.
The panel expands to display the New Device properties.
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 **User Name** and **Password** fields, type the administrator user name and password for the managed device.
5. Click the **Add** button.

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

Viewing 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. To display the details for all managed devices, verify that the filter field at the top of the screen is clear, and then click the show details (|>) button in the Devices panel header.
   The panel expands to display the details for all of the managed devices.
2. To view the details for a specific device, click the device listed in the Device panel, and then click the change view button in the panel header.
   The screen refreshes to display the details for the selected device.
3. To export the data to a CSV file, click the **Export** button on the device details screen.

You can modify the report as required in Microsoft™ Excel™.

Monitoring device health and performance

You must discover at least one device before you can view its properties and health.

Centrally managing your devices with the BIG-IQ™ system means you can easily asses the health and performance of your network.

1. On the Devices panel, click the gear icon next to the device that you want to monitor.
   The panel expands to display the device properties, and performance and health details.
2. If modification or intervention is required, log in to the device by typing the user name and password.

Chapter 3

UCS File Backup and Restoration

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

Backing up a UCS file

You must discover a device before you can create a backup for it.

It is best practice to create a backup of the UCS file for each device in your network, on a regular basis, so that you always have a copy of a configuration. The UCS file backup provides your network with added stability in the event that a system needs to be restored.

1. At the top of the BIG-IQ Device screen, click **Maintenance.**
2. Hover on the Backups header, and click the + icon when it appears.
   The panel expands to display the Backup Properties.
3. In the **Name** and **Description** fields, type a name and description to identify this UCS file backup.
4. From the **Device** list, select the device for which you want to create the UCS file backup.
5. Click the **Save** button
6. To view the status of the backup or change its description, click the gear icon.

This backup is now available to restore on the specified device.

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. At the top of the BIG-IQ Device screen, click **Maintenance.**
2. Click the gear icon next to the backup that you want to restore.
3. Click the **Restore** button.

BIG-IQ Device restores the saved UCS file backup onto the associated device.

Chapter 4

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. 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.

2. 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 5

User Roles

About users and roles

A role is defined by its specific privileges. When you associate a role with a user, that user is granted all of the role's corresponding privileges.

Standard roles defined

There are two standard roles for the BIG-IQ system. Access to features is defined by the user's role and license.

Role	Definition
Administrator	This user has complete access to all system functionality and licensed software panels. The cloud administrator performs the tasks required for licensing, adding new users, and cloud management.
Security Manager	This user has access only to the firewall panel, and performs tasks specific only to firewall security.

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 the BIG-IQ system with the administrator user name and password.
2. At the top of the screen, click **System >Users**.
3. On the Users panel, click the properties gear for **Admin User**.
4. In the **Password** and **Confirm Password** fields, type a new password.
5. 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 the BIG-IQ system with the administrator user name and password.
2. At the top of the screen, click **Users**.

3. On the Users panel, click the gear icon for the **root** user.
4. In the **Password** and **Confirm Password** fields, type a new password.
5. Click the **Save** button.

Adding a new user

You add a user before you specify the role that defines their access to specific BIG-IQ™ system functionality and resources.

1. Log in to the BIG-IQ system with the administrator user name and password.
2. At the top of the screen, click **Users**.
3. In the **Username** field, type the user name.
4. 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.
5. In the **Password** and **Confirm Password** fields, type the password for the new user.
6. Click the **Add** button.

You can now specify a role for this user.

Assigning a standard role to a user

Before you can specify a user role for a user, you must have added the user.

When you specify a role for a user, you define the resources the user can view and modify. You can associate a user with multiple roles.

1. In the Users panel, click the name of the user to which you want to assign a role, and drag and drop it on one of the following roles in the Roles panel.

Option	Description
Administrator	This user has complete access to all system functionality and licensed software panels. The administrator performs the tasks required for licensing, adding new users, and cloud management.
Firewall Manager	This user has access only to the firewall software panel, and performs tasks associated only with security.

   A confirmation pop-up screen opens.
2. Click the **Confirm** button to assign this user the selected role.

This user 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 the BIG-IQ system with the 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 6

Software Image Deployment and Configuration Back Up and Restoration

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.

Deploying software images to physical or virtual devices

You must first discover and license a device before you can deploy a software image to it.

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 **Physical** or **Virtual**, depending on the type of device you are configuring.
5. On the Images panel, click the software image that you want to deploy, drag it to the Device panel, and drop it onto the device to which you want it installed.
6. Hover on the Deployment panel and click the (+) icon.
7. On the Deployment panel, click the gear icon to view the options for the deployment job.
   The panel expands to display deployment options.
8. Modify the options as required.
9. For the **Install Method** setting:
   - If you select the **Factory Install** option, BIG-IQ Device reformats the device's hard drive. For this option, you can select a set of saved configuration files from the **Config Files** list to load onto the device and choose and option from the **Licensing** list.

     Important:

     To manage this device after deploying the software image, you must re-install the required BIG-IQ system components back onto the device after the job runs. For more information, refer to the *Installing required BIG-IQ components on BIG-IP devices* chapter.
   - If you select the **Live Install** option, you can select the **Reboot to Target Volume After Live Install** and the **Set Target Volume as Default Boot Volume** check boxes.
10. Click the **Deploy** button to immediately initiate the job, or click the **Save** button for later deployment.
11. 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.

Before you can manage this device, you must install the required BIG-IQ system components on it. For more information, refer to the *Installing required BIG-IQ components on BIG-IP devices* chapter. After you install the required components, you can associate the device with a license and configuration.

Using a script to install required BIG-IQ components on managed BIG-IP devices

You can perform this task only after you have licensed and installed the BIG-IQ™ system and at least one BIG-IP® device running version 11.3 or later.

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)

Installing requisite BIG-IQ components onto your managed BIG-IP devices results in a REST framework that supports the required Java-based management services. You must perform this installation task on each device before you can discover it.

Important: *When you perform this task, the traffic management interface (TMM) on each BIG-IP device restarts. Before you perform this task, verify that no critical network traffic is targeted to the BIG-IP devices.*

1. Log in to the BIG-IQ system terminal 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. 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 files reside.
   `cd /usr/lib/dco/packages/upd-adc`
4. Run the installation script.
   - For devices installed in an Amazon EC2 environment: `./update_bigip.sh -a admin -p <password> -i /<path_to_PEM_file> <BIG-IP Management IP Address>`
   - For devices installed in any other environment: `./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 root@<big-ip addr> 'cat /var/ssh/root/authorized_keys' | grep -v -F -f
   /root/.ssh/identity.pub | ssh root@<big-ip addr> 'cat -
   >/var/ssh/root/authorized_keys.tmp && mv /var/ssh/root/authorized_keys.tmp
   /var/ssh/root/authorized_keys'
   ```

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

Important: *Before you begin using this BIG-IQ system in a production capacity, depending on your security policies, you will likely want to stop using the security group rules that you added as prerequisite to this task.*

Backing up and restoring a set of configuration files

You must discover, license, and configure a device before you can back up and restore a set of configuration files to it.

Creating a backup of a set of configuration files for a device ensures that you can quickly and easily replicate or restore a configuration.

1. Use SSH to log in to the BIG-IQ system's management IP address as the root user, and type the following command: `f5ad-create-config -f <configuration file set name> <host name>`
   BIG-IQ Device backs up the configuration files located in the following directories (including all of the files in the sub-directories) into its `/shared/config` directory in a folder named `<configuration file set name>`, and displays the configuration file name in the Config Files panel.

```
/config/bigip_base.conf
/config/bigip.conf
/config/bigip_user.conf
/config/startup
/config/eav/
/config/failover/
/config/filestore/
/config/partitions/
```

   Important: *If you do not want BIG-IQ Device to overwrite any existing configuration file set with the same name, do not include the `f` flag for this command.*

2. Log in to BIG-IQ Device with the administrator user name and password.
3. At the top of the screen, click **Physical** or **Virtual**, depending on the type of device you are configuring.
4. On the Deployment panel, click the gear icon to view the options for the deployment job.
   The panel expands to display deployment options.

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

Chapter 7

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) cluster. 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 cluster fails, a peer BIG-IQ system takes over the device management that was previously done by the original device.

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

You must install and license at least two BIG-IQ systems before you can configure them in an active-active high availability cluster.

Configuring BIG-IQ Cloud in a high availability cluster means you always have management access to the BIG-IP devices in your network. (Configuring a high availability cluster is optional.)

Important: *To synchronize properly, BIG-IQ systems in a cluster must be running the same version of software. The exact configuration in terms of hardware is not required; however, the systems should have comparable resources. This is required because, in the event of a fail over, a peer must be able to maintain the process requirements. This is especially important in terms of disk space and data collection.*

---

1. At the top of the screen, click **System** and **Overview**.
2. Click **High Availability**.
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. Click the **Add** button to add this device to this high availability cluster.
5. In the **User Name** and **Password** fields, type the administrative user name and password for the system.

If discovery 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 8

License Pools

About license pools

The BIG-IQ™ system helps you manage resource usage in a dynamic application environment through the use of license pools. Each license pool is limited to a specific number of licenses. After you perform the initial license activation, BIG-IQ automatically grants and revokes licenses for the BIG-IP® virtual edition systems as resource demands change. This gives you the flexibility to license devices only as needed, keeping your operating costs fixed. You can also use different license pools for different applications, allowing for flexible provisioning options.

You initiate the pool 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 can manually retrieve the activation key from a system that is connected to the internet, and transfer it to the BIG-IQ system.

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

Automatically activating a license pool

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 use this procedure to activate the license pool.

1. Log in to the BIG-IQ system with the administrator user name and password.
2. At the top of the screen, click **Device** and **Virtual**.
3. Hover on the License Pools header, and click the + icon when it appears.
   The panel expands to display New License properties.
4. In the **License Name** field, type the name you want to use to identify this license pool.
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 BIG-IQ system contacts the F5 Networks licensing server and displays the End User License Agreement (EULA).
8. To accept the EULA, click the **Accept** button.
   The screen refreshes and displays the license details.

Manually activating a license pool

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

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

1. Log in to the BIG-IQ system with the administrator user name and password.
2. At the top of the screen, click **Device** and **Virtual**.
3. Hover on the License Pools header, and click the + icon when it appears.
   The panel expands to display New License properties.

4. In the **License Name** field, type the name you want to use to identify this license pool.
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 **Activate** button.
   The BIG-IQ system refreshes and displays the dossier in the **Dossier** field.
8. Copy the displayed dossier and transfer it to a system connected to the internet and navigate to the F5 Licensing Server at `https://activate.f5.com/license/`.
9. Paste the dossier into the **Enter your dossier** text box, or click the **Browse** button to locate it on the system, and click the **Next** button.
10. Copy or save the activation key and transfer it to the BIG-IQ system.
11. The End User License Agreement (EULA) displays.
    When you click **Accept**, the screen refreshes to display the license details.
12. To accept the EULA, click the **Accept** button.
    The screen refreshes and displays the license details.

Chapter 9

Templates

About templates

You use templates to provide users with access to cloud resources. The template provides two services. First, you can use it to identify a specific set of resources, much like a virtual container, and second, it provides integration with third-party cloud services.

About Amazon EC2 integration

Using Amazon Web Services (AWS) is less expensive and more flexible than building and maintaining a physical computer infrastructure. BIG-IQ™ Cloud provides you with a seamless way to manage Amazon's elastic cloud services (*Amazon EC2*). To support communication between BIG-IQ Cloud and an AWS account, you use the BIG-IQ Cloud's Amazon EC2 Cloud Connector. This EC2 Cloud Connector makes it possible for you to discover BIG-IP® VE virtual machines and application servers running in an AWS account.

You can use this feature to coordinate management-plane changes to a private, public, or hybrid cloud environment. For example, to accommodate seasonal traffic fluctuations, you might need to periodically add devices or application servers in the EC2 environment (referred to as, *cloud bursting*) or retract devices or application servers.

Task summary

Network requirements for communication Amazon EC2 cloud services

For proper communication to devices located in an Amazon EC2 cloud, BIG-IQ™ Cloud must have network access to those resources. Before you can manage cloud resources, you must define a network route between the BIG-IQ Cloud internal VLAN and the public Internet, or the Amazon EC2 endpoint, for proper communication to devices located in a public cloud. For specific instructions, refer to your Amazon EC2 documentation.

Creating a new virtual private cloud

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

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

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

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

Launching a new virtual machine

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

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

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

---

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

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

   The Launch on EC2 page is displayed.
4. Click the **Launch with EC2 Console** tab.

   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 a new IAM user account

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

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

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

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

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

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.

Creating an EC2 cloud connector and discovering cloud resources

If you want BIG-IQ Device to automatically provision additional BIG-IP VE servers and devices for your tenant when more resources are needed, you must first purchase and activate a license pool to associate with this template.

You create an AWS EC2 template to provide users access to EC2 cloud services.

1. Hover on the Templates header and click the + sign 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 **Connector Type** list, select Amazon EC2.
4. 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.
5. In the **Key ID** and **Secret Key** fields, type the credentials of an EC2 user that can access your account.

   For security purposes, it is important to specify a user that has Amazon EC2 Full Control Access.
6. 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.
7. 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 uses the first one it discovers in the Availability Zone.
8. Click the arrow next to Device & Server Provisioning to display associated options.
9. If you do not want to automatically provision additional BIG-IP VE servers and devices when more resources are needed, for the **Device Elasticity** setting, select **Disable**.

   If you do want to provide server elasticity options to a tenant, you must leave the **Cloud Connector** setting as **Tenant Selectable**.
10. For the **Licensing** setting, select the license pool associated with this Amazon EC2 connector.

    If there is no license pool associated with this Amazon EC2 connector and you enabled elasticity, Amazon will charge for additional resources on a per-instance basis. Refer to Amazon for their EC2 instance purchasing options.
11. If you do not want to automatically provision additional application servers when more resources are needed, for the **Server Elasticity** setting, select **Disable.**.
12. Review network settings populated when you selected a connector and make any necessary corrections.
13. Click the **Save** button at the top of the Template panel.
14. If the system discovered devices, you must expand the device's properties panel, and provide the device's credentials to finalize the discovery process.
15. Review network settings populated when you selected a connector and make any necessary corrections.

You can now deploy this template to a device.

Chapter 10

Glossary

- *BIG-IQ Cloud terminology*

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 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

V