HP BladeSystem c-Class Virtual Connect Support Utility Version 1.6.0 Release Notes

Abstract

This document provides release information for the HP BladeSystem c-Class Virtual Connect Support Utility Version 1.6.0, which remotely upgrades the VC-Enet and VC-FC module firmware in HP BladeSystem c-Class c3000 and c7000 Enclosures. This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Important notes and recommendations

- **IMPORTANT:** If you have FCoE connections configured through a mezzanine card, please read the "Known issues" section for an important workaround required to avoid a temporary FCoE outage during firmware update.

- For upgrading to VC 3.00 or later, the embedded Virtual Connect GUI and CLI FW update options have been removed. VCSU is the only stand alone method of FW update.

- HP strongly recommends running the healthcheck option on an enclosure before performing any management tasks. These tasks include, but are not limited to, the following:

  o Onboard Administrator firmware upgrade

  o Virtual Connect firmware upgrade

  o Onboard Administrator planned failover

  o Virtual Connect planned failover

- When entering an OA user name from a Linux command shell with the domain\username format, use quotation marks around the username so it is not expanded by the Linux shell.

  Example:

  ```
  vcsu -a collect -i 128.88.142.141 -u "dvt\ldapuser" -p hp123
  ```

- When entering an OA user password interactively with password masking from a Linux command shell, use quotation marks around the asterisk so it is not expanded by the Linux shell.

  Example:

  ```
  vcsu -a version -i 192.168.1.100 -u Administrator -p "*"
  OA Password            :***********
  ```

New features

The HP BladeSystem c-Class Virtual Connect Support Utility Version 1.6.0 contains the following new features:

- A VCSU update operation can be performed from a server blade in the same enclosure that is being updated. However, this feature is only supported when using a redundant network configuration on the server blade running the VCSU client.
- If the enclosure is in VCM mode, a support dump is downloaded before an update operation begins.

General requirements

- A supported operating system must be installed on the client:
  - Microsoft Windows XP (Service Pack 1 or 2)
  - Windows Vista
  - Windows Server 2003, 2008
  - HP-UX 11.23 and 11.31
  - Linux (Red Hat 4, Red Hat 5, SLES 10, SLES 11)
- 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.
- When upgrading from Virtual Connect 4Gb FC module version 1.31 or earlier, users must have Administrative or Power User privileges on the client system to install and run the utility.
- A valid HP Virtual Connect firmware package must be available to install. Download the firmware from the HP website (http://www.hp.com/go/bladesystemupdates). View the BladeSystem for ProLiant Release Set Compatibility Table and select the appropriate download.
- Do not close the console application when a firmware update is in progress. If the application is closed before the update completes, the module firmware might not update correctly, causing the module firmware to be inoperative.
- An Onboard Administrator user account with Administrative privileges and access to all Onboard Administrators and interconnect bays 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.
- The user must have Ethernet network connectivity between the client system and the enclosure Onboard Administrator. To validate this connectivity, open a web browser to the enclosure Onboard Administrator before running the utility.
- The user must have Ethernet network connectivity between the client system and the interconnect modules in the enclosure.
- Add the Virtual Connect Support Utility application to the list of exceptions for any host-based firewall on the client if you do not have a healthy Backup VCM module.
- No firewalls can exist between the client system and the remote enclosure Onboard Administrator if you do not have a healthy Backup VCM module. If a firewall exists, and it is blocking ports, then the utility cannot open a connection with the remote modules to perform the update.
- Onboard Administrator firmware v1.30 or higher is required for correct VCSU operation.
- Only one instance of the VC Support Utility accessing a single enclosure can be run on a single client at one time.
- During firmware update operations, the modules are unavailable for use. Any attempt to reset or remove the modules during the update process could result in a corrupted firmware image. In addition, do not reset the Onboard Administrator of the target enclosure or update its firmware while VC modules are being updated. Doing so can interfere with the firmware update process and cause it to fail. During

the firmware update process, connectivity through the modules, which might be hosted to servers in the enclosure, can be interrupted temporarily.

- During a firmware update session, only use a single client to update modules in a specific remote enclosure. Using multiple clients to interface remotely with the same enclosure can interrupt the firmware update process and prevent it from completing successfully.

- If the firmware update client is interrupted or loses network connectivity during the update, reset the affected module and restart the firmware update process.

- VCSU supports only IPv4 addresses. IPv6 support is not yet available.

- In a multi-enclosure environment, the Onboard Administrator username and password must be identical across the local and all remote enclosures in the Virtual Connect domain. Otherwise, firmware update of the remote enclosures will not succeed.

Resolved issues

The following issues that existed in previous versions of Virtual Connect Support Utility have been resolved in Virtual Connect Support Utility Version 1.6.0:

- At the final stage of a firmware update, VCSU waits a fixed amount of time for a primary VC module to become active. VCSU exits when this timer has expired, which results in a FAILURE status. VCSU has increased the amount of wait time to ensure that VCSU does not exit before VC Manager has completed its activation process.

- The VCSU library function to support HPSUM now reports the correct failure status when at least one module has failed its firmware update.

- VCSU now sets tty settings correctly so that it works under any type of terminal emulation.

- When in VCSU interactive mode, VCSU now recognizes the space character as part of a pathname for a VC package.

- VCSU now accepts the "\" character as part of the user name used to access Onboard Administrator.

- The "@" symbol is now accepted in Packageinfo for FTP package locations.

- Previously, VCSU terminated when encountering an upgrade failure. Now VCSU skips any failed modules and continues to upgrade the remaining modules.

- Previously, VCSU aborted in interactive mode when the "Force Update" prompt was left blank, and **Enter** was pressed.

- Resolved an issue where VCSU exited with an error when in VCSU interactive mode if a firmware pathname provided contained quotes.

- Resolved an issue where VCSU did not perform a firmware update when there was no VC domain defined.

- Resolved an issue where activation would fail with the message, "VCM configuration not in sync."

- Resolved an issue where the firmware update would fail in a multi-enclosure environment using the maximum configuration.

- Resolved an issue where users would receive a segmentation fault error when running VCSU in a multi-enclosure environment.

- Resolved an issue where an update would fail in an unimported enclosure.

- Resolved upgrade failures when using certain newer versions of Onboard Administrator and Virtual Connect Manager.

- If a disruption to the network connection occurs during a firmware update, VCSU now gracefully exits the update session.

- Previously, VCSU would terminate abnormally when processing an IP address in IPv6 format. VCSU now gracefully exits the update session.

- Resolved an issue where VCSU would terminate abnormally while updating certain large configurations.

- Resolved an issue where the firmware update for FC modules would fail due to an interrupted previous firmware update.

- Resolved an issue where a firmware update would fail with an error message `"Unable to create SSH session."`

- In some cases where VCM was in NO_COMM with the primary module, the VCSU `healthcheck` command incorrectly reported modules IN SYNC.

Known issues

Issue

When running Virtual Connect Support Utility in Interactive Mode, do not use quotation marks around the firmware package path even if the path has spaces. Only use quotation marks around the firmware package path when specifying the package location on the command line with the "-l" command-line parameter.

Issue

For important VCEM compatibility and version details when upgrading to VC 3.30 in VCEM 6.1, 6.2, and 6.3 environments, see the "Known Issues" section of the VC 3.30 Release Notes when available.

Issue

Upgrading VC firmware using Virtual Connect Support Utility (VCSU) or HP Smart Update Manager (HP SUM) from 3.15, 3.17, or 3.18 to a newer version might result in a temporary Fibre Channel over Ethernet (FCoE) outage.

This behavior is limited to systems using HP ProLiant or Integrity server blades with a FlexFabric Mezzanine adapter and a corresponding FCoE connection to an HP VC FlexFabric 10Gb/24-port module. This behavior does not appear for FCoE connections using an embedded FlexFabric adapter (LOM).
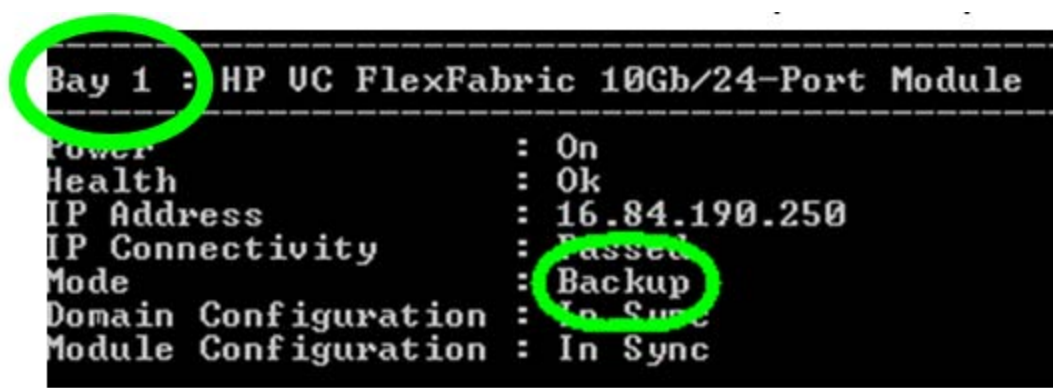
If a server blade in the enclosure is booted from SAN though a FlexFabric Mezzanine adapter, it experiences a loss of access to the SAN based boot target, and an indicator corresponding to the type of operating system appears on the server management console, for example, a blue screen for a Windows operating system.

For the server blades that were not booted from SAN, but are connected to a SAN-based storage, a temporary loss of SAN connectivity occurs. SAN connectivity is restored upon VC firmware update completion.

Workaround

To avoid a temporary SAN outage, use the following firmware upgrade steps:

1. Run VCSU healthcheck to determine which bays contain the primary and backup VC modules.

2. If the Virtual Connect domain is managed by Virtual Connect Enterprise Manager (VCEM):

   a. If the VC Domain is already in maintenance mode, go to the VCEM user interface and click **Cancel VC Domain Maintenance**. Cancelling maintenance mode rolls back any VC Domain changes that

were made while in maintenance mode. Verify that all running and pending jobs are allowed to complete before proceeding to step b.

    b. Click the **VC Domains** tab, select **VC domain**, and then click **VC Domain Maintenance**.

    c. Click **Make Changes via VC Manager**. This action releases control to the VCM.

3. Run VCSU `update` using the `-oe manual` option to avoid the activation phase.

   Example:
   ```
   vcsu -a update -i 192.168.1.100 -u Administrator -p password -vcu John -vcp
   vcPass -l C:\images\vcfw-120.bin -oe manual -of parallel
   ```

4. From the Onboard Administrator (OA), reset the backup VC module reported in step 1.

5. Log into VCM. Do not proceed to the next step as long as a checkpoint pending indicator is present.

6. From the VCM tools menu select **Reset Virtual Connect Manager**, and then select the Force Failover checkbox.

7. Wait until VCM fully restarts and you are able to log in through the GUI, and the checkpoint pending indicator is not present.

   The backup and primary modules have now switched roles. For example, if the original backup module was bay 2, then the new backup module is now bay 1 and the primary module is bay 2.

8. From the OA, reset the remainder of the VC Ethernet modules on the same side as the new primary.

9. Wait until the checkpoint pending indicator is no longer present.

10. From the VCM interconnect module page, wait until those modules that were reset in step 8 show a status of **OK**.

11. From the OA, reset the remaining VC Ethernet modules (all modules on the new backup module side).

12. If the Virtual Connect Domain is managed by Virtual Connect Enterprise Manager (VCEM), go to the VCEM user interface, click **Cancel VC Domain Maintenance**, and then wait for the job to complete.

   Cancelling maintenance mode prevents unnecessary propagation of changes to other members of the VC Domain Group.

No workaround is available for HP SUM. The VCSU workaround provided previously must be used.