Technical white paper

HP Virtual Connect Firmware Upgrade Steps and Procedures

Table of contents

About this document

This document specifies the versions of firmware and software as well as recommended steps for updates to Virtual Connect (VC) version 4.01 or later from previous versions in HP BladeSystem single and multi-enclosure VC Domain environments. The firmware and software versions listed in this document have been tested as a solution set and are fully supported by HP.

It is recommended that administrators read this entire document before attempting to update Virtual Connect firmware and clearly understand all of the steps and procedures outlined in it.

This document was last updated 6/4/2013

△ CAUTION: The specific firmware and software versions listed in this document provide support for HP Virtual Connect environments. These versions have been tested as a set and must be used together to ensure complete solution component compatibility and full functionality. . Using other version levels might result in operational issues.

Firmware and Software Updates

Setup of your HP BladeSystem c-Class enclosure with HP Virtual Connect modules and supported adapters (integrated and mezzanine cards) will require use of the latest HP BladeSystem Firmware Release Set 2013.02.0 with updates for specific components of the solution. For best results, follow the pre-deployment planning steps in the HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide and the HP BladeSystem ProLiant Firmware Management Best Practices Implementer Guide (See Additional Resources sections for download sites) to deploy the baseline set with component updates.

Always install the firmware recommended for this release for the following items:

- HP BladeSystem Onboard Administrator
- HP Virtual Connect
- Server blade system ROMs
- Ethernet mezzanines
- Fibre Channel mezzanines
- iLO

For a complete list of recommended firmware and software versions for HP BladeSystem environments with VC modules and supported adapters, see the HP BladeSystem Firmware Maintenance website (http://www.hp.com/go/bladesystemupdates). Click the **Compatibility & Downloads** tab and navigate to the **Additional Information** section to download the recommended HP Virtual Connect FlexFabric Solution Recipe White Paper.

Baseline Firmware Release Set contents

HP Service Pack for ProLiant	**Latest Version**
HP Service Pack for ProLiant (SPP) SPP replaces Insight Foundation (PSPs, Smart Update Firmware DVD, and other systems software). To download the update, see the HP Service Pack for ProLiant website http://www.hp.com/go/spp, click on the 'Download' button on and look for the appropriate version under 'Available Downloads'.	2013.02.0[1]

[1] If the desired version of Virtual Connect firmware is not available on the SPP DVD, Virtual Connect HP SUM smart components for Windows and Linux may be downloaded separately.

Onboard Administrator

Firmware	Latest Version
HP BladeSystem c7000 Enclosure Onboard Administrator (OA) Go to http://h20180.www2.hp.com/apps/Nav?h_product=3709945&h_client=S-A-R163-1 1. Select BladeSystem Enclosures and choose the appropriate enclosure 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Firmware-Blade Infrastructure" category 5. Find "HP BladeSystem c-Class Onboard Administrator Firmware", select the latest version and click the "Download" button	3.70

Virtual Connect

Firmware	Latest Version
HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition Component for Windows HP BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 4/8Gb 20-port and 8Gb 24-port FC Edition Component for Linux Go to the “VC Support Page” http://www.hp.com/support/vc 1. Select appropriate VC module 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Firmware-Blade Infrastructure" category 5. Select the latest version of Smart Component or VCSU supported firmware image file and click Download button	4.01

Virtual Connect Support Utility

Firmware	Latest Version
Virtual Connect Support Utility v1.8.1 for Windows, Linux or HP-UX (VCSU) Go to the “VC Support Page” http://www.hp.com/support/vc 1. Select appropriate VC module 2. Select Download Drivers and Software 3. Select the appropriate Operating System 4. Select the "Utility - Tools" category 5. Select the latest version of Virtual Connect Support Utility and click Download button	1.8.1

Virtual Connect is a set of interconnect modules and embedded software for HP BladeSystem c-Class enclosures. HP Virtual Connect includes the following supported components:

- HP Virtual Connect Manager
- HP Virtual Connect Flex-10/10D Module for BladeSystem c-Class
- HP Virtual Connect FlexFabric 10Gb/24-Port Module for BladeSystem c-Class
- HP Virtual Connect Flex-10 10Gb Ethernet Module for BladeSystem c-Class
- HP Virtual Connect 8Gb 24-Port Fibre Channel Module for BladeSystem c-Class

- HP Virtual Connect 8Gb 20-Port Fibre Channel Module for BladeSystem c-Class
- HP 1/10Gb Virtual Connect Ethernet Module for c-Class BladeSystem
- HP 1/10Gb-F Virtual Connect Ethernet Module for the c-Class BladeSystem
- HP Virtual Connect 4Gb Fibre Channel Module for BladeSystem c-Class (enhanced NPIV)
- HP 4Gb Virtual Connect Fibre Channel Module for c-Class BladeSystem

NOTE: Releases of VC firmware beyond v3.60 and VCSU beyond 1.6.0 no longer support HP 1/10Gb Virtual Connect and HP 1/10Gb-F Virtual Connect Ethernet Modules.

BladeSystem Firmware Installation Order

For Virtual Connect deployments where the Operating System is not yet installed on the servers or servers are not present in the enclosure, HP recommends the following component update order:

1. Update the OA first by using the Smart Update Firmware DVD for Windows and Linux. Use a workstation connected to the same network as the OA.
2. Update the VC firmware using VCSU v1.8.1 or later from a workstation connected to the same network as the OA and VC Ethernet modules.
3. Update all server-specific offline and online firmware components with the HP Firmware Maintenance DVD.

For Virtual Connect deployments where the Operating System is already installed on the servers, HP recommends the following component update order:

1. Update the blades and the OA by using the Smart Update Firmware DVD for Windows and Linux using a workstation connected to the same network as the OA.
2. Update any offline-only firmware components with the HP Firmware Maintenance DVD.
3. Update the VC firmware using VCSU v1.8.1 or later from a workstation connected to the same network as the OA and VC Ethernet modules. Be sure to update the VC firmware after all other updates are applied, after servers are rebooted, and after all other firmware is activated.

Firmware Update Requirements

VCSU v1.8.1 or later is recommended to upgrade VC Ethernet, FlexFabric and VC-FC module firmware. VCSU is also used to perform other maintenance tasks remotely on both HP BladeSystem c-Class c7000 and c3000 enclosures with Virtual Connect deployments.

VCSU's default upgrade workflow activates firmware on all of the VC Ethernet modules on one side of the enclosure before activating all of the modules on the other side of the enclosure. This minimizes disruption of network connectivity during the upgrades. Firmware activation on VC Fibre Channel modules is done serially starting from the highest IO Bay. VCSU displays a progress message indicating that an update is taking place and the percentage completed. After the module firmware updates are complete, the utility activates all modules. Different firmware activation choices are available in VCSU as optional parameters and allow parallel, serial or manual activation.

General Requirements

There are a number of general requirements that need to be met to update Virtual Connect firmware using VCSU utility.

- VCSU version 1.6.0 and later may be executed from a client inside the VC Domain that is being updated. VCSU 1.5.2 or earlier must be run from a client outside of the VC Domain being updated. If VCSU 1.5.2 or earlier resides on a server blade inside the domain that is being updated, VCSU may lose network connectivity to the VC Ethernet and Fibre Channel modules. This can cause unexpected firmware update failures and risks leaving the Virtual Connect Manager in non-operational state.

- To run VCSU, the minimum, required, available free disk space is 600 MB per install instance. For example, if you run VCSU three times in parallel against three different enclosures, you must have approximately 1.8GB of available disk space.
- VCSU v1.7.0 and VC v3.70 and higher do not support the HP VC 1/10 Gb VC-Enet Module and the HP 1/10 -Gb-F VC-Enet Fibre Channel Module. These unsupported modules must be removed from the domain before proceeding with firmware updates to VC v3.70 or later.
- For Windows users – Microsoft® Windows® XP (Service Pack 1 or 2), Windows Server® 2003, Windows Server® 2008 or Windows Vista® operating systems must be installed on the VCSU client system.
- For Linux users – RedHat 4, RedHat 5, SLES 10, and SLES 11 for x86 Servers must be installed on the VCSU client system (only VCSU version 1.5.2 or newer).
- For HP-UX users – HPUX 11.23 and 11.31 must be installed on the client system (only VCSU version 1.5.2 or newer).
- VCSU supports IPv4 addresses.
- When upgrading Virtual Connect 4Gb Fibre Channel modules running version 1.31 or earlier, VCSU must be installed and run from an account with Administrator or Power User privileges on the Windows client system.
- A valid HP Virtual Connect firmware package must be available to install. Download the firmware from the HP website (http://www.hp.com). Click Software and Driver Downloads, and then search for "Virtual Connect Firmware."
- Do not close the VCSU console application while a firmware update is in progress. If VCSU is closed before the update completes, the module firmware might not update properly. This can result in an incomplete update and cause the module firmware to become inoperable.
- If the VCSU firmware update process is interrupted, any future VCSU firmware update operations as well as attempts to login to the VCM GUI or CLI will be rejected until VC-Ethernet modules are restarted via a “Reset” Interconnect Bay operation from the Onboard Administrator management interface.
- An Onboard Administrator user account with Administrative privileges and access to all Onboard Administrators and interconnect bays in the domain must be available for use. If the enclosure is imported into a Virtual Connect domain, a Virtual Connect user account with Domain privileges is also required.
- In a multi-enclosure environment, the Onboard Administrator username and password must be identical across all enclosures in the Virtual Connect Domain. If the credentials are not identical, attempts to update firmware for the remote enclosures will fail.
- The VCSU client system must have Ethernet network connectivity to the enclosure Onboard Administrator. To validate this connectivity, open a web browser to the enclosure Onboard Administrator before running VCSU.
- All Virtual Connect Modules must have valid IP addresses on the OA management network from EBIPA or external DHCP and be reachable from the client system.
- If utilizing VCSU v1.5.2 or newer, it is no longer necessary to disable network or host-based firewalls, open up TCP port 21, disable local Windows firewalls, Symantec Endpoint Protection (SEP), or McAfee firewall protection or add VCSU to the list of firewall exceptions.
- Only one instance of the VCSU utility accessing a single enclosure or Virtual Connect domain can be run on the same client system at one time. Using multiple VCSU clients to interface remotely with the same enclosure can interrupt the firmware update process and prevent it from completing successfully.
- During a firmware update operation, the Virtual Connect Manager User Interfaces will become temporarily inaccessible. Any attempt to reset or remove the modules during the update process may result in a corrupted firmware image.
- Do not remove or reset the Onboard Administrator of the target enclosure or update its firmware while Virtual Connect modules are being updated. Doing so can interfere with the firmware update process and cause the update to fail.
- If the VCSU system is interrupted or loses network connectivity during the update, reset the affected module and restart the firmware update process.

- If Virtual Connect Enterprise Manager (VCEM) is in use, it must be at a revision that is compatible with the target VC firmware version prior to the VC firmware upgrade attempt. For the correct VCEM version, refer to the Virtual Connect Enterprise Manager Support section of this document.
- VCSU 1.8.1 and later detect VC Domains managed by VCEM and restrict incompatible firmware upgrades to ensure firmware compatibility across the VC Domain Group.
- When updating VC Domains that are under VCEM control, the Virtual Connect domain must be placed into Maintenance Mode or Firmware update mode before initiating the update. Maintenance mode is available for all versions of VCEM and VC firmware. The firmware update workflow requires VCEM 7.1 or later, together with VC v3.50 or later and VCSU 1.7.0 or later.
- When using VCSU v1.5.2 to update HP VC 8Gb 24-port FC modules, a healthy VC-Enet backup module must be installed in either IO Bay 2 or IO Bay 1 (if the primary VC module is in IO Bay 2). If no backup module is available, VCSU reverts to the FTP-based method. If there is a firewall blocking FTP communication, the firmware update will fail. VCSU v1.6.0 lifts this restriction.

- VCM 4.01 together with VCSU 1.8.1 provide customizable VC user role permissions. This means operations such as firmware update, domain backup and exporting support information to be delegated to Network, Storage or Server Administrator roles.

Pre-installation Instructions

Perform the following pre-installation checks to ensure the health of the VC domain before updating VC firmware.

1. VCSU automatically creates a backup of the Virtual Connect domain configuration during the firmware update. The backup is stored in a file on the workstation where VCSU is installed (typically under C:\Program Files\Hewlett-Packard\Virtual Connect Support Utility\). If a backup file was not created or appears to be zero size, back up the VC domain configuration using the steps outlined below.

   To back up using the Virtual Connect GUI:

   ○ Log in to VCM through a supported browser by browsing to the IP address or DNS name of the VCM and providing administrator credentials.

   ○ Select “Tools → Backup/Restore Domain Configuration” from the top menu.

   ○ Select “Backup Configuration”, and then click OK.

   ○ Save the file to your system in case it is needed for recovery at a later time.

   ○ Log out of VCM, and close your browser.

To back up using interactive mode of VCSU v1.5.2 or later, execute the configbackup command from the VCSU command prompt.

Note: In a multi-enclosure environment or when redundant OA modules are present, the Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

To perform a non-interactive back up use the following command:

```
vcsu -a configbackup -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>] [-l <FILE>] [-cp <CFG PASS>]
```

IP = IP Address of the active Onboard Administrator in enclosure

USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays

PWD = Password of the Onboard Administrator user. Use * to prompt for password

VCM USER = Name of Virtual Connect user with Domain privileges is required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain

VCM PASS = Password for VCM USER

FILE = File name or full path of the file on the local file system to which the Virtual Connect Domain configuration will be saved (optional parameter).

CFG PASS = Password for Config Backup of Virtual Connect Domain Only used in Virtual Connect 3.00

and later.

Example:

```
vcsu -a configbackup -i 192.168.1.100 -u Admin -p password
```

2. VCSU v1.7.0 and higher automatically performs health check operation and will block firmware update on the VC Domains that are not healthy. When using VCSU versions prior to v1.7.0 run a health check for Virtual Connect deployments by executing the “healthcheck” command from the VCSU command prompt.

Note: In a multi-enclosure environment or when redundant OA modules are present, the Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

The following command may be used for this operation:

vcsu -a healthcheck -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>]

IP = IP Address of the active Onboard Administrator in enclosure

USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays

PWD = Password of the Onboard Administrator user. Use * to prompt for password

VCM USER = Name of Virtual Connect user with Domain privileges is required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain

VCM PASS = Password for VCM USER

Example:

```
vcsu -a healthcheck -i 192.168.1.100 -u Administrator -p password
```

Verify that the status of all VC Ethernet and FlexFabric modules is normal as shown in the output below.

- Health = OK
- IP Connectivity = Passed
- Domain Configuration = In Sync (Primary and Backup modules only)
- Module Configuration = In Sync

```
--------------------------------------------------------------------------------
Bay 1 : HP VC Flex-10 Enet Module
--------------------------------------------------------------------------------
Power                : On
Health               : Ok
IP Address           : 171.50.0.81
IP Connectivity      : Passed
Version              : 3.70
Mode                 : Primary
Domain Configuration : In Sync
Module Configuration : In Sync

--------------------------------------------------------------------------------
Bay 2 : HP VC Flex-10 Enet Module
--------------------------------------------------------------------------------
Power                : On
Health               : Ok
IP Address           : 171.50.0.84
IP Connectivity      : Passed
Version              : 3.70
Mode                 : Backup
Domain Configuration : In Sync
Module Configuration : In Sync
--------------------------------------------------------------------------------
Bay 5 : HP VC FlexFabric 10Gb/24-Port Module
--------------------------------------------------------------------------------
Power                : On
Health               : Ok
```

```
IP Address           : 171.50.0.91
IP Connectivity      : Passed
Version              : 3.70
Mode                 : Subordinate
Domain Configuration : In Sync
Module Configuration : In Sync

-------------------------------------------------------------------------------
Bay 6 : HP VC FlexFabric 10Gb/24-Port Module
-------------------------------------------------------------------------------
Power                : On
Health               : Ok
IP Address           : 171.50.0.94
IP Connectivity      : Passed
Version              : 3.70
Mode                 : Subordinate
Domain Configuration : In Sync
Module Configuration : In Sync
```

If any modules in the enclosure exhibit the following status, take the action recommended below

- Health = Degraded/Failed

The Onboard Administrator is reporting that this module is unhealthy. Log in to the Onboard Administrator for additional information to determine the potential problem. A reset of the failed module may correct this condition.

- Domain Configuration = Not In Sync

The domain configuration is not synchronized between the Primary and Backup VC modules. This may be a transient condition. Wait up to 5 minutes and rerun the “healthcheck” command. If the Domain Configuration is still “Not In Sync”, collect VC Support Information and Contact HP Support. A reset of the VCM may help to clear up this condition. Please refer to Appendix A for instructions on how to reset VCM.

- Module Configuration = Invalid/Not In Sync

The interconnect module configuration is not synchronized with the VC domain configuration. This may be a transient condition. Wait up to 5 minutes and rerun “healthcheck” command. If the Module Configuration is still “Not In Sync”, collect VC Support Information and Contact HP Support. A reset of the VCM may help to clear up this condition. Please refer to Appendix A for instructions on how to reset VCM.

Verify that the status of all VC Fibre Channel modules is normal as shown in the output below.

- Health = OK
- IP Connectivity = Passed

```
-------------------------------------------------------------------------------
Bay 3 : HP VC 8Gb 24-Port FC Module
-------------------------------------------------------------------------------
Power                : On
Health               : Ok
IP Address           : 171.50.0.89
IP Connectivity      : Passed
Version              : 1.04

-------------------------------------------------------------------------------
Bay 4 : HP VC 8Gb 24-Port FC Module
-------------------------------------------------------------------------------
Power                : On
Health               : Ok
IP Address           : 171.50.0.90
IP Connectivity      : Passed
```

```
Version              : 1.04
```

If any modules in the enclosure exhibit the following status, take the action recommended below

- Health = Degraded/Failed

The Onboard Administrator is reporting that this module is unhealthy. Log in to the Onboard Administrator for additional information to determine the potential problem. A reset of the failed module may correct this condition.

- IP Connectivity = Failed

Ethernet network connectivity between the client system and the VC Fibre Channel modules has failed. Log in to the Onboard Administrator and validate that VC Fibre Channel modules are assigned valid IP addresses from the same management IP subnet as the client system. Once IP addresses are properly configured, rerun the "healthcheck" command.

For any instance where "Contact HP Support" is recommended, please use the following steps to gather support information:

1. Login into Virtual Connect Manager, Select "Tools→Export Support Information".
2. Login to Onboard Administrator CLI, execute "show all" command and save the output to a file.
3. On the VCSU client system, collect all fwupdate-xxx.log files from where VCSU is installed (typically under C:\Program Files\Hewlett-Packard\Virtual Connect Support Utility\)

Firmware Update Instructions

Installation Notes

- If you are using the Virtual Connect Enterprise Manager (VCEM) to manage your Virtual Connect domains, you will need to place them in "Maintenance" or "Firmware Update" mode before using the VCSU utility.
- VCSU does not update modules that are not physically present, are powered off, or are non-functional. Please run the VCSU "healthcheck" command to determine module's state and status before initiating the update.
- VCSU does not update non-VC modules, including pass-thru and switch modules.
- If the firmware image location is specified in VCSU as a hyperlink to an HTTP or HTTPS website, this site must not require additional authentication.
- If the firmware image location is specified in VCSU as a link to an FTP site, this site must be a non-SSL/TLS, Passive Transfer Mode FTP site, and you must include the authentication information in the link. For example: ftp://user:password@hostname-or-ipaddress/directory/filename.
- If the firmware image location is specified in VCSU as a Windows path and any of the directory names in the path contain spaces, the entire path including the filename must be enclosed in double quotation marks.

Installation Process

After all of the checks have completed successfully, the VC firmware must be downloaded from the web. The latest version of the firmware can be found on the **Compatibility & Downloads** tab of the HP BladeSystem Firmware Maintenance page http://www.hp.com/go/bladesystemupdates.

Once the VC firmware package is downloaded from the web, launch VCSU 1.8.1 or later from your local Windows, Linux or HP-UX workstation and execute the "update" command from the VCSU command prompt.

Both the OA and VC credentials are required for the update process. The OA credentials must be Administrator equivalent credentials so VCSU can access specific OA data to perform the upgrade.

Under no circumstances should VC modules be restarted or the VCSU Console Window closed while the update process is in progress. Such interruptions cause the firmware update to fail and can render modules inoperable. If the VCSU firmware update process is terminated, any future VCSU firmware update operations as well as attempts to login into the VCM GUI or CLI will be rejected until VC-Ethernet modules are restarted via a "Reset" Interconnect Bay operation from the Onboard Administrator management interface.

Firmware Update Process

The typical firmware update process that most administrators are familiar with is the update of a single switch which generally has a deterministic update time. Updating the firmware of the VC modules is not as deterministic and predictable and so may be unexpected to some users. The update process takes approximately 20 minutes for each VC-Enet module and 5 minutes for each VC-FC module. These times vary depending on the number and types of the modules in the enclosure, as well as the presence and complexity of the VC Domain configuration. VC update times also vary based on whether a Single- vs. Multi-Enclosure domain configuration is being updated.

There are two key reasons why the VC update experience is different from other network gear:

1. The update of a VC Domain in a redundant configuration takes place while the VC modules maintain connectivity and provide uninterrupted services to the servers in the VC Domain. Virtual Connect maintains a configuration database for the overall VC Domain as well as individual VC Ethernet and Fibre Channel modules. VC must ensure that each module has the correct configuration prior to bringing the module back online after the upgrade. This process takes time and varies depending on the size and complexity of the VC Domain.

When updating a VC Domain, VCSU performs the following steps required for a successful update:

Step #'s	Stages	Detailed Description	VCSU % completion
1	**Initialization**	Download firmware package (local file or HTTP/HTTPS/FTP site) and unpack it locally	N/A
2		Gather current running firmware information from the modules in the Domain.	
3		Compare firmware package information with currently running firmware information.	
4		If enclosure(s) have been imported into the VCM domain: a. Store which IO Bay is currently Primary VC module. b. Verify that the VC Domain is stable, i.e. no operations are in progress. c. Backup VCM config and optionally password protect it.	
5		Check for previously incomplete, in progress, or failed firmware update operations.	
6	**Update**	Temporarily make VC Manager inaccessible to the external management applications (GUI, CLI, and VCEM) in order to prevent VC configuration changes while the firmware update is in progress.	0%
7		In parallel, via sFTP, copy firmware image to each of the VC Ethernet or FlexFabric modules.	28%
8		Simultaneously begin firmware update on all VC Ethernet and FlexFabric modules.	28%
9		Continuously monitor all modules' update progress and wait to complete the update operation.	57%
10		If enclosure(s) have been imported into the VCM domain: • Verify that the VC Domain is stable, i.e. no operations are in progress.	71%
11	**Activation**	Make VC Manager accessible to the external management applications (GUI, CLI, and VCEM).	0%
12		If enclosure(s) have been imported into the VCM domain: • Verify that the VC Domain is stable, i.e. no operations are in progress.	10%
13		Begin the firmware activation process utilizing the default firmware activation method (odd-even)	10%
14		Reboot all VC Ethernet or FlexFabric modules in the enclosure(s) that are on the same side of the enclosure(s) as the Backup VC module.	20%

15		Wait for all of the rebooted modules to come back online and report the correct firmware version.	25%
16		If enclosure(s) have been imported into the VCM domain: • Verify that the VC Domain is stable, i.e. no operations are in progress.	25%
17		Reboot all VC Ethernet or FlexFabric modules in the enclosure(s) that are on the same side of the enclosure(s) as the Primary VC module EXCEPT for the Primary VC module itself.	30%
18		Wait for all of the rebooted modules to come back online and report the correct firmware version.	35%
19		If enclosure(s) have been imported into the VCM domain: • Verify that the VC Domain is stable, i.e. no operations are in progress.	35%
20		Force failover of the VC Manager from the Primary VC module to the adjacent IO Bay.	40%
21		Wait for the previous backup VCM module to become the new primary	40%
22		If enclosure(s) have been imported into the VCM domain: • Verify that the VC Domain is stable, i.e. no operations are in progress. This operation may take an extended period of time since the VC Domain may be required to be reconfigured.	40%
23		As the final step[1], the previous Primary VC module to complete activation process.	45%

[1] Above steps do not include VC-FC modules' update process. VC-FC modules are updated in parallel and their firmware is activated serially.

Firmware Update Considerations

VC Ethernet and FlexFabric modules reboot during the firmware activation process. This will affect connectivity to these modules. The impact of module firmware activation can be minimized by ensuring a redundant hardware configuration, proper networking connectivity setup and NIC teaming/bonding enabled on the servers in the domain. These network design methods are strongly recommended and must be a prevalent practice. VC-FC modules may experience an outage depending on the specific old and new FW versions. In most cases VC-FC modules utilize a Non-Disruptive Code Load and Activation (NDCLA) where no current I/O paths are affected by the update. Regardless of this VC-FC module feature, SAN connectivity must always be configured redundantly to avoid application outages.

When designing VC Domain connectivity, administrators must take into consideration all of the dependencies that may influence the VC Domain's ability to sustain a firmware update while continuing to pass traffic without interruption. The following aspects of a redundant design have to be verified prior to firmware update in downtime sensitive environments:

1. In the VC v1.2x firmware releases when firmware update was done using the VC Manager UI, a workaround was added for firmware upgrade to bounce stacking links to prevent the loss of communication on the management VLAN between the Primary and Standby modules. Prior to this improvement, older firmware versions would not see the Standby modules receive a checkpoint from the Primary. Subsequently, a function to monitor for a successful checkpoint was added to VCSU. This checks for the valid checkpoint and prevents the firmware update from proceeding without one. In VC v3.60 the behavior associated with bouncing stacking link was eliminated. Since the logic to bounce stacking links is in the installer script contained in the new firmware image, updating to VC 3.60 improves the behavior and eliminates the unnecessary network outage. VC multi-enclosure domains were more susceptible to this issue than single enclosure domains.
2. In VC firmware v3.18 and earlier there was the potential for a network outage of up to ~20 sec due to a physical link on the NICs staying up even though the forwarding path was being blocked by VC during graceful module shutdown for firmware activation. Both VCSU v1.6.0 and VC v3.30 resolved this issue by forcing the physical link down on all VC Enet module interfaces prior to activating firmware for the module.
3. Proper stacking link configuration between VC modules and enclosures provides connectivity for any blade server to any uplink port in the VC domain, regardless of the server location. This reduces the overall number of cables needed for uplink connectivity, provides the ability to move a server profile between enclosures, reduces

datacenter core switch traffic, and plays a major role in sustainability of the individual VC module outage during firmware upgrade.

Please consult both the Virtual Connect Multi-Enclosure Stacking Reference Guide and Virtual Connect Setup and Install Guide for recommended stacking link configurations and requirements.

4. The order of module activation in VCSU plays a crucial role in how network and storage connectivity will be interrupted or preserved during a firmware update. VCSU's default upgrade workflow alternates activating VC Ethernet modules on the left and right (odd and even) side modules to minimize disruptions of network and storage connectivity during the upgrade.
5. In order to minimize the potential of an outage, VC networks and SAN fabrics should be created with both A and B side connectivity to allow either all links to be in an active state at all times or to provide a controlled failover. More physical uplinks could be utilized and additional Virtual Connect networks defined to reduce latency and provide more bandwidth to the networking layer, based on application demands.
6. The configuration of the blade host operating system is vital in order to maintain uptime during the firmware update process. Properly configured NIC teaming/bonding and vSwitches will ensure both redundancy of the network connectivity, fast network path failure detection and timely failover to a redundant path, if available.

   The following operating system settings allow faster link failure detection and failover initialization.

   - Under normal operating conditions, the Virtual Connect SmartLink setting will alter the individual NIC state in the vSwitch, vDS, or teaming/bonding software by turning off the corresponding server NIC port. This will cause the vSwitch, vDS or NIC teaming/bonding to detect a failure and fail-over traffic to an alternate path. In order for the SmartLink functionality to operate as designed, valid DCC-compatible NIC firmware and drivers must be installed on a blade server. During the firmware update process when VC Ethernet and FlexFabric modules are reset for activation, SmartLink and the DCC protocol will not be able to send a message to the NIC indicating that the link went down since the module is being rebooted. Therefore, during firmware update operation it is the responsibility of the NIC and host OS to detect the link failure.
     - Configuring the vSwitch or vNetwork Distributed Switch (vDS) Network Failover Detection option for "Link Status Only" in VMware ESX/ESXi Server network configuration is recommended.
     - In some cases, during firmware update when VC Ethernet and FlexFabric modules are reset for activation and undergo graceful shutdown, there is the potential for a network outage of up to 20 sec. In these cases, enabling VMware ESX Beacon Probing, Linux ARP Monitoring and Windows Path Validation Heartbeat will work faster and more consistently. Please note that for VMware ESX Beacon Probing is most useful with three or more NICs in a team and only available with vSwitch and vDS, not with NX1000v. Review the VMware Knowledge Base articles specified below for the pros and cons of enabling Beacon Probing.
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1005577
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1017612
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1039177
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1024435
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1004373
       http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1012819
   - In the VMware ESX/ESXi environments it is recommended to either turn OFF the High Availability (HA) mode or increase the VMware HA timeout from the default of 13 seconds to 30-60 seconds. When the above options are configured, all guest OSes will be able to survive the upgrade with expected network outage due to the stacking link re-convergence and optimal network path recalculation by VCM.
   - Use VCSU manual firmware activation order for environments where changing Network Failover Detection options or HA settings is not possible. In this case, modules will be updated but not activated and the administrator can perform manual activation by resetting (rebooting) modules via the OA GUI or CLI interface. This approach eliminates the potential 20 sec maximum network outage that may occur on a graceful shutdown of VC Ethernet and FlexFabric modules.
   - The Spanning Tree Port Fast feature of Cisco switches allows a switch port to bypass the 'listening' and 'learning' stages of spanning tree and quickly transition to the 'forwarding' stage. By enabling this feature, edge devices are allowed to immediately begin communication on the network instead of having to wait on Spanning Tree to determine if it needs to block the port to prevent a loop – a process that can take 30+

seconds with default Spanning Tree timers. VC is an edge device and this feature allows server NICs to begin immediate communication on the network rather than waiting for the additional 30 seconds to allow the spanning tree algorithm to recalculate. The following examples show how to enable PortFast:

- Catalyst switches use the commands:
  ```
  spanning-tree portfast
  spanning-tree portfast trunk
  ```
- Nexus switches use the commands:
  ```
  spanning-tree port type edge
  spanning-tree port type edge trunk
  ```

  *** Nexus switches will also accept the *portfast* commands.

7. In Multi-Enclosure VC Domains it is recommended to insert an additional 5 min delay into the VCSU utility execution script. This option delays firmware activation of the VC modules between left and right sides of the enclosure while allowing VCM to stabilize and checkpoint the configuration across recently rebooted modules. This also allows NIC teaming/bonding software and vSwitches, as well as multi-pathing storage software to fully recover from one path failure due to an update before failing over to a secondary path.
8. When upgrading the HP VC 4Gb FC module's firmware from version 1.2x to version 1.4x, the HP VC 4Gb FC module will temporarily drop SAN connectivity during the activation process due a required module reset. Properly configured multi-pathing storage software will allow for a failover with no loss of application connectivity to the fabric.
9. Upgrades from VC versions 3.18 or earlier to VC 3.60 may fail to complete successfully as described in the Customer Advisory c03395976. The advisory provides additional details and a choice of workarounds to avoid the problem.

Installation Options

VCSU only updates supported VC modules that are reporting good status and that require an update. In addition to the default installation options, there are several optional parameters available.

1. It may be necessary to update just a single VC-Enet or VC-FC module. The option to target a specific module for upgrade or downgrade (-b bay_id) has been removed in VCSU v1.6.0 and later. Typically this option was not recommended because VCSU's main goal is to get all modules to the same level of firmware that is contained in the installation package.

   However, a situation may exist where a module is being replaced with a spare that shipped with a different firmware revision installed. An update will be required to this single module to bring it to the same level of the firmware as the other the modules in the enclosure. To update a single module place it into any IO Bay that doesn't correspond to the location of the Primary VC-Enet module in the enclosure. An upgrade or downgrade of a single module can be performed by executing VCSU and specifying the location of the firmware image file corresponding to the version of the firmware on the Primary VC-Enet module. VCSU will automatically detect modules that are out of sync and update those modules to the desired firmware level.
2. As one of the first steps during the firmware update process, VCSU takes a snapshot of the Virtual Connect Domain configuration and stores it locally in the directory where VCSU is installed. VCSU provides the option to encrypt the configuration backup file if you specify a password for the configuration backup.
3. It is possible to force an update of the modules under the following circumstances:
   a. version – the target module contains a running firmware image that is the same version as the one in the source package.
   b. health – the target module is in a degraded or failed state.

4. By default, VCSU installs the new firmware package on all VC modules simultaneously. Following installation, VC Ethernet modules' firmware activation alternates between left and right side modules to minimize disruption to the network connectivity during the upgrades. Firmware activation on VC Fibre Channel modules is performed sequentially starting from the highest IO Bay.

   Alternate firmware activation methods are available in VCSU as optional parameters and allow activation in parallel, serially, or manually. Plan carefully before proceeding with one of the alternate methods and understand the potential implications on the server network and storage connectivity. For more details on the alternate firmware activation methods please refer to the Virtual Connect Support Utility Version 1.8.1 User Guide.

```
-------------------------------------------------------------------------------
 HP BladeSystem c-Class Virtual Connect Support Utility
 Version 1.8.1 (Build 23)
 Build Date: May 16 2013 16:04:55
 Copyright (C) 2006-2013 Hewlett-Packard Development Company, L.P.
 All Rights Reserved
-------------------------------------------------------------------------------

Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 171.50.0.40
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: ********
Please enter firmware package location: vcfwall401.bin
Please enter Configuration backup password (Optional):
Please enter Force Update options if any (eg: version,health):
Please enter VC-Enet module activation order if any (eg: parallel or odd-even
or serial or manual. Default: odd-even):
Please enter VC-FC module activation order if any (eg: parallel or odd-even or
serial or manual. Default: serial):
```

5. VCSU's default upgrade workflow alternates activating VC Ethernet modules on the left and right (odd and even) side modules to minimize disruptions of network and storage connectivity during the upgrade.In some instances is it recommended to insert an additional 5 min delay into VCSU utility execution script to delay activation of the VC modules' firmware between left and right sides of the enclosure, thereby allowing VC Manager and the host operating system to stabilize before continuing with the update.

```
-------------------------------------------------------------------------------
 HP BladeSystem c-Class Virtual Connect Support Utility
 Version 1.8.1 (Build 23)
 Build Date: May 16 2013 16:04:55
 Copyright (C) 2006-2013 Hewlett-Packard Development Company, L.P.
 All Rights Reserved
-------------------------------------------------------------------------------

Please enter action ("help" for list): update
Please enter Onboard Administrator IP Address: 170.50.0.40
Please enter Onboard Administrator Username: Administrator
Please enter Onboard Administrator Password: ********
Please enter firmware package location: VCpackage4.01.bin
Please enter Configuration backup password (Optional):
Please enter Force Update options if any (eg: version,health):
Please enter VC-Enet module activation order if any (eg: parallel or odd-even
or serial or manual. Default: odd-even):
Please enter VC-FC module activation order if any (eg: parallel or odd-even or
serial or manual. Default: serial):
Please enter the time (in minutes) to wait between activating or rebooting
VC-Enet modules (max 60 mins. Default: 0 mins): 5
Please enter the time (in minutes) to wait between activating or rebooting
VC-FC modules (max 60 mins. Default: 0 mins): 5
```

6. Once all of the required and optional parameters have been specified, VCSU verifies the validity of the specified firmware image file, gathers information about the VC modules in the target enclosure as well as the firmware running on those modules, compares firmware package information with the currently running firmware information to determine if this operation will be an update or a downgrade. If all of the checks passed and no errors were detected, VCSU produces a report with the types of the modules, their location, currently running firmware version and the new intended firmware version waits for administrator input on whether to proceed with the firmware update.

```
The following modules will be updated:

 ==============================================================================
 Enclosure   Bay  Module           Current Version       New Version
 ==============================================================================
 USE64426NH  1    HP VC Flex-10    3.70                  4.01
                  Enet Module      2012-08-26T22:02:23Z  2013-05-21T16:57:08Z
 ------------------------------------------------------------------------------
 USE64426NH  2    HP VC Flex-10    3.70                  4.01
                  Enet Module      2012-08-26T22:02:23Z  2013-05-21T16:57:08Z
 ------------------------------------------------------------------------------

 During the update process, modules being updated will be temporarily
 unavailable. In addition, the update process should NOT be interrupted by
 removing or resetting modules, or by closing the application. Interrupting
 the update or the modules being updated may cause the modules to not be updated
 properly.

 Please verify the above report before continuing.

 Would you like to continue with this update? [YES/NO]:
```

Firmware Downgrade Considerations

VC firmware downgrades were blocked beginning with VC version 3.15 and later. Administrators were required to delete the VC Domain prior to initiating a firmware downgrade. VC Domain deletion was required even when downgrading to the same major revision (e.g. downgrading from 3.15 to 3.10). The VC Domain configuration was not preserved through the downgrade process.

When the VC Domain is deleted, all VC modules revert to their default factory state. Server network and storage connectivity is removed. Any VC-assigned configuration parameters such as MAC addresses, WWNs, server serial numbers, boot target and boot order parameters are cleared from the servers. Any user accounts created under VCM are removed and only Administrator credentials remain valid.

Table 1: VC Domain Firmware Downgrade Scenarios

VC version		VC version	VC Domain Preservation
1.xx	→	1.yy (xx < yy)	Yes
2.xx	→	1.xx	Yes, if Flex-10 is not configured
2.xx	→	2.yy (xx < yy)	Yes
3.10	→	3.01	Yes
3.xx	→	1.xx	No
3.xx	→	2.xx	No
3.xx (xx >= 15)	→	3.yy (yy < xx)	No
3.70	→	3.zz (zz>=30)	Yes (via rollback, VCSU v1.7.0)
3.75	→	3.zz (zz>=30)	Yes (via rollback, VCSU v1.7.0)
4.01	→	3.zz (zz>=30)	Yes (via rollback, VCSU v1.8.1)

Firmware Downgrade Process

It is imperative to follow procedures outlined in this document when performing a VC Domain downgrade. The steps outlined below require preparatory actions for a successful VC Domain downgrade for both single and multi-enclosure environments when utilizing versions other than VCM v.4.01 and VCSU v1.8.1.

1. Locate a known good VC Domain configuration backup file corresponding to the intended firmware version. If this file is incompatible or corrupted, VCM will be unable to recover the domain configuration.
2. Execute the VCSU healthcheck command as outlined in the “Pre-installation Instructions” section of this document. Verify that the status of all VC Ethernet and FlexFabric modules is healthy. Take a note of the location of the Primary VC module (specifically the OA and Primary VC-Enet module IP Address information).
3. Login into VCM and perform the “Delete Domain” operation. In a multi-enclosure environment, deleting the domain releases the primary and non-primary enclosures back to an unintegrated state.
4. Using VCSU, downgrade each enclosure. There is no need to enter the VCM username or password during VCSU firmware downgrade operation since the VC Domain is no longer present.
5. To begin recovery of the VC Domain, locate information about the OA and the Primary VC-Enet module from step #2 above. Connect to the IP Address of the Primary VC-Enet module and login into the VC Manager GUI.
6. Once the enclosure is identified by VCM choices are available to either Import a New Enclosure or Recover from a previously saved configuration backup file. Choose the option to recover from the previously saved configuration backup file located in step #1.
7. VC Manager validates the backup file and proceeds with the recovery if no issues are identified with the file contents.

8. After importing the configuration backup file, VC Manager counts down to 0 seconds remaining and reloads the GUI login screen. The “Loading, Please Wait…” message is displayed during the recovery and is cleared once the domain is fully restored.
9. Login into the VCM once the login screen is displayed.
10. The secondary enclosures will not be seen by VCM in a multi-enclosure environment. The administrator must re-enter the corresponding OA username and password information.
    a. Using the VC GUI, navigate to the name of the enclosure that is marked with “?” or red “X” and click on the enclosure name. Select the Enclosure Status tab and re-enter the OA username and password information.
    b. If VCM reports that the enclosure is already part of another VC Domain, connect to the corresponding OA CLI and issue the following command – “clear vcmode” and repeat step (10.a) again.
    c. Once VCM locates these enclosures, it proceeds with the import and reloads the GUI login screen. The “Loading, Please Wait…” message is displayed while the enclosure is being imported and is cleared once the enclosure has been fully imported.
11. The VC Domain has now been fully restored including all of its enclosures.

Firmware Rollback Process

Beginning with VCM v3.70 and VCSU v1.7.0 a new firmware downgrade process is provided. This feature allows administrators to downgrade a VC Domain running v3.70 or newer to a previously installed version of VCM without having to delete the domain. The following restrictions must be taken into consideration when using this capability:

1. Modules that are part of the existing VC Domain must have been upgraded prior to attempting the rollback.
2. All servers in the domain must be powered off in order to perform the rollback.
3. Multiple, consecutive firmware downgrades are not allowed.
4. Administrators may only downgrade to the previously installed version of VCM which was running on the Primary module.
5. The VC configuration, including physical connections, uplink port connections, module positions in the enclosure, server types, etc. must be identical to the target downgrade configuration.
6. The current VCM credentials must be the same as those used prior to the upgrade.
7. The domain must be running VC v3.70 or higher to perform a rollback.
8. It is not possible to rollback to a VC version lower than v3.30.
9. The primary VC-Enet module must be in the lowest numbered IO Bay.

Virtual Connect Enterprise Manager

Virtual Connect Enterprise Manager (VCEM) centralizes network connection management and workload mobility for HP BladeSystem servers that use Virtual Connect to access local area networks (LANs), storage area networks (SANs), and converged network environments. VCEM helps organizations increase productivity, respond faster to workload and infrastructure changes, and reduce operating costs.

Built on the Virtual Connect architecture integrated into every HP BladeSystem c-Class enclosure, VCEM provides a central console to administer network address assignments, perform group-based configuration management, and to rapidly deploy, move, and failover server connections and workloads for 250 Virtual Connect Domains (designed to support up to 1,000 enclosures and 16,000 server blades when used with Virtual Connect multi-enclosure domains).

The Virtual Connect Enterprise Manager (VCEM) support matrix details VCEM and VC supported versions.

Table 2: VCEM Support Matrix

VCEM Version	Supported VC Firmware versions
6.1	2.1x, 2.2x, 2.3x, and 3.0x
6.2.2	2.1x, 2.2x, 2.3x, 3.0x, 3.1x, and 3.15 (pre-enabled)
6.3	2.1x, 2.2x, 2.3x, 3.0x, 3.10, 3.15, 3.17, and 3.18
6.3u2	2.1x, 2.2x, 2.3x, 3.0x, 3.10, 3.15, 3.17, 3.18, and 3.3x (pre-enabled)
7.0	2.1x, 2.3x, 3.0x, 3.10, 3.15, 3.17, 3.18, and 3.30
7.1	3.15, 3.17, 3.18, 3.30, 3.51 and 3.60
7.1.1	3.30, 3.51, 3.60, and 3.70
7.2	3.30, 3.51, 3.60, 3.70, 3.75, and 4.01

Verify that the intended VCM firmware version is supported by the VCEM version in use before updating a VC Domain that is controlled by VCEM. It is possible to add a VC Domain with a newer firmware version to an existing VC Domain Group (VCDG) by using compatibility mode in which VCM enables only those features supported by the older firmware.

The VCEM User Guide contains detailed information on compatibility mode features. VCEM implements the concept of a “group firmware mode” to allow mixed versions of VC firmware to coexist in a VC Domain Group. The group firmware mode is the functional level at which the domains within a VC Domain Group operate. By disabling features that aren’t known to the older VC Domain Group members, the newer version of VC firmware matches the behavior of the other domains in the group. This allows the incremental update of VC firmware on the domains in the VC Domain Group. After all the domains have been upgraded, the group firmware mode for the VC Domain Group can be upgraded to allow use of the new features.

VCEM v7.1and above provide two workflows for updating the VC firmware on the VC Domains belonging to VC Domain Groups. The first method relies on “Maintenance Mode” and is available for all supported versions of VCEM and VC. The procedure for using Maintenance Mode is:

1. Select the VC Domain to be updated and click **VC Domain Maintenance**.
2. Use VCSU to update the VC Domain to the new VC firmware version.
3. Click **Complete VC Domain Maintenance** to close the operation. If no other changes have been made in VCM while in maintenance mode, it can be faster to “cancel” maintenance rather than “completing” it. This is because completing maintenance propagates the base configuration to all the VC Domains in the VC Domain Group. Cancelling maintenance eliminates the propagation step but will leave the new firmware in place on the updated domain.
4. If needed, update the VC Domain Group firmware mode to the new level.

The second firmware update workflow that is added in VCEM v7.1 works in combination with VCSU 1.7.0 or later and VCM 3.50 or later. It has the benefit that multiple VC Domains in a VC Domain Group can be enabled for firmware update at the same time. The procedure for using "Firmware Update" is:

1. Select the VC Domain to be updated and click **VC Domain Firmware Update**.
2. Use VCSU to update the VC Domain to the new VC firmware version.
3. Click **Complete VC Firmware Update** to close the operation.
4. If needed, update the VC Domain Group firmware mode to the new level.

If a VC Domain is in firmware update mode, no VC Domain in the VC Domain Group can be put into maintenance mode. Likewise, if a VC Domain in the VC Domain Group is in maintenance mode, no VC Domain in the VC Domain Group can be put into firmware update mode. Firmware Update mode does not allow changes using the VCM user interface. If changes to VCM are desired, use VCEM Domain Maintenance mode instead of Firmware Update mode.

For VCEM availability and full product details and support, visit the HP website (http://www.hp.com/go/vcem) or contact your HP representative.

HP Smart Update Manager

HP Smart Update Manager (HP SUM) is a technology for installing and updating firmware and system software components on HP ProLiant and HP Integrity servers, enclosures, and network-based targets such as OA and VC Ethernet and Fibre Channel modules.

HP SUM has an integrated hardware and software discovery engine that finds the installed hardware and current versions of firmware and software. HP SUM insures that updates are installed in the correct order and that all dependencies are met before deploying an update. It also prevents version-based dependencies from destroying an installation, and ensures firmware updates are handled in a manner that reduces any downtime required for the firmware update process.

HP SUM is a firmware delivery engine for the HP Service Pack for ProLiant for both Windows and Linux. VC firmware support was added to the HP SUM starting with version 3.5.0. HP SUM can deploy the VC firmware using the embedded VCSU smart components. If the desired version of VC firmware components is not included in the HP Service Pack for ProLiant DVD, it may be downloaded separately from VC Support page. To deploy smart components that are not on the HP Service Pack for ProLiant DVD, please refer to the "Deploying Components not on HP Smart Update Firmware DVD" section of the HP Smart Update Manager User Guide.

HP SUM 5.0.0 is the preferred mechanism for firmware updates. However, Virtual Connect Support Utility (VCSU) must be used if any of the following conditions exist:

1. VC is in one of the following states:
   - VC modules are unhealthy – HP SUM reports the modules as unhealthy during the initial discovery. The administrator can fix the problem and re-scan the targets. If HP SUM finds the health status has changed, it will allow the update to proceed without the need to exit HP SUM and restart the process.
   - Non-redundant VC configuration – HP SUM will alert the administrator that the configuration is not redundant and will block any firmware operations. This prevents an inadvertent outage on the servers in the enclosure, especially when applying a large number of updates across multiple enclosures.
   - VC modules are not part of a domain – HP SUM doesn't have any additional information about interconnect modules beyond IP addresses and credentials. If the VC modules are not part of a domain, HP SUM is prevented from logging into the modules since VCM will return an error that the module needs to be imported into the domain first. HP SUM will report such targets as an unknown type and a failed discovery because it cannot communicate with the individual VC modules.
   - VC Domain is managed by VCEM – When HP SUM discovers VC modules managed by VCEM, it gets a notification that the VC modules are not in maintenance mode and it fails the update. Administrators may correct this

condition by going to the VCEM UI and placing the Domain containing the desired modules into Domain Maintenance to be updated by HP SUM. Once the VC Domain is in maintenance mode or firmware update mode (if applicable), the administrator can go back to HP SUM and rescan the target for HP SUM to proceed with the installation.

2. The administrator wants to:
   - Force same version upgrade – HP SUM does not allow an update to the same firmware version.
   - Update single module – HP SUM is an all-inclusive experience today.
   - Specify order of component deployment – HP SUM utilizes the default odd/even VCSU firmware update process. It does not provide optional parameters to alter module activation order nor does it allow for insertion of a time delay when activating VC firmware.
   - Downgrade VC firmware – HP SUM does not support forced downgrade of the VC firmware. Please refer to the Firmware Downgrade Considerations section of this document for more details.
   - Manually back-up VC configuration – HP SUM does not issue the commands to back up the configuration.

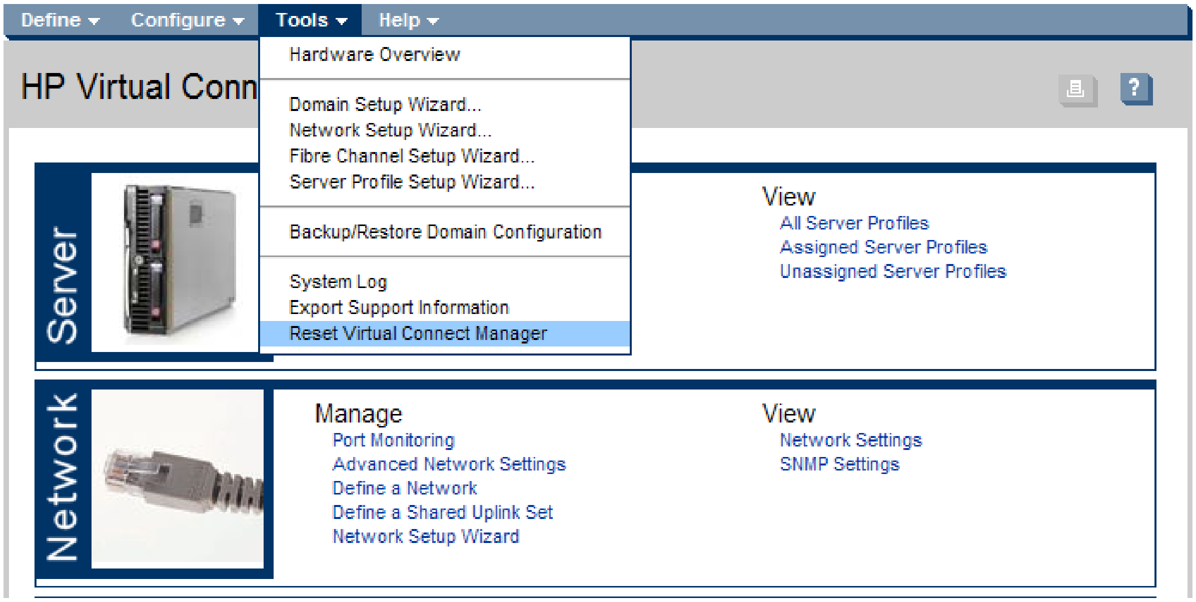
HP SUM uses the VC firmware smart component which contains the firmware image plus VCSU executable – HPsumCli.exe. HP SUM v5.0.0 provides dependency checking to ensure the OA, VC and servers are at versions that can be updated and also handles the order of installation to ensure they are updated in the correct sequence. Using VCSU by itself does not provide this capability. Starting with HP SUM v5.0.0, the VCSU smart component always performs a health check operation equivalent to the VCSU ‘healthcheck’ command.

Discovery of the VC modules with HP SUM does not begin the firmware installation process. HP SUM can discover the health, redundancy, VCEM presence and other conditions before the allowing the administrator to choose whether to initiate the firmware update sequence. This gives administrators the opportunity to fix issues and ensure the configuration is valid before deploying the new firmware to the VC modules. HP SUM can report dependencies, versions and other information without initiating any firmware installation.

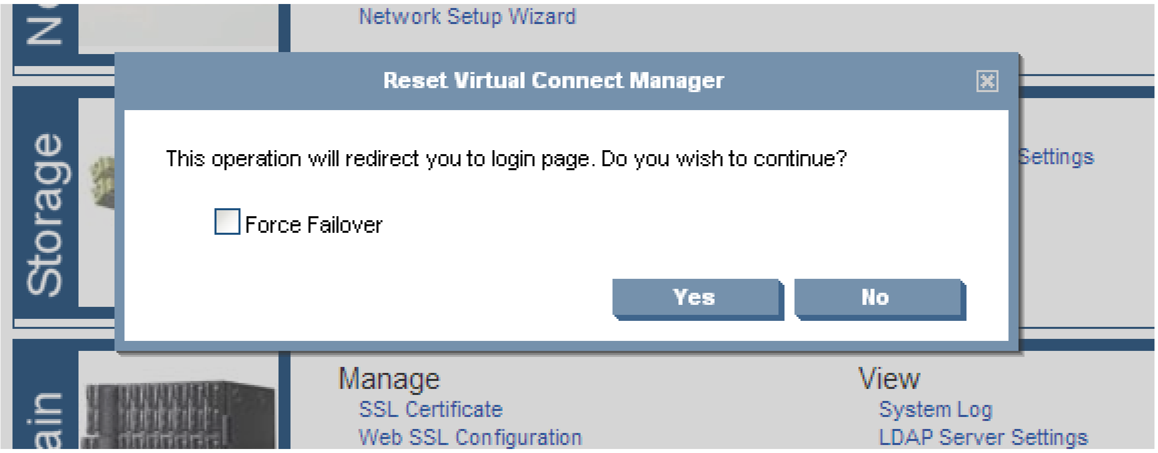
Appendix A: Resetting VC Manager

If a Reset of the Virtual Connect Manager is needed due to an incomplete or failed firmware update, please follow the steps outlined below to perform this operation. The Network and FC SAN connectivity for servers in the Domain is not disturbed during reset or failover of the Virtual Connect Manager.

To reset the Virtual Connect Manager application running on the primary Virtual Connect Ethernet module from the VCM GUI, select “Tools→Reset Virtual Connect Manager”.



The Reset Virtual Connect Manager popup is displayed.



Reset Virtual Connect Manager

This operation will redirect you to login page. Do you wish to continue?

□ Force Failover

- If the Force Failover checkbox is selected and a Virtual Connect Ethernet module is available in the horizontally adjacent IO Bay, the VCM UI is redirected to that Ethernet module after the Virtual Connect Manager reset completes.
- If the Force Failover checkbox is not selected or a Virtual Connect Ethernet module is not available in the horizontally adjacent IO Bay, the Virtual Connect Manager restarts on the current Ethernet module, and the logon screen for the current Ethernet module is displayed after the Virtual Connect Manager reset completes.
- Reset times depend on the size and complexity of the VC domain configuration.

It is also possible to use the VCM command line to reset the Virtual Connect Manager. Use the ***reset vcm*** command to reset VCM running on the primary VC Ethernet module:

```
> reset vcm
> reset vcm [-failover]
```

If the command line option '-failover' is included in the ***reset vcm*** command and a backup Virtual Connect Ethernet module is available, the command line displays the following message:

```
SUCCESS: The Virtual Connect Manager is being reset. Please wait...
```

You will be logged out of the session after approximately 1 minute. Any attempt to login to the same Virtual Connect Ethernet module will be rejected with the following error message:

```
Virtual Connect Manager not found at this IP address.
```

Any attempt to login to the backup module will present the following error message:

```
Unable to communicate with the Virtual Connect Manager. Please retry
again later.
```

Log into the specified interconnect bay and restart the Virtual Connect Manager service. This is the same process as the menu option "Reset VC Manager" from the Virtual Connect user interface.

As an alternative, the "Reset VC Manager" operation may be performed using interactive mode of VCSU by executing the "resetvcm" command from the VCSU command prompt.

Note: In a multi-enclosure environment or when redundant OA modules are present, the Onboard Administrator IP Address must be the IP address of the active OA in the primary enclosure.

A VCSU non-interactive method to reset Virtual Connect Manager is also available. The following command may be used for this operation:

```
vcsu -a resetvcm -i <IP> -u <USER> -p <PWD> [-vcu <VCM USER> -vcp <VCM PASS>]
```

IP = IP Address of the active Onboard Administrator in enclosure.
USER = Name of the Onboard Administrator user with privileges to access all enclosure interconnect bays.
PWD = Password of the Onboard Administrator user. Use * to prompt for password.
VCM USER = Name of Virtual Connect user with Domain privileges required if Enclosure is in a Virtual Connect Domain. N/A if Enclosure is not in a Virtual Connect Domain.
VCM PASS = Password for VCM USER.
Example:

vcsu -a resetvcm -i 192.168.1.100 -u Administrator -p password

For more information

To read more about Virtual Connect, go to www.hp.com/go/virtualconnect

The following documents provide additional information regarding setup and operation of HP BladeSystem enclosures and HP Virtual Connect FlexFabric Modules and FlexFabric Adapters:

Deployment related resources

HP Virtual Connect Firmware 4.01 Release Notes
http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c03801912/c03801912.pdf

HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide
http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c03801914/c03801914.pdf

HP BladeSystem ProLiant Firmware Management Best Practices
HP BladeSystem ProLiant Firmware Management Best Practices Implementer Guide
http://h18004.www1.hp.com/products/servers/management/literature.html

HP BladeSystem Firmware Maintenance Website
www.hp.com/go/bladesystemupdates

HP BladeSystem c-Class Virtual Connect Support Utility Version 1.8.1 User Guide
http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c03753554/c03753554.pdf

Best practice resources

HP Virtual Connect FlexFabric Cookbook
http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02616817/c02616817.pdf

HP Virtual Connect Multi Enclosure Stacking Reference Guide
http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02102153/c02102153.pdf

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

P/N: c02885443, Updated July 2013