Introduction

HP provides technologies and tools for efficiently managing Virtual Connect (VC) environments of all sizes. HP Virtual Connect Manager (VCM) is a software component embedded within Virtual Connect Ethernet modules. It is the core application for configuring and managing single and multi-enclosure Virtual Connect (VC) domain environments. Access to VCM occurs over the same Ethernet connection used to access the Onboard Administrator in BladeSystem c-Class enclosures and server blade iLO connections.

HP Virtual Connect Enterprise Manager (VCEM) is a software application that manages up to 250 VC domains. VCEM allows you to create domain groups that use a master configuration profile for multiple VC domains connected to the same networks. VCEM is part of the HP Insight Software suite of applications that also includes Systems Insight Manager, Matrix Operating Environment, and Insight Control. Information about VCEM is available in the “HP Virtual Connect Enterprise Manager 6.3 User Guide” found at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02786915/c02786915.pdf.

In this paper, we focus on VCM and underlying HP technologies that allow you to manage servers and network connection configuration as well as their deployment, monitoring, maintenance, troubleshooting, and security. We also touch on non-VC management tools that integrate with VC to provide broader management options.

VCM interfaces

You can access VCM through a browser-based GUI or through the VCM Command Line Interface. VCM domain management includes control of networks, SAN fabrics, server profiles, and user accounts that make it simpler to set up and manage server connections.

VCM GUI

VCM GUI is a web-based console built into the firmware of VC Ethernet modules. The VCM web interface requires an XSLT-enabled browser with support for JavaScript 1.3 or the equivalent. VCM 3.00 and later requires Adobe Flash Player. HP recommends updating to Adobe Flash Player 10.2 or higher.

This easy-to-use management interface allows you to configure, monitor, troubleshoot, and maintain security within the VC environment. For example, you can use the VCM GUI to do these tasks:

- Search for logical and physical objects by typing the name of the item in the “Find Configuration Items” search field
- Get information on networks and interconnect bay status from the information summary screens
- Create and edit Network Access Groups with group task actions

The VCM GUI navigation system consists of a tree view on the left side of the screen that remains visible at all times. Figure 1 shows the tree view listing all system devices.
Figure 1: VCM GUI listing all system devices

A pull-down menu displays details for the selected device or activity. The appearance of the tree view and the available user options depends on the privileges assigned to a user account. The tree view provides category-based navigation for the major systems configured within Virtual Connect.

VCM CLI

The VC web-based GUI and CLI interfaces provide nearly identical capabilities for managing a VC domain. For example, you can use the VCM CLI in the following ways:

- Give batch commands using script files that you can run manually or schedule to run automatically
- Perform debugging and troubleshooting for VC system and networking issues
- Develop tools that use VCM functions for data collection, provisioning, and configuration
- Access management data and do configuration tasks
- Remotely access VCM using SSH sessions

The VCM CLI supports command scripts containing blank lines and comments. It allows you to maintain descriptive notes within the configuration script.

You can enter multiple VCM CLI commands in a single command line. That is useful for batching several commands together and executing them in a sequence within the same SSH session. Table 1 compares formats for the same series of commands batched and unbatched. This batching method improves the overall performance of lengthy script processing.
**Table 1**: CLI commands with and without batching

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without batching add profile Profile1</td>
</tr>
<tr>
<td>Batched</td>
</tr>
</tbody>
</table>

**Configuration and deployment**

GUI and CLI management capabilities of VCM let you configure and deploy server profiles, networks, and SAN connections in the VC environment.

**VCM GUI setup wizards**

The first time you log in to the HP VCM GUI, a series of setup wizards automatically launches the four wizards described in Table 2. You can launch these wizards anytime using the Tools pull-down menu at the top of the VCM GUI.

**Table 2**: VCM GUI setup wizards

<table>
<thead>
<tr>
<th>Wizard</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP VCM domain setup</td>
<td>Lets you perform enclosure import/recovery, modify domain name, and create/modify user accounts within a domain to make server setup and administration easier.</td>
</tr>
<tr>
<td>HP VCM network setup</td>
<td>• Lets you establish external Ethernet network connectivity for HP BladeSystem c-Class enclosures if you have a user account with network privileges or full administrative privileges.</td>
</tr>
<tr>
<td></td>
<td>• Choose the MAC addresses used on the servers deployed within a VC domain.</td>
</tr>
<tr>
<td></td>
<td>• Choose how to handle VLAN-tagged packets from servers.</td>
</tr>
<tr>
<td></td>
<td>• Set up connections from an HP c-Class enclosure to the external Ethernet networks. The connections can be uplinks dedicated to a specific Ethernet network or shared uplinks that carry multiple Ethernet networks by using VLAN tags. You can create mixed-mode networks that simultaneously support both tunneled (dedicated) and mapped (shared uplink) VLANs.</td>
</tr>
<tr>
<td>HP VCM Fibre Channel setup</td>
<td>Lets you configure external Fibre Channel connectivity if you have a user account with storage privileges. You can use this wizard to identify WWNs used on server blades within a VC domain. You can also define fabrics.</td>
</tr>
<tr>
<td>HP VCM server profile setup</td>
<td>Lets you set up and configure network/SAN connections for server blades within an enclosure, as well as Boot from SAN and iSCSI boot parameters, if you have a user account with server privileges. You can apply server profiles to the server blades or unpopulated device bays in the enclosure. Then you can edit the profiles of individual servers.</td>
</tr>
</tbody>
</table>

**VCM SAN boot options**

By default, VCM does not configure SAN boot settings. However, because booting from a SAN decreases downtime when a server fails, VCM lets you set Fibre Channel SAN boot parameters and enable or disable Fibre Channel boot. If you choose to do that, the parameters you set will override settings established in other tools, such as RBSU.
Table 3 lists the SAN boot options available through the VCM GUI “Define Server profile” and “Edit Server profile” screens or through the VCM CLI.

Table 3: SAN boot options with VCM

<table>
<thead>
<tr>
<th>SAN boot selection</th>
<th>SAN boot option description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use BIOS (default)</td>
<td>Uses BIOS settings. VCM does not configure SAN boot settings.</td>
</tr>
<tr>
<td>Primary</td>
<td>Port enabled for SAN boot and is first in the boot order</td>
</tr>
<tr>
<td>Secondary</td>
<td>Port enabled for SAN boot and is second in the boot order</td>
</tr>
<tr>
<td>Disabled</td>
<td>Port disabled for SAN boot</td>
</tr>
</tbody>
</table>

If you don’t select “Use BIOS,” any SAN boot option you choose will override the settings established in other tools, such as RBSU.

VCM iSCSI Boot Assistant

Both the VCM GUI and the VCM CLI let you use the iSCSI Boot Assistant with the HP P4000 SAN to make booting from a remote iSCSI target part of the VC server profile. VCM support for other iSCSI storage arrays does not include iSCSI boot assistant. After you identify the iSCSI target, VCM performs most of the setup work and retrieves storage parameters directly from the target. The iSCSI Boot Assistant then attaches the boot configuration parameters to the server profile, highlighted in Figure 2.
Figure 2: VCM GUI showing iSCSI Boot Assistant and boot configuration fields

The iSCSI boot configuration process looks like this:

- Create boot volumes on target
- Provide access from VCM to iSCSI target
- Create server profile with iSCSI connections
- Use iSCSI Boot Assistant to attach boot configuration parameters to server profile

VCM does not add iSCSI connections to server profiles by default. User action is required. The VCM GUI lets you create iSCSI connections if the VC domain includes at least one Flex-10 module.


Creating and configuring VC network access groups

Within the VCM GUI and CLI, you can define network access groups to manage groups of networks. Association of a network access group with a server profile allows you to clearly define the separation of networks by designated function and to prevent unintended network-server connections. You can assign only one network access group to each server profile, but you can assign the same network access group to multiple server profiles.

VC allows up to 128 network access groups in a single domain. You can have one network access group per server profile. A double-dense single VC domain environment supports up to 128 servers. Ethernet networks and server profiles that you do not assign to a specific network access group automatically go into the default network access group for the domain. All server profiles can reach
all networks within the default network access group. The ability of network access groups to isolate networks also plays an important security role, as you will read in the “Security” section of this paper.

**Monitoring**

You can monitor the VC system with the VCM GUI and CLI, VCEM, and with third party SNMP-based tools. VCM uses SNMP as the underlying technology and is typically more useful for troubleshooting than other SNMP-based tools.

**Simple Network Management Protocol**

SNMP allows you to monitor network-attached devices in the VC domain. The SNMP agent software resides in VCM on the primary VC module as well as any other VC Ethernet and FC module in the domain. VCM controls the SNMP configuration for all VC-Ethernet and Fibre Channel modules and provides access to the management information base (MIB). A VC Module-specific MIB describes the state of a specific VC module. In addition to unique VC module attributes, the MIB defines traps and the trap severity level for reporting alerts on port statistics, such as throughput, errors, and discards. The HP BladeSystem Onboard Administrator (OA) generates SNMP traps. The OA SNMP Settings screen allows you to enter system information and designate the management stations that can receive SNMP traps from the OA.


GUI port status

Figure 3 shows the VCM GUI port status display.

This screen also lists why any port lacks connectivity:

- Not linked
- Not logged in
- Unsupported
- Incompatible

VCM CLI telemetry also reports port status, which is useful for troubleshooting. For a full listing of port status conditions and possible causes, see the “HP Virtual Connect for c-Class BladeSystem Version 3.30 User Guide.”

VCM CLI telemetry

The VCM CLI telemetry lets you monitor multiple parameters:

- System health, VC module memory and CPU utilization, and display firmware version
- Layer 2 MAC address table and associated FlexNICs, ports, and link aggregation groups (LAGs)
- MAC addresses based on the associated FlexNICs/ports and LAGs
• Networks (VLANs)
• IGMP Multi-cast groups
• Uplink status (enhanced uplink port status if you use pluggable transceiver modules), type, speed, connected devices, and LAG IDs
• Historical throughput (bandwidth and packets) utilization data on all physical ports (uplinks, stacking links, and downlinks)

You can use CLI telemetry commands and scripting to diagnose and troubleshoot system issues.

Integration with other management tools

VC uses SNMP to integrate with other management tools such as HP Insight Control, HP Intelligent Management Center, and HP Network Node Manager. SNMP also allows VC integration with third party tools.

**Insight Control for VMware vCenter Server**

HP Insight Control for vCenter integrates with VC to deliver end-to-end converged infrastructure hardware management. With this graphics-based tool, you can provision, monitor, and manage HP servers, networks, and storage from within the vCenter management console using a single HP plug-in. This plug-in allows you to monitor the relationship between VMware virtualized networking and VC. You can visually trace the network from the host all the way to the individual VC modules connected within the domain, as shown in Figure 4.

---

**Figure 4:** End-to-end network monitoring with VC and Insight Control for vCenter

---

**End-to-End VC network diagram**

---

**HP Intelligent Management Center**

You can use HP Intelligent Management Center (IMC) to monitor mission-critical VC networks across the data center. IMC reads VC device SNMP MIBs, providing visibility to information such as port count and statistics.
**HP Simple SAN Connection Manager**

HP Storage Simple SAN Connection Manager (SSCM) enterprise software simplifies storage network management for virtual server environments, including VCM. Deploying and managing virtual server connections to network and storage resources with VCM (in turn managed by VCEM) and SSCM is simple and efficient.

SSCM is a GUI-based application for managing SAN components, such as host bus adapters (HBAs), switches, and storage arrays. SSCM uses Microsoft Virtual Disk Service (VDS) to manage storage arrays, using a wizard-based user interface.


**Third party tools**

You can use any management tools that support CLI scripting to configure VC remotely. Any management tool that supports SNMP can monitor VC. In addition to local statistics and SNMP polling of statistics, VC provides SNMP traps for events that cause VC domain status changes. Embedded SNMP v1, v2, and SMI-S agents allow network management applications to query VC for statistics and trap information. Third party tools that integrate with VC include EMC Ionix, Solar Winds, and NAGIOS.

**Maintenance**

VCM capabilities ensure that you have the most advanced tools to maintain, update, save, and restore VC system configurations. We designed these tools to minimize or avoid disruption of service.

**VC support utility**

VC support utility (VCSU) is an installable application that you can use interactively or by command line to script the backup, configuration, or firmware deployment to a VC domain. We include VCSU on the HP Smart Firmware DVD. When used with HP Smart Update Manager (HP SUM), VCSU lets you automate the upgrade of VC firmware across one or many VC domains. VCSU lets you perform the following tasks:

- Upgrade Virtual Connect Ethernet and Virtual Connect-Fibre Channel module firmware
- Perform other maintenance tasks remotely on VC Ethernet and Fibre Channel modules installed in HP BladeSystem c-Class c7000 and c3000 enclosures using a standalone Microsoft Windows or Linux-based command-line utility

The healthcheck command automatically displays VC status information (such as domain configuration). VCSU does this prior to an OA firmware upgrade, preventing a possible outage.

Currently, the VCSU can update VC Ethernet, FlexFabric, and Fibre Channel modules. The VCSU cannot update other types of firmware in an enclosure.


HP SUM is the internal deployment engine that allows you to update, standardize, and/or restore specific Onboard Administrator and VC firmware versions on BladeSystem c7000 enclosures.

HP SUM has a GUI and a CLI scriptable interface for deploying firmware on a local host or on one or more remote hosts. The remote hosts must be online and running the same operating system as the system running HP SUM. Remote installations do not require an agent.
You can use HP SUM either offline (in automatic or interactive mode), or online (in a scripted or interactive mode). HP SUM can do updates without disrupting production workloads.

In addition to offering VCSU as a standalone tool, we include VCSU as a component of HP SUM. When you need to update all server firmware, we recommend that you use HP SUM. When you only want to update VC firmware, we recommend using the VCSU tool.

You can read more about the HP Smart Update Firmware DVD in the “HP ProLiant firmware management architecture” found at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02844392/c02844392.pdf.

Backup and restore configuration capability

VC includes a GUI Backup/Restore screen and CLI commands that let you back up, save, and restore VC domain configurations. These are three of the most important commands:

- The `showconfig` command lets you easily duplicate a domain configuration.
- The `save configbackup` command generates and transfers a VC binary configuration backup file to a remote TFTP or FTP server.
- The `restore configbackup` command transfers a VC configuration backup file from a remote TFTP or FTP server and restores configuration.

VC Ethernet module recovery

We've optimized the VC Ethernet module recovery algorithm to recover odd-side modules and then even-side modules. Previously, the algorithm fully reset/recovered all modules in parallel. Depending on the domain configuration, this change reduces or eliminates a potential network outage during a full-enclosure recovery.

Troubleshooting

The VCM GUI and CLI give you tools for handling service events ranging from performance issues to system attacks. You have access to VCM CLI telemetry information such as port status, errors, packet drop, and historical throughput to troubleshoot your network.

This section contains troubleshooting examples using a few of the CLI telemetry commands. Network connectivity ID issues and network performance bottlenecks are some of the issues that concern consumers.

Network connectivity debug

VCM CLI telemetry enables you to identify causes of network connection issues. You can use the CLI telemetry command `show network` to identify misconfigured VLAN IDs and overloaded VLANs. The `show network` command displays the internal and external networks (VLANs) that the VC module manages as it performs aggregation and switching.

You can use the VCM CLI telemetry command `show network` to display configured networks. It’s similar to `show vlan` on traditional switches, but it is more powerful:

- VLAN mapping capability is more powerful on VC networks than on traditional Ethernet switches and has more configuration information.
- `Show networks` makes it easy to identify overloaded or multi-use VLANs that exist in different VC networks.
- `Show networks` lets you filter results based on ports, networks, or VLAN IDs.

VC firmware and VC module stacking links allow you to create networks that span all modules in the VC domain. This VC network spanning exists even if a VC module does not contain uplinks or
downlinks associated with that VC network. The show network command does not display stacking links. Instead, it displays a message indicating that a VC network has no server or external ports associated with it on this module. Future releases of VC will provide information for correlating VC networks with stacking links.

You can also use the VCM CLI telemetry command show interconnect-mac-table to assist in network connectivity debug activities:

- Display Virtual Connect forwarding database (includes L2 MAC address forwarding table)
- Display all MAC addresses and the ports/FlexNICs from which they were discovered
- Support addresses learned on Link Aggregation Groups
- Provide visibility to server, Ethernet port and FlexNIC
- Display VC networks on which MAC addresses reside
- Filter the display based on port, LAG ID, VC network ID or name, or even specific MAC addresses to quickly isolate the network area of interest

Network performance debug

The CLI telemetry show statistics-throughput command provides a historical view for ingress and egress bandwidth utilization and throughput data. The command provides this data for all server, uplink, and stacking ports.

The show statistics-throughput command displays both port bandwidth (the amount of data transmitted or received from a port) and throughput (the number of packets transmitted or received from a port) in 5-minute intervals for up to the past 60 minutes of operation. To use the show statistics-throughput command, you must activate the statistics function, which is disabled by default.

Security

As server, storage, and network management intersect, securing information and providing appropriate access become more complex. HP offers role-based security that offers authentication, authorization, and accounting (activity logging) based on an assigned role. We also offer diagnostic and management technologies that match your established preferences and investment. Each data center team can use their preferred method on the same module with simultaneous multi-mode access. At VCM login, each user specifies the appropriate authentication method and VCM role. The authentication methods are local, Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access-Control System Plus (TACACS+), and Remote Authentication Dial-In User Service (RADIUS). You can specify the VCM role as domain, network, server, or storage. These roles are configurable for all types of authentication methods.

LDAP

Instead of using local authentication groups, LDAP uses active directories to simplify managing user account information. You can use the VCM GUI or CLI to set up an LDAP server to authenticate users based on user name, password, and role.
TACACS+ and RADIUS

We’ve extended security support with TACACS+ and RADIUS role-based security. TACACS+ and RADIUS are security technologies that network and storage teams use more often than LDAP. TACACS+ and RADIUS give you the following functionality:

- Consistent role-based authentication
  - User authentication
  - Command authorization (privileges)
  - Command logging for activity audit trail (TACACS+ support only)
- Simultaneous multi-mode access
- Command logging to redundant TACACS+ and RADIUS: The VC implementation extends the existing LDAP and local account users (domain, server, storage, and network), privileges, and logging to TACACS+ and RADIUS.

VC supports logging to TACACS+ servers, and we plan to support logging to RADIUS servers in a future release.

Using Network Access Groups to enhance security

IT security is a key concern for network administrators. Growing requirements for secure multi-tenancy environments increase that concern. Previously, you could assign any server profile to any set of networks. If networking policy required isolating some networks (for example, the Intranet and the Extranet), there was no way to enforce that policy automatically. VC Network Access Groups let network teams prevent assigning undesirable network combinations to the same server profile.

Conclusion

With new and enhanced VCM capabilities, we continue to extend the management capabilities within VC environments and give you greater visibility into VC modules. Secure VCM GUI and scriptable CLI interfaces provide you with unified VC domain configuration and management. VCM allows you to pre-set server network configurations before server installation for easy deployment. You can move, add, or change server network connections on the fly without affecting LAN and SAN administration.

VCM uses industry standard SNMP to monitor and manage the VC domain, and VC integrates with other HP and third party management tools. VCM offers you centralized configuration of boot from iSCSI capability, or Fibre Channel network storage. VCM CLI based telemetry addresses many of the needs expressed by networking teams. Server teams can now assure their networking partners that they have the tools required to manage VC in the network.

New role-based security as well as diagnostic and management technologies assure network administrators that VC security enhancements eliminate risk in their environments without investing in new security tools.
For more information

Visit the URLs listed below if you need additional information.

<table>
<thead>
<tr>
<th>Resource description</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Virtual Connect for c-Class BladeSystem</td>
<td><a href="http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180">http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180</a></td>
</tr>
<tr>
<td>Version 3.30 User Guide</td>
<td></td>
</tr>
<tr>
<td>HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem</td>
<td><a href="http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180">http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180</a></td>
</tr>
<tr>
<td>Version 3.30 User Guide</td>
<td></td>
</tr>
<tr>
<td>HP Virtual Connect for c-Class BladeSystem</td>
<td><a href="http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180">http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;contentType=SupportManual&amp;prodTypeId=3709945&amp;prodSeriesId=4144084&amp;docIndexId=64180</a></td>
</tr>
<tr>
<td>Setup and Installation Guide</td>
<td></td>
</tr>
<tr>
<td>Building Virtualization-Optimized Data Center Networks</td>
<td><a href="http://h17007.www1.hp.com/docs/mark/4AA3-3346ENW.pdf">http://h17007.www1.hp.com/docs/mark/4AA3-3346ENW.pdf</a></td>
</tr>
<tr>
<td>HP Virtual Connect and HP Storage Simple SAN Connection Manager Enterprise Software</td>
<td><a href="http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-2646ENW.pdf">http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-2646ENW.pdf</a></td>
</tr>
</tbody>
</table>

Send comments about this paper to TechCom@HP.com.

Follow us on Twitter: http://twitter.com/ISSGeekatHP.