Features of CMC for PowerEdge VRTX Features—Enabled by Digital Licensing

This Dell™ Technical White Paper provides information about the CMC for PowerEdge VRTX features enabled by digital licensing

Author(s)

Michael Brundridge

Contents

Introduction

This Whitepaper provides an overview of the features enabled by the Digital Entitlement License Manager embedded within the VRTX Chassis Management Controller (CMC).

Understanding the VRTX CMC Express and Enterprise Offerings

For VRTX CMC, Dell offers the following license types:

1. Express
2. Enterprise

Express license offers embedded tools, console integration, and simplified remote access. Enterprise provides the administrator a management experience that makes the administrators feel they are in the physical vicinity of a chassis.

VRTX CMC Feature Guide

Table 1 compares the features available for VRTX CMC Express license and CMC Enterprise license.

If you are unable to decide about a CMC option, or if you would like to try the features before you buy, you can evaluate the features of CMC Enterprise by requesting for a 30–day trial license, and then download and install the license on the target system and the features will be activated for 30days.

Table 1. A Detailed Comparison of CMC Features

Feature	CMC Express	CMC Enterprise
RACADM (SSH, Local and Remote)	✓	✓
WS-MAN	✓	✓
SNMP	✓	✓
Telnet	✓	✓
SSH	✓	✓
Web-based Interface	✓	✓
CMC Network	✓	✓
CMC Serial Port	✓	✓
Stacking Port	n/a	n/a
Email Alerts	✓	✓
Enclosure Restore	✓	✓
LCD Deployment	✓	✓
Extended iDRAC Management		✓
Server Module Firmware Update		✓
Remote Syslog		✓
iDRAC Single Sign-On		✓

CMC for PowerEdge VRTX Features Enabled by Digital Licensing

Server Configuration		✓
Chassis Grouping		✓
Enclosure-level Backup		✓
Two-Factor Authentication	*	✓
PK Authentication	*	✓
Remote File Share	*	✓
Directory Services	*,[1]	✓
Server Power Management	[2]	✓
FlexAddress Enablement	[3]	✓
Slot Resource Assignment/Management	[4,5]	✓
Dynamic Power Supply Engagement	[6]	✓

[1] For Non default directory service setting, only Reset Directory Services is allowed with Express license. Reset Directory Services will set the Directory services to the factory default.

[2] For non-default power cap setting, only Restore Power Cap is allowed with Express license. Restore Power Cap will reset the Power Cap settings to factory default.

[3] For non-default Flex Address settings, only Restore Default is allowed with Express license. Restore Default will reset the Flex address settings to factory default.

[4] A maximum of two PCIe adapters can be assigned per server with an Express License.

[5] For non-default mapping of virtual adapters, only Default mapping is allowed with Express license. Restore Default will change virtual adapter mapping to factory default.

[6] For non-default DPSE settings, only Restore DPSE is allowed with Express license. Restore DPSE will reset the DPSE to factory default.

* To utilize server-based iDRAC Two-Factor Authentication, PK Authentication, Remote File Share, or Directory Services requires the server(s) to also have an Enterprise license installed.

License Manager

The VRTX CMC utilizes the same License Manager utilized in 12G iDRAC. The License Manager is capable of managing digital entitlements for the VRTX CMC and chassis infrastructure. To utilize the VRTX CMC License Manager, log in to the CMC and navigate to the **Chassis Overview** > **Setup** > **Licenses** tab. The **License Manager** displays an inventory of licensable devices on its main page.

Tracking Your VRTX CMC Licenses

Dell offers an online portal to keep track of all your VRTX CMC licenses and other Dell digital entitlements. For example, information is shown about the chassis or server that has Enterprise licenses, or even Trial licenses. Chassis or servers can be sorted on the basis of service tags. In the unlikely event of a non-functioning device with an associated license, Dell stores a copy of the entitlement and makes it available to you in an online License Management portal (www.dell.com/support/retail/lkm). The only additional task that you must complete after deploying your new chassis and servers into production is to set up your "My Account", and authorize users who can access the digital license on Dell's License Management Portal. The online portal is the best way to review all your Dell licenses.

For more information about using License Manager, see the *Chassis Management Controller for PowerEdge VRTX User's Guide* available at dell.com/support/manuals. For more information about using License Manager and the online licensing, see the VRTX Licensing White Paper.

Licensed Feature Description

The following sections will briefly describe each Enterprise licensed feature:

Extended iDRAC Management

Reserved for a future use.

Server Module Firmware Update

The **Server Module Firmware Update** feature allows you to manage the firmware of the components and devices on the servers through the CMC using the servers Lifecycle Controller service. The Lifecycle Controller is a service available on each server and is facilitated by an iDRAC.

Remote Syslog

The **Remote Syslog** feature allows an administrator the ability to use additional remote targets for log messages supporting remote syslog. Various VRTX Chassis events can be configured to output to a remote syslog service by using an event filter in the **VRTX CMC Web interface** under **Chassis Overview > Alerts**.

Directory Services

The **Directory Services** maintains a common database for storing information about users, computers, printers, and others on a network. If you use either Microsoft® Active Directory® or Generic Lightweight Directory Access Protocol (LDAP) services, you can configure the service to provide access to the CMC, allowing you to add and control CMC user privileges to the existing users in your directory service.

iDRAC Single Sign-On

The **iDRAC Single Sign-On** feature allows a user to launch the iDRAC GUI or Remote Console from the CMC without having to sign on to the target server, a second time. The Single Sign-On policy is as follows:

- A CMC user who has the **Server Administrative** privilege is automatically logged in to iDRAC using single sign-on. After logging in to the iDRAC GUI, this user is automatically granted Administrator privileges. The login occurs even if the user does not have an iDRAC account, or has an account without an Administrator's privileges.
- A CMC user without the **Server Administrative** privilege, but having the same account on iDRAC is automatically logged in to iDRAC using single sign-on. After logging in to the iDRAC GUI, the user is granted the privileges assigned to the iDRAC account.
- A CMC user who does not have the **Server Administrative** privilege, or the same account on the iDRAC will not be automatically logged in to iDRAC using single sign-on. This user is directed to the iDRAC login page when the **Launch iDRAC GUI** or the **Launch Remote Console** button is clicked.

Two-Factor Authentication

Two-factor Authentication provides a higher-level of security by requiring users to have a password or PIN, and a physical card containing a private key or digital certificate. Kerberos uses this two-factor authentication mechanism allowing systems to prove their authenticity.

PK Authentication

PK Authentication allows you to configure up to six public keys that can be used with the service username over an SSH interface. The service username is a special user account that can be used when accessing the CMC through SSH. When the PKA over SSH is set up and used correctly, you need not enter username or passwords to log in to the CMC. This can be very useful to set up automated scripts to perform various functions.

Remote File Share

The **Remote File Share** feature enables the ability to connect, disconnect, or deploy a media file available on the network. When connected, the remote file is accessible in a similar manner as a local file. Two types of media are supported: floppy disk drives and CD/DVD drives.

Slot Resource Assignment/Management

Slot Resource Assignment/Management is used to map or un-map an individual PCIe device to a server slot. It also supports mapping a Virtual Adapter to any of the servers.

Server Configuration/Cloning

The **Server Configuration** feature enables the ability to configure the BIOS, Boot Settings, and iDRAC configuration using the nodes interfaces, and then save the configuration to the CMC such that it can be restored or cloned to other servers. This speeds up the deployment of new servers being installed in the chassis. The clone file is in an XML format, and may be edited by the administration to meet the requirements.

The **Server Configuration** feature also enables the **One-to-Many Configuration for iDRAC** functionality, which allows the administrator to select the **Auto-Populate Using QuickDeploy Settings** option to populate the iDRAC Network Settings section, and then click **Apply iDRAC Network Settings** to apply the setting changes to the listed iDRACs. To configure server network settings on one or more individual iDRACs, type or select values for the following properties, and then click **Apply iDRAC Network Settings**.

Slot	Displays the slot number where the server is installed in the chassis. Slot numbers are sequential IDs, from 1 to 4 (for the 4 slots in the chassis), that help identify the location of the server in the chassis. *NOTE: Only those slots populated by servers display a slot number*.
Name	Displays the name of the server in each slot. *NOTE: The slot name cannot be blank or NULL.*
Enable LAN	Select this option to enable the LAN channel.
Change Root Password	Select this option to allow the user to change the password of the iDRAC root user. Make sure to enter the **iDRAC Root Password** and **Confirm iDRAC Root Password** options before enabling this option.

Server Power Management

The **Power Management** feature enables the ability to set the enclosure-level power cap. This allows the administrator to set a limit on the maximum power that can be input to the system:

- W: In Watt. Automatically calculated during the runtime and displayed in the box.
- BTU/h: British Thermal Unit For example, 16719.
- %: Type a value that indicates the actual percentage of power input versus the maximum power that can be supplied.

Chassis Grouping

The **Chassis Grouping** feature helps conveniently manage multiple VRTX chassis in the same environment. Chassis can be assigned to a Chassis Group. You can assign the chassis to a Chassis Group and administer it through Multi-Chassis management. In this configuration, one chassis is assigned the 'lead' role, while the other in the same group is assigned the 'member' role. Only the lead chassis has access to the information about a member chassis.

Enclosure Backup

The **Enclosure Backup** feature allows you to make a backup copy of the CMC and chassis configuration settings on the file system of your remote client workstation. The enclosure backup will save information and settings about the overall chassis, including network settings, security certificates, user configuration, and power policy. The enclosure backup also contains slot information, such as slot name and FlexAddress settings. Server-specific information is not saved. The enclosure backup does not include the CMC firmware image. The backup file is encrypted and keyed to this chassis so it cannot be loaded on to another chassis.

FlexAddress Enablement

The **FlexAddress Enablement** features are optional upgrades that allow the CMC to assign WWN/MAC (World Wide Name/Media Access Control) addresses to Fiber Channel and Ethernet devices. Chassis assigned WWN/MAC addresses are globally unique and specific to a server slot within a given chassis. FlexAddress allows the CMC to assign the WWN/MAC address (Chassis Assigned IDs) that stays with a particular slot in the chassis.

If a server is replaced, the FlexAddress for the slot remains the same for the given server slot. If the server is inserted in a new slot or chassis, the server-assigned WWN/MAC is used unless that chassis has the FlexAddress feature enabled for the new slot. If you remove the server, it will revert to the server-assigned address. You need not reconfigure deployment frameworks, DHCP servers, and routers for various fabrics for identifying the new server.

Dynamic Power Supply Engagement

Dynamic Power Supply Engagement (DPSE) mode, the power supplies are turned on or turned off on the basis of power consumption, optimizing the energy consumption for the entire chassis.

For example:

- Your power budget is 1050 Watt
- Redundancy policy is set to **AC redundancy mode**
- Four power supply units (PSUs) are installed

CMC determines that one of the PSUs is required to support the current power requirements, a second is required to support the AC redundancy policy, and the others remain in standby mode. However, if up to an additional 1050 Watt of power is required for the newly-installed servers, the

standby PSUs are engaged. Standby PSUs are also engaged in the event of an issue with a power grid.

June 2013| Rev 1.0