Dell Lifecycle Controller Integration Version 1.2 for Microsoft System Center 2012 Virtual Machine Manager

User's Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2016 - 03

Rev. A00

Contents

1

About Dell Lifecycle Controller Integration for Microsoft System Center 2012 Virtual Machine Manager

Dell Lifecycle Controller Integration (DLCI) for Microsoft System Center 2012 Virtual Machine Manager (SC2012 VMM) enables hardware configuration, provides a solution to simplify and improve the process of firmware updates, and hypervisor deployment on Dell servers. This plug-in uses the remote deployment feature of the Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC), providing a seamless user experience. You can leverage Dell's value additions through Microsoft System Center Consoles to manage virtualized environments.

For information about Microsoft System Center Virtual Machine Manager, see Microsoft documentation.

What's new in this release

The features for this release are as follows:

- Update sources — support for Hypertext Transfer Protocol (HTTP) type of update source.
- Test connection — validating the location of update source and the credentials before creating the update source.
- Update groups — group the servers for creating, managing, and performing firmware updates on custom update groups.
- Polling and notifications — configure notifications to receive alerts when new catalogs are available in update source.
- Protection vaults — location to save system configuration profiles.
- Export server profiles — including firmware images on components such as Basic Input Output System (BIOS), Redundant Array of Independent Disks (RAID), Network Interface Controller (NIC), integrated Dell Remote Access Controller (iDRAC), LC, and so on, to an internal or external location.
- Import server profiles — either retaining or excluding the current RAID settings for the same server or server groups when the existing server profile is corrupt.
- Filters — are used to display information based on the criteria selected in the **Maintenance Center**.
- Allow Downgrade — if enabled, allows you to downgrade the firmware version to an earlier version.
- Cluster-Aware Updating (CAU) — automates the software updating process by using the features of Microsoft on cluster update groups while maintaining the server's availability.
- Integration with Dell Repository Manager (DRM) — providing the server inventory information of the existing servers from the appliance to DRM.

Existing features

With DLCI for SC2012 VMM, you can continue to do the following:

- Auto discover unassigned Dell servers — connect the factory delivered Dell servers to the network, power on the servers, and enter the provisioning server details of the DLCI appliance to automatically discover the servers.

  Servers discovered by the appliance are known as unassigned servers, and these servers are available for hypervisor deployment.
- Manually discover unassigned Dell servers — discover the 11th, 12th, and 13th generation of PowerEdge servers and deploy the servers in a virtual environment.
- View inventory of discovered servers — key inventory details about the Dell servers are provided.
- Check for server compliance — for using the features available in the appliance, Dell servers must have the required firmware versions of iDRAC, LC, and Basic Input Output System (BIOS). For information about version numbers, see *DLCI for SC2012 VMM Release Notes*.
- Prepare an ideal server configuration, also known as golden configuration — replicate this configuration on the servers that are deployed into the virtual environment. Also you can:
  - Edit and modify the golden configuration for boot order and BIOS.
  - Customize Dedicated Hot Spare (DHS) strategy for RAID.
- Create and maintain profiles and templates.
- Customize Microsoft Windows Preinstallation Environment (WinPE) — prepare customized WinPE images with the latest Dell OpenManage Deployment Toolkit (DTK) drivers.
- Use LC Driver Injection feature on the latest factory delivered servers that are shipped with the latest driver packs.

  Deploy hypervisors with or without LC Driver injection — from the appliance, perform hypervisor deployment based on the golden configuration.
- Launch iDRAC Console from the DLCI Console to view inventory information and do troubleshooting.
- View information on jobs — view information logged for various jobs that are performed in the appliance.
- Simplified licensing — you do not require Dell Connections License Manager (DCLM) to manage your licenses any more. More information on licensing is available under **License Center** in Admin portal.
- New credential profile types:
  - Device credential profile — use to login to iDRAC or Chassis Management Controller (CMC).
  - Windows credential profile — use to access Windows Shares.
  - FTP credential profile — use to access FTP site.
  - Proxy server credentials — use to provide proxy credentials.
- Discovery — discover servers with cluster details if the host is a part of a cluster, and chassis details if it is a modular server.
- Synchronize with SCVMM — synchronize all Dell host systems listed in the SCVMM environment with DLCI for SC2012 VMM, where hosts are Hyper-V hosts managed by SCVMM.
  - Resolve Sync Errors — resynchronize the host servers that were not synchronized during an earlier attempt.

- Server management — manage Dell servers in SCVMM environment and keep the servers up-to-date as per Dell recommendations based on latest firmware and other updates. Server management of 11th generation to 13th generation of Dell PowerEdge servers is supported.
  - Key features in server management are as follows:
    * Viewing comparison report — view comparison reports with criticality from an update source, and then create a baseline version. Criticality is how important the update is.
    * Refreshing and exporting firmware inventory — refresh firmware inventory and export the inventory details in `xml` format.
    * Applying updates — apply firmware updates or schedule updates.
    * Applying specific updates — apply only specific component updates, or apply the latest update available on Dell FTP.
    * Applying updates before operating system deployment — before an operating system deployment, apply firmware updates using an appropriate update source.
  - Remotely update servers (one-to-one or one-to-many) for the latest firmware versions for the following:
    * BIOS
    * NIC or LAN on Motherboard (LOM)
    * Power Supply Units (PSUs) from 12th generation of PowerEdge servers onwards
    * PowerEdge RAID Controller (PERC) or Serial Attached SCSI (SAS)
    * Backplane
    * iDRAC (modular and monolithic) with LC

      NOTE: Available components are listed under Dell servers.
- Update groups — all the discovered servers are added into appropriate predefined update groups.
- Update sources — create a repository by using DRM, or by connecting to an FTP site.
  - Integration with DRM — export the system inventory information from DLCI for SC2012 VMM into DRM and use DRM to prepare a repository.
  - FTP — connect to Dell FTP (local or online), and get the latest Dell Online catalogs.

2

Installing and setting up DLCI Console Add-in

Installing and setting up DLCI Console Add-in for SC2012 VMM includes the following:

- Review and complete system requirements and then install **DLCI Console Add-in for SC2012 VMM**. For more information, see Installing DLCI Console Add-in.
- Import DLCI Console into the VMM Console. For more information, see Importing DLCI Console into VMM Console.
- View DLCI Console in the VMM Console. For more information, see Viewing DLCI Console.
- Uninstall the DLCI Console. For more information, see Uninstalling DLCI Console.

Installing DLCI Console Add-in

Before you begin working with the appliance, install the DLCI Console in the system where the SC2012 VMM Console is installed. Once you install the DLCI Console, you can import the DLCI Console into the SC2012 VMM Console.
Prerequisites: SC2012 VMM SP1 or SC2012 VMM R2 Console is installed.

If you are installing the DLCI Console for the first time from **Setup and Configuration**, then start from step 3, else start from step 1.

To install the DLCI Console, perform the following steps:

1. In the **DLCI Admin Portal — SC2012 VMM**, click **Downloads**.
2. From **DLCI Console Add-in for SC2012 VMM Installer**, click **Download Installer** and save the file to a location.
3. Run the installer file.
4. On the **DLCI Console Add-in for SC2012 VMM** Welcome page, click **Next**.
5. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
6. In the **Destination Folder** window, by default an installation folder is selected. To change the location, click **Change**, complete the changes, and then click **Next**.
7. On the **Ready to Install the Program** page, click **Install**.
8. On the **InstallShield Wizard Completed** page, click **Finish**.

Removing or repairing DLCI Console add-in

To remove or repair the DLCI Console add-in, perform the following steps:

1. Run the **DLCI Console Add-in for SC2012 VMM** installer.
2. In **Program Maintenance**, select **Remove** or **Repair** and then click **Next**.
3. In **Ready to Repair or Remove the program**, click **Install**.
4. When the remove or repair task is complete, click **Finish**.

Importing DLCI Console Add-in into VMM

To work with the DLCI appliance, import DLCI Console into the VMM Console.

Prerequisites: For the connection with the appliance to work, in the web browser, clear the proxy setting; however, if the web browser's proxy settings are configured, then in the proxy exception list, include the fully qualified domain name (FQDN) of the appliance.

To import the DLCI Console into the VMM Console:

1. From SC2012 VMM, click **Settings**.
2. In the **Home** ribbon, click **Import Console Add-in**.
3. Click **Import Console Add-in Wizard → Select an add-in to import**, browse to select the DLCI Console Add-in for SC2012 VMM (**DLCI_VMM_Console_Addin.zip**), and then click **Next**.
4. In **Confirm the settings**, confirm that the settings are as required and then click **Finish**.

   The DLCI Console is imported into the VMM Console and is available under **VMs and Services → All Hosts**.

Viewing DLCI Console Add-in

To view the DLCI Console in SC2012 VMM:

1. In SC2012 VMM Console, select **Fabric**, and then select **All Hosts Group**.

   NOTE: To launch DLCI Console, you can select any host group you have access to.
2. In the **Home** ribbon, select **DLCI Console**.

Uninstalling DLCI Console Add-in

To uninstall DLCI Console:

1. In SC2012 VMM, click **Settings**.
2. Click **Settings → Console Add-ins** and then, select **DLCI Console Add-in for SC2012 VMM**.
3. In **Home**, click **Remove**.

3

Getting Started

Management systems are the systems on which DLCI for SC2012 VMM, also known as the appliance and its components, are installed. The components of appliance are:

- Dell Lifecycle Controller Integration (DLCI) Integration Gateway for Microsoft System Center 2012 Virtual Machine Manager (SC2012 VMM), also known as DLCI Integration Gateway for SC2012 VMM.
- Dell Lifecycle Controller Integration (DLCI) Console Add-in for Microsoft System Center 2012 Virtual Machine Manager (SC2012 VMM), also known as DLCI Console Add-in for SC2012 VMM.

Logging in to the DLCI Admin Portal — SC2012 VMM

To log in to DLCI Admin Portal — SC2012 VMM, perform the following steps:

1. From the appliance, note the DLCI Admin Portal — SC2012 VMM URL.
2. In a web browser, go to URL: **https://<IP Address>** or **<FQDN>**.
   For example: **192.168.20.30** or **DLCIforSC2012vmm.myorgdomain.com**.
3. Log in to DLCI Admin Portal — SC2012 VMM by using the user credentials provided while configuring the appliance.

DLCI admin portal — SC2012 VMM

The DLCI Admin Portal — SC2012 VMM user interface contains the following options:

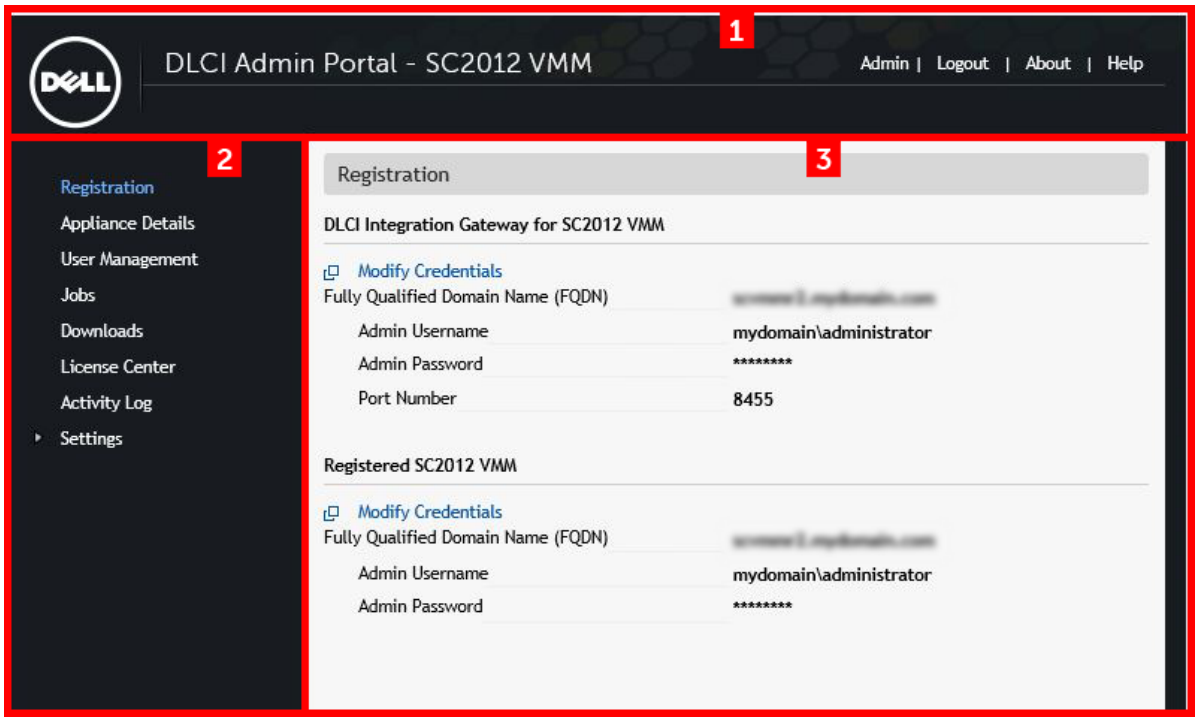


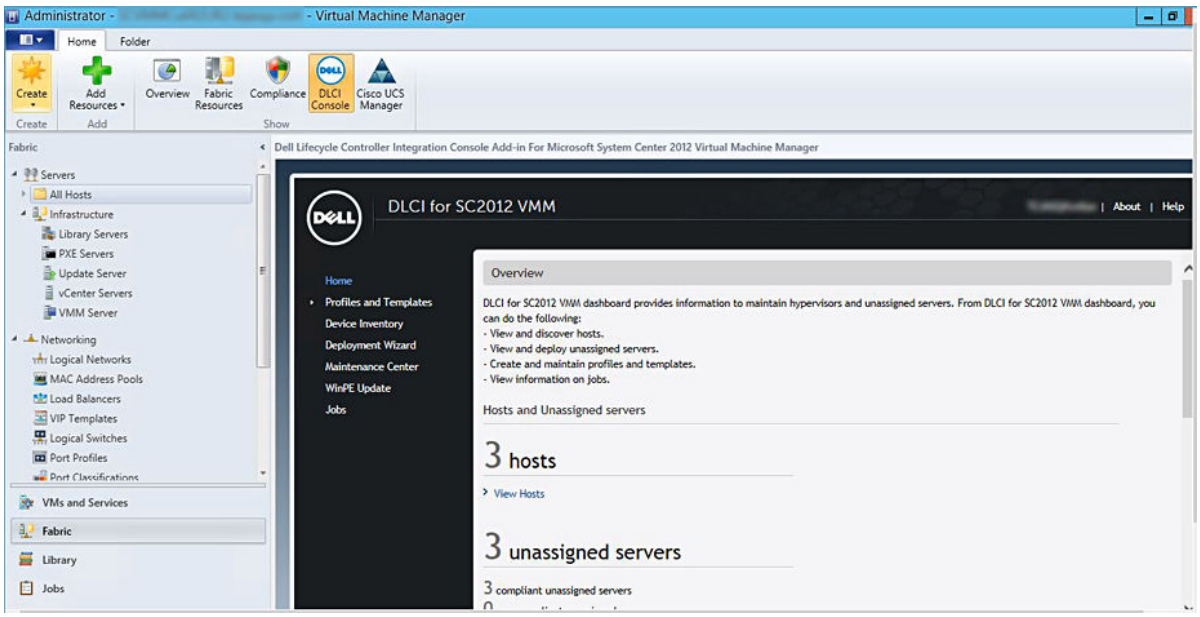
Figure 1. DLCI admin portal — SC2012 VMM

1. The heading banner includes the product name and the following options:
   - **Admin** — displays information about the user who has logged in to DLCI for SC2012 VMM — Admin Portal.
   - **Logout** — enables you to log out of the DLCI for SC2012 VMM Admin Portal.
   - **About** — provides information about the DLCI for SC2012 VMM version.
   - **Help** — launches the context sensitive online help.
2. The navigation pane contains the following options. For more information about each option see the Online help:
   - **Registration**
   - **Appliance Details**
   - **User Management**
   - **Jobs**
   - **Downloads**
   - **License Center**
   - **Activity Log**
   - **Settings**
     - **Service Pack Updates**
     - **Logs**
3. The console area displays information about the option selected by you in the navigation pane.

Logging in to DLCI Console Add-in for SC2012 VMM

To log in to DLCI Console Add-in for SC2012 VMM:

1. In SC2012 VMM, select **Fabric**, and then select **All Hosts**.
2. In the **Home** ribbon, select **DLCI Console**.



DLCI Console add-in for SC2012 VMM

The DLCI Console Add-in user interface contains the following options:

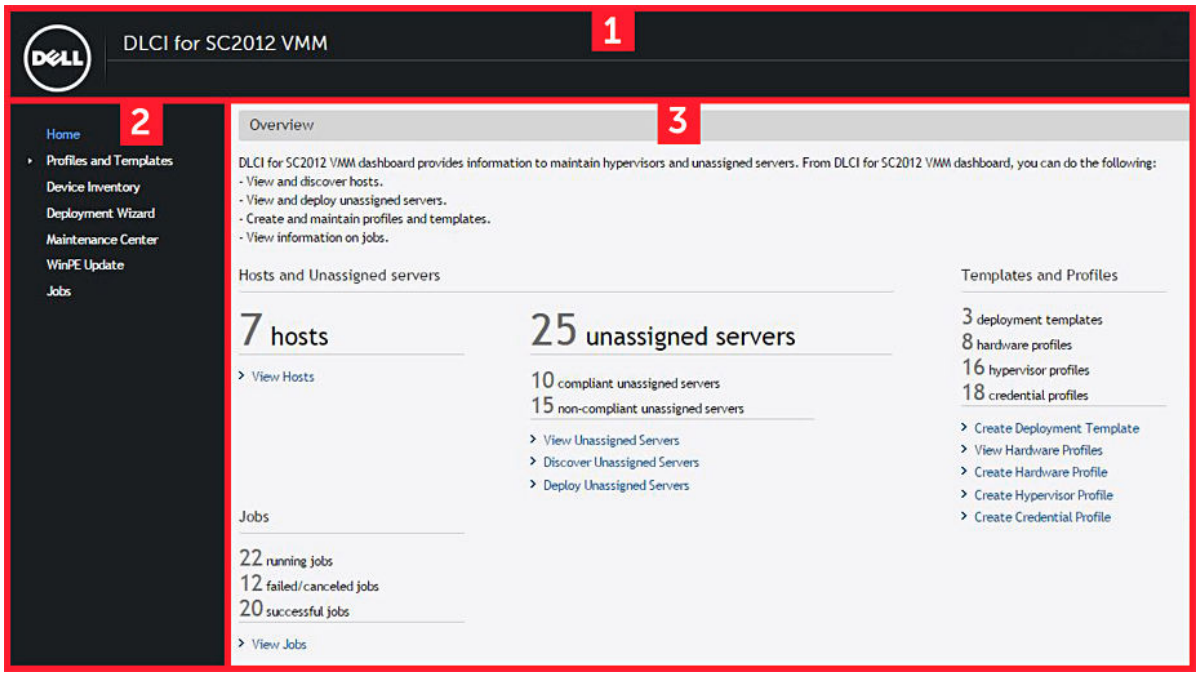


Figure 2. DLCI Console add-in for SC2012 VMM

1. The heading banner contains the product name and the following options:
   - **<Domain>\adminstrator** — displays information about the user who is logged in to DLCI for SC2012 VMM.
   - **About** — provides information about the DLCI for SC2012 VMM version.
   - **Help** — launches the context-sensitive online help.
2. The navigation pane contains the following options:
   - **Home** — displays the DLCI for SC2012 VMM dashboard.
   - **Profiles and Templates**
     - **Deployment Template**
     - **Hardware Profile**
     - **Hypervisor Profile**
     - **Credential Profile**
   - **Device Inventory**
   - **Deployment Wizard**
   - **Maintenance Center**
   - **WinPE Update**
   - **Jobs**
3. The console area displays information about the option selected by you in the navigation pane.

NOTE: In DLCI Console for SC2012 VMM, if you are working in a wizard, for example a Hardware Profile wizard, and you navigate to any other tab or link in SC2012 VMM Console and then view the DLCI Console Add-in for SC2012 VMM again, the information you had provided is not saved and the DLCI Console displays the home page.

4

Workflows

This section contains the following workflows:

- Creating golden configurations
- Creating and managing credential profiles
- Creating and managing update sources
- Creating and managing custom update groups
- Applying updates on servers or server groups
- Hypervisor deployment
- Creating, managing and deleting protection vaults
- Exporting server profile
- Importing server profile
- Deleting servers

About golden configurations

A server configuration with the preferred Boot sequence, BIOS, and RAID settings ideally suited for the organization is referred to as golden configuration. These settings are gathered in a hardware profile and deployed on identical servers during hypervisor deployments.

Creating golden configurations

To prepare and use a golden configuration:

1. Ensure that the server with the ideal configuration is discovered and available. For more information on server discovery, depending on the requirement, see Discovering servers using auto discovery or Discovering servers using manual discovery.
2. Ensure that the server's inventory is up-to-date. For more information, see Viewing and refreshing firmware inventory.
3. To record the ideal configuration, create a hardware profile. To create a hardware profile, see Creating hardware profile.
4. If you want to modify configurations, see Modifying hardware configuration profile.

Creating, managing, and deleting credential profiles

To create a credential profile, see Creating a credential profile.

To manage a credential profile, see Modifying a credential profile.

To delete a credential profile, see Deleting a credential profile.

Creating, managing, and deleting update sources

To create an update source, see Creating an update source.

To manage an update source, see Modifying an update source.

To delete an update source, see Deleting an update source.

Creating, managing, and deleting custom update groups

To create a custom update group, see Creating a custom update group.

To manage a custom update group, see Modifying a custom update group.

To delete a custom update group, see Deleting a custom update group.

Applying updates on servers, or server groups

You can update the selected servers or server groups using the following sources:

- Online FTP and local FTP source
- Online HTTP and local HTTP
- Local DRM repository

To apply updates on selected servers or server groups:

1. Before you begin updates, view information on update sources and update groups. For more information, see Update management.
2. Discover servers. For more information, see Discovering servers using auto discovery, or Discovering servers using manual discovery.
3. Synchronize servers present in SCVMM environment with DLCI for SC2012 VMM. For more information on synchronization, see Synchronization with SCVMM.
4. Ensure that the servers inventory is up-to-date. For more information, see Viewing device inventory.
5. Ensure that there is an update source created. For more information, see Creating an update source.
6. Ensure that the update source is regularly updated with the latest catalog using polling and notification. For more information, see Polling and notification.
7. Ensure that the required server groups are selected to apply the updates. For more information, see Applying updates on servers.

   NOTE: Select **Allow Downgrade** to downgrade the firmware version of the components.

Creating, managing, and deleting protection vaults

1. To create a protection vault, see Creation of protection vault.
2. To manage a protection vault, see Modifying protection vault.
3. To delete a protection vault, see Deleting protection vault.

Exporting server profile

To export server configuration:

1. Create a protection vault. For more information, see Creating protection vault.
2. Export server profile immediately, or schedule it for a later date. For more information, see Creating export jobs.

Importing server profile

To import a server profile:

1. Create a protection vault. For more information, see Creating protection vault.
2. Export a server profile. For more information, see Creating export jobs.
3. Import an exported server profile including, or excluding the RAID configuration. For more information, see Importing server profile.

Hypervisor deployment

Using the appliance, you can perform firmware update and hypervisor deployment based on the golden configuration. You can use the LC Driver Injection feature for the factory delivered servers that ship with the latest driver packs. Also, you can update the driver packs, and get the same benefits of installing latest drivers during hypervisor deployments and firmware updates.

Table 1. Different scenarios for hypervisor deployment

If you require the latest factory drivers and out-of-band drivers	While creating a hypervisor profile, enable LC (Lifecycle Controller) driver injection.
If you want to retain the existing hardware configuration	While creating a deployment template, select only the hypervisor profile.

To work with hypervisor deployment, see the following:

1. About deployment
2. Creating credential profiles
3. Creating update sources
4. Creating hardware profiles
5. Creating hypervisor profiles
6. Creating deployment templates
7. (Optional) Creating custom update groups
8. (Optional) Applying updates on servers
9. Deploying hypervisors

Deleting servers

For information on deleting servers in the appliance, see Deleting servers from DLCI Console.

5

Setting up the environment for deploying hypervisors

To set up an environment for hypervisor deployment:

1. Prepare Golden configurations.
2. Create a physical computer profile in SC2012 VMM. For more information, see SC2012 VMM documentation.
3. Create a target host group in SC2012 VMM. For more information, see SC2012 VMM documentation.
4. Download the latest Dell Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot ISO image. For more information, see WinPE update.
5. Set up the systems for auto discovery. For more information, see Discovering servers using auto discovery.
6. Create an update source. For more information, see Creating an update source.
7. (Optional) create a custom update group. For more information, see Creating custom update group.
8. (Optional) create a hardware profile. For more information, see Creating a hardware profile.
9. Create a hypervisor profile. For more information, see Creating a hypervisor profile.
10. Create a deployment template. For more information, see Creating a deployment template.
11. After the systems are discovered and available in the appliance, do firmware update (optional), and then do the hypervisor deployment. For more information on applying updates, see Applying updates on servers. For more information on deploying hypervisor, see Deploying hypervisors.
12. View job status on firmware update and deployment. For more information, see Viewing job status.

6

Server discovery

You can do out-of-band discovery of unassigned Dell servers and import information about Dell servers into the appliance. For discovering servers, connect the Dell servers to the network, power on the servers, log in to iDRAC, update the provisioning server IP with the IP of the DLCI appliance and disable the administrator account for DLCI appliance to automatically discover the servers. For more information about configuring the server, see *Integrated Dell Remote Access Controller* documentation.

You can also discover unassigned Dell servers by using the following options:

- Auto discovery of unassigned servers.
- Manual discovery based on IP addresses.

You can discover Hyper-V hosts and modular Hyper-V hosts along with unassigned servers. After discovery, the servers are added to respective predefined update groups. For more information on classification of groups, see Update Management.

Server discovery notes:

- When you discover a Dell PowerEdge server with an operating system and present in SCVMM, then the server is listed as a host server and marked as compliant or non-compliant.
  - A host server is compliant when it contains minimum versions of LC firmware, iDRAC, and BIOS that are required to work with the appliance.
  - If the host is a modular server, then the service tag of the chassis containing the server is displayed. If the host is part of a cluster, then the Fully Qualified Domain Name (FQDN) of the cluster is displayed.
- When you discover a Dell PowerEdge server that is not listed in SCVMM, then the server is listed as an unassigned server and marked as compliant or noncompliant.
- If you provide incorrect credential details, then based on the iDRAC version, the following resolutions are available:
  - While discovering a 12th generation Dell PowerEdge server with iDRAC version 2.10.10.10 and later, during login if you input incorrect details for credential profile, based on your attempts, the server discovery fails with the following behavior:
    * For first attempt, server IP address is not blocked.
    * For second attempt, server IP address is blocked for 30 seconds.
    * For third and subsequent attempts, server IP address is blocked for 60 seconds.

    You can reattempt server discovery with correct credential profile details once the IP address is unblocked.
  - While discovering an 11th or 12th generation PowerEdge server with iDRAC versions prior to 2.10.10.10, if server discovery attempts fail due to input of incorrect credential profile details, then rediscover the server with the correct credential profile details.
  - For iDRAC versions prior to 2.10.10.10, blocking of IP addresses is configurable. For more information, see iDRAC documentation at **dell.com/support/home**. Based on your requirement,

you can also disable blocking of IP addresses. And you can also check if the iDRAC.IPBlocking.BlockEnable feature is enabled in iDRAC.

– After a server is discovered using the default credential profile and added in the appliance, if the default iDRAC credential profile is changed, then you cannot perform any activity on the server. To work with the server, rediscover the server with the new credential profile.

System requirements for managed systems

Managed systems are the systems that are managed using the appliance. For appliance to discover managed systems, following are the system requirements:

- For the 11th, 12th, and 13th generation of Dell PowerEdge servers, the appliance supports modular and monolithic server models.
- For source configuration and destination configuration, use same type of disks — only Solid-state Drive (SSD), SAS or only Serial ATA (SATA) drives.
- For successful hardware profile RAID cloning, for destination system disks, use same or greater size and number of disks as present in the source.
- RAID sliced virtual disks are not supported.
- iDRAC with shared LOM is not supported.
- Unified Extensible Firmware Interface (UEFI) boot mode is not supported.
- RAID configured on external controller is not supported.
- Enable Collect System Inventory on Start (CSIOR) in managed systems. For more information, see Enabling CSIOR in managed systems.

Enabling CSIOR in managed systems

To enable CSIOR for 12th and 13th generation of Dell PowerEdge servers:

1. Select **F2** during the post to enter **System Setup**.
2. Select **iDRAC** Settings and click **Lifecycle Controller**.
3. For **Collect system inventory on Restart (CISOR)**, set the option to **Enabled**.

To enable CSIOR for 11th generation PowerEdge servers:

1. Restart the system.
2. During Power-on Self Test (POST), when the system prompts you to enter the iDRAC Utility, press **CTRL + E**.
3. From the available options, select **System Services** and press **Enter**.
4. Select **Collect System Inventory on Restart** and press the right or down keys and set it to **Enabled**.

Discovering servers using auto discovery

Connect the Dell servers to the network and power on the servers for DLCI appliance to automatically discover the servers. The appliance auto discovers unassigned Dell servers by using the remote enablement feature of iDRAC. The appliance works as the provisioning server and uses the iDRAC reference to auto discover Dell servers.

To perform auto discovery on Dell servers:

1. In the appliance, create a device type credential profile (by specifying the iDRAC credentials and marking it as default) for Dell servers. For more information, see Creating a credential profile.
2. In Dell servers that you want to auto discover, do the following:
   a. Disable the existing Admin accounts in iDRAC.
   b. In the iDRAC settings, in remote enablement, enable Auto-Discovery.
   c. After enabling auto discovery, provide the provisioning server (that is DLCI Appliance) IP address and restart the server.

Discovering servers using manual discovery

You can manually discover servers using an IP address or an IP range. To discover servers, provide the servers' iDRAC IP and the servers' device type credentials. When you are discovering servers using an IP range, specify an IP (IPv4) range (within a subnet).

To manually discover Dell servers:

1. In DLCI Console Add-in for SC2012 VMM, do any of the following:
   - In the dashboard, click **Discover Unassigned Servers**.
   - In the navigation pane, click **Device Inventory** and in **Inventory** click **Discover**.
2. In **Discover**, select the required option:
   - **Discover Using an IP Address**
   - **Discover Using an IP Range**
3. Select the required device type credential profile, or click **Create New** to create a credential profile.
4. In **Discover Using an IP Address or IP Address Range**, do any of the following:
   - If you selected **Discover Using an IP Address**, then provide the IP address of the server you want to discover.
   - If you selected **Discover Using an IP Range**, then provide the IP address range you want to include and if you must exclude an IP address range, select **Enable Exclude Range** and provide the range that you want to exclude.
5. In **Job Options**, to track this job, assign a job name and to view the job list, select **Go to the Job List after completing**.
6. Click **Finish**.

Deleting servers from DLCI Console

You can delete the unassigned servers and host servers based on the following criteria:

- You can delete an unassigned server that is listed in the appliance.
- If a host server is provisioned in SCVMM and present in the appliance, first delete the server in SCVMM and then delete the server from the appliance.

  In DLCI Console:

  - To delete unassigned servers — in **Unassigned Servers**, select the server and click **Delete** and in the confirmation message click **Yes**.

- To delete host servers — in **Host Servers**, select the server and click **Delete** and in the confirmation message, click **Yes**.

Viewing device inventory

The **Device Inventory** page lists unassigned servers and host servers. Using the host name or IP address of the server, you can view the server details such as compliance status, firmware versions and son on.

From the device inventory page, you can do the following:

- Discovering servers
- Refresh server information
- Deleting servers from DLCI Console
- Synchronizing with SC2012 VMM
- Resolving synchronization errors
- Correlate host servers to cluster group and the chassis to which the server belongs to
- Launching iDRAC Console

If the unassigned server is a modular server, then the chassis service tag is added in the inventory details for the chassis containing the modular server.

If the host server is a part of a cluster, to correlate a server to its cluster group and to know the chassis information, see cluster FQDN and chassis service tag.

To work with the servers discovered in the prior versions of the appliance, rediscover the servers.

To view servers:

In DLCI Console, click **Device Inventory**.

Synchronization with SC2012 VMM

You can synchronize all Dell Hyper-V hosts, Hyper-V host clusters, and modular Hyper-V hosts in the SC2012 VMM environment with the appliance. You can also get the latest firmware inventory of the servers after synchronization.

Synchronization notes:

- Synchronization uses the servers' default iDRAC credential profile details.
- If the host server's Baseboard Management Controller (BMC) is not configured in SC2012 VMM with the iDRAC IP address, then you cannot synchronize the host server with the appliance. Hence, configure BMC in SC2012 VMM (for more information, see MSDN article at `technet.microsoft.com`), and then synchronize the appliance with SC2012 VMM.
- SC2012 VMM R2 supports numerous hosts in the environment, due to which synchronization is a long running task. Synchronization occurs as follows:

  a. Hosts listed in SC2012 VMM environment are added to the **Hosts** tab in appliance.

  b. If host servers deleted from SC2012 VMM environment are resynchronized, then host servers are moved to the **Unassigned** tab in the appliance during resynchronization. If a server is decommissioned, then remove that server from the list of unassigned servers.

c. If a server is listed as an unassigned server and manually added to SCVMM, then after synchronization the server is added in to the **hosts** tab in the appliance.

d. If a host server belongs to a Hyper-V cluster, then the cluster details are available in the device inventory. The host server is added or moved to the cluster update group.

e. If a host is a modular server, then the service tag of the chassis containing the modular server is added to the device inventory page. If the modular server does not belong to a Hyper-V cluster, the host server is added or moved into the chassis update group.

f. Any changes to the host inventory details such as hostname, iDRAC IP address, memory, cluster membership and so on are updated in device inventory.

g. DLCI for SCVMM can provide the latest firmware inventory information. If a default update source is provided, then the firmware inventory is compared against the update source and the latest information is added to the update group.

Synchronizing appliance with SCVMM

To perform synchronization:

In **DLCI for SC2012 VMM**, click **Device Inventory**, and then click **Synchronize with SCVMM**.

Resolving synchronization errors

The servers that are not synchronized with appliance are listed with their iDRAC IP address and host name.

Consider the following when you are resolving synchronization errors:

- For servers that are not synchronized due to credentials, iDRAC, connectivity, or other issues; Resolve the issues first, and then resynchronize.

To resynchronize the servers:

1. In DLCI Console Add-in for SC2012 VMM, click **Device Inventory** and then click **Resolve Sync Errors**.
2. Select the servers you want to synchronize and select the credential profile or create new credential profile.
3. Provide a job name and select **Go to the Job List** to view the job status, and then click **Finish**.

Launching iDRAC Console

To launch iDRAC Console:

In **Device Inventory**, under **Unassigned Servers** or **Hosts**, click the **iDRAC IP**.

7

License for the appliance

Agent-free configuration, deployment, and firmware update features in DLCI for SC2012 VMM are licensed. Five licenses are available for evaluation purposes at no additional charge. To download the five licenses, see `marketing.dell.com/software-download-DLCISCVMM`. For more information on licensing, go to Dell TechCenter website and then OpenManage Integration Suite for Microsoft System Center wiki page.

To view license details, from **DLCI Admin Portal — SC2012 VMM** launch the **License Center**.

8

Server management

Using **Maintenance Center**, you can perform all the tasks related to managing Dell updates in the SCVMM environment. You can maintain up-to-date firmware versions of Dell server components as per Dell recommendations.

You can view, create, and maintain protection vaults, update sources, custom groups, and view the predefined update groups. You can create, and schedule jobs for firmware updates, and schedule notifications to receive alerts when new catalogs are available at update source. A comparison report for the existing firmware version and the baseline version is provided, based on this information, you can create an inventory file, import and export server profiles. Also you can filter the information on the type of updates, server components, and server models.

You can perform updates only on compliant servers because iDRAC updates are available only for minimum compliant version and later.

NOTE:

- After upgrading from DLCI for SC2012 VMM version 1.1 to version 1.2, all the servers discovered earlier are added to **Default unassigned update groups** or **Default host update groups**. To add the servers into the respective predefined update groups, rediscover the servers.
- After upgrading to DLCI for SC2012 VMM version 1.2, if the connection to **ftp.dell.com** or **downloads.dell.com** fails, default Dell online FTP, or Dell HTTP update source cannot download the catalog file, and hence the comparison report is not available. To view a comparison report, edit the default Dell online FTP, or Dell HTTP update source, create proxy credentials, and then select the same from the **Select Update Source** drop-down menu. For more information on editing an update source, see Modifying update source.
- After upgrading to DLCI for SC2012 VMM version 1.2, if the connection to **ftp.dell.com** or **downloads.dell.com** fails, default Dell online FTP, and Dell HTTP update source cannot download the catalog file, and hence the comparison report is not available. To view a comparison report, create a new update source and select the same from the **Select Update Source** drop-down menu. For more information on creating an update source, see Creating update source.

DLCI for SC2012 VMM provides the following update actions:

- Downgrade — there is an earlier version available at update source and you can downgrade the firmware to this version.
- No Action Required — the firmware version is at the same level as the one in the repository.
- No Update Available — no firmware updates are available for the component.
- Upgrade - Optional — updates consist of new features or any specific configuration upgrades that are optional.
- Upgrade - Urgent — critical updates used for resolving security, performance, or break-fix situations in components such as BIOS, and so on are available.
- Upgrade - Recommended — updates carry bug fixes or any feature enhancements in the product. Also, compatibility fixes with other firmware updates are included.

DLCI for SC2012 VMM provides the following methods to perform firmware updates:

- **Update using DRM repository** — export the inventory information of the discovered servers from appliance to prepare a repository in DRM.
  - After exporting the xml file, to create a repository in DRM, in **My Repositories** click **New**, and then click **Dell Modular Chassis inventory**. In **Modular Chassis Inventory** select the exported xml file from the appliance. For more information on creating a repository in DRM, see *Dell Repository Manager* documents.
  - After the repository is created, select the relevant servers and initiate an update on the servers. Consider other factors such as testing on test environment, security updates, application recommendations, Dell advisories, and so on, to prepare the required updates.
- **Update using FTP or HTTP** — update any specific component to the latest update provided on the FTP or HTTP site. Dell IT prepares a repository at quarterly cadence.
  - Integration with Dell Online Catalog — connect to Dell FTP and download the catalog file in the cache directory in case of FTP update source, or connect to `downloads.dell.com` in case of HTTP update source, and then make it as a reference inventory.
  - View the comparison report against the update source, select the relevant servers or server components, and then initiate an update on the servers.
- **Referencing firmware inventory and comparison** — create a reference inventory file that contains the firmware inventory of the selected servers or groups of servers. Later, you can compare the inventory information of servers present in the appliance against the saved reference inventory file. Note that the reference server inventory file can contain inventory information from a single server of same type or model, or can have multiple servers of different types or models.

Integration with DRM

DLCI for SC2012 VMM is integrated with DRM version 2.2 onwards providing the server inventory information of the existing servers from the appliance to DRM. Using the inventory information you can create a custom repository in DRM and set it as an update source in the appliance for performing firmware update jobs on the servers, or group of servers. For more information on creating a repository in DRM, see *Dell Repository Manager* documents.

NOTE: After upgrading to DLCI for SC2012 VMM version 1.2, perform a rediscovery of the servers to update the inventory information that is consumed by DRM.

To create a repository for the appliance using DRM:

1. Open the **Dell Repository Manager Data Center** version.
2. Click **My Repositories**, click **New** and then click **Dell Console Integration**.
3. Enter the **URL (Rest API)** in the following format: `https:// IP address of appliance/ genericconsolerepository/` and then click **Next**.
4. Provide the **UserName** and **Password** that was used in the appliance, click **Ok**, and then click **Ok**

Filters

Apply filters to view selected information in the comparison report.
The appliance supports three categories of filters:

- **Nature Of Update** — select to filter and view only the selected type of updates on servers.
- **Component Type** — select to filter and view only the selected components on servers.
- **Server Model** — select to filter and view only the selected server models.

NOTE: You cannot export and import server profiles if the filters are applied.

To apply filters:

In DLCI Console Add-in, click **Maintenance Center**, click the filters drop-down menu, and then select the filters.

To remove filters:

In DLCI Console Add-in, click **Maintenance Center**, then click **Clear Filters** or clear the selected check boxes.

Update source overview

Update source enables you to select and apply updates from Dell's update sources. You can create, view, and manage the update sources. The types of update sources supported are DRM repository, FTP, and HTTP. You can create a DRM, HTTP, or FTP update source and set it as a default update source.

Update sources have the catalog files that contain Dell updates (BIOS, firmware, application, drivers, and driver packs) and carry the self-contained executable file called Dell Update Packages (DUPs). A local copy of the catalog file is cached in the appliance at the time of creation. When a catalog file is updated in the update source, the locally cached catalog file is not automatically updated. To update the catalog file saved in cache, edit the update source or delete and recreate the update source.

You can compare the inventory information available at the update source against the inventory information of a selected server or group of servers inventory information and create a baseline version. You can also change the update source and compare the inventory information of the servers or group of servers against the version information available from the selected update source.

Dell recommends that you upgrade to the latest firmware to use security, bug fixes, and new feature requests. Dell publishes the following updates through PDK catalogs posted on Dell FTP at monthly cadence:

- Server BIOS and firmware
- Dell certified operating system driver packs (for operating system deployment)

Predefined and default update source

DELL ONLINE CATALOG is a predefined update source of type FTP available in the appliance after a fresh installation or upgrade. You cannot delete, or change the name of a predefined update source.

DELL ONLINE HTTP CATALOG is a default update source available in the appliance after a fresh installation or upgrade. You cannot delete or change the name of this default update source. However, you can create another update source and mark it as a default update source.

NOTE:

- After installing DLCI for SC2012 VMM, add the proxy details for **DELL ONLINE CATALOG** and, **DELL ONLINE HTTP CATALOG** update source and save it.
- After upgrading to DLCI for SC2012 VMM version 1.2, set **DELL ONLINE HTTP CATALOG** as default update source.

Test connection

Use **Test Connection** to verify if the location of the update source is reachable by using the credentials mentioned while creating the update source.

You can create an update source, only after confirming that the catalog location is accessible through the provided credentials.

Setting up local FTP

To set up your local FTP:

1. Create a folder structure in your local FTP that is an exact replica of the online FTP, **ftp.dell.com**.
2. Download the **catalog.xml.gz** file from online FTP and extract the files.
3. Open the **catalog.xml** file and change the **baseLocation** to your local FTP URL, and compress the file with **.gz** extension.

   For example, change the **baseLocation** from `ftp.dell.com` to **ftp.yourdomain.com**.
4. Place the catalog file and the DUP files in your local FTP folder replicating the same structure as in **ftp.dell.com**.

Setting up local HTTP

To set up HTTP server on a local system, perform the following:

1. Create a folder structure in your local HTTP that is an exact replica of **downloads.dell.com**.
2. Download the **catalog.xml.gz** file from the online HTTP from the following location: **http://downloads.dell.com/catalog/catalog.xml.gz** and extract the files.
3. Extract the **catalog.xml** file, and change the **baseLocation** to your local HTTP URL, and compress the file with **.gz** extension.

   For example, change the **baseLocation** from **downloads.dell.com** to **hostname.com**.
4. Place the catalog file with the modified catalog file, and the DUP files in your local HTTP folder replicating the same structure in **downloads.dell.com**.

Viewing update source

To view update source:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**.
2. In **Maintenance Center**, click **Maintenance Settings**, and then click **Update Source**.

Creating update source

Prerequisites:

- Based on the update source type, a Windows or an FTP credential profile is required.
- If you are creating a DRM update source, then ensure that DRM is installed and the Administrator roles are configured.

To create an update source:

1. In **DLCI Console Add-in for SC2012 VMM**, click **Maintenance Center** and then click **Maintenance Settings**.
2. In **Update Source** click **Create New** and provide the required information.
   - If you are creating an FTP source, provide your FTP credentials along with proxy credentials if the FTP site is reachable by using proxy credentials.
   - If you are creating a DRM source, provide your Windows credentials and ensure that the Windows shared location is accessible. In the location field provide the complete path of the catalog file with the file name.

     NOTE: Use only 32–bit DUPs to create the update source in DRM.
   - If you are creating an update source of type HTTP, provide the complete path of catalog with the catalog name and your proxy credentials to access the update source.
3. (Optional) To make it as a default update source select **Make this as default source**.
4. Click **Test Connection** to verify the location of the update source, and then click **Save**.

   NOTE: Once the location is verified, you can create the update source.

Modifying update source

Consider the following when you are modifying an update source:

- You cannot change the type of an update source and the location after the update source is created.
- You can modify an update source even if the update source is in use by an in-progress or a scheduled job, or if it is used in a deployment template. A warning message is displayed while modifying the in-use update source. Click **Confirm** to continue with the changes.

To modify an update source:

Select the update source you want to modify, click **Edit** and update the source as required.

Deleting update source

You cannot delete an update source in the following circumstances:

- The update source is a predefined update source — **Dell Online Catalog** and **DELL ONLINE HTTP CATALOG**.
- The update source is used in a deployment template.
- The update source is being used by an in-progress, or a scheduled job.
- The update source is a default update source.

To delete an update source:

Select the update source you want to delete and click **Delete**.

Update groups

Update groups are a group of servers that require similar update management. There are two types of update groups available, predefined and custom update groups. You can view the predefined groups. However, you can create, and maintain the custom update groups.

NOTE: After upgrading from DLCI for SC2012 VMM version 1.1 to version 1.2, all the servers discovered earlier are added to **Generic update groups** or **Host update groups**. To add the servers into the respective predefined update groups, rediscover the servers.

Predefined update groups

The description and behavior of the predefined update groups are as follows:

- **Generic update groups**
  - **All update groups**
  - **Default unassigned server update groups**
- **Cluster update groups**
- **Host update groups**
  - **Default host update groups**
- **Chassis update groups**

Generic update groups — this group consists of hosts and unassigned servers that are updated in a single session.

All update groups — this group consists of all the server groups. Any group present in the appliance is a member of the all update groups. This group is of the type generic update group.

Default unassigned server update group — this group consists of all the unassigned servers that are not part of any other group. This group is of the type generic update group. The servers are added to the default unassigned server update group after:

- A fresh discovery or rediscovery of bare metal servers.
- A synchronization or resynchronization, after it is deleted from SCVMM but present in the appliance.

Cluster update group — this group consists of Windows Server Failover clusters. If a modular server belongs to a cluster, then it is added to the cluster update group. If a 12th generation or 13th generation of Dell PowerEdge modular server is part of cluster, then the CMC information is also added in the inventory in the **Maintenance Center** page.

To know the cluster update group to which a server belongs to, see the device inventory page where the host name and cluster FQDN is displayed for all the servers listed in the appliance.

Host update group — this group consists of host servers, and updates are applied in a single session, wherein, the single session is updating all servers within the group at once.

Default host update group — this group consists of all the discovered hosts that are not part of any other update group. This group is of the type host update group.

Chassis update group — modular servers belonging to a chassis and not part of any cluster group are classified as chassis update group. 12th generation or 13th generation of Dell PowerEdge servers are discovered along with their CMC information. By default, a group is created with the naming format — **Chassis-Service-tag-of-Chassis-Group** for example, `Chassis-GJDC4BS-Group`. If a modular server is deleted from a cluster update group, then the server is added to the chassis update group along with its CMC information. Even if there are no modular servers in the corresponding chassis update group, since all modular servers in the chassis are in a cluster update group, the chassis update group continues to exist, but displays only the CMC information.

Custom update groups

You can create, modify and delete the custom update groups. However, you can add a server into a custom update group only from **Default unassigned update groups** and **Default host update groups**. After you add a server into a custom update group, the server is removed from the predefined update group and this server is available only in the custom update group. To add the servers in custom update group, search for the servers using their service tag.

Updating methods

You can apply selected updates to selected server groups that are compliant.

- You can perform the following updates on server groups:
  - **Agent-free staged updates** — is staging of firmware updates. The firmware updates that are immediately applicable and that do not require a restart are applied immediately. The remaining updates that require a system restart are applied at the time of restarting the server. Updates are performed in batches at the scheduled time by using iDRAC. The batch size is determined when the update is happening. The appliance assumes that the update is successful when iDRAC reports that the update is successful. The statuses of the updates are not logged in the appliance after the job is submitted to iDRAC. Hence refresh the inventory to check if all the updates are applied. The entire update job fails if the operation fails on even one server.
  - **Agent-free updates** — is out of band update with immediate server restart.
  - **Cluster-Aware Updating (CAU)** — automates the update process by leveraging Windows CAU feature on cluster update groups to maintain server's availability. Updates on servers happen through cluster update coordinator which is present on the same system where Integration Gateway (IG) is installed and not through iDRAC. The updates are not staged and are applied immediately. Using CAU you can minimize any disruption or server downtime allowing continuous availability of the workload. Hence, there is no impact to the service provided by the cluster group. For more information on CAU, see Cluster-Aware Updating Overview section at `technet.microsoft.com`.

Update group notes

- You cannot create, modify or delete the predefined update groups manually.
- You cannot update the CMC firmware directly from the appliance; however, you can update the firmware of the modular server present in CMC. For updating CMC firmware, see — Updating CMC firmware in *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide*. For updating CMC firmware in VRTX, see — Updating firmware in *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide*, and for updating CMC firmware in FX2, see — Updating firmware in *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide*.

Viewing update groups

To view update groups:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center** and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**.

Creating custom update groups

To create custom update groups:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, and then click **Create**.
   The **Firmware Update Group** page is displayed.
3. Provide the details, and select the type of update group that you want to create.
   Custom update groups can have servers only form the following update group types:
   - Generic host update group — consists servers from default unassigned update groups and host update groups.
   - Host update group — consists servers from default host update groups.
4. To add servers in the update group, search for the servers using their service tag, and click **Save**.

Modifying custom update groups

Consider the following when you are modifying a custom update group:

- You cannot change the type of an update group after it is created.
- To move servers from one custom update group to another custom update group:
  - Remove the server from the existing custom update group. Then It is automatically added into the predefined update group.
  - Now edit the custom group to add the server into, and then search for the server using the service tag.

To modify a custom update group:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Edit** to modify the update group.

Deleting custom update groups

Consider the following when you are deleting a custom update group in the following circumstances:

- You cannot delete an update group if it has a job scheduled, in-progress, or waiting.
- You can delete an update group even if servers are present in that update group. However, after deleting such an update group, the servers are moved to their respective predefined update groups.

To delete a custom update group:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Delete** to delete the update group.

Applying updates on servers

You can apply immediate updates or schedule the updates on servers or on a group of servers by creating firmware update jobs. The jobs created for updates are listed under **Job Viewer**. Also, you can downgrade the firmware version to the suggested version by selecting **Allow Downgrade**. If this option is not selected, then there is no action on the component that requires a firmware downgrade.

NOTE:

- You can apply firmware updates on a single component of a server, or to the entire environment.
- If there are no applicable upgrades or downgrades for a server or a group of servers, performing a firmware update on that server or a group of servers cause no action on the server or group of servers.
- When you are updating component level information, if the existing firmware version is same as the firmware version at the update source, then there is no action on that component.

Prerequisites:

- To perform updates on servers, you require an update source available on a Dell online FTP site, local FTP site, HTTP, or Dell Repository Manager (DRM).
- Before applying the updates, clear the iDRAC job queue on the servers where the updates are applied.
- Make sure that the IG user has local administrator privileges on all the cluster nodes.
- Before applying the updates on cluster update groups, check the Cluster Readiness report for the following:
  - Connectivity to update source.
  - Availability of failover clusters.
  - Ensure that Windows Server 2012 or Windows Server 2012 R2 OS is installed on all failover cluster nodes to support the CAU feature.
  - Configuration of automatic updates is not enabled to automatically install updates on any failover cluster node.
  - Enablement of a firewall rule that allows remote shutdown on each node in the failover cluster.
  - Validate the configured Updating Run options. For more information, see Requirements and Best Practices for Cluster — Aware Updating section at technet.microsoft.com.
  - Cluster group should have minimum of two nodes.
  - Check for cluster update readiness. For more information on CAU, see Requirements and Best Practices for Cluster — Aware Updating section at technet.microsoft.com.

NOTE: Make sure there are no major errors and warnings in the report for applying the CAU method.

To apply updates on servers:

1. In DLCI Console Add-in for SC2012 VMM, click **Maintenance Center**, select the server or server group and an update source, and then click **Run Update**.

   NOTE:
   - For a component level update, expand the server groups to its component level, and click **Run Update**.
   - When performing a firmware update for 11th generation of Dell PowerEdge servers, you cannot upgrade the Power Supply Unit (PSU) firmware versions.
2. In **Update Details**, provide the firmware update job name and description.
3. In **Schedule Update**, select one of the following:
   - **Run Now** — to apply the updates now.
   - Select the date and time to schedule a firmware update in future.
4. Select the method for updating by using **Agent-free Update**, or **Agent-free Staged Update**, and then click **Finish**.

NOTE: After submitting a firmware update job to iDRAC, the appliance interacts with iDRAC for status of the job and provides status updates in **Jobs** and **Activity Log** in the Admin Console. Sometimes iDRAC does not provide any status updates on the jobs tracked by the appliance. Appliance waits for maximum 6 hours, and if there is no response from iDRAC then the firmware update job status is considered as failed.

Polling and notification

You can receive notifications when new catalogs are available during system generation and default update sources.

The color of the notification bell is changed to orange color when there is a new catalog file available at the update source. Click the bell icon to replace the locally cached catalog available at the update source. After the latest catalogs are replaced with the old catalogs, the bell color changes to green.

Setting notifications

To set the polling frequency:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, click **Maintenance Settings** and then click **Polling and Notification**.
2. Select how frequently the polling has to happen:
   - **Never** — by default this option is selected. Select to receive updates about new catalogs available at update source only once for the scheduled time.
   - **Once a week** — select to receive updates about new catalogs available at update source on a weekly basis.
   - **Once every 2 weeks** — select to receive updates about new catalogs available at update source once every two weeks.
   - **Once a month** — select to receive updates about new catalogs available at update source on a monthly basis.

Protection vault

Protection vault is a secure location where you can export and import server profiles for a server or a group of servers. You can save this server profile on a shared location in the network by creating an external vault or on a vFlash SD card by creating an internal vault. At one instance, you can associate only one server or a group of servers with one protection vault. However, you can associate one protection vault with many servers or group of servers.

Creating protection vault

Prerequisite: Ensure that the vault location is accessible.
To create a protection vault:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Center**, click **Protection Vault**, and then click **Create**.
3. Select the type of protection vault you want to use and provide the required details.
   - If you are creating a protection vault of type **Network Share**, provide the location to save the profiles, credentials to access this location and a passphrase to secure the profile. And this type of protection vault provides support file sharing of type Common Internet File System (CIFS).
   - If you are creating a protection vault of type **vFlash**, provide the passphrase to secure the profile.

Modifying protection vault

Consider the following when you are modifying a protection vault:

- You cannot modify the name, description, type of protection vault, and passphrase.

To modify a protection vault:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Center**, click **Protection Vault**, and then click **Edit** to modify the vault.

Deleting protection vault

You cannot delete a protection vault in the following circumstances:

- The protection vault is associated with a server or a group of servers.
- There is a scheduled job associated with the protection vault. However to delete such a protection vault, delete the scheduled job, and then delete the protection vault.

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Center**, click **Protection Vault**, and then click **Delete** to delete the vault.

Exporting inventory

In DLCI for SC2012 VMM, you can export the inventory of selected servers and group of server in an `inventory.xml` file. You can save this information in a Windows shared directory or on a management system. Also, you can import this inventory file into DRM and create a repository based on the inventory file and create a reference configuration.

To export firmware inventory of the servers, or server groups while using Internet Explorer version 10 and later, add the console add-in IP address to **Local Intranet** site. To export the inventory file, go to **IE Settings → Internet Options → Advanced → Security**, and clear the **Do not save encrypted pages to disk** option.

When you export the component information of a server, the complete inventory information of the server is exported.

To export the inventory of discovered servers:

In **DLCI Console Add-in for SC2012 VMM**, under **Maintenance Center**, select the servers for which you want to export the inventory, and click **Export Inventory**.

NOTE: After exporting the XML file, to create a repository in DRM, in **My Repositories** click **New**, and then click **Dell Modular Chassis inventory**. In **Modular Chassis Inventory** select the exported XML file from the appliance. For more information on creating a repository see, *Dell Repository Manager* documents available at **dell.com/support/home**.

Viewing and refreshing firmware inventory

You can view and refresh the firmware inventory of Dell-compliant servers after selecting a server or a specific group of servers.

You can view comparison report of server or chassis inventory against a selected update source. You can change the update source, and view the comparison report of inventory information of the selected servers, server groups or chassis against the changed update source.

You can refresh the firmware inventory for a server, a group of servers, or chassis to view the latest information. When you refresh the component information of a server, the complete inventory information of the server is refreshed.

NOTE:

- DLCI for SC2012 VMM version 1.2 is packaged with a catalog that displays an earlier version of the comparison report for the predefined FTP and HTTP update source. Hence, download the latest catalog to display the latest comparison report.
- When you upgrade to this version of DLCI for SC2012 VMM, the latest information is not shown for servers discovered in prior versions. For the latest server information and correct comparison report, rediscover the servers.

To view or refresh firmware inventory for a server or a group of servers:

1. In **DLCI Console Add-in for SC2012 VMM**, under **Maintenance Center** select an update group from **Select Update Group**.
2. (Optional) To change the update source, select an update source from **Select Update Source**.
3. To view firmware information of the current version, baseline version, and update action recommended by appliance, expand the server group from **Device Group/Servers** to the server level, and then to the component level.

   NOTE:
   When viewing component level information, the NIC-related information for the 11th generation of PowerEdge server is displayed as follows:

   - After applying filters based on **Nature of Update** as **Urgent**, a report with the components only with urgent updates are displayed. If this report is exported then components with downgrade action which in turn have critical update is also exported.
   - When there are multiple network interfaces available in a single NIC card, there is only one entry for all the interfaces in the **Component Information** list. Once the firmware update is applied, all the NIC cards are upgraded.
   - When a NIC card is added along with the existing cards, the newly added NIC card is listed as another instance in the **Component Information** list. Once the firmware update is applied, all the NIC cards are upgraded.
4. Select the server or group of servers that you want to refresh, and then click **Refresh Inventory**.

Exporting server profiles

You can export a server profile, including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller and the configuration of those components. The appliance creates a file containing all the configurations, which you can save on a vFlash SD card or network share. Select a protection vault of your choice to save this file. You can export the configuration profiles for a server or a group of servers immediately or schedule it for a later date. Also, you can select the relevant recurrence option as to how frequently the server profiles are exported. At an instance, you can schedule only one export configuration job for a group of servers. You cannot perform any other activity on that server or group of servers whose configuration profiles are being exported.

NOTE:

- Make sure that the **Automatic Backup** job in iDRAC is not scheduled at the same time.
- You cannot export server profiles after applying the filters. To export server profiles, clear all the applied filters.

Creating export jobs

To export the server configurations:
Prerequisites: Disable the **F1/F2 Prompt on Error** option in **BIOS Settings**.

1. In **DLCI Console Add-in for SC2012 VMM**, click **Maintenance Center**, and then click **Export Server Profile**.
2. In **Export Profile**, provide the job details, and then select a protection vault.

   In **Export Server Profile** select:

   - **Run Now** — to export the server configuration immediately of the selected servers, or group of servers.
   - **Schedule** — provide a schedule for exporting the server configuration of the selected group of servers.
     - **Never** — select to export the server profile only once during the scheduled time.
     - **Once a week** — select to export the server profile on a weekly basis.
     - **Once every 2 weeks** — select to export the server profile once every two weeks.
     - **Once every 4 weeks** — select to export the server profile once every four weeks.

Canceling export server configuration jobs

To cancel an export job:

1. In **DLCI Console Add-in for SC2012 VMM**, click **Maintenance Center**, and then click **Manage Jobs**.
2. Select **Export and Import Jobs** from the filter, select the jobs you want to cancel and make sure that the job is in **Scheduled** state.
3. Click **Cancel**, and then click **Yes**.

Importing server profile

You can import a server profile which was previously exported for that same server, or group of servers. Importing server profile is useful in restoring the configuration and firmware of the server to the state stored in the profile. In such cases, you can replace the server profile on that server, or group of servers by importing a previously exported server profile of that server or group of servers.

You can import server profiles in two ways:

- Quick import server profile — allows you to automatically import the latest exported server profile for that server. You need not select individual server profiles for each of the servers for this operation.
- Custom import server profile — allows you to import server profiles for each of the individually selected servers. For example, if exporting server profile is scheduled, and the server profile is exported every day, this feature allows you to select a specific server profile that is imported from the list of server profiles available in the protection vault of that server.

Import server profile notes:

- You can import a server profile from the list of exported server profiles for that server only. You cannot import the same server profiles for different servers or server groups. If you try to import server profile of another server or server group, the import server profile job fails.
- If a server profile image is not available for a particular server or group of servers, and an import server profile job is attempted for that particular server or group of servers, the import server profile job fails

for those particular servers that do that have server profile and a log message is added in the Activity logs with the details of the failure.

- After exporting a server profile, if any component is removed from the server, and then an import profile job is started, all the components information are restored except the missing component information is skipped. This information is not available in the activity log of DLCI for SC2012 VMM. To know more about the missing components, see iDRAC's **LifeCycle Log**.
- You cannot import a server profile after applying the filters. To import server profiles, clear all the applied filters.

Importing server profile

To import inventory of discovered servers:

1. In **DLCI for SC2012 VMM**, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import Server Profile**.
2. Provide the required details, select the **Import Server Profile Type** you want, and then click **Finish**.

   NOTE: Clear the **Preserve Data** option if you do not want to preserve the present RAID configurations of the server.

Manage jobs

All the firmware update, export and import server configuration jobs are listed with their status information. Also, you can cancel only the scheduled jobs.

Canceling firmware update jobs

Prerequisites: Make sure that the job is in **Scheduled** state.
To cancel a scheduled firmware update job:

1. In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Manage Jobs**.
2. Select the jobs that you want to cancel, click **Cancel**, and then click **Yes**.

9

Profiles and templates

About credential profile

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of the user. Each credential profile contains a user name and password for a single user account. A credential profile authenticates a user's role-based capabilities. The appliance uses credential profiles to connect to the managed systems' iDRAC.

Also, you can use credential profiles to access the FTP site, resources available in Windows Shares, and when working with different features of iDRAC.

You can create four types of credential profiles:

- Device Credential Profile — this profile is used to log in to iDRAC or Chassis Management Controller (CMC).

  NOTE:

  – When no default profile is created or selected, the default iDRAC factory setting is used. The default user name as `root` and password as `calvin` is used.

    * The default iDRAC profile is used to access the server when you discover a server or perform synchronization.

  – The default CMC profile has user name as `root` and password as `calvin`, and is used to access the modular server to get information about the chassis.

  – Use the device type credential profile to discover a server, log in to CMC, resolve synchronization issues, and deploy operating system.
- Windows Credential Profile — This profile is used for accessing Windows Shares while creating a DRM update source.
- FTP Credential Profile — This profile is used for accessing an FTP site.
- Proxy Server Credentials — This profile is used for providing proxy credentials for accessing any FTP sites for updates.

Predefined credential profiles

SYSTEM DEFAULT FTP account is a predefined credential profile of the type FTP credentials having **Username** and **Password** as **anonymous**. It is not editable. This profile is used to access `ftp.dell.com` .

Creating credential profile

Consider the following when you are creating a credential profile:

- When a device type credential profile is created, an associated **RunAsAccount** is created in **SC2012 VMM** to manage the server and the name of the RunAsAccount is `Dell_CredentialProfileName`.

  - (Recommended) Do not edit or delete the **RunAsAccount**.
- When no credential profiles are created and no default credential profile for iDRAC is available; During auto discovery, the default iDRAC factory setting credential profile is used. The default username as **root** and password as **calvin** is used.

To create a credential profile:

1. In DLCI Console Add-in for SC2012 VMM, do any of the following:
   - In the dashboard, click **Create Credential Profile**.
   - In the navigation pane, click **Profiles and Templates** → **Credential Profile**, and then click **Create**.
2. In **Credential Profile**, select the credential profile type that you want to use and provide user credential details and then click **Finish**.

   NOTE: When creating **Device Credential Profile** select **iDRAC** to make it as default profile for iDRAC, or **CMC** to make it default for Chassis Management Controller (CMC). Select **None** if you chose to not set this profile as a default profile.

Modifying credential profile

Consider the following when you are modifying a credential profile:

- Once created, you cannot modify a credential profile's type. However, you can modify other fields. Refresh screen to view the modifications.
- You cannot modify a device type credential profile that is used for hypervisor deployment.

To modify a credential profile:

Select the credential profile you want to modify, click **Edit** and update the profile as required.

Deleting credential profile

Consider the following when you are deleting a credential profile:

- When a device type credential profile is deleted, the associated **RunAsAccount** from SC2012 VMM is also deleted.
- When the **RunAsAccount** in SCV2012 VMM is deleted, the corresponding credential profile is not available in the appliance.
- To delete a credential profile that is used in server discovery, delete the discovered server information and then delete the credential profile.
- To delete a device type credential profile that is used for deployment, first delete the servers deployed in SCVMM environment and then delete the credential profile.
- You cannot delete a credential profile if it is used in an update source.

To delete a credential profile:

Select the profile that you want to delete, and then click **Delete**.

Creating hardware profile

You can create a hardware profile by using a server with golden configuration and then using that profile to apply hardware configurations to managed systems.

Before you apply hardware configurations to managed systems, confirm that the managed systems are identical to the server with the golden configuration on the following parameters:

- Components available
- Server model
- RAID controller
- Disks:
  - Number of disks
  - Size of disks
  - Type of disks

NOTE: Once you upgrade from DLCI for SC2012 VMM version 1.0.1 to version 1.2, edit and save the hardware profiles created in DLCI for SC2012 VMM version 1.2 before you apply them on servers.

To create a hardware profile:

1. In the DLCI Console Add-in for SC2012 VMM page, do any of the following:
   - In the dashboard, click **Create Hardware Profile**.
   - In the navigation pane, click **Profiles and Templates** → **Hardware Profile**, and then click **Create**.
2. In the **Hardware Profile** welcome screen, click **Next**.
3. In **Profile**, provide the profile name and description, and the iDRAC IP of the reference server, and then click **Next**.

   The the hardware details of the reference server are collected and saved as the required profile. During deployment, this profile is applied to the servers.
4. In **Profile Details**, select the BIOS, boot, and RAID settings, and customize DHS based on the requirement and then click **Next**.

   NOTE:

   Irrespective of your selection preferences, all information is gathered during hardware profile creation; However, during deployment, only your preferences are applied.

   For example, if you have selected a RAID setting, then all the information on BIOS, boot and RAID settings are gathered; However, during deployment only the RAID settings are applied.
5. In **Summary**, click **Finish**.

   You can use this hardware profile and apply it to required managed systems.

Modifying hardware configuration profile

Consider the following when you are modifying a hardware configuration profile:

- You can modify the BIOS settings and boot order.

- For 11th and 12th generation of PowerEdge servers, you can modify DHS for RAID as **One** or **None** and for 13th generation of PowerEdge servers you can retain only the existing RAID settings of the server.

To modify a hardware configuration profile:

1. In DLCI Console Add-in for SC2012 VMM, click **Hardware Profile**.
2. Select the profile that you want to modify and click **Edit**.
3. Make the required changes and click **Finish**.

Deleting hardware profile

Consider the following when you are deleting a hardware profile:

- If you delete a hardware profile, the deployment template associated with this hardware profile is updated.

To delete a hardware configuration profile:

1. In DLCI Console Add-in for SC2012 VMM, click **Hardware Profile**.
2. Select the hardware profile that you want to delete and click **Delete**.

Creating hypervisor profile

You can create a hypervisor profile and use the profile to deploy the operating system on the servers. A hypervisor profile contains a customized WinPE ISO (WinPE ISO is used for hypervisor deployment), host group and host profile taken from SC2012 VMM, and LC drivers for injection.
Prerequisites:

- The required WinPE ISO is created and the ISO is available in the share folder of DLCI Integration gateway for SC2012 VMM. To update WinPE image, see WinPE image update.
- In SC2012 VMM, a Host group, a Host profile, or physical computer profile is created.

To create a hypervisor profile:

1. In DLCI Console Add-in for SC2012 VMM, do any of the following:
   - In dashboard, click **Create Hypervisor Profiles**.
   - In the left navigation pane, click **Profiles and Templates**, click **Hypervisor Profiles**, and then click **Create**.
2. In the **Hypervisor Profile Wizard**, **Welcome** page, click **Next**.
3. In **Hypervisor Profile**, provide a name and description for the profile, and then click **Next**.
4. In **SC2012 VMM** information page, provide the **SC2012 VMM Host Group Destination** and **SC2012 VMM Host Profile/Physical Computer Profile** information.
5. In **WinPE Boot Image Source**, provide the **<Network WinPE ISO file name>.iso** information, and then click **Next**.
6. (Optional) To enable LC driver injection; if enabled, select the operating system that you want to deploy so that the relevant drivers are picked up. Select **Enable LC Drivers Injection** and in **Hypervisor Version**, select the required hypervisor version.
7. In **Summary**, click **Finish**.

Modifying hypervisor profile

Consider the following when you are modifying a hypervisor profile:

- You can modify host profile, host group, and drivers from Lifecycle Controller.
- You can modify the WinpE ISO name; however, you cannot modify the ISO.

To modify a hypervisor profile:

1. In DLCI Console Add-in for SC2012 VMM, in **Hypervisor Profile**, select the profile that you want to modify and click **Edit**.
2. Provide the details and click **Finish**.

Deleting hypervisor profile

Consider the following when you are deleting a hypervisor profile:

- If a hypervisor profile is deleted, then the deployment template associated with the hypervisor profile is also deleted.

To delete a hypervisor profile:

In DLCI Console Add-in for SC2012 VMM, in **Hypervisor Profile**, select the profile that you want to delete and click **Delete**.

WinPE Update

A PreExecution Environment (PXE) server of SC2012 VMM is required for creating a WinPE image. A WinPE ISO is created from the WinPE image and Dell OpenMange Deployment Toolkit (DTK).

NOTE: While using the latest version of DTK for creating a WinPE ISO image, use the **Dell OpenManage Deployment Toolkit for Windows** file. The **Dell OpenManage Deployment Toolkit for Windows** file contains the necessary firmware versions required for systems on which you are deploying the operating systems. Use the latest version of the file, and do not use the **Dell OpenManage Deployment Toolkit Windows Driver Cabinet** file for WinPE update.

To create a WinPE ISO image:

1. Add the PXE server to the appliance.
2. After adding the PXE server, copy the **boot.wim** file from the PXE server to DLCI Integration Gateway for SC2012 VMM share WIM folder. The **boot.wim** is present in the following path: **C:\RemoteInstall \DCMgr\Boot\Windows\Images**.

   NOTE: Do not change the filename of the **boot.wim** file.

DTK is a self-extracting executable file.

To work with DTK:

1. Double click the DTK executable file.
2. Select the folder to extract the DTK drivers, for example **C:\DTK501**.
3. Copy the extracted DTK folder to the Integration Gateway's DTK share folder. For example **\\DLCI IG Share\DTK\DTK501**.

NOTE: If you are upgrading from SC2012 VMM SP1 to SC2012 VMM R2, then upgrade to Windows PowerShell 4.0. and create a WinPE ISO image.

To update a WinPE image:

1. In DLCI Console, select **WinPE Update**, under **Image Source**, for **Custom WinPE Image Path**, provide the WinPE image path.

   For example, \\DLCI IG Share\WIM\boot.wim.
2. Under **DTK Path**, for **DTK Drivers Path**, provide the location for the Dell Deployment Toolkit drivers.

   For example, \\DLCI IG Share\DTK\DTK501.
3. Provide ISO name.
4. To view the job list, select **Go to the Job List**.

   A unique job name is assigned to each Windows Preinstallation Environment (WinPE) update.
5. Click **Update**.

   WinPE ISO with the name provided in the preceding step is created under \\DLCI IG Share\ISO.

About hypervisor deployment

Hypervisor deployment is a profile-based workflow. This workflow enables you to specify hardware configurations, hypervisor configurations, SC2012 VMM configurations, and update source for firmware updates. Also, you can continue with hypervisor deployment even if the firmware update fails. However, all the components of the selected servers or groups of servers get updated during hypervisor deployment. This workflow uses logical network and host profile available in SCVMM required at the time of creation of hypervisor profile along with hardware configuration for hypervisor deployment in the appliance. Hypervisor deployment supports one-to-one and one-to-many deployment.

Creating deployment template

You can create deployment templates with the required hardware and hypervisor profile and an update source and apply the deployment template to unassigned servers. It enables you to create the template once and use it multiple times.
To create a deployment template:

1. In the appliance, do any of the following:
   - In the appliance dashboard, click **Create Deployment Template**.
   - In the appliance navigation pane, click **Profiles and Templates**, and then click **Deployment Template**.
2. In **Deployment Template**, enter the template name and template description, and then select a hypervisor profile, hardware profile, and update source.
3. (Optional) Select an update source, a hardware profile, and to continue with deployment even if firmware update fails select **Continue OSD even if firmware update fails**.

   NOTE: By default downgrade is not supported.
4. (Optional) If the hardware or hypervisor profile is not created, you can create the profiles by clicking **Create New**.

Modifying deployment template

NOTE: You can modify the name, description, and selection of hypervisor profile, hardware profile, and update source.

To modify a deployment template:

1. In DLCI Console Add-in for SC2012 VMM, click **Deployment Templates**.
2. Select the deployment template that you want to modify and click **Edit**.
3. Make the required changes and click **Finish**.

Deleting deployment template

NOTE: Deleting a deployment template does not impact the associated hardware, hypervisor profiles and update source.

To delete a deployment template:

1. In DLCI Console Add-in for SC2012 VMM, click **Deployment Templates**.
2. Select the deployment template that you want to delete, and click **Delete**.

10

Deploying hypervisors

Operating systems are deployed only on servers that are compliant.

Before hypervisor deployment, consider the following: upgrade the firmware versions to the latest versions available at **ftp.dell.com** or **downloads.dell.com**, and then continue with hypervisor deployment.

To deploy to servers:

1. In the appliance do the following:
   - In the appliance dashboard, click **Deploy Unassigned Servers**.
   - In the appliance navigation pane, click **Deployment Wizard**.
2. In **Welcome**, click **Next**.
3. In **Select Servers**, select the servers to which you want to deploy, and check for available licenses and then click **Next**.
4. In Select **Template and Profile**, select the appropriate deployment template and the associated device type credential profile.

   NOTE: You can assign multiple credential profiles to multiple servers.

   You can also create a deployment template and a credential profile.
5. In **Server Identification**, select servers and provide host name, MAC address and network information either static or DHCP that you want to apply to the servers, and then click **Next**.
6. In **Job Details**, provide a job name to track the job and the deployment status and click **Next**.
7. In **Summary**, view the deployment options you have provided and click **Finish**.
8. In the **Confirmation** message, click **Yes**.

11

Viewing information in appliance

Viewing job status

To quickly search and view logs for a particular update job from among the logged messages, see the timestamp of the update job log messages. You can view the jobs from the DLCI Admin Portal — SC2012 VMM and DLCI Console Add-in for SC2012 VMM.

1. In the left navigation pane, click **Jobs**.
2. From Filter, based on the jobs you want to view, select **Deployments**, **Firmware Update**, **Discovery Jobs**, **WinPE Creation Jobs**, **Sync Jobs** or **Export and Import Jobs**.

Viewing managed jobs

To view the firmware update jobs:

In **DLCI for SC2012 VMM**, click **Maintenance Center**, and then click **Manage Jobs**.

Viewing activity logs

The appliance logs information about all the activities that happen in the appliance in activity log. You can view the detailed status of the jobs such as how many servers and which all servers are pending in a job and so on. To know information about a failed job, you can view the activity log.
To view activity log information:

1. In DLCI Admin Portal — SC2012 VMM, click **Activity Log**.
2. To refresh the page for information on the latest activities, click **Refresh**.

Viewing appliance logs

Displays a web page with the list of files that contain logged information on the activities that have occurred in DLCI for SC2012 VMM.
To view the appliance logs:

In DLCI admin portal — SC2012 VMM, click **Settings** → **Logs**.

NOTE: You can view the firmware update LC logs under `lifecyclecontrollerlogs dir`. However, for 11th generation of Dell PowerEdge servers, there is no entry in LC logs for firmware update jobs in iDRAC.

12

Troubleshooting

Account deletion in SC2012 VMM

SC2012 VMM creates an account for the appliance with the name **DLCI-VMM Addin Registration Profile**. If this profile is deleted, then you cannot work with the appliance.

Recommend you to not delete the account. However, reinstall the appliance if the account is deleted.

Comparison report not displayed in Maintenance Center

If the update source is created using 64-bit DUPs, and this update source is used to generate the comparison report, then you cannot view the comparison report in **Maintenance Center** as there is no support for update source creation using 64-bit DUPs.

As a workaround, use 32–bit DUPs for creating an update source.

Compatibility issue of appliance with ADK

Any existing functionality of DLCI for SC2012 VMM may fail after installing a software with an incompatible version of ADK.

As a workaround, upgrade the ADK version as per the prerequisites mentioned in *Dell Lifecycle Controller Integration for Microsoft System Center 2012 Virtual Machine Manager Installation Guide*.

Empty cluster update group does not get deleted during autodiscovery or synchronization

When a cluster group is discovered in the appliance, a cluster update group gets created in the **Maintenance Center** with all the servers listed in the cluster update group. Later, if all the servers are removed from this cluster through SCVMM, and an autodiscovery or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Maintenance Center**.

As a workaround, to delete the empty server group, rediscover the servers.

Discovery jobs not submitted

When you press the backspace key to dismiss an error message on the discovery screen, subsequent discovery jobs are not submitted for backend processing.

As a workaround, close the current discovery screen and relaunch the discovery screen from the **Inventory** page. Submit the new discovery job after entering the required inputs.

Duplicate VRTX chassis group gets created

When modular servers that were previously in another chassis are added to a VRTX chassis and discovered, the modular servers carry previous chassis service tag information and create a duplicate VRTX chassis group in the appliance.

To resolve, do the following:

1. Remove a modular server from one chassis, and add it in another chassis. For more information, see Server modules section in *Dell PowerEdge VRTX Enclosure Owner's Manual*.
2. Configure CMC. For more information, see Installing and Setting Up CMC in *Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX User's Guide*, available at dell.com/support /home.

After you do the preceding tasks, if there are duplicate chassis group entries, then as a workaround, do the following:

1. Enable CSIOR and reset iDRAC on the newly added modular server.
2. Manually delete all the servers in the VRTX chassis group, and then rediscover the servers.

Exporting configuration profile of another server after IP address is changed

After an **Export Server Profile** job on a server is scheduled, if the IP address of this server is assigned to another server, then the appliance exports the server profile of this new server.

As a workaround, cancel the **Export Server Profile** job, rediscover the server whose IP address has changed, and then schedule the **Export Server Profile** job on this server.

Error accessing the appliance after changing network configuration

After setting up the appliance, if the network settings are changed, then the appliance may not reflect the changes.

As a workaround, to apply these changes restart the appliance.

Error accessing plugin after updating SCVMM R2

If DLCI for SC2012 VMM plugin is installed, and then you apply Update Rollup 8 for SC2012 R2 VMM, then there is an error displayed by SCVMM for security reasons. As a result you cannot access the DLCI for SC2012 VMM plugin.

As a workaround, do the following:

1. Delete the folder at default path: C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>.
2. Close and then open SCVMM.

3. Uninstall and then reimport the Console Add-in as mentioned in *Dell Lifecycle Controller Integration for Microsoft System Center 2012 Virtual Machine Manager Installation Guide*.

Failure to connect to server

After installing the DLCI for SC2012 VMM console addin in SCVMM environment, on clicking the DLCI console icon the following error is displayed: `Connection to server failed`.

As a workaround, do the following:

- Add the appliance IP and FQDN as a trusted site.
- Add the appliance IP and FQDN in **Forward Lookup Zones** and **Reverse Lookup Zones** in DNS.
- Check if there are any error messages in **C:\ProgramData\VMMLogs\AdminConsole** file.

Failure of creation of update source

When the Domain Name System (DNS) network configuration of the appliance is changed, creation of HTTP or FTP type of update source fails.

As a workaround, restart the appliance, and then create the update source of type HTTP or FTP.

Failure of firmware update on cluster update group

After scheduling a firmware update job on a cluster update group, if the firmware update job fails for various reasons such as IG is unreachable, the cluster group becomes unresponsive, or the firmware update job was canceled in CAU for an in-progress job, the DUPs are downloaded and placed in each server cluster node belonging to the cluster group. All the DUP files are placed under the folder called Dell consuming memory.

As a workaround, delete all the files in Dell folder, and then schedule a firmware update job.

Failure of a scheduled job on an update group

After scheduling a job on an update group, if all the servers are moved out of the update group and there are no servers present in the update group then, the scheduled job fails.

As a workaround, cancel the scheduled job, add the servers to another update group, and then schedule a job on the update group.

Failure of firmware update because of job queue being full

Firmware update jobs submitted from the appliance to iDRAC fail, and the appliance main log displays the following error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

As a workaround, manually delete the completed jobs in iDRAC, and retry the firmware update job. For more information on deleting jobs in iDRAC, see iDRAC documentation at **dell.com/support/home**.

Failure to connect to FTP using system default update source

After setting up and configuring, or upgrading the appliance, trying to access the FTP site using system created update source **Dell Online Catalog** might fail if proxy credentials are required.

To access the FTP site using **Dell Online Catalog** as an update source edit, and add the proxy credentials.

Failure to create a repository during a firmware update

Creation of a repository may fail during a firmware update because of network issues, improper credentials, or server not reachable, and so on.

As a workaround, ensure that the FTP server is reachable from where the appliance is hosted, there are no network issues, and provide the right credentials during a firmware update.

Failure to delete a custom update group

After scheduling a job on a server belonging to a custom update group, if the server is deleted from SCVMM and synchronization is done, the server is removed from the custom update group and is moved to the appropriate predefined group. You cannot delete such custom update groups, because it is associated with a scheduled job.

As a workaround, to delete this custom update group, delete the scheduled job from jobs page, and then delete the custom update group.

Failure to export server profiles

After scheduling an export server profile job, the server profile is not exported, and the following error message is displayed: "The selectors for the resource are not valid".

As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see iDRAC documentation available at **dell.com/support**.

Firmware update on a few components irrespective of the selection

Same components on identical servers get updated during a firmware update irrespective of the selection of components made on individual servers. This behavior is seen for 12th and 13th generation of Dell PowerEdge servers with Enterprise license of iDRAC.

As a workaround, do one of the following:

- To prevent irrelevant updates on identical servers, apply common components on identical servers and then apply specific components separately on individual servers.
- Perform staged updates with planned outage times to accommodate the required firmware update.

IG installation issue while running multiple instances of the installer on the same server

After you start installing the IG, if you try running another instance of the IG, then an error message is displayed. After you click OK, you are prompted to save another IG MSI file.

As a workaround, do not save this file and continue with the first installation.

Importing server profile job gets timed out after two hours

After submitting the import server profile job in the appliance, it may get timed out after two hours.

As a workaround, perform the following steps:

1. Press F2 and enter **BIOS Settings**.
2. Click **System Setup** and select **Miscellaneous Settings**.
3. Disable **F1/F2 Prompt on Error**.

After performing the following steps, schedule the export server profile job and use the same to complete the import server profile job successfully.

Hypervisor deployment failure

Hypervisor deployment is failing and the activity log displays the following error: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

This error may occur due to either of these reasons:

- Dell Lifecycle Controller's state is bad.

  As resolution, log in to iDRAC user interface and reset Lifecycle Controller.

  After resetting Lifecycle Controller, if you still face the problem try the following alternative.
- The anti-virus or firewall may restrict the successful run of the WINRM command.

  See the following KB article for workaround: support.microsoft.com/kb/961804.

Hypervisor deployment failure due to driver files retained in library share

Hypervisor deployment is failing and the activity log displays the following error:

- **Error:** `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information:** `Successfully deleted drivers from library share sttig.tejasqa.com for <server uuid>`
- **Error:** `Deleting staging share (drivers) for <server uuid> failed.`

These errors may occur due to exception output by the VMM command-let `GET-SCJOB status` and driver files are retained in the library share. Before you retry or do another hypervisor deployment you must remove these files from the library share.

To remove files from library share:

1. From SC2012 VMM Console, select **Library** → **Library Servers** and then select the Integration Gateway server that was added as the library server.
2. In the library server, select and delete the library share.
3. After the library share is deleted, connect to the Integration Gateway share using **\\<Integration Gateway server>\LCDriver**.
4. Delete the folder that contains the driver files.

Now, you can deploy operating systems.

Latest inventory information is not displayed even after firmware update

Even though the firmware update job is complete on an 11th generation of Dell PowerEdge server, in the appliance, the inventory does not display the latest firmware versions.

In the appliance, refreshing the inventory is an activity performed immediately after a firmware update job is complete. Firmware update is completed even before the PowerEdge server's CSIOR activity is complete, due to which the earlier firmware inventory information is displayed.

As a workaround, check if the CSIOR activity is complete in the PowerEdge server, and then in the appliance, refresh the firmware inventory. Also, make sure to restart the server after applying agent-free staged update. For more information on refreshing the inventory, see Viewing and refreshing firmware inventory.

For more information on CSIOR, refer to the Troubleshooting section in the latest version of the *Dell Lifecycle Controller GUI User's Guide* available at **dell.com/support/home**.

SC2012 VMM error 21119 while adding servers to active directory

While adding servers to Active Directory, SC2012 VMM error 21119 is displayed. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

As a workaround, do the following:

1. Wait for some time to see if the server is added to the Active Directory.
2. If the server is not added to the Active Directory, then manually add the servers to the Active Directory.
3. Add the server in to SC2012 VMM.
4. Once the server is added in to SC2012 VMM, rediscover the server in the DLCI Console.

   The server is listed under the **Host** tab.

Connection lost between appliance and Integration Gateway

When you restart the server in which Integration Gateway is installed, connectivity is lost between the appliance and Integration Gateway. This is because the execution policy of the Integration Gateway for the user is not active. Log in to the Integration Gateway server using the Integration Gateway user account to make the execution policy active. However, after login the connection is not restored until the following steps are completed.
To set the PowerShell execution policy:

1. Set PowerShell execution policy for local system as `RemoteSigned` and for the **Integration Gateway Service Account** as `Unrestricted`.

   For information on policy settings, refer the following MSDN articles:

   - **PowerShell Execution policy**: technet.microsoft.com/en-us/library/hh847748.aspx
   - **PowerShell Group Policy**: technet.microsoft.com/library/jj149004
2. Once the execution policy is set, restart the Integration Gateway server.

Hypervisor deployment fails for 11th generation PowerEdge blade servers when using Active Directory

Hypervisor deployment fails on the 11th generation PowerEdge blade servers when using the Active Directory user credentials. The 11th generation PowerEdge blade servers use the Intelligent Platform Management Interface (IPMI) protocol for communication. However, the IPMI standard is not supported for using credentials from the Active Directory setup.
As a workaround to deploy operating systems on these servers, use supported credential profiles.

RAID configuration failure for virtual disks with RAID10

RAID configuration fails when virtual disks are created with RAID level 10 for controller H200 using more than four physical disks.
RAID 10 with more than four physical disks fail.

As a workaround, use minimum number of physical disks required for that RAID level.

Configuration of RAID failure due to configuration of hot spares on software RAID S130

RAID configuration on software RAID controller S130 fails when we try to configure RAID with more than three hot spares including the Global Hot Spare (GHS) and DHS.
As a workaround:

- Use only three hot spares (GHS and DHS) to apply on a profile.
- Use the PowerEdge RAID controller (PERC) card.

13

Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Enterprise Systems Management documents — Dell.com/SoftwareSecurityManuals
  - For OpenManage documents — Dell.com/OpenManageManuals
  - For Remote Enterprise Systems Management documents — Dell.com/esmmanuals
  - For OpenManage Connections Enterprise Systems Management documents — Dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Serviceability Tools documents — Dell.com/ServiceabilityTools
  - For OpenManage Connections Client Systems Management documents — Dell.com/DellClientCommandSuiteManuals
- From the Dell Support site:
  a. Go to Dell.com/Support/Home.
  b. Under **Select a product** section, click **Software & Security**.
  c. In the **Software & Security** group box, click the required link from the following:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Serviceability Tools**
     - **Dell Client Command Suite**
     - **Connections Client Systems Management**
  d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.