# Managing the Dell PowerEdge VRTX Chassis with Dell OpenManage Essentials

**OME Engineering Team**

July 2016| Version 1.1

# Contents

## Executive Summary

The PowerEdge VRTX chassis is a new and innovative approach on an established theme … bringing together server, networking, and storage in a compact package, while allowing for the expansion of storage and processing power as needs grow. No longer is the blades (referred to as server nodes in VRTX) concept limited to the Datacenter … now it can exist in any office anywhere. The Dell PowerEdge VRTX solution introduces several new, while maintaining many familiar, concepts for chassis and server node management, and Dell OpenManage Essentials (OME) version 1.2 offers the most up-to-date solution for management of this new offering. Some new features in OME v1.2 include:

- Discovery, inventory, and monitoring of the VRTX chassis and its server nodes using the WS-Man protocol, a more WAN- and firewall-friendly protocol.
- A dedicated PowerEdge VRTX group in the device tree, where all discovered chassis components will be grouped together.
- Inventory of the shared storage and PCIe components of the VRTX chassis, including server node assignments.
- Firmware update of server node and shared chassis components.
- A completely new Map View … place your PowerEdge VRTX servers anywhere on the globe in OME and let OME keep track of them (VRTX Enterprise license required).

# I. Setup of PowerEdge VRTX for Management

## a. Setup in a Datacenter

The VRTX chassis is Datacenter-friendly, with the ability to fit the chassis into 5U of rack space with the appropriate kit. The optimal network environment is expected in this environment, with plenty of bandwidth and reliable delivery. Provisioning/setup of the chassis (or the Chassis Management Controller) for management is very similar to the Dell PowerEdge M1000e chassis. Unlike the M1000e, the WS-Man protocol is the preferred management protocol to get the most thorough inventory and management of the chassis with OME. SNMP can also be used, but the following is not supported with this protocol: shared storage inventory, shared PCIe inventory, firmware updates, and the map feature detailed below. When it comes to eventing, SNMP traps is the method used, therefore, the chassis will need to have OME as its event destination.

For the server nodes in the chassis, a similar setup is recommended if using the iDRAC for management: WS-Man is the protocol of choice for retrieving information, while SNMP traps are used for asynchronous alerting. If managing through the Operating System is an option, OpenManage Server Administrator (OMSA) can also be used with the recommended SNMP protocol used for both synchronous and asynchronous communication.

### b. Setup in a Remote Office

The VRTX chassis was designed with the remote/back office in mind. Assuming a Wide-Area-Network (WAN) environment, the network strongly recommended in this environment is a Virtual Private Network (VPN) with at least 5-10 Mbps bandwidth to the console. It is reasonable to expect more network latency with this type of setup; OME has adjustments for this (discussed later). The WS-Man protocol, although requiring more network bandwidth than SNMP, provides more reliable delivery of data, as well as data encryption and authentication. Using SNMP in a WAN environment can be a questionable choice if there is increased latency, reduced reliability, and little or no security. While SNMP traps are the only way to do asynchronous alerting at this time, OME has an event log viewer capability that can synchronously pull logs in real time if asynchronous events do not work reliably.

For server nodes in the chassis, the WS-Man protocol is also strongly recommended for retrieving data, using the iDRAC as the main point of management. While SNMP traps are also used here for asynchronous events, again OME provides a system event log viewer should events not be delivered reliably.

Note: WS-Man uses HTTP(s) over TCP/IP, while SNMP is over UDP/IP, accounting for the differences in reliability, speed, and encryption. OM Essentials does not support SNMP via TCP/IP, nor is SNMPv3 supported at this time.

## II. Installation / Upgrade of OM Essentials

OpenManage Essentials has one of the simplest installations among systems management consoles. The time lapse from install to manage is as little as just under 30 minutes. Whether you are new to OME or are upgrading from a previous version, the latest OME release (version 1.2) offers a comprehensive and easy-to-understand overview of the VRTX chassis and server nodes in your

environment. See the OME users guide for system and operating system requirements. OME is a two-tier application: the services tier, which does all communication to the VRTX system, and the UI tier, which communicates to the OME services tier. It is strongly recommended that the services tier sits behind a firewall, along with any other remote devices OME must monitor and manage. As mentioned before, it is recommended to have a VPN between OME and the devices it must manage to reduce the chances of data sniffing. OME secures communication between the UI and services using HTTP(s).

Once OME is installed, you can bring up the UI locally by double-clicking the icon on the desktop or remotely through the URL (assuming the default port): *https://<ome_services_box_ip_address>:2607*

For management setup to go quickly, you should have your network and protocol information ready to enter from your VRTX installation. Setup parameters include IP Address and Netmask data for your chassis and server node(s), ICMP timeout(s), SNMP community name(s) and timeout(s) (if using SNMP), and WS-Man credentials and timeout(s) if using WS-Man. As mentioned before, WS-Man is recommended as the protocol for retrieving data from your VRTX chassis and server nodes.

## III. Licensing Considerations

While OME itself is free and has no licensing, both the VRTX chassis and server nodes have their own licensing options. For the best and most complete management experience from OME, it is recommended to purchase Enterprise level licenses for both the server nodes and the VRTX chassis. This can be done at the point of purchase or after. Should licenses be purchased after the point of sale, they can be pushed out to the server nodes through the Dell License Manager (DLM) console included with the OME install package (selection of DLM may be required at the time of OME install). DLM has its own icon on the desktop of the OME services box. Through DLM, licenses for the server nodes can be imported from the local file system, and then pushed-out to their respective nodes once those node's iDRACs have been discovered in DLM. Note that the VRTX chassis license is not supported by DLM at this time; the user will need to import the VRTX license via the CMC interface.

TIP: DLM only uses the WS-Man protocol to discover and push licenses to remote systems; when discovering systems through DLM, make sure to use the iDRAC IP Address and not the Operating System IP Address(es).

Note: To use the new *Map View* feature in OME, the VRTX chassis must have an Enterprise license. Refer to the new license report in OME to assure that your managed chassis has an *Enterprise* license.

## IV. Discovery / Inventory of Poweredge VRTX

If you have the Datacenter environment mentioned above, using the default protocol timeouts and retries in OME should likely suffice; if you have a WAN situation where there is network latency above a few hundred milliseconds, and/or where packet reliability is questionable, then increasing the protocol timeouts/retries might be option to consider. OME uses the ICMP (ping) protocol to discover devices on the network, so measuring the ICMP round trip time and packet loss and making appropriate adjustments in the OME discovery wizard can lead to a more successful discovery, inventory, and monitoring experience. Finding these statistics is as easy as opening a command prompt from the OME services tier and performing a ping to the chassis and/or server node IP Address(es).

Note: Using the WS-Man protocol with the VRTX chassis controller and the server node's iDRAC is strongly recommended to give the best results for management of the VRTX solution.

TIP: If you have VRTX systems spread throughout the region or globe, you can setup specific discovery ranges in OME for each location with their unique latencies to optimize the retrieval of data in OME.

TIP: OME includes a troubleshooting tool, located on the desktop of the OME services box, that can help troubleshoot any protocol problems, including testing timeouts and credentials.

Should your VRTX systems span a WAN with non-congruent IP Address(es), it is highly recommended that each VRTX (or cluster of VRTX) system, both chassis and server nodes, at a location have its own discovery range instance. In OME, it is easy to type in multiple IP Address(es) at once for a discovery range in the discovery wizard, located at:

*Manage -> Discovery and Inventory -> Add Discovery Range*

You can also group these IP Address(es) into a discovery range group by using the *Add Discovery Range Group* Task at the same location in the UI. Should you have reliable DNS services and/or using DHCP to assign IP Address(es) to your managed devices, using hostnames instead of IP Address(es) is also allowed. The hostnames/IP Address(es) of the CMC, server node iDRACs, and server node Operating Systems can all be entered, if desired.

TIP: For a server node, if the Dell OMSA agent is not installed, using the WMI protocol for Windows and SSH protocol for Linux are the best choices for OME to communicate to the respective Operating Systems. OME can even push the OMSA agent to the server after discovery of the operating system; however, pushing the agent is not recommended for networks with limited bandwidth. It is not required to discover the Operating System nor have OMSA installed to manage the VRTX solution in most cases (assuming management occurs with the iDRAC).

See Figure 1 for an example of the VRTX CMC and server node IP Addresses grouped together into the *Austin_VRTX* group. If all IP Address(es) in the group use the same protocol settings and credentials, it can save time to group IP Address(es) together in a discovery range group; later, should the credentials need to be changed, they can be updated for all IP Address(es) in the group by just changing it once.

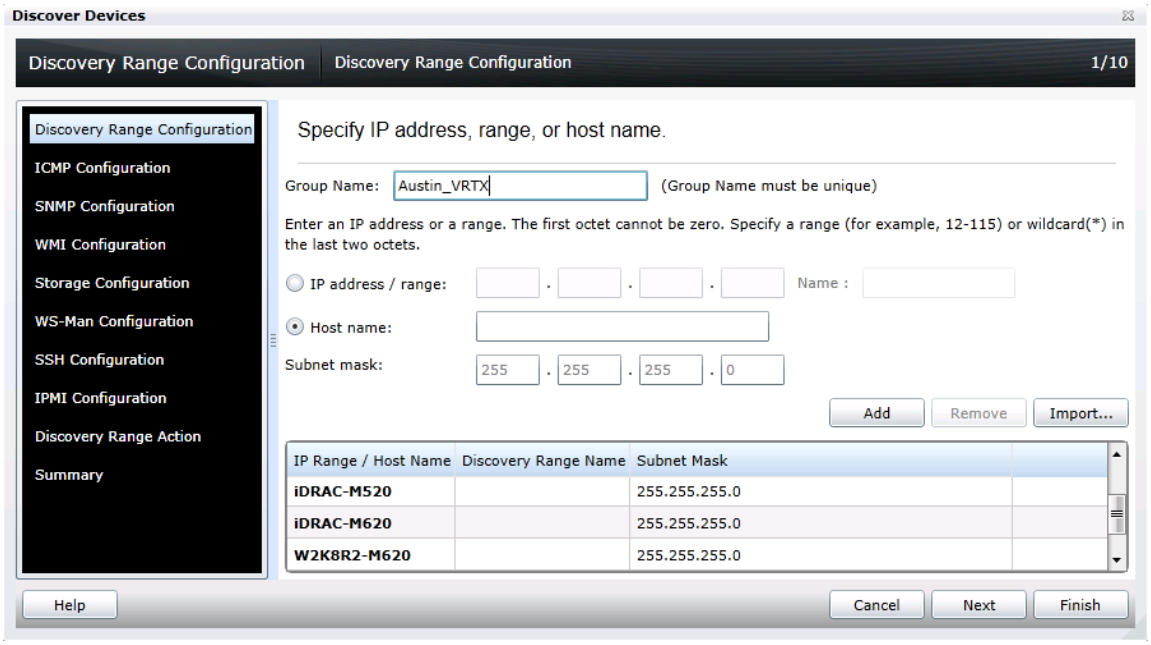


Figure 1: Grouping IP Address(es) into one discovery range group called *Austin_VRTX*

TIP: Do not repeat IP Address(es) in different discovery ranges with different protocols enabled and setup (for example: SNMP in one and WS-Man in another). To do so could result in periodic mis-representation of that device in OME. Should an IP Address need its own discovery range due to unique credentials for at least one protocol, all other protocols wanted should be setup for that IP Address in the same discovery range.

The recommended protocol (WS-Man) setup screen is shown in Figure 2. Both the chassis management controller (CMC) and iDRAC on the server node offer the most manageability via this protocol. The user id/password fields are the respective credentials setup on the remote device and that user has a role of administrator and can perform remote actions; multiple credentials cannot be entered, so more than one discovery range will be needed if the credentials are different among the server node(s)/CMC. The timeout parameter is set for a Datacenter environment; in a WAN, this setting may need to be 10's of seconds higher. Both the iDRAC/CMC communicate securely over HTTP(s) using port 443. Once the *Secure Mode* checkbox is selected, the port will automatically become 443.

The fields enabled for Secure Mode are as follows:

*Skip Common name check*: If there is a concern about the remove device being spoofed, this setting can remain unchecked; however, if this check is not skipped, the certificate presented by the remove device (CMC or iDRAC) must have the same name as what the remote device is known by on the network. This usually means generating and importing a certificate into the CMC or iDRAC which typically contains the DNS hostname of the server.

*Trusted site*: Leaving this unchecked mandates that a certificate file which contains the same trusted root authority must be imported into OME as well as the remote device.

Skipping the common name check and trusting the site (both options selected) will still result in HTTP(s) being used, but the extra safeguards mentioned above are not enabled. For most cases, on a VPN behind a firewall, this will suffice; otherwise, it is recommended to consider enabling these extra precautions. However, it can take several iterations for someone who is new to these concepts to get certificates working. To verify that the protocol works with the supplied credentials and timeout, is it recommend to bypass these options (both are checked), at least at first, before attempting to use them.

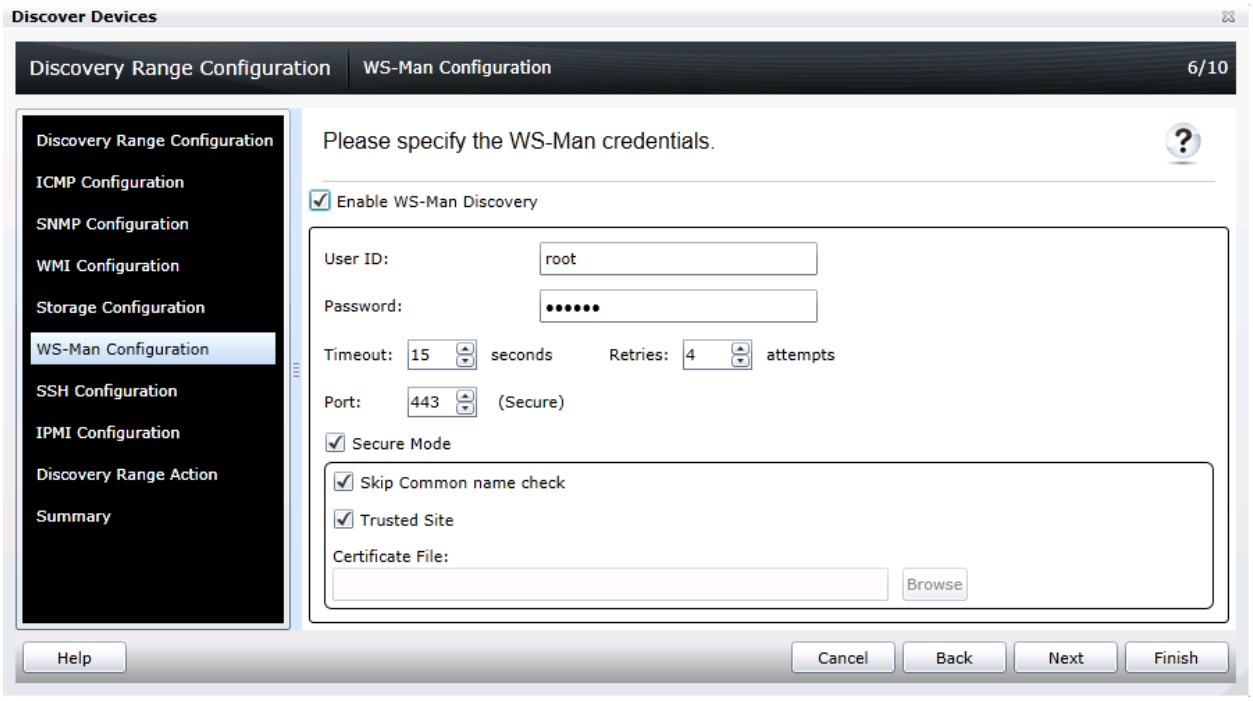


Figure 2: WS-Man setup screen for a discovery range.

TIP: The SNMP protocol can also be enabled along with WS-Man. OME will automatically select the protocol that provides the best management (WS-Man in this case). Unlike WS-Man, multiple community name credentials can be entered for SNMP, separated by commas, if desired.

Once the IP Address(es) and the protocols have been setup in the discovery range wizard, select to perform both a discovery and inventory. Once discovery is done, your VRTX components should show up under the *All Devices -> Modular Systems -> PowerEdge VRTX* node in the device tree (see Figure 3). A tree node, having the name *<CMC_hostname>_Chassis* will automatically be created for each VRTX chassis, with the chassis controller, server nodes, and network switch under it.

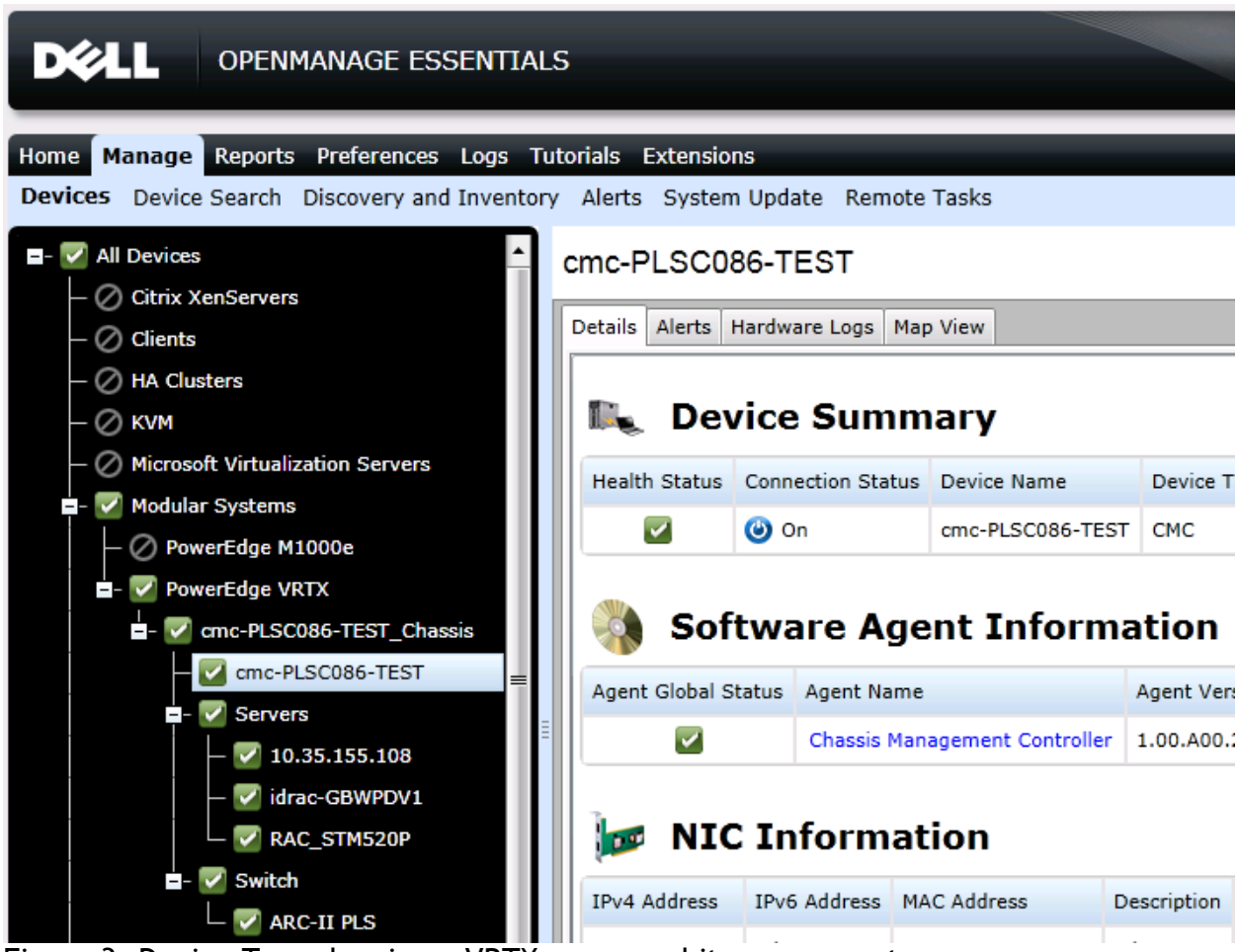

Figure 3: Device Tree showing a VRTX group and its components.

To see all the shared components of the chassis, including the shared storage and PCI cards, click the CMC node in the tree. See Figure 4 for some of the new information shown for the chassis.

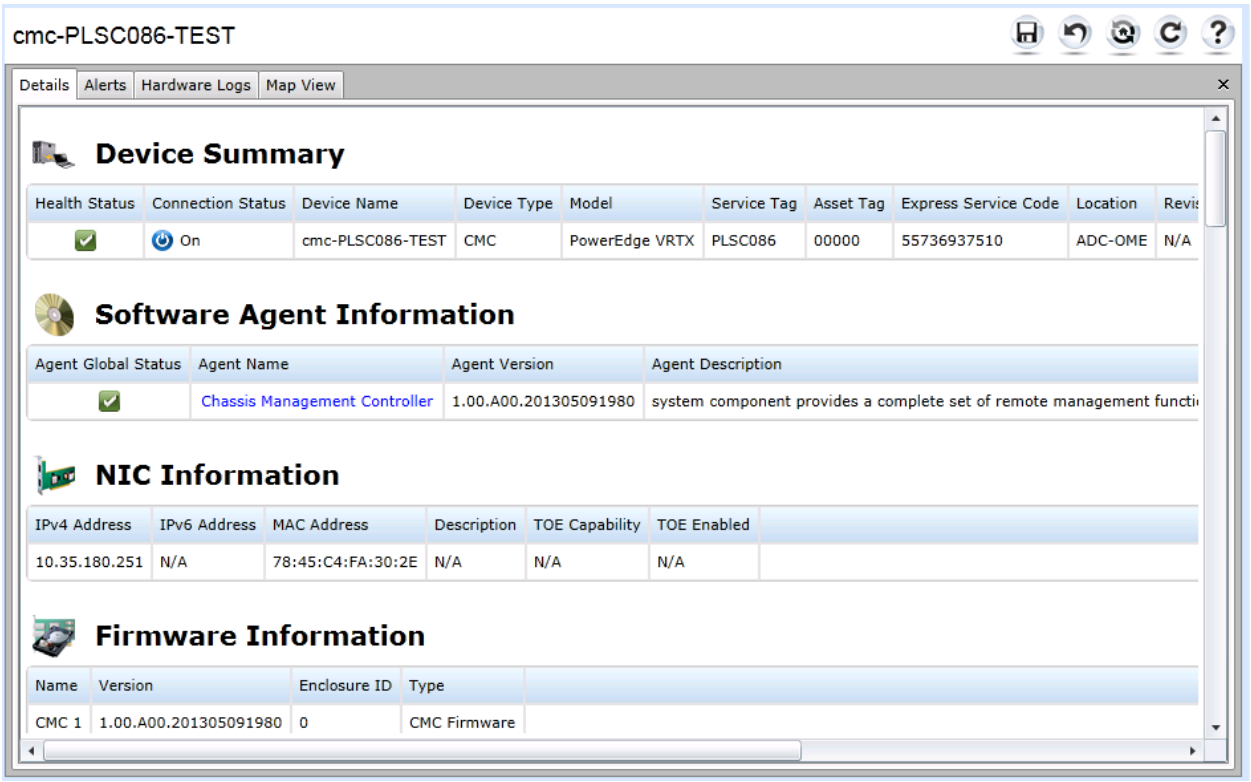


Figure 4: Chassis summary screen.

# V. Monitoring of VRTX

Monitoring of the VRTX chassis is more important than ever before, as it will also roll-up the status of the shared storage components (controller and drives). Many new defined storage events that are emitted by the chassis controller will be recognized by OME v1.2 and the controller's global status will include the status of the PERC cards and the physical/virtual disks (to see individual statuses, launch the CMC GUI and drill down to the *Storage* node).

Monitoring a device in OME includes the rolled-up status of the hardware, typically viewed in the device tree, as well as the asynchronous events from the device in the form of traps. In a Datacenter, the delivery of SNMP traps can typically be trusted to be reliable – this is one reason the status polling interval in OME can be kept at the default one hour interval or greater. However, when managing devices over a WAN and/or sharing limited bandwidth with other back office functions, the delivery of traps may not be as reliable. If traps seem unreliable or not an option, it is recommended to set the status polling rate to a shorter duration, but have an interval wide enough to not tax the network. The default one hour may suffice in many cases. Additionally, OME

now provides the *Hardware Logs* tab for the VRTX chassis node in the device tree – this tab should contain the same log as the *Chassis Log* tab in the CMC GUI and is retrieved in real time. While this can give you a summary of the hardware events, storage events and configuration changes for the chassis, it is recommended to launch the CMC GUI and view the detailed logs there. Note that event actions (such as send an email) cannot be used with real time hardware logs.

TIP: If there is a timeout while obtaining the Hardware Logs from the CMC or the iDRAC, increase the WS-Man timeout parameter in the discovery wizard for the device(s).

TIP: If you have setup traps, but suspect that there may be a problem with trap delivery, you can schedule a RACADM task in OME to periodically have the remote device send OME a test trap (CMC/iDRAC), or use the OMSA Remote Command Line task to have OMSA send a periodic test trap to OME.

Introduced with OME v1.1, OME has a feature to generate an internal alert when the global status of any device being monitored changes status (turn this on by navigating to *Preferences -> Alert Settings*), so OME can poll for health state changes and send the user an email when an alert action is setup for the internal health state change alert.

# VI. Using the Map Feature

Getting Started

Map View allows you to view the location and current status of all of your PowerEdge VRTX devices with an enterprise license on an interactive global map at the local, regional, or global level.

Note: The Map View features also supports Dell PowerEdge FX2/FX2s devices.


Figure 5: Map View in OME

Prerequisites:

- Device must be a PowerEdge VRTX or FX2/FX2s with enterprise license only
- Device must be discovered and inventoried using WS-Man
- Internet connection required for zoom to street level and address lookup
- User must input device locations to view them on the map
- A MapQuest or Bing key is required for rendering the map

Adding devices to the map can be accomplished multiple ways:

- Add device at the click location on the map (right click -> ‘Add Licensed Device’)

- Add device by address lookup (Use the search window at top left; Internet connection required)
- Add multiple devices by importing. (right click -> 'Import Licensed Devices')

The map pin representing the device contains summary information (tooltip) about the device and can be used to initiate several actions on the device.

When viewing the map view in the device portal, selecting the device updates all tabs in the portal to be specific to that device, so you can instantly see the inventory, alerts, etc., from one click.

The map has two view modes.

- Default view mode – the map shows only devices in the current device group selection. Clicking on a device in this mode will further filter the view to just that device.
- View all mode – the map will always show all supported devices, regardless of selection

See the OpenManage Essentials User's Guide for a full list of features and procedures related to the map.

## VII. Updates

As before, OME can update the server nodes either through the iDRAC (out-of-band) or through OMSA (inband, through the OS). If you wish to update drivers as well as Firmware/BIOS and are running OMSA on the server nodes, it is recommended to use OMSA as iDRAC cannot update drivers in the OS.

Since OME typically schedules multiple parallel threads to update multiple systems at once, if there are bandwidth concerns, it is recommended that you schedule multiple update tasks that are staggered by 30 minutes or more apart from each other for each system.

TIP: If there is limited bandwidth, updating through the iDRAC may be a better choice as one package at a time is downloaded as opposed to a large zip file of all update packages chosen, sent to OMSA at once; however, be aware that, when using the iDRAC, it must contact the OME services box through HTTP to pull the package – the appropriate port has to open to allow remote communication back to the OME services box.

When scheduling updates, it is important to include the VRTX chassis, and to actually update it first before any server nodes. OME will update the chassis first if it happens to be included in the list of devices to update (which may include server nodes). There are several components to update in the chassis - see Table 1 for the list of VRTX updates. For some updates, the server nodes must be power off, otherwise data corruption would occur. Should an update that requires the server nodes are power off be scheduled and one or more server nodes are not power off, the update task will fail, but it is still recommended that these updates be scheduled carefully in advance and that no one tries to power-on a server node while a chassis update is in progress. OME will not automatically power off server nodes for a chassis update, nor is there an option for the user to elect this. OME does not update the VRTX network switch. See Figure 6 for a suggested workflow for updating the chassis and server nodes.

Note: For OME to support VRTX chassis updates, the VRTX chassis must be discovered and inventoried using WS-Man protocol. OME does not support the update feature for the VRTX chassis using SNMP discovery and inventory.

| Chassis Component | Requires Server Powered Down |
|---|---|
| PowerEdge RAID Card (PERC) | Yes |
| Mainboard | Yes |
| Expander | No |
| Hard Disk Drives (HDD) | No |
| Chassis Management Controller (CMC) | No |

Table 1: Components OME can update in the VRTX Chassis

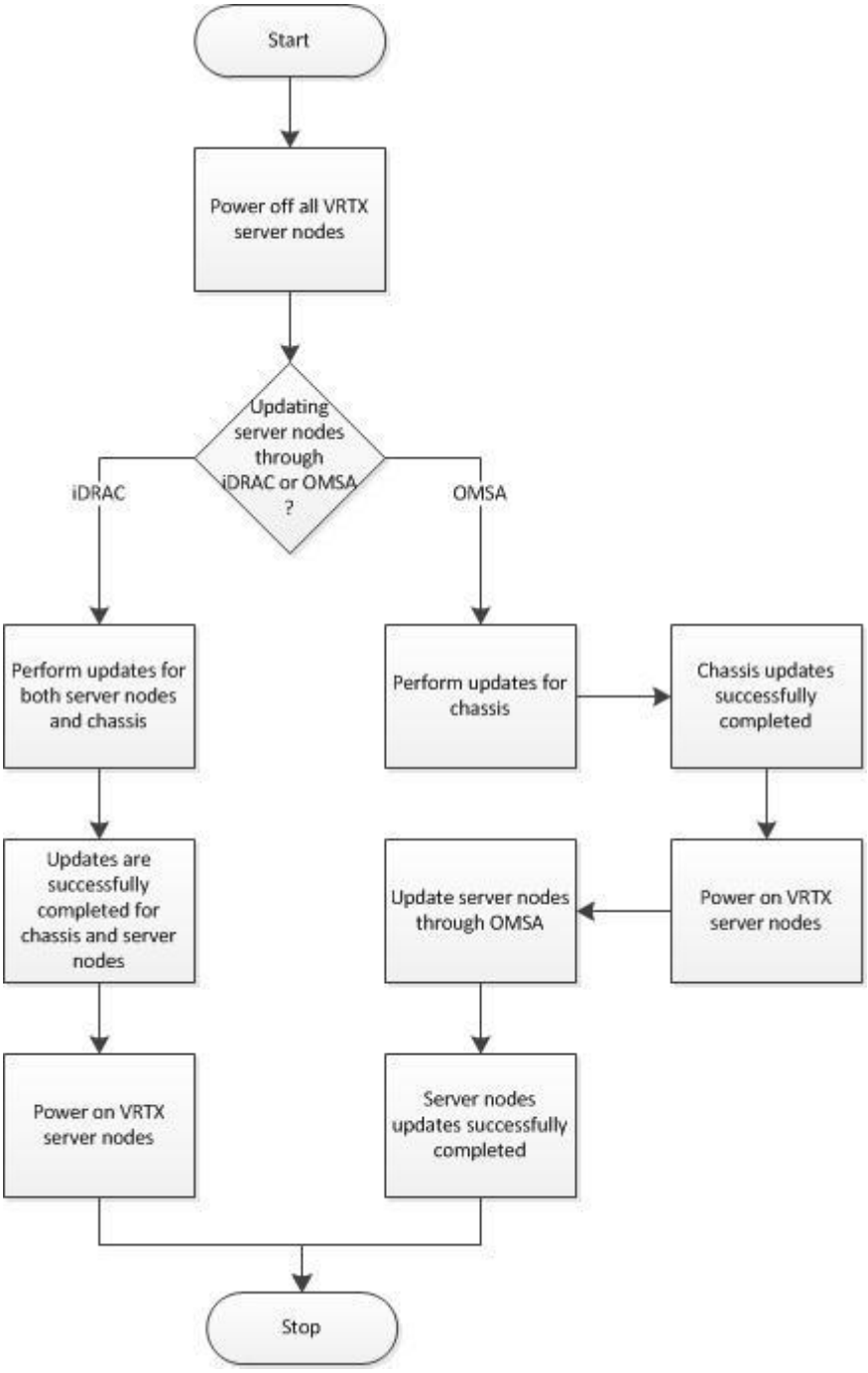


Figure 6: Workflow of updating the chassis and server nodes.

# VIII. Troubleshooting / FAQs

## Troubleshooting Map View

**Question:** Why is the Map View feature not available?

**Answer:** The Map View feature is available only if you have discovered any Dell PowerEdge VRTX or FX2/FX2s CMC with an Enterprise license, using the WS-Man protocol. If the PowerEdge VRTX or FX2/FX2s CMC with an Enterprise license is discovered using the SNMP protocol, the Map View feature is not available. Rediscovering the PowerEdge VRTX or FX2/FX2s CMC using the WS-Man protocol is required, if the Map View tab is not displayed in the device details portal of a Dell PowerEdge VRTX or FX2/FX2s CMC with an Enterprise license.

**Question:** Why am I unable to add a particular device on the map?

**Answer:** Only PowerEdge VRTX or FX2/FX2s devices with an Enterprise license can be added to the map.

**Question:** The map does not load with the MapQuest or Bing map provider. What should I do?

**Answer:** This indicates a problem with the Internet connectivity.

Verify if you are able to connect to the Internet through the browser.

If the system connects to the Internet through the proxy:

For MapQuest map provider — Configure the proxy settings in the OpenManage Essentials Preferences → Console Settings page.

For Bing map provider — Verify if you have configured the proxy server settings in Internet Explorer.

Verify if you are able to access the MapQuest website.

**Question:** Why is the map loading slowly?

**Answer:** The map may load slowly as it requires more network bandwidth and graphic processing capability compared to normal browsing. Constant zooming and panning on the map may also slow the loading of the map. For MapQuest, map performance is impacted by both the connection between the OME client and the OME Server and between the OME server and the MapQuest servers. Bing offers better performance as the OME client can connect directly to the Bing servers.

**Question:** Why am I unable to locate an address using the search bar or Edit Device Locations dialog box?

**Answer:** There may be a problem with your Internet connection or the map provider may not be able to resolve the address.

Verify if you are able to connect to the Internet through the browser.

If the system connects to the Internet through the proxy:

For MapQuest map provider — Configure the proxy settings in the OpenManage Essentials Preferences → Console Settings page.

For Bing map provider — Verify if you configured the proxy server settings in Internet Explorer.

Try to provide a variation of the address you provided. You can try providing a more complete address. Abbreviations such as state, country, airport code, may have an unexpected result.

**Question:** Why can't I use one map provider on the Home portal and another on the Devices portal?

**Answer:** The Map View available through the Home portal and the Devices portal are synchronized. Changes to the Settings or device locations on the Map View are affected on both the portals.

**Question:** How can I enhance the Map View experience?

**Answer:** Improving the network bandwidth will accelerate the loading of the map. A more powerful graphic card will enable faster zooming and panning capability. The Bing provider offers faster load times, an aerial view, and more consistent search results for things like abbreviations and airport codes.

**Troubleshooting Discovery**

**Question:** Why can't I discover my VRTX chassis and/or server nodes?

**Answer:** There are several tips throughout this paper which help the reader successfully manage their VRTX platform. The essential checklist includes setting appropriate timeouts for the protocols used based on network latency and even bandwidth constrictions, opening the appropriate network ports for communication (see the latest *Dell OpenManage Port Information Guide* online), and assuring that the right credentials are used. The Troubleshooting Tool that is installed with OME is a great tool to test for successful connections.

Additionally, make sure to setup asynchronous alerting (SNMP traps) and test the setup for reliable delivery to OME.

## Conclusion

The VRTX chassis is the newest modular solution from Dell, bringing compute and storage expandability to the office and Datacenter in a compact package. OpenManage Essentials has expanded its chassis management support for the VRTX that includes more secure and reliable communication for a distributed network, deeper inventory, and a map view for locating your VRTX or FX2/FX2s assets around the globe. No other console provides the same level of manageability for VRTX.