Dell Lifecycle Controller Integration Version 1.1 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.

2015 - 08

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 and 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.

New features

The features for this release are as follows:

- Simplified licensing — to manage licenses, you do not require Dell Connections License Manager (DCLM). More information on licensing is available under **License Center** in Admin portal.
- New credential profile types:
  - Device credential profile — use to login to integrated Dell Remote Access Controller (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 the 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.
- Update 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. In this release, we support update management of 11th generation to 13th generation of Dell PowerEdge servers.
  - Key features in update 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.
    * Refresh and export firmware inventory — refresh firmware inventory and export the inventory details in an `xml` format.
    * Applying updates — apply firmware updates immediately or schedule updates.

    * Applying specific updates — apply only specific component updates, or apply the latest update available on Dell FTP.
    * Apply updates before operating system deployment — before an operating system deployment, apply firmware updates using a selected update source.
  - Remotely update servers (one — to — one or one — to— many) for the latest firmware versions for the following:
    * Basic Input Output System (BIOS)
    * Network Interface Controller (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 using Dell Repository Manager (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.

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 for 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 — ensure that the Dell servers are compliant.

  Compliance of Dell servers — 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, refer to *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 Redundant Array of Independent Disks (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.

- Leverage 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.

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, you must 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 **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 **Destination Folder** window, by default an installation folder is selected. To change location, click **Change**, complete the changes, and then click **Next**.
7. On **Ready to Install the Program** page, click **Install**.
8. On **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, you must import DLCI Console into the VMM Console.
Prerequisites: For the connection with 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: You can select any host group you have access to, to launch DLCI console.
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**, 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 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 login 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 using the user credentials provided while configuring the appliance.

DLCI admin portal — SC2012 VMM

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

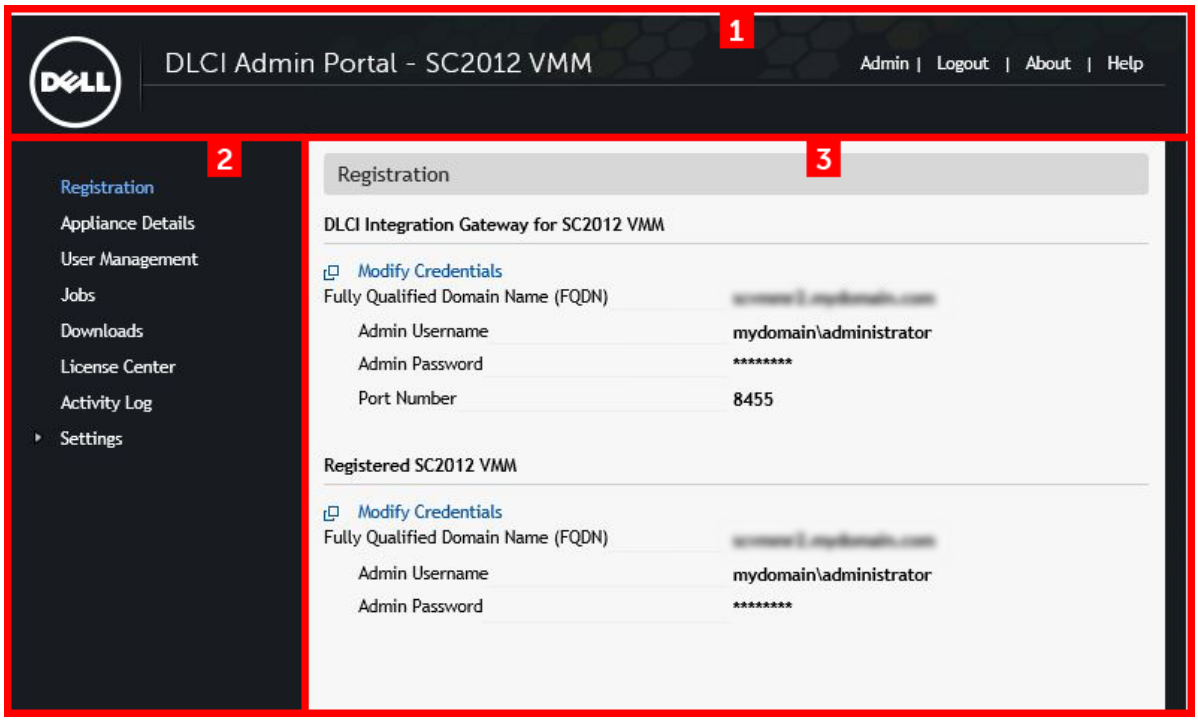


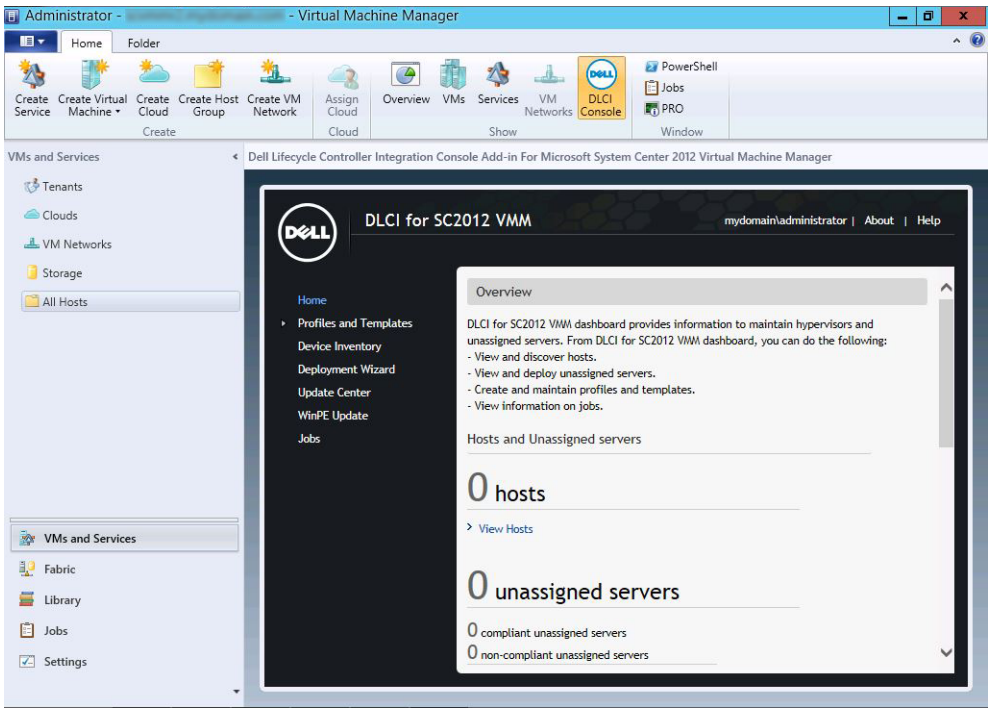
Figure 1. DLCI admin portal — SC2012 VMM

1. Heading banner includes the product name and the following options:
   - **Admin** — displays information about the user who has logged into DLCI for SC2012 VMM – Admin Portal.
   - **Logout** — enables you to log out 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. Navigation pane contains the following options and for more information about each option refer the online help:
   - **Registration**
   - **Appliance Details**
   - **User Management**
   - **Jobs**
   - **Downloads**
   - **License Center**
   - **Activity Log**
   - **Settings**
     - **Service Pack Updates**
     - **Logs**
3. 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

DLCI console Add-in user interface contains the following options:

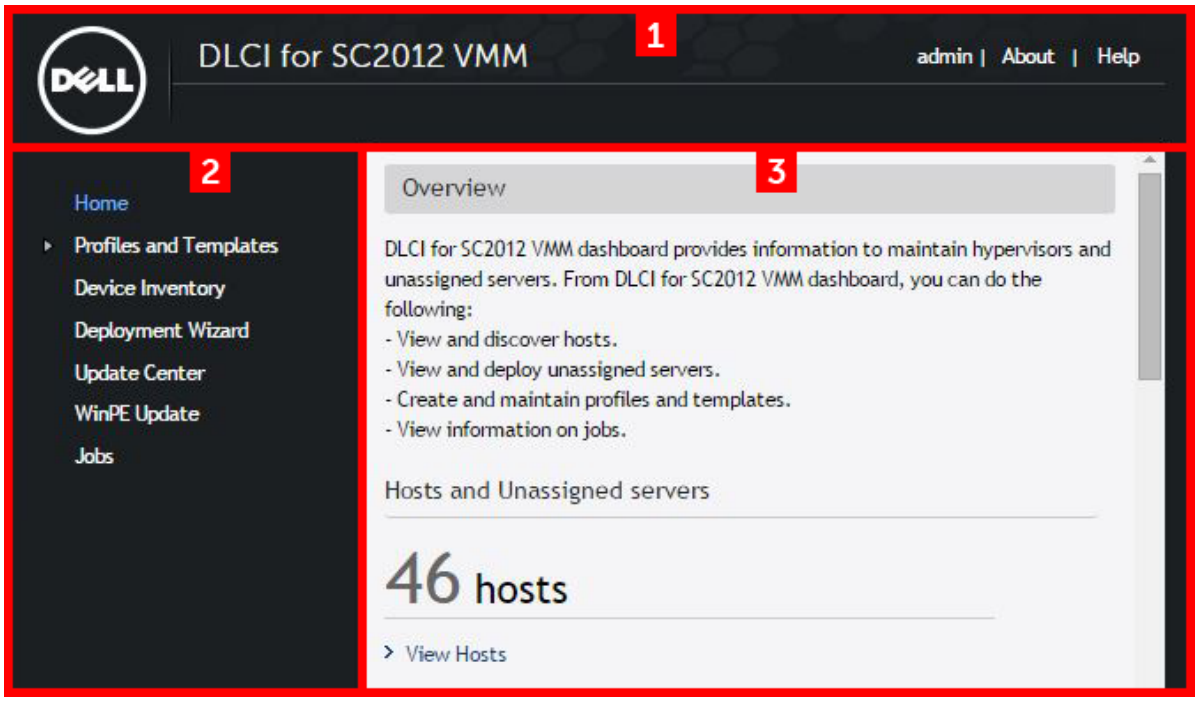


Figure 2. DLCI console add-in for SC2012 VMM

1. Heading banner includes the product name and the following options:
   - **<Domain>\adminstrator** — Displays information about the user who is logged into DLCI for SC2012 VMM.
   - **About** — Provides information about the DLCI for SC2012 VMM version.
   - **Help** — Launches the context sensitive online help.
2. 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**
   - **Update Center**
   - **WinPE Update**
   - **Jobs**
3. 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 will display the home page.

4

Workflows

This section contains the following workflows:

- Creating golden configurations
- Creating and managing credential profiles
- Creating and managing update sources
- Applying updates on servers or server groups
- Hypervisor deployment
- Deleting servers

About golden configurations

A server configured 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, you must 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.

Applying updates on servers or server groups

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

- Local FTP and online FTP source
- 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 required server groups are selected to apply the updates. For information, see Applying updates on servers.

Hypervisor deployment

Using appliance, you can perform firmware update and hypervisor deployment based on the golden configuration. You can leverage 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 hardware profiles
4. Creating hypervisor profiles
5. Creating deployment templates

6. (Optional) Applying updates on servers
7. Deploying hypervisors

Deleting servers

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

5

Setting up 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 hardware profile. For more information see, Creating a hardware profile.
8. Create a hypervisor profile. For more information see, Creating a hypervisor profile.
9. Create a deployment template. For more information see, Creating a deployment template.
10. 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.
11. 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, login 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. Refer to the *Integrated Dell Remote Access Controller* documentation for information about configuring the server.

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, modular hyper-v hosts along with unassigned servers and 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, having an operating system deployed on it, and present in SCVMM, then the server is listed as a host server. And marked as compliant or noncompliant.
  - 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 chassis 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 a 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 (including Microsoft hyper-v hosts, modular hyper-v hosts), note the following 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 value 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 Integrated Dell Remote Access Controller Utility, press **CTRL + E**.
3. Select **System Services** from the options available 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 appliance, create a device type credential profile (by specifying the iDRAC credentials and mark 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 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, you must 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.
4. (Optional) click **Create New** to create a credential profile.
5. For **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.
6. 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**.
7. 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, then you must 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 so on.

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

- Discover servers
- Refresh server information
- Deleting servers from DLCI console
- Synchronization with SC2012 VMM
- Resolve synchronization errors
- Correlate host servers to cluster group and the chassis to which the server belongs to
- Launch iDRAC console

If the unassigned server is a modular server, then the chassis service tag is added in 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.

Consider the following when you are viewing device inventory:

- If 11th and 12th generation of Dell PowerEdge servers are discovered and inventoried in DLCI for SC2012 VMM version 1.0 and you are upgrading to version 1.1, then in the **Device Inventory** page, the already discovered servers appear as non-compliant; Hence to make the servers compliant, rediscover the servers.

To view servers:

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

Synchronization with SC2012 VMM

Use to synchronize all Dell hyper-v hosts, hyper-v host clusters, and modular hyper-v hosts in the SC2012 VMM environment with the appliance. 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 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 resynchonised, 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 chassis 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 with DLCI for SC2012 VMM

To perform a 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 credentials, iDRAC, connectivity, or other issues respectively, 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 a new credential profile.
3. Provide a job name and select the **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**, for a server, 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

Update management

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

In **Update Center** you can view, create, and maintain update sources, and view server groups. Also, you can create, and schedule jobs for firmware updates. A comparison report for the existing firmware version and the baseline version is provided, based on this information, you can create an inventory file.

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

NOTE:

- Update management is not available in the earlier versions of the appliance.
- To use the new features in the appliance, rediscover the servers discovered in earlier versions of the appliance.

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 consists 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 do 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** — update any specific component to the latest update provided on the FTP site. Dell IT prepares a repository at quarterly cadence.

  - Integration with Dell Online Catalog — connect to Dell FTP, download the catalog file, 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 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.

Update source

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

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 catalogue file is cached in the appliance at the time of creation. When a catalogue file is updated in the update source, the locally cached catalogue file is not automatically updated. To update the catalogue 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 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 selected servers or server groups against the version information available from the selected update source.

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

1. Server BIOS and firmware
2. Dell certified operating system driver packs (for operating system deployment)

Predefined update source

There is a predefined update source available in the appliance. You cannot delete or change the name of the predefined update source. **DELL ONLINE CATALOG** is the default FTP update source. After installing DLCI for SC2012 VMM or upgrading to the new version, add the proxy details for the default update source and save it.

Update groups

Update groups are a group of servers that require similar management. 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 firmwares 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 using iDRAC. The batch size is determined when the update is happening. The appliance assumes that the update is successful, as soon as iDRAC reports that the update is successful. The status 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.

You can view the update groups in the update center page. The description and behavior of the 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 group. This group is of 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 type generic update group. The servers are added to 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 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 Update Center page.

To know the cluster update group to which a server belongs to, see the device inventory page where the hostname and cluster FQDN is displayed for all 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 pertains to 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 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 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, chassis update group continues to exist but displays only the CMC information.

Update group notes

- You cannot create, modify or delete the 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 source

To view update source:

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

Setting up local FTP

To set up your local FTP :

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

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

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 **Update Center** and then click **Update 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 using proxy credentials.
   - If you are creating DRM source, provide your Windows credentials and ensure that the Windows shared location is accessible and in the location field provide the complete path of catalog file with the file name.

– Use only 32–bit DUPs to create the update source.

3. (Optional) To make it as a default update source select **Make this as default 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**.
- The update source is used in a deployment template.
- The update source is 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**.

Viewing update groups

To view update groups:

In **DLCI for SC2012 VMM** , click **Update Center** and then select a group from the **Select Update Group** drop-down menu.

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**.

NOTE: 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.

Prerequisites:

- To perform updates on servers, you require update sources available on a Dell FTP site, local FTP site, or Dell Repository Manager (DRM).
- Before applying the updates, clear the iDRAC job queue on the servers where the updates are applied.

You can apply firmware updates on a single component of a server, or to the entire environment. However, you can update a single component only through an FTP source.

To apply updates on servers:

1. In DLCI Console Add-in for SC2012 VMM, click **Update 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 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.
   - 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 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.

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 a server's component information, the complete servers' inventory information is refreshed.

NOTE: 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 **Update 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 on 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 Network Interface Card (NIC) related information for 11th generation of PowerEdge server is displayed as follows:

- 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 server groups that you want to refresh, and then click **Refresh Inventory**.

Exporting inventory

In DLCI for SC2012 VMM you can export inventory of selected servers and server groups, 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 new 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 addin 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 a server's component information, the complete servers' inventory information is exported.

To export inventory of discovered servers:

In **DLCI Console Add-in for SC2012 VMM**, under **Update Center**, select the servers' whose inventory you want to export, 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**.

Manage jobs

All the firmware update jobs are listed here with their status information. Also, you can cancel the scheduled firmware update jobs.

Cancelling firmware update jobs

To cancel a scheduled firmware update job:

1. In **DLCI for SC2012 VMM**, click **Update Center**, and then click **Manage Jobs**.
2. Select the jobs that you want to cancel, and make sure they are in **Scheduled** state, click **Cancel**, and then click **Yes**.

9

Profiles and templates

About credential profile

Each credential profile contains a username and password for a single user account. Credential profiles simplify the use and management of user credentials. 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 login 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 username 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 username 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, login to CMC, resolve synchronization issues, and deploy operating system.
  - After you upgrade to DLCI for SC2012 VMM version 1.1, then all the existing credential profiles are classified to device type credential profiles. Also, a credential profile created and made as default profile in the earlier version of DLCI for SC2012 VMM is classified as device type credential profile and the profile is set as the default credential profile to login to iDRAC.
- 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 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 type FTP credentials having **Username** as anonymous and the **Password** is blank. This 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.
- You cannot delete a credential profile that is used in server discovery. However, to delete such a credential profile, delete the discovered server information and then you can delete the credential profile.
- You cannot delete a device type credential profile if it is used for deployment. However, to delete such a credential profile, 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 for the following criteria:

- 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 to version 1.1, edit and save the hardware profiles created in DLCI for SC2012 VMM version 1.0 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 reference server's iDRAC IP, and then click **Next**.

   The reference server's hardware details 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, 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 only retain the server's existing RAID settings.

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 operating system in to 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 name and description, 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 hzpervisor 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 deployment

The 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 if the firmware update fails. However, all the components of the selected servers or server groups 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 in the appliance for hypervisor deployment. Hypervisor deployment supports one-to-one, and one–to–many deployment.

Creating deployment template

You can create deployment templates with required hardware and hypervisor profile, and an update source and apply the deployment template to unassigned servers. This 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 template name, template description, 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**.
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 will not impact the associated hardware and hypervisor profiles.

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** , 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 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 the jobs you want to view, select **Deployments**, **Firmware Update**, **Discovery Jobs**, **WinPE Creation Jobs** or **Sync Jobs**.

Viewing managed jobs

To view the firmware update jobs:

In **DLCI for SC2012 VMM** , click **Update 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 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 Update 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 Update 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.

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 **Update 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 auto-discovery, or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Update 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 creates 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 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.

Failure of firmware update because of job queue being full

Firmware update jobs submitted from the appliance to iDRAC fails, and the appliance main log displays the 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 refer to iDRAC documentation at **dell.com/support/home**.

Failure to connect to FTP using system default update source

After set up and configuration, or upgrade accessing 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, you must 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.

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 GUI and reset Lifecycle Controller.

  After resetting Lifecycle Controller, if you still face the problem try the following alternative.
- The antivirus 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 a 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 appliance and Integration Gateway. This is because the execution policy of the Integration Gateway for the user is not active. Login to the Integration Gateway server using 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 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 will fail.

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

Firmware update on 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:

- In order 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.

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 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.