F5 Virtual Network Functions Manager Release Notes

These release notes provide product information and system requirements for the F5® Virtual Network Functions Manager (VNFM) support for version 3.0.0. This release contains fixes for known issues and new/changed functionality.

Version notice:

This content applies to F5® VNF Manager version 3.0.0.

Contents

- F5® BIG-IQ® Centralized Management®
  - Version 6.0.1.0.0.813 Release Notes
  - Version 8.2 (LTS) Release Notes (currently PREVIEW ONLY)

- F5® BIG-IP® Virtual Edition (VE):
  - BIGIP-14.1.4.6-0.0.8.ALL_1SLOT Virtual Edition Release Notes
  - BIG-IP 15.1.5.1 Virtual Edition ALL_1SLOT Release Notes (currently PREVIEW ONLY)
  - BIG-IP 16.1.2 Virtual Edition ALL_1SLOT Release Notes (currently PREVIEW ONLY)

- CentOS-7-x86_64-GenericCloud-1503

- OpenStack Release Notes:
  - Newton Version 10
  - Queens Version 13

- Vmware Release Notes:
  - VMware vSphere ESXi Version 6.5-7.3
  - VMware Integrated OpenStack (VIO) 5.1
  - vCloud Director 10.3

- F5 VNFM platform support requirements
  - VNF Manager
  - VNFM Sizing guidelines
  - Additional platforms
  - VIM compatibility
  - F5 VNFM open source components

- F5 VNFM features
- F5 VNFM what's new
- F5 VNFM user documentation
- F5 security vulnerabilities

- F5 VNFM known issues
- F5 VNFM fixed Issues
- F5 VNFM installation overview
- F5 VNFM upgrade overview

Platform support requirements

This section provides system requirements for VNFM and additional platform components.

VNF Manager

F5 VNF Manager version 3.0.0 requires the following system requirements:

Platform name	Platform ID	System Requirements
F5 VNF Manager	All versions	**vCPUs**: 4 minimum, 8 recommended **RAM**: 8GB minimum, 16GB recommended **Root Disk Storage**: 160GB minimum **Storage**: 5GB minimum, 64GB recommended **64-bit host**: with RHEL/CentOS 7.9 **Private network**: dedicated for communicating with other VNFM components, including cluster members

VNFM Sizing guidelines

The following table includes some guidelines and insights for determining VNF Manager sizing.

VNFM Component	Sizing guideline
Tenants	Define a maximum of 1000 tenants in a VNF Manager
Users	Currently, no limit to the number of users you can define in the system; however, the maximum, concurrent users interacting with VNFM is 200.
Blueprints	Allocate 50GB of storage to the VNF Manager. Currently, no limit to the number of blueprints, as the average blueprint storage requires less than 1M of disk space and database space.
Plugins	Plugins are stored in the VNF Manager hard drive. Typically, plugins can consume approximately 5M to 20M of storage.

VNFM Component	Sizing guideline
Deployments	A single VNFM can maintain up to 500K of deployed nodes. Typical deployment size consumes 10K maximum of disk size and very few entries in the database
Workflows	A VNFM can operate up to 100 concurrent workflows; a default limit enforced by the system. However, you can modify this threshold.
Secrets	No limit to the number of secrets.
Agents	A maximum of 2000 agents deployed per a single VNFM.
UI/CLI/API requests/second	Although the REST API performance varies depending on multiple factors, typically VNF Manager can support a maximum of 10 requests/second.
Events	The system can process a maximum of 100 events/second.
Logs, events, and metrics	Define enough storage to store the logs, events, and metrics sent from the hosts, configuring log rotation to minimize the amount of storage space required.

Additional platforms

The following table provides system requirements for the additional components.

Platform name	Platform ID	System Requirements
F5® BIG-IP® Application Services 3 Extension (AS3)	3.39.0-7 LTS	F5® BIG-IP® Application Services 3 Extension (AS3) version 3.39.0-7 (LTS) documentation
F5® BIG-IP® Declarative Onboarding	1.34.0-5	F5® BIG-IP® Declarative Onboarding (DO) version 1.34-05 (LTS) documentation
F5® BIG-IP® Telemetry Streaming	1.31.0-2	F5® BIG-IP® Telemetry Streaming v1.31.0-2 documentation
CentOS-7-x86_64-GenericCloud-1503	GenericCloud-1503	Release Notes

Virtual Infrastructure Manager (VIM) compatibility

F5 VNF Manager and VIM compatibility matrix:

VNF Manager ID	VIM Platform ID	VIM System Requirements
F5 VNF Manager 1.1.X	OpenStack Newton Version 10	Environment requirements
F5 VNF Manager 1.2.0	VMware vSphere ESXi Version 6.5	Requirements and patch notices
F5 VNF Manager 1.2.1	VMware vSphere ESXi Version 6.5 OpenStack Newton Version 10	See previous links for requirements information.
F5 VNF Manager 1.3.0	OpenStack Newton Version 10 and Queens Version 13 VMware vSphere ESXi Version 6.5	Newton Version 10 Environment requirements Queens Version 13 Environment requirements vSphere ESXi Version 6.5 Requirements and patch notices
F5 VNF Manager 1.3.1	OpenStack Newton Version 10 and Queens Version 13 VMware vSphere ESXi Version 6.5	See previous links for compatible platform requirements.
F5 VNF Manager 1.4.0	OpenStack Newton Version 10 and Queens Version 13 VMware vSphere ESXi Version 6.5	See the previous links for compatible other platform requirements.
F5 VNF Manager 2.0.0 - 2.0.2	OpenStack Newton Version 10 and Queens Version 13 VMware vSphere ESXi Version 6.5 and VIO version 5.1	See VMware Integrated OpenStack (VIO), and the previous links for other compatible platform requirements.

VNF Manager ID	VIM Platform ID	VIM System Requirements
F5 VNF Manager 3.0.0	OpenStack Newton v10 and Queens v13 VMware vSphere ESXi v6.5-7.3 VIO version 5.1 VMware Cloud Director (vCD) v10.3	See vCloud Director 10.3 Release Notes with API version 32 through version 35, and the previous links for other compatible platform requirements.

Note

To verify supported versions of OpenStack compatibility for all versions of VNFM, F5 used Red Hat and VIO infrastructures; however, F5 is confident that VNFM is compatible with supported versions of OpenStack in other infrastructures.

Opensource components

F5 VNF Manager is built with the following open-source components.

- Nginx
- Gunicorn and Flask
- PostgreSQL
- Logstash
- RabbitMQ
- Pika

Component	Description
Nginx	Nginx is a high-performing Web server. In F5 VNF Manager, it serves two purposes: • A proxy for the F5 VNFM REST service and F5 VNFM Console • A file server to host F5 VNFM-specific resources, agent packages, and blueprint resources. **File server** The file server served by Nginx, while tied to Nginx by default, is not logically bound to it. Although currently it is accessed directly frequently (via disk rather than via network), we will be working towards having it decoupled from the management environment so that it can be deployed anywhere. The file server served by Nginx, is available at https://{manager_ip}:53333/resources, which is mapped to the /opt/manager/resources/ directory. You must authenticate in

Component	Description
	order to access the file server. To access subdirectories that include tenant names in their path, you must have privileges on that tenant. These subdirectories include: • blueprints • uploaded-blueprints • deployments • tenant-resources The directories that are stored in snapshots include: • blueprints • uploaded-blueprints • deployments • tenant-resources • plugins • global-resources **Note**: The tenant-resources and global-resources directories are not used by F5 VNF Manager; therefore, users can create these directories for storing custom resources.
Gunicorn and Flask	Gunicorn is a Web server gateway interface HTTP server. Flask is a Web framework. Together, Gunicorn and Flask provide the F5 VNFM REST service. The REST service is written using Flask, and Gunicorn is the server. Nginx, is the proxy to that server. The F5 VNFM's REST service is the integrator of all parts of the F5 VNFM environment.
PostgreSQL	PostgreSQL is an object-relational database that can handle workloads ranging from small single-machine applications to large Internet-facing applications. In F5 VNF Manager, PostgreSQL serves two purposes: • Provides the main database that stores the application's model (for example, blueprints, deployments, runtime properties) • Provides indexing, and logs' and events' storage Recommended system requirements include: • vCPUs: 2 • RAM: 16GB • Storage: 64GB These recommended specifications consider the average use of 1000-2000 workflows per hour and certified for 1 million deployments. To increase this

Component	Description
	scaling volume, increase your hardware specification; for example, the equivalent AWS instance is r5.large.
Logstash	Logstash is a data handler. It can push/pull messages using inputs, and apply filters and output to different outputs. Logstash is used by F5 VNFM to pull log and event messages from RabbitMQ and index them in PostGresSQL.
RabbitMQ	RabbitMQ is a queue-based messaging platform. RabbitMQ is used by F5 VNFM as a message queue for different purposes: • Queueing deployment tasks • Queueing logs and events • Queueing metrics Recommended system requirements include: • vCPUs: 2 • RAM: 4GB • Storage: 32GB These recommended specifications consider the average use of 1000-2000 workflows per hour and certified for 1 million deployments. To increase this scaling volume, increase your hardware specification; for example, the equivalent AWS instance is c5.large.
Pika	Pika is a pure-Python implementation of the AMQP 0-9-1 protocol. The VNF management worker and the host agents are using pika to communicate with RabbitMQ. **Management worker (or agent)** Both the Workflow Executor and the Task Broker that appear in the diagram are part of the F5 VNFM Management Worker. • The Workflow Executor receives workflow execution requests, creates the tasks specified by the workflow, submits the tasks for execution by host agents and the Task Broker, and manages workflow state. • The Task Broker executes API calls to IaaS providers to create deployment resources, and executes other tasks specified in central_deployment_agent plugins. **Note**: All agents (the management worker, and agents deployed on application hosts) are using the same implementation.

Features

Feature Name	Description
Install/Uninstall	Installs the target deployment, lifecycle operations, and starts all instances. Uninstalls target deployment, frees resources allocated during install, performs uninstall lifecycle operations, stops/deletes deployments and additional blueprints created during install.
Scale out	Adds and installs BIG-IP Virtual Editions (VEs) and VNF instances on demand as your network needs resources based on configurable parameters.
Scale in	Removes and uninstalls BIG-IP Virtual Editions on demand as your network reduces its need for resources based on configurable parameters.
Heal VEs and layers	Creates a new copy of any BIG-IP VEs, layers, and related objects on demand as your network reports dysfunctional instances.
Purge VEs and layers	Uninstalls and removes dysfunctional VEs, VNF layer instance(s), and related objects, which you start **manually** after heal layer workflow runs and problem investigation is complete.
Upgrade	Initiates the upgrade process and sets new software reference data. Disables VEs with lower revision numbers. Scaled and healed VEs are installed using the new software reference data.
Update NSD	Updates AS3 declaration pushed to the VE as a part of NSD definition.
High Availability (HA)	The three-cluster VNFM HA solution in VNFM 2.0.0 **and later** no longer works as designed. For a workaround solution, see the Backup and Restore Guide.
REST API	Provides all VNFM functionality using a REST-based API.

What's new

The following table describes new/changed functionality added in VNF Manager version 3.0.0.

Feature	Description
Bug fixes	This release contains several fixes for existing issues.
F5 BIG-IQ Version 8.2 (LTS) Release Notes	Support for the F5 BIG-IQ v8.2.0.1 license manager, which REQUIRES a policy-compliant password. See knowledge article K49507549 for complete details.

Feature	Description
VMware vCloud Director 10.3	Support for VMware Cloud Director v10.3 VIM

User documentation

You can find the user documentation on: https://clouddocs.f5.com/cloud/nfv/latest/.

Security Vulnerabilities

The following list provides **known** common vulnerabilities and exposures (CVEs) shipped with the VNF Manager 3.0.0 release. Visit the F5 Security Center for complete F5 BIG-IP and F5 BIG-IQ Centralized Management security information. For the **latest** list of known and fixed vulnerabilities related to versions of BIG-IP VE and BIG-IQ Centralized Management, visit the *F5 Documentation Center* and select the Security Advisory document type to narrow the search results.

Important

The following libraries listed in the Known CVEs are NOT accessible directly from F5 VNF Manager. You must run the Gi-LAN plugin and launch a blueprint, to access these libraries. Therefore, a bad actor must write a blueprint and launch that blueprint in the VNF Manager in order to exploit these libraries. F5 recommends that you always deploy the VNF Manager on a secure management network, which is NOT accessible externally.

Known CVEs

CVE-2022-1388 on BIG-IP iControl REST

Due to BIG-IP iControl REST vulnerability CVE-2022-1388 you must use the following versions containing the fix for this CVE:

- BIG-IP-14.1.4.6-0.0.8.ALL_1SLOT Virtual Edition
- BIG-IP-15.1.5.ALL_1SLOT Virtual Edition
- BIG-IP-16.1.2.ALL_1SLOT Virtual Edition

bottle-0.12.7.tar.gz and bottle-0.12.18.tar.gz

Vulnerability Code	Severity	Description
CVE-2020-28473	Medium	The package bottle from 0 and before 0.12.19 are vulnerable to Web Cache Poisoning by using a vector called parameter cloaking. When the

Vulnerability Code	Severity	Description
		attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.
CVE-2022-31799	High	Bottle before version 0.12.20 mishandles errors during early request binding. Upgrade to bottle version 0.12.20.
CVE-2016-9964	Low	The redirect() in bottle.py in bottle version 0.12.10 does not filter a \r\n sequence, which leads to a CRLF attack, as demonstrated by a redirect("233\r\nSet-Cookie: name=salt) call (see full details).

ipaddress-1.0.23-py2.py3-none-any.whl

Vulnerability Code	Severity	Description
CVE-2020-14422	Medium	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.

pycrypto-2.6.1.tar.gz

Note

This vulnerability is in the product as a dependency but is NOT used.

Vulnerability Code	Severity	Description
CVE-2013-7459	Critical	Heap-based buffer overflow in the ALGnew function in block_template.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py.

Vulnerability Code	Severity	Description
CVE-2018-6594	High	The lib/Crypto/PublicKey/ElGamal.py library in PyCrypto through 2.6.1 generates weak ElGamal key parameters, which allows attackers to obtain sensitive information by reading ciphertext data (for example, it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for PyCrypto’s ElGamal implementation.

pip-20.3.4-py2.py3-none-any.whl

Vulnerability Code	Severity	Description
CVE-2021-3572	Medium	A security issue in pip version 21.1 and older. Maliciously formatted tags with potential use for hijacking a commit-based PIN. Using the fact that all of unicode’s whitespace characters were allowed as separators, which Git allows as a part of a tag name. It is possible to force a different revision to install, if an attacker accesses the repository. Upgrade to version pip version 21.1 (see full details).

pipenv-2021.5.29-py2.py3-none-any.whl

Vulnerability Code	Severity	Description
CVE-2022-21668	High	Flaw in pipenv versions 2018.10.9 - 2021.11.23 parsing of requirements.txt files, an attacker can insert a specially crafted string inside a comment anywhere within a requirements.txt file, causing pipenv users to install the requirements file (using pipenv install -r requirements.txt) and therefore download dependencies from a package index server controlled by an attacker. By embedding malicious code in packages served from a malicious index server, the attacker can trigger arbitrary remote code execution (RCE) on victims’ systems. Upgrade to pipenv version v2022.1.8 (see full details).

safety-1.8.5-py2.py3-none-any.whl

Vulnerability Code	Severity	Description
CVE-2020-5252	Medium	The command-line safety version 1.0-1.8.7 package for Python has a potential security issue. There are two Python characteristics that allow malicious code to poison-pill command-line Safety package detection routines by disguising, or obfuscating other malicious or non-secure packages. Upgrade to safety version 1.9.0 (see full details).

async-1.0.0.js

Vulnerability Code	Severity	Description
CVE-2021-43138	High	In Async versions < 2.6.3 and 3.x - 3.2.1, a malicious user can obtain privileges using the mapValues() method (lib/internal/iterator.js createObjectIterator) prototype pollution. Upgrade to Async version 2.6.4 or 3.2.2 (see full details).

Known issues

The following table lists known issues in the designated version release:

Platform name	Description
F5 VNF Manager Version 3.0.0	• If deploying the F5-VNF-BIG-IQ blueprint from a VMware vSphere ESXi VIM, you must NOT use 192.168.1.200 and 192.168.1.245 IP addresses on the same network the F5 VNF Manager is connected, until AFTER you deploy the BIG-IQ blueprint and the BIG-IQ HA pair is online. Once the BIG-IQ HA pair is online, those IP addresses become available. • In VMware vSphere ESXi, when using the VNFM REST API, you must set up your networks to use unique port group names, regardless of the directories in which they reside. • OpenStack v10 (Newton) has an issue with privileges and connecting devices residing outside the OpenStack environment with those residing inside the OpenStack environment, including F5 VNF Managers. To work around this issue, you must add the VNF Manager to the admin project, or upgrade to OpenStack v13 (Queens). • When instantiating the VNFM image in your VIM, the image at boot-up requires proper networking. If not, then your user accounts are not created correctly, and login to the OS VM is not possible. Additionally, services do not start and there is no access to the VNF Manager UI. This prohibits

Platform name	Description
	logging into VNFM and adding the required networking. Workaround depends upon your VIM: ○ VMware vSphere (step 4a) ○ OpenStack (step 2 tip) • The failover_state does not update as expected for deployment outputs on VNF layer. This issue is partially fixed. • No validator for the security_groups input setting. • A few inaccurate descriptions in the UI of some data types for various blueprint inputs. • The current UI description of the **Scale** workflows and inputs for **VNF group** is inaccurate. The description should read, **add_layers**, NOT **add_instances**. • The starting_ip_number input definition corresponds to the natSourceTranslation addresses value for VNF VE on the CGNAT layer. The starting_ip_number parameter has a **functional limit** of 3000 addresses; however, you can define a larger value. This **functional limit** will increase in a future release. • For **Gi-LAN** blueprint solution deployments, an error occurs, resulting in the second worker (follower) failing on check_all_services node. This issue occurs rarely. • If the **Heal** workflow is in progress, you may experience DISRUPTED traffic flow/transition. • Vsphere cluster is not synchronizing; therefore, HA cannot execute as designed. • When assigning networks that do NOT currently exist in OpenStack/VIO for a deployment, the deployment fails to create that network correctly, resulting in a failed deployment. To workaround this issue, create the network BEFORE deploying a blueprint. • You cannot restore a snapshot, as currently documented. This functionality is critical, and will be restored in the next VNFM release. However, we have documented a workaround in the Backup and restore guide. • You MUST define the vnf_as3_nsd_payload input; otherwise, leaving the value null (undefined) results in a failure. • Currently, external NTP server is hardcoded. • Currently, there is no option to enable/disable the internal NTP service during a deployment. • In OpenStack, the NSD DAG deployment may NOT uninstall while uninstalling the associated, main deployment. This issue occurs randomly and rarely. • During the **Heal** workflow of a worker (follower) node, the original traffic group will drop all existing connections. • After **Scale-in** workflow is run on a VNF group deployment, the vnf_pool for the DAG layer is NOT updated. This issue occurs rarely. • BIG-IQ *404 error* occurs while checking pool license. This issue occurs rarely.

Platform name	Description
	- The **Uninstall** workflow does NOT finish in the expected timeframe, due to the failover_state not updating as expected for deployment outputs on the VNF layer. If the faulty layer is not purged after running a **Heal** workflow, VNFM continues to monitor the faulty main instance and new, minor **Heal** workflows can occur, periodically. This can affect the time needed to uninstall the affected deployment.
BIG-IP Virtual Edition	- BIG-IP-14.1.4.6 Issues list - 15.1.5.1 Issues list (PREVIEW ONLY) - 16.1.2 Issues list (PREVIEW ONLY)
BIG-IQ 6.0.1 and 8.2.0.1	6.0.1 Issues list and 8.2 Issues list
CentOS-7-GenericCloud-1503	Issues list
OpenStack Newton	Issues list for v10 and Issues list for v13
VMware vSphere ESXi 6.5 and VIO v5.1	Issues list and documents for VMware Integrated OpenStack (VIO)

Fixed issues

The following table lists issues that were fixed in the designated version release:

Platform name	Fixed in version	Description
F5 VNF Manager	3.0.0	- When running the **Update Declaration** workflow for a Master deployment, the workflow is no longer triggered twice. - When assigning security groups that do NOT currently exist in OpenStack/VIO for a deployment, the deployment no longer fails. - BIG-IQ blueprint on VMware no longer fails to reinstall if a failure has occurred during a previous install workflow due to sticky ARP table entries. - BIG-IQ blueprint on VMware no longer fails to reinstall due to IP assignment issues. - Changing the password from the default password using the VNFM UI no longer causes some services (like rabbitmq) to stop working.

Platform name	Fixed in version	Description
		• VNFD install no longer fails on prepare_onboard - SSH exception bad authentication type, using a password instead of a key. • VNFD install no longer fails for OpenStack on check_all_services No key or index items. • BIG-IQ blueprint no longer fails during inputs validation. • BIG-IP VE v14.1 deploying the Gi-LAN blueprint on vSphere, you no longer receive the code":401,"message":"Authentication failed: Password expired error message. The password is updated by way of /mgmt/shared/authz/users. • Cloud-Init ISO mounts correctly on vSphere for BIG-IP VE v14.1.3.1.x. • vSphere - corrected the NIC ordering for Declarative Onboarding in VNFM. • iControl REST no longer sticks/locks while on-boarding a BIG-IP and now resets the rest-node service over SSH, when a REST lock is detected. • Nagios no longer fails during installation. • Base blueprint solution now works with Declarative Onboarding for both vSphere and OpenStack. • CGNAT-Offering blueprint in vSphere no longer fails to install. • Traffic for CGNAT-Offering blueprint flows as expected on the deployment with a single VNF layer. • For all vSphere blueprints, renamed the openstack_validator node to vsphere_validator node. • Removed the obsolete set_mac_addr_to_cloudinit_userdata input for vSphere blueprints, as it was used in the removed onboard-network-nic.sh script. • Declarative Onboarding calls no longer have the wrong BIG-IP hostnames. • To avoid file names reaching the maximum 255 character limit, introduced lockfile name character limits and a guard to trim lockfile names. • Added values check for db_ inputs (based the required, allowed methods).
BIG-IP Virtual Edition	14.1.4.6, 15.1.5.1, or 16.1.2	• BIG-IP-14.1.4.6 Issues list • 15.1.5.1 Issues list (PREVIEW ONLY) • 16.1.2 Issues list (PREVIEW ONLY)

Platform name	Fixed in version	Description
BIG-IQ	6.0.1 and 8.2.0.2	6.0.1 Issues list and 8.2 Issues list
CentOS-7-x86_64	GenericCloud-1503	Issues list
OpenStack	10.0 and 13.0	Issues list for v10 and Issues list for v13
VMware vSphere ESXi and VIO	6.5 and 5.1	Issues list and documents for VMware Integrated OpenStack (VIO)

Installation overview

To install F5 VNF Manager, point your browser to the F5 Downloads site and download locally, either a qcow2 file (OpenStack/VIO) or an OVA file (vSphere).

Additionally, you will need the following F5 product license keys:

Platform name	Product license
BIG-IQ 8.2.0.1	F5-BIQ-VE-LIC-MGR-LIC
BIG-IP-14.1.4.6, 15.1.5.1, or 16.1.2 Virtual Edition	F5-BIG-MSP-LOADV12-LIC
CentOS-7-x86_64-GenericCloud-1503	NA

Upgrade overview

You can upgrade HA clusters two ways:

- Upgrade on new hosts (recommended method).
- In-place upgrade (prevents ability to rollback).

Important

This method works only if you leave the IP, AMQP credentials and certificates unchanged.

For the complete F5 NFV Solutions and VNF Manager software upgrade policy, consult this K35549824 article. For BIG-IP VE upgrade procedures, visit BIG-IP VE upgrade guide.