Deployment and Managing Configurations with Dell OpenManage Essentials

A how to and best practices guide for using Dell OpenManage Essentials to deploy bare metal Dell servers and to manage and detect configuration drift.

Dell Engineering
September 2014

A Dell Technical White Paper

Revisions

Date	Description
September 2014	Initial release

Table of contents

Executive Summary

Configuring a server or chassis to match precise standards can be an arduous task. Configuring an entire datacenter is even more difficult. OpenManage Essentials (OME) version 2.0 introduces two new portals and features to streamline device configuration management. This white paper covers using the new features to configure a bare metal device, automatically configure and image recently ordered devices and detect drift of a device from a baseline.

This white paper also describes step by step how to create, deploy and check compliance using the deployment and configuration features in OpenManage Essentials version 2.0 as well as best practices and troubleshooting for the deployment and configuration features.

1 Covered Features

This white paper covers the following topics and features.

1. Full use case examples for using OpenManage Essential's device configuration features.
2. Requirements and setup for using the features.
3. Create a template from a server or chassis.
4. Deploy a template to a server or chassis.
5. Deploy a template to undiscovered devices by service tag ('Auto Deploy').
6. Deploy an ISO image from your network to a server.
7. Check the compliance of devices against a template.

2 Preparing OME for Device Configuration

Device prerequisites and file share settings are required to use the configuration and deployment features in OME. This section covers the device requirements, how to setup the file share settings and troubleshooting for the file share settings.

2.1 Target device requirements

Target Server requirements:

1. For Dell's 12th generation PowerEdge servers, the minimum supported version of iDRAC is 1.57.57.
2. For Dell's 13th generation PowerEdge servers, the minimum supported version of iDRAC is 2.0.
3. 'Server configuration for OpenManage Essentials' license installed on the iDRAC. This is a separate license from the iDRAC license.
4. iDRAC Enterprise or iDRAC Express license. This is a separate license from the 'Server configuration for OpenManage Essentials' license.

Target Chassis requirements:

1. For the PowerEdge M1000e, the minimum supported version of CMC firmware for is 4.6.
2. For the PowerEdge VRTX, the minimum supported version of CMC firmware is 1.3.

2.2 File share settings

The device configuration and deployment features require a staging area (file share). This section explains the details of the file share and how to setup the file share.

2.2.1 File share requirement explanation

The file share is a staging area for deployment. To use the deployment and configuration feature, a file share is required to send and receive configuration files to and from a device. During a create or deploy task, configuration files will briefly exist in the file share folder. On completion of the create or deploy task, the file is deleted. Security attributes (passwords and other sensitive data) are not included in the file.

2.2.2 How to setup the file share

The file share settings must be entered in OME. The file share settings require a username and a password. The username and password must be a user on the OME system that has enough privileges to read and write files on the system. During a deployment/configuration task, the username and password are sent to the remote targets to access the file share. Using an administrator account is recommended.

1. Navigate to the 'Deployment' portal.
2. Click 'File Share Settings' in the left hand navigation under the 'Common Tasks' section.
3. Enter the username and password of a user on the OME system that has enough privileges to read and write files to the system and click 'Apply'.

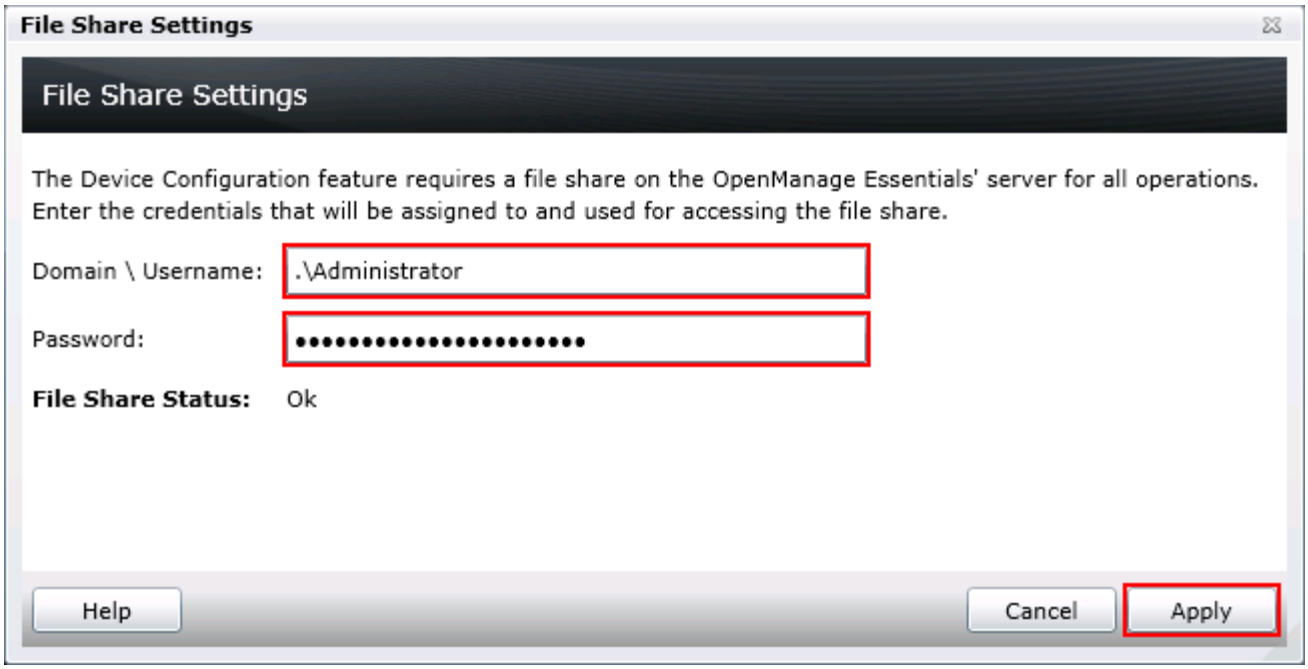

Figure 1 The file share settings popup

3 How to deploy to a bare metal device

Example use case – Based on your data center's needs, you configure all the settings of one server or chassis. You have a new bare metal device or device you want to repurpose. You wish to copy all of the settings of the configured device and apply them to bare metal/repurpose device.

To accomplish this use case you must perform the following steps.

1. Get the configuration from the device that is already configured and save it in OME as a template. (See the How to create a template from a reference device section).
2. Add the target device (the bare metal device) to the 'Repurpose and Bare Metal' device group. (See the How to add devices to the 'Repurpose and Bare Metal' device group section).
3. Deploy the template to the target device. (See the How to deploy a template section).

Note: Creating a template and deploying a template have requirements for the OME system and for the target devices.
To review the requirements for creating a template, see the Template definition
A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.
Requirements for creating a template section.
To review the requirements for deploying a template, see the Deploy requirements section.

4 How to automate hardware configuration and operating system deployment (Auto Deploy) of recently ordered devices

Example use case - Your Company orders several new devices. The devices are shipped and may come in at different times. When a device is connected to the network, you want a template you created deployed to the device and for the devices to boot to an ISO on your network.

Note: Auto deploy is only for devices that have not been discovered by OME. To deploy to devices discovered by OME, see the Create Templates

Understanding and creating templates is necessary for using the deployment and configuration features. This section explains what a template is and how to create a template from a reference device or from a file.

4.1 Template definition

A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.

4.2 Requirements for creating a template

To create a template from a reference device, the device must meet the same requirements in the Target device requirements section. To create a template, a server **does not** need a license.

4.3 How to create a template from a reference device

This section describes how to create a template from a discovered device. A 'reference device' is a device that has been discovered in OME, configured a desired way and the functionality of the device is intended to be replicated on other devices. The reference template is crucial to the success of configuring your other devices. Make sure that the reference device is correctly configured before you create a template from it.

4.3.1 Create a template from a reference server

1. Navigate to the 'Deployment' tab.
2. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the template.
4. Select 'Create from Device'.
5. Select the target server from the device tree

Note: Alternatively you can select the target by entering the device name or service tag in the search box next to the 'Create from Device' button.

6. Enter 'Execution credentials' for the target. The credentials must have administrator privileges on the target iDRAC.

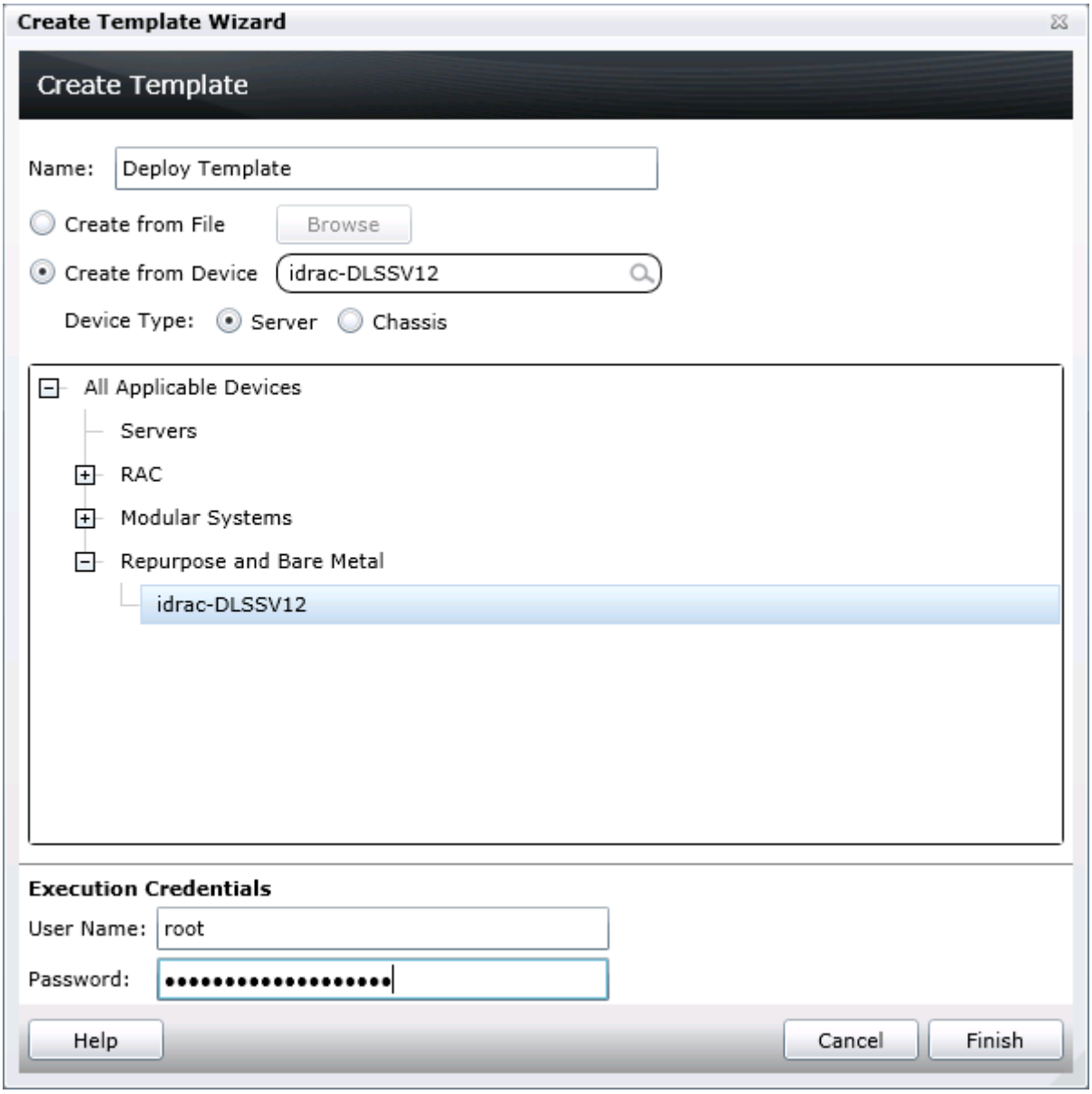

Figure 2 Create template from reference device wizard

7. Click 'Finish'.
8. Click 'OK' to the task created message.

A task is created when the wizard is closed. To view the created task, click the 'Tasks' tab in the 'Deployment' portal. To view the progress of the task, look at the 'Task Execution History' grid. To view the details of the execution history, double click the task execution history entry, or right click the task execution history entry and select 'Details'. The details will inform you if any problems occurred (such as incorrect credentials, etc.).

If the task is successful, a template is created and displayed in the 'Server Templates' tree.

If the task is not successful, view the details of the task by double clicking the execution history. The task can be run again by right clicking the task execution history or the task and clicking 'Run'. Rerunning the task requires entering the iDRAC credentials.

4.3.2 Create a template from a reference chassis

Follow the steps in the Create a template from a reference server section. After step 4, select 'Chassis' in the device type section. The execution credentials in step 6 must have administrator privileges on the CMC.

4.4 How to create a template from an XML or INI configuration file

The section below describes how to create a template from an XML or INI configuration file. Configuration XML is used for server templates. The INI format is used for chassis templates. A configuration file can be obtained by exporting a template to file in OME. Configuration template files are also available from the Dell TechCenter.

4.4.1 File requirements

Files used for a template must meet the following requirements.

XML file:

1. Must be well formed XML.
2. Must contain at least one attribute.

INI file:

1. Must be well formed INI.

4.4.2 Create a template from an XML file

1. Navigate to the 'Deployment' tab.
2. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the template.
4. Select 'Create from File'.
5. Click the 'Browse' button and browse to the file's location.
6. Select the file and click 'Open'.

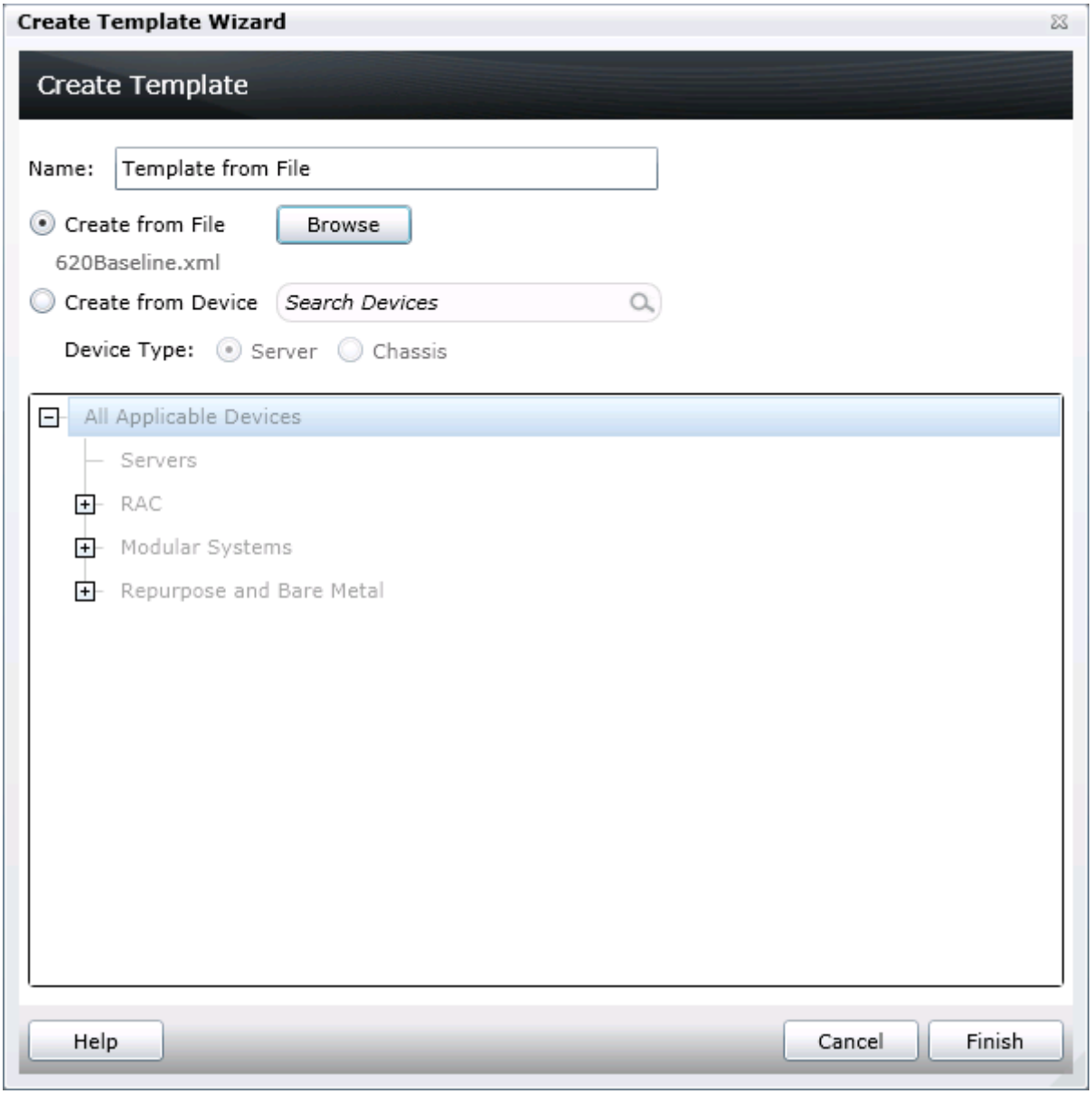

Figure 3 Create template from file wizard

7. Click Finish to create the template.
8. The template name will be added in the 'Server Templates' tree.

4.4.3 Create a template from an INI file

The INI format is for chassis devices and creating a template from an INI file will create a chassis template. Follow the same steps in the Create a template from an XML file section. In step 5 when browsing for the file's location, select the '.ini' file type option. The template will be added in the 'Chassis Templates' tree.

Deploy Templates section.

To accomplish this use case you must perform the following steps.

1. Create a template from a configured device or sample template. (See the How to create a template from a reference device section).
2. Add deployment instructions for the devices (auto deploy entries) you want automatically configured after they are discovered. Devices are added by service tag. (See the How to setup auto deploy of a template section).
3. Discover the devices in OME when the devices are running and connected to the network.

Note: Creating a template and auto deploying a template has requirements for the OME system and for the target devices.
To review the requirements for creating a template, see the Template definition
A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.
Requirements for creating a template section.
To review the requirements for auto deploying a template, see the Auto deploy requirements section.

5 How to detect and manage configuration drift of a device in a production environment

Example use case - You have deployed templates to several servers and chassis and want to verify that the attribute values of the template match the attribute values of the devices. If a device does drift from the template, you want to know which attributes are different.

To accomplish this use case you must perform the following steps.

1. Get the configuration data from a device, import a template, or use an existing template for compliance. This template will be used to check configuration drift of target devices and will be referred to as a 'compliance template'. (See the How to create a template from a reference device section).
2. Set a schedule and credentials for getting the current configuration inventory from target devices. The process is called 'Configuration Inventory Schedule'. (See the How to setup and run the configuration inventory section).
3. Select a compliance template for the devices by associating the devices to a template. (See the How to associate devices to a template section).
4. Use the 'Configuration' portal to determine compliance and drift. (See the How to view and leverage the compliance report section).

Note: Device specific attributes are not used for compliance (see the How to edit the device specific attributes of a deploy template task section for more information on device specific attributes). Creating a template and configuration compliance has requirements for the OME system and for the target devices.
To review the requirements for creating a template, see the Template definition
A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.
Requirements for creating a template section.
To review the requirements for the configuration compliance, see the Configuration compliance requirements section.

6 Create Templates

Understanding and creating templates is necessary for using the deployment and configuration features. This section explains what a template is and how to create a template from a reference device or from a file.

6.1 Template definition

A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.

6.2 Requirements for creating a template

To create a template from a reference device, the device must meet the same requirements in the Target device requirements section. To create a template, a server **does not** need a license.

6.3 How to create a template from a reference device

This section describes how to create a template from a discovered device. A 'reference device' is a device that has been discovered in OME, configured a desired way and the functionality of the device is intended to be replicated on other devices. The reference template is crucial to the success of configuring your other devices. Make sure that the reference device is correctly configured before you create a template from it.

6.3.1 Create a template from a reference server

5. Navigate to the 'Deployment' tab.
6. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
7. Enter a unique name for the template.
8. Select 'Create from Device'.
9. Select the target server from the device tree

Note: Alternatively you can select the target by entering the device name or service tag in the search box next to the 'Create from Device' button.

10. Enter 'Execution credentials' for the target. The credentials must have administrator privileges on the target iDRAC.

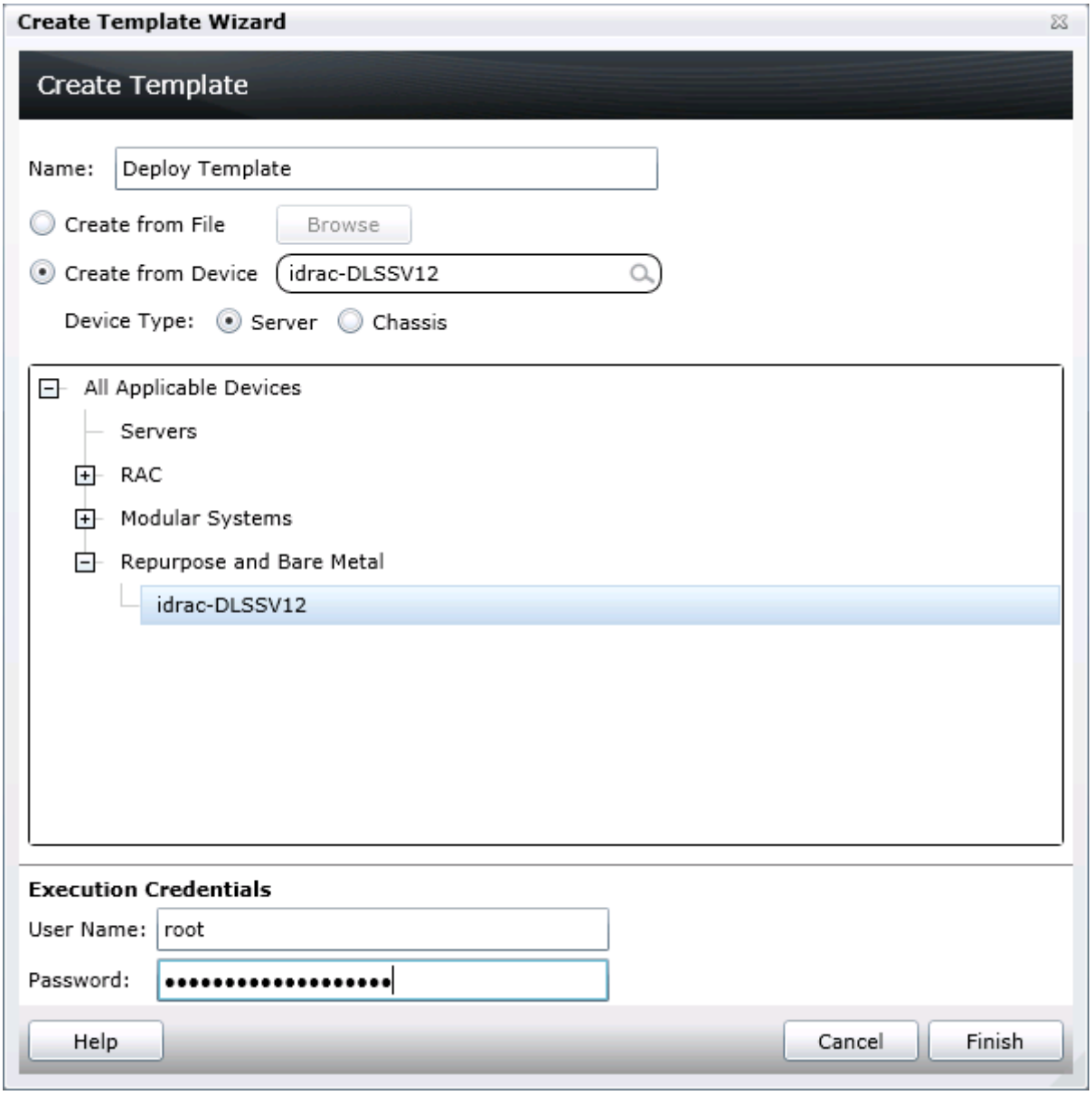

Figure 4 Create template from reference device wizard

11. Click 'Finish'.
12. Click 'OK' to the task created message.

A task is created when the wizard is closed. To view the created task, click the 'Tasks' tab in the 'Deployment' portal. To view the progress of the task, look at the 'Task Execution History' grid. To view the details of the execution history, double click the task execution history entry, or right click the task execution history entry and select 'Details'. The details will inform you if any problems occurred (such as incorrect credentials, etc.).

If the task is successful, a template is created and displayed in the 'Server Templates' tree.

If the task is not successful, view the details of the task by double clicking the execution history. The task can be run again by right clicking the task execution history or the task and clicking 'Run'. Rerunning the task requires entering the iDRAC credentials.

6.3.2 Create a template from a reference chassis

Follow the steps in the Create a template from a reference server section. After step 4, select 'Chassis' in the device type section. The execution credentials in step 6 must have administrator privileges on the CMC.

6.4 How to create a template from an XML or INI configuration file

The section below describes how to create a template from an XML or INI configuration file. Configuration XML is used for server templates. The INI format is used for chassis templates. A configuration file can be obtained by exporting a template to file in OME. Configuration template files are also available from the Dell TechCenter.

6.4.1 File requirements

Files used for a template must meet the following requirements.

XML file:

3. Must be well formed XML.
4. Must contain at least one attribute.

INI file:

2. Must be well formed INI.

6.4.2 Create a template from an XML file

13. Navigate to the 'Deployment' tab.
14. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
15. Enter a unique name for the template.
16. Select 'Create from File'.
17. Click the 'Browse' button and browse to the file's location.
18. Select the file and click 'Open'.

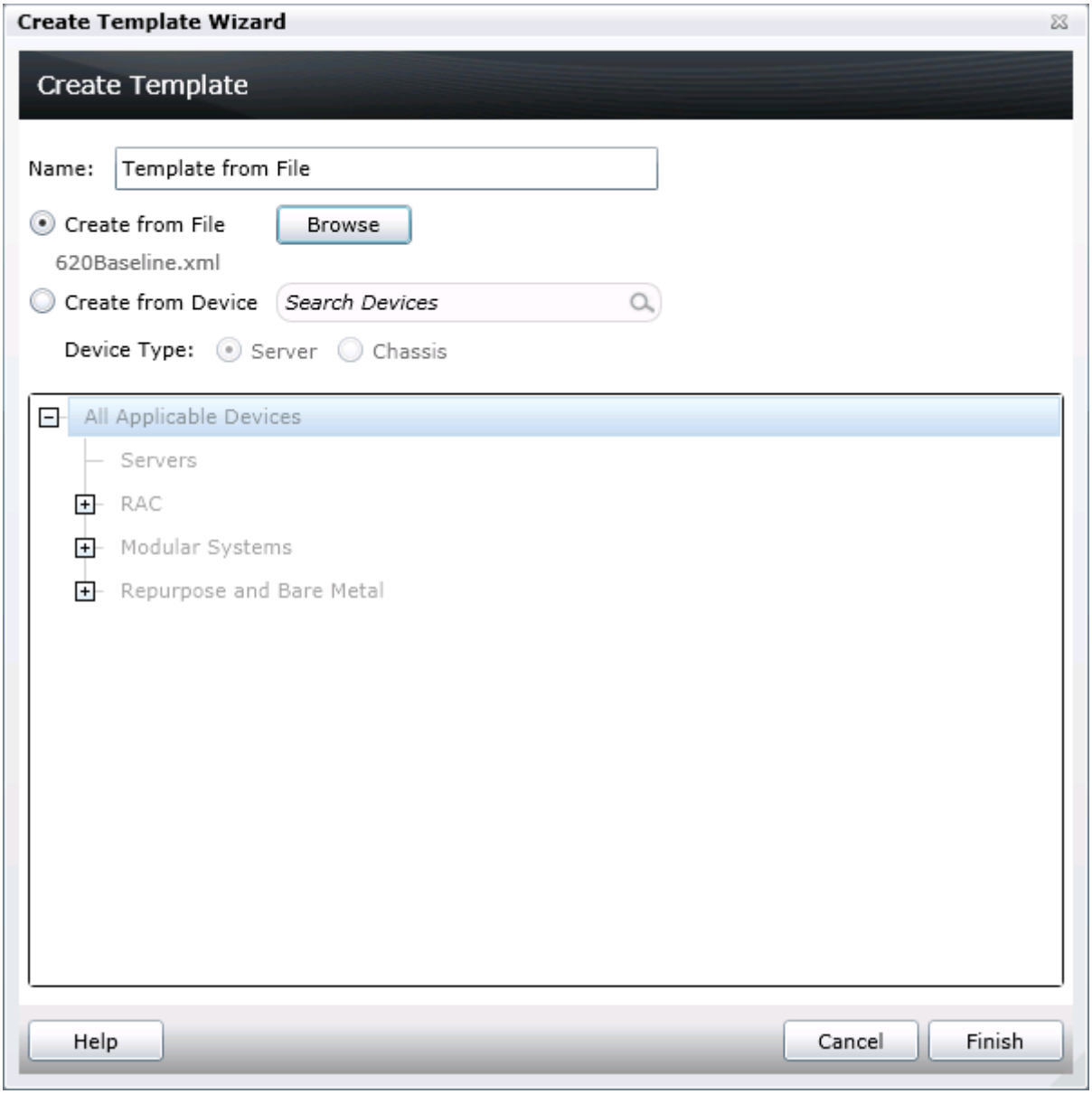

Figure 5 Create template from file wizard

19. Click Finish to create the template.
20. The template name will be added in the 'Server Templates' tree.

6.4.3 Create a template from an INI file

The INI format is for chassis devices and creating a template from an INI file will create a chassis template. Follow the same steps in the Create a template from an XML file section. In step 5 when browsing for the file's location, select the '.ini' file type option. The template will be added in the 'Chassis Templates' tree.

7 Deploy Templates

Deploying templates is the process of sending and applying configuration settings to remote devices. A template may contain a single configuration setting, configuration settings for one or more specific functional areas, or a full device configuration. To deploy a template, you must first create a template. The template is crucial to the success of the deploy task. Make sure the device you are creating the template from is configured exactly how you wish to deploy it when you create the template. To create a template, see the Create Templates section.

A template that was created from a target may contain destructive attributes (especially if it contains RAID configuration settings). Deploying destructive attributes may cause data loss, connectivity issues, failure to boot and other problems. It is important to review and understand each destructive attribute before deploying it to target devices.

7.1 Deploy requirements

1. The file share must be configured (see the How to setup the file share section).
2. The target devices must meet the minimum requirements for the deployment and configuration features (see the Target device requirements section).
3. The target devices must be added to the Repurpose and Bare Metal device group (see the How to add devices to the 'Repurpose and Bare Metal' device group section).
4. At least one user created template (a cloned sample template is a user created template).

7.2 Purpose and definition of the 'Repurpose and Bare Metal' device group

The Repurpose and Bare Metal device group is a device group containing all the devices eligible for the deploy template task. Only add devices to this group if you intend to deploy a template or an ISO image to the devices. If you do not intend to deploy a template or an ISO image to the devices, it is recommended that you remove the devices from the Repurpose and Bare Metal device group. You should not add production devices to the Repurpose and Bare Metal device group because deploying a template can be destructive and cause downtime or a loss of data.

7.2.1 How to add devices to the 'Repurpose and Bare Metal' device group

1. Navigate to the 'Deployment' tab.
2. Click 'Deployment Portal' in the left hand navigation under the 'Deploy Device Configuration Portal' heading.
3. Click the 'Repurpose and Bare Metal Devices' tab in the upper left area of the deployment portal.
4. Click the 'Modify Devices' button in the bottom right corner of the grid.
5. Check the target devices in the popup. The target devices must be discovered and any target server must have a 'Server configuration for OpenManage Essentials' license.

Note: Only devices that satisfy the deploy requirements appear in the device selection. To review the requirements, see the Deploy requirements section.

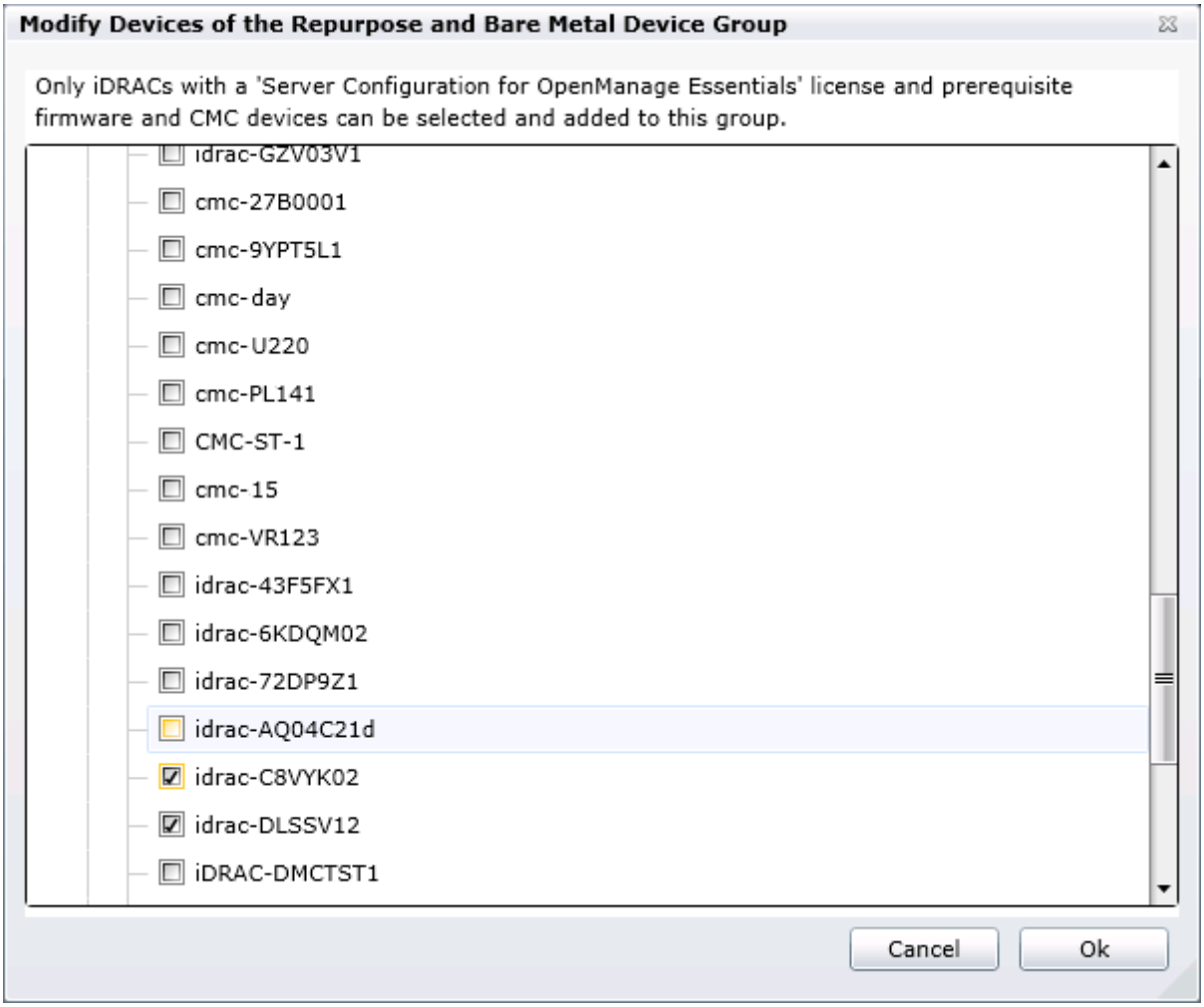

Figure 6 Modify repurpose and bare metal device group popup

6. Click 'Ok'.

7.3 How to deploy a template

This section describes how to deploy a template to servers and chassis.

7.3.1 Deploy a template to servers

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left hand navigation under 'Common Tasks').

3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Make sure 'Deploy Template' is checked and click 'Next'.
5. Select the template to be deployed on the target server/iDRAC and click 'Next'.
6. Select the target devices and click 'Next'.

Note: Only devices in the 'Repurpose and Bare Metal' device group and match the device type of the selected template (Server or Chassis) may be selected. See the How to add devices to the 'Repurpose and Bare Metal' device group section to add devices to the device group.

7. Enter the system specific attributes for each target device. These are attributes, such as 'Gateway IP Address', that are not included in templates because they do not necessarily apply to all target devices. For more details, see the How to edit the device specific attributes of a deploy template task section. Click 'Next'.
8. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the iDRAC. Click 'Next'.
9. Review the task in the Summary pane and click 'Finish'.
10. Review the warning message. The deploy action can be destructive. It is important you review and understand the template you are deploying.

7.3.2 Deploy a template to chassis

A chassis template can be deployed to an unlicensed chassis. Follow the same steps in the Deploy a template to servers section. In step 5, select a Chassis template. In step 8, use credentials that have administrative privileges on the target CMCs.

7.3.3 How to edit the device specific attributes of a deploy template task

Device specific attributes are attributes, such as 'Gateway IP Address', that are not included in templates because they do not necessarily apply to all target devices. Editing and deploying device specific attributes is optional because a device may already have the device specific attributes configured or the attributes may not be applicable to that specific device. If the template being deployed has device specific attributes, the device specific attributes will appear in the 'Edit Attributes' page of the deploy wizard. The 'Edit Attributes' page lists the target devices on the left hand side and displays the device specific attributes for the selected device in the right hand side grid. To edit the attributes follow the steps below.

1. Select a device in the left hand tab.
2. Check 'Deploy' on the attributes that you want to deploy to that device.
3. Edit the 'Value' of each checked attribute. For more information, navigate to the Dell Attribute Registry site from the Additional resources section.
4. Click 'Save'.

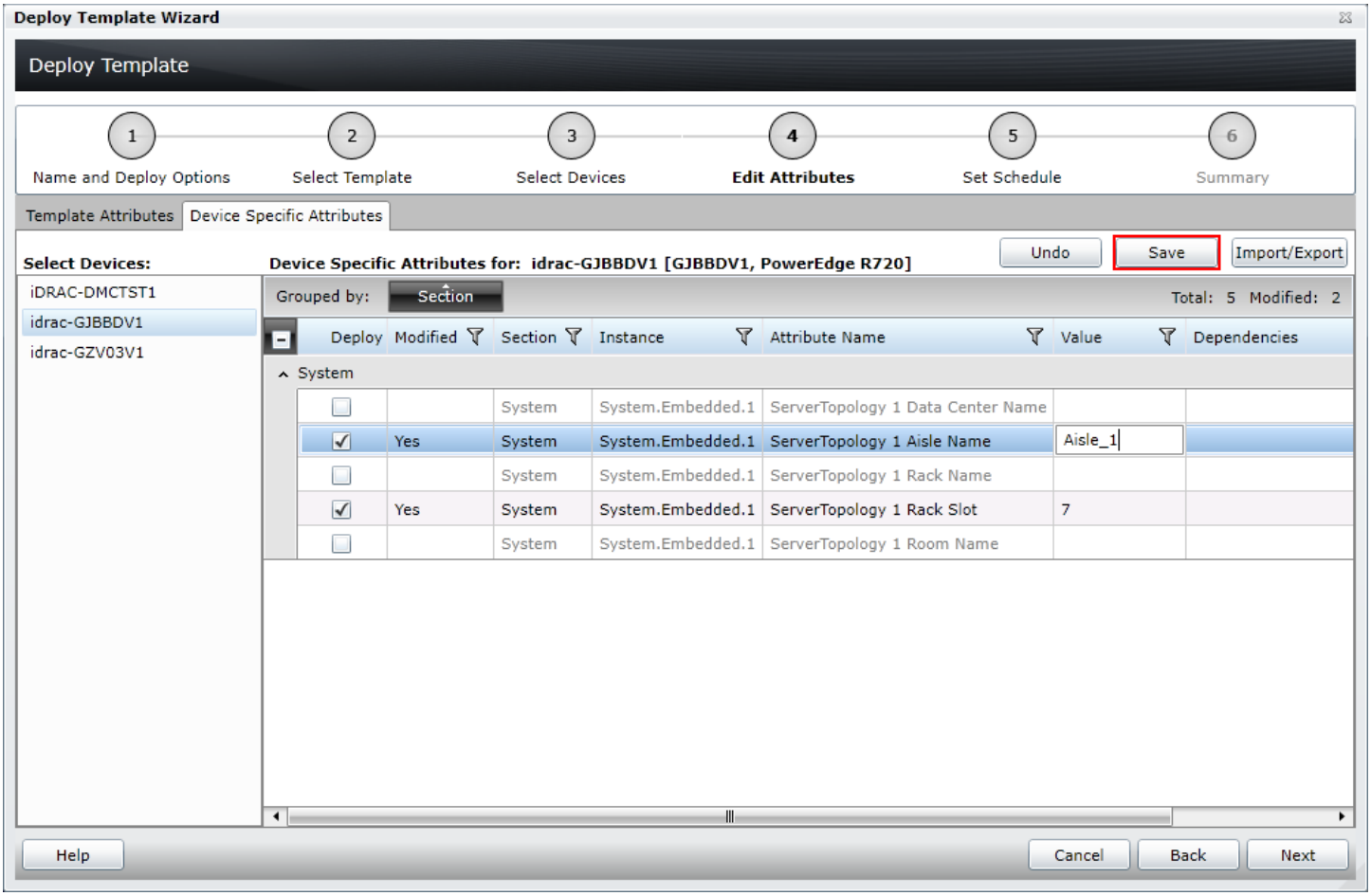

Figure 7 Edit attributes pane

5. Repeat for each device.

Alternatively, you can import and export the grid to file to edit. You may want to export/import if you have a large number of devices with a large number of device specific attributes. The device specific attributes grid can be exported by selected device or all devices. All devices will export to a single file that can be opened in a spreadsheet processing application. When edits are finished in the file, the file may be imported. The edited values must be valid values for the attribute (see the attribute registry link in the Additional resources section). The grids will be populated with the import data. The UI logs will report any problems with format or values of the import file.

8 Auto Deploy Templates

Auto deploying templates applies all the template's attribute's values to a device after it has been discovered. To add auto deploy entries for devices that have not been discovered by OME, a list of service tags for the target devices must be provided. To auto deploy a template, you must first create a template. To create a template go to the Create Templates section.

Note: Auto deploy is only for devices that have not been discovered by OME. To deploy to devices discovered by OME, see the Create Templates

Understanding and creating templates is necessary for using the deployment and configuration features. This section explains what a template is and how to create a template from a reference device or from a file.

8.1 Template definition

A template is a collection of attributes that describe the settings of a device. The settings describe the behavior of a device's hardware. A device may have several hundred attributes depending on the device's hardware. An attribute is a name value pair that describes a particular setting of a device. OME installs with sample server and chassis templates for specific use cases. A user can deploy, edit, clone, delete, or rename a template. Sample templates must be cloned to deploy or use for compliance.

8.2 Requirements for creating a template

To create a template from a reference device, the device must meet the same requirements in the Target device requirements section. To create a template, a server **does not** need a license.

8.3 How to create a template from a reference device

This section describes how to create a template from a discovered device. A 'reference device' is a device that has been discovered in OME, configured a desired way and the functionality of the device is intended to be replicated on other devices. The reference template is crucial to the success of configuring your other devices. Make sure that the reference device is correctly configured before you create a template from it.

8.3.1 Create a template from a reference server

6. Navigate to the 'Deployment' tab.
7. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
8. Enter a unique name for the template.
9. Select 'Create from Device'.
10. Select the target server from the device tree

Note: Alternatively you can select the target by entering the device name or service tag in the search box next to the 'Create from Device' button.

11. Enter 'Execution credentials' for the target. The credentials must have administrator privileges on the target iDRAC.

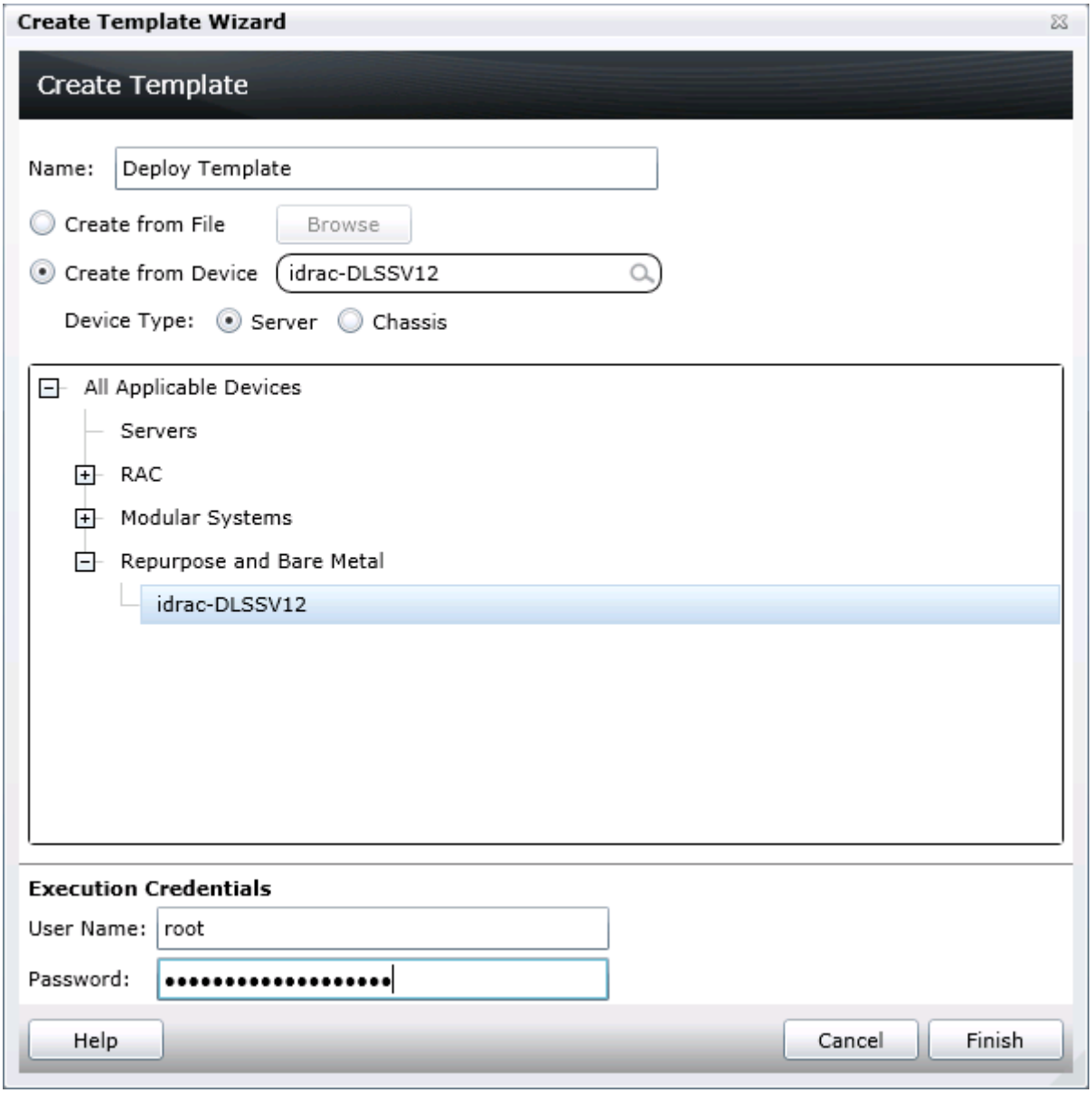

Figure 8 Create template from reference device wizard

12. Click 'Finish'.
13. Click 'OK' to the task created message.

A task is created when the wizard is closed. To view the created task, click the 'Tasks' tab in the 'Deployment' portal. To view the progress of the task, look at the 'Task Execution History' grid. To view the details of the execution history, double click the task execution history entry, or right click the task

execution history entry and select 'Details'. The details will inform you if any problems occurred (such as incorrect credentials, etc.).

If the task is successful, a template is created and displayed in the 'Server Templates' tree.

If the task is not successful, view the details of the task by double clicking the execution history. The task can be run again by right clicking the task execution history or the task and clicking 'Run'. Rerunning the task requires entering the iDRAC credentials.

8.3.2 Create a template from a reference chassis

Follow the steps in the Create a template from a reference server section. After step 4, select 'Chassis' in the device type section. The execution credentials in step 6 must have administrator privileges on the CMC.

8.4 How to create a template from an XML or INI configuration file

The section below describes how to create a template from an XML or INI configuration file. Configuration XML is used for server templates. The INI format is used for chassis templates. A configuration file can be obtained by exporting a template to file in OME. Configuration template files are also available from the Dell TechCenter.

8.4.1 File requirements

Files used for a template must meet the following requirements.

XML file:

5. Must be well formed XML.
6. Must contain at least one attribute.

INI file:

3. Must be well formed INI.

8.4.2 Create a template from an XML file

14. Navigate to the 'Deployment' tab.
15. Click 'Create Template' (located in the left hand navigation under 'Common Tasks').
16. Enter a unique name for the template.
17. Select 'Create from File'.
18. Click the 'Browse' button and browse to the file's location.
19. Select the file and click 'Open'.

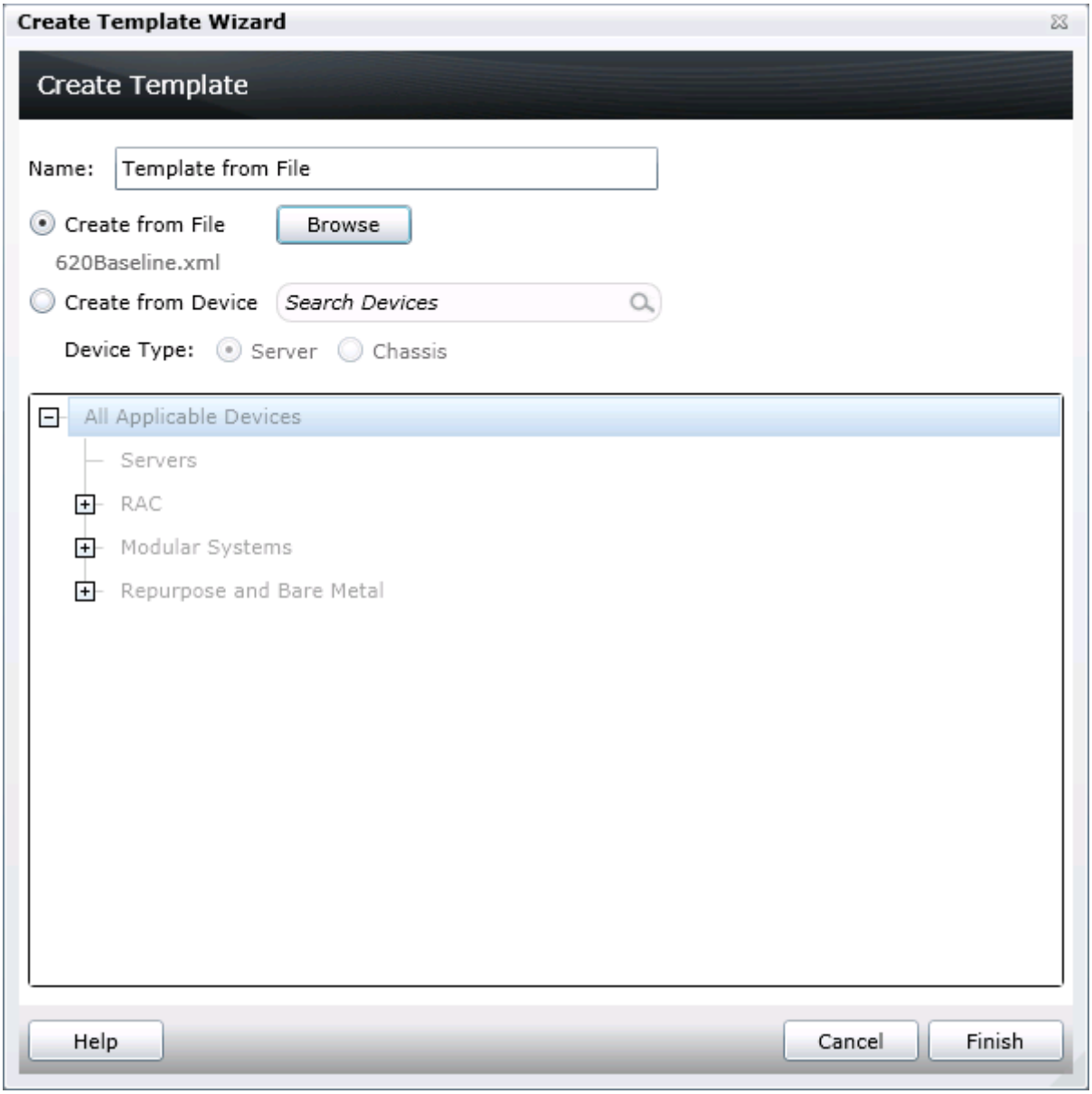

Figure 9 Create template from file wizard

20. Click Finish to create the template.
21. The template name will be added in the 'Server Templates' tree.

8.4.3 Create a template from an INI file

The INI format is for chassis devices and creating a template from an INI file will create a chassis template. Follow the same steps in the Create a template from an XML file section. In step 5 when browsing for the file's location, select the '.ini' file type option. The template will be added in the 'Chassis Templates' tree.

Deploy Templates section

8.5 Auto deploy requirements

In order to add auto deployment entries, the following requirements must be met:

1. Must have a template to deploy (see the How to create a template from a reference device section).
2. Must meet all device configuration target device requirements (see the Target device requirements section).
3. Target service tags cannot match a service tag of a discovered device.
4. A CSV file with the service tags (see the Create a service tag CSV section).

8.6 How to setup auto deploy of a template

This section describes how to setup auto deployment of a template against service tags. This section will cover the creation and format of the auto deployment CSV file and the auto deployment wizard.

8.6.1 Create a service tag CSV file

1. Create a csv file containing the target service tags to be deployed against. Follow the format below.
   a. Must have a column named 'ServiceTag'.
   b. Each service tag must match Dell standards for service tags.
   c. Service tags may not match the service tag of a discovered device in OME.

	A
1	ServiceTag
2	ABCDEFG
3	HY3912B
4	A123456
5	VNX189W

Figure 10 Format of an example CSV file.

8.6.2 Setup auto deploy of a template to server service tags

1. Navigate to the 'Deployment' tab.
2. Click 'Setup Auto Deployment' (located in the left hand navigation under 'Common Tasks').
3. Make sure 'Deploy Template' is checked and click 'Next'.
4. Select a server or chassis template (as applicable to the type of target devices) to be deployed on the target servers or chassis and click 'Next'.
5. Click the 'Import' button to import the csv file that contains the Service Tags. The imported service tags must be compatible with the type of template selected in the step above.

6. Browse to the location where the file is saved, select the file and click Open. All the Service Tags in the file will be imported and listed in OME. The 'Import Summary' window is displayed. Review and click OK to close the window. Click 'Next'.
7. (optional) Enter the unique attributes per service tag (for more details, see the How to edit the device specific attributes of a deploy template task section) and click 'Next'.
8. Select the execution credentials for the service tags. Instead of entering the credentials for each target device, credential definitions must be created. Credential definitions can be added as needed. Credential definitions can be assigned to multiple targets. Credentials are required for each target device.
    a. If no credentials exists yet, at least one (a default set of credentials) must be created. Follow these steps, otherwise go to step 9.
    b. Click 'Add New Credential'.
    c. Enter a description for the credential set (the description text is displayed in the credential selection page).
    d. Enter the username and password.

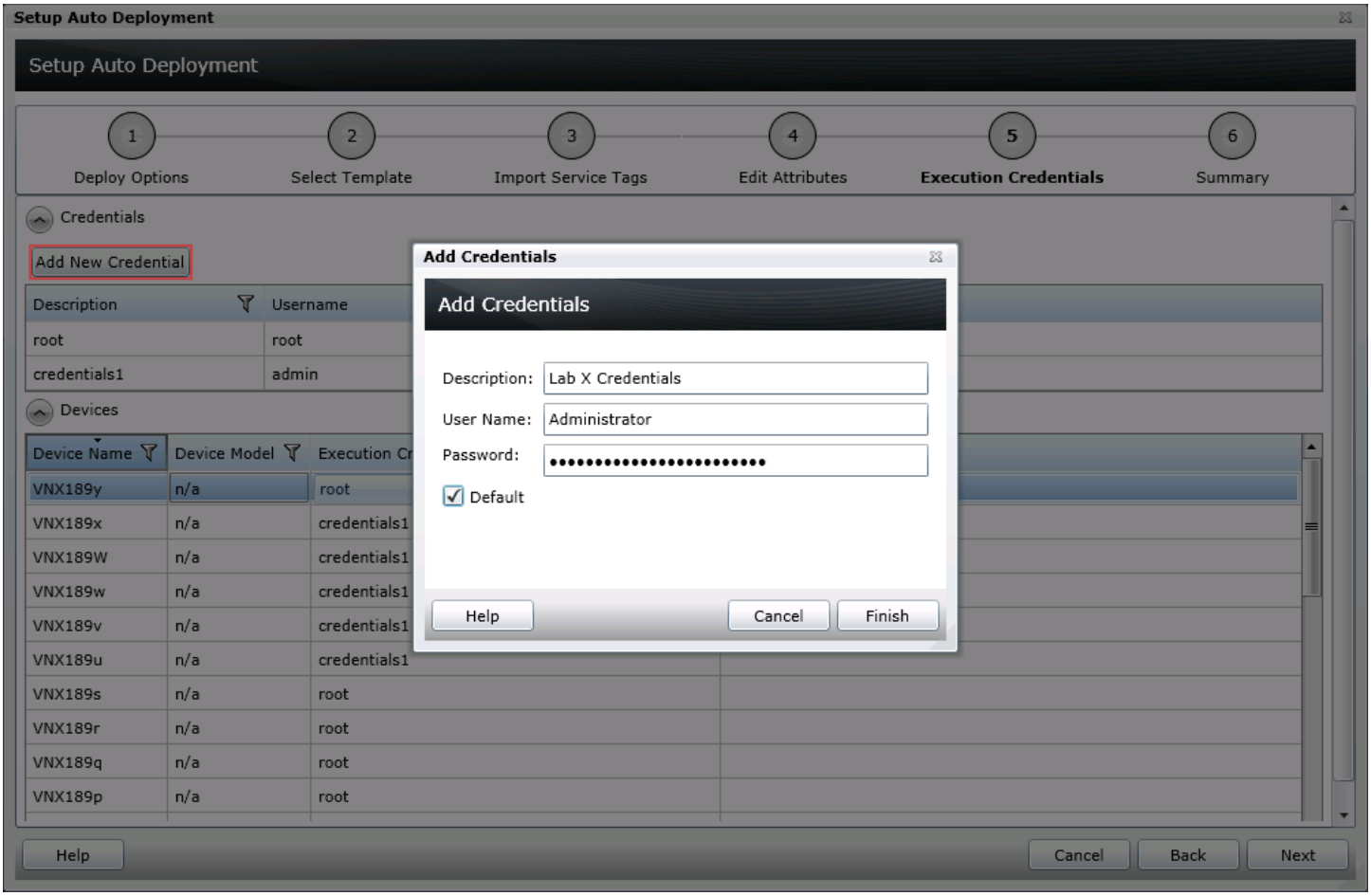

Figure 11 Auto deployment target credentials page

    e. Click 'Finish'.
9. Review the task in the Summary pane and click 'Finish'.

10. All the service tags that were imported are listed in the 'Auto Deployment' tab.
11. The service tags remain in the 'Auto Deployment' tab until they are discovered and inventoried in OME and the 'Deploy Configuration to Undiscovered Devices' task creates a deploy task for the device with the service tag. The 'Deploy Configuration to Undiscovered Devices' task checks periodically if the devices are discovered and inventoried in OME. Once the discovery and inventory is complete and a deploy task is created, the devices will move to the Bare Metal/Repurpose Devices group and the auto deployment entry will be deleted. Deploy configuration tasks are created to deploy the templates that were selected. The tasks created for the service tag entries can be found under the tasks tab in the deployment portal. Double click on the task to view the task details. Task execution history entries can be found in the task execution history grid. Double click on a task execution history entry to view the task execution history details.

8.6.3 Setup auto deploy of a template to chassis service tags

A chassis template can be deployed to an unlicensed chassis. Follow the same steps in the Setup auto deploy of a template to server service tags section. Select a service tag CSV file of chassis in step 6.

8.7 How to modify the auto deployment settings

By default, the 'Deploy Configuration to Undiscovered Devices' task runs every 60 minutes. When this task runs, it checks if any of the auto deployment service tags were discovered. If the device matching an auto deployment service tag was discovered, a deploy template task is automatically created and the specified template is deployed to that device. To modify the execution interval for the 'Deploy Configuration to Undiscovered Devices' task or to enable/disable it, follow the steps below.

1. Navigate to the 'Deployment Settings' tab under the 'Preferences' tab.
2. Check or uncheck the 'Enable auto deployment for recently discovered devices' to enable or disable the 'Deploy Configuration to Undiscovered Devices' task.

Note: If the task is disabled, the service tags in the 'Auto Deployment' grid will not be deployed to automatically.

3. Adjust the interval using the numeric control. The number is the minute interval that the 'Deploy Configuration to Undiscovered Devices' task will run.

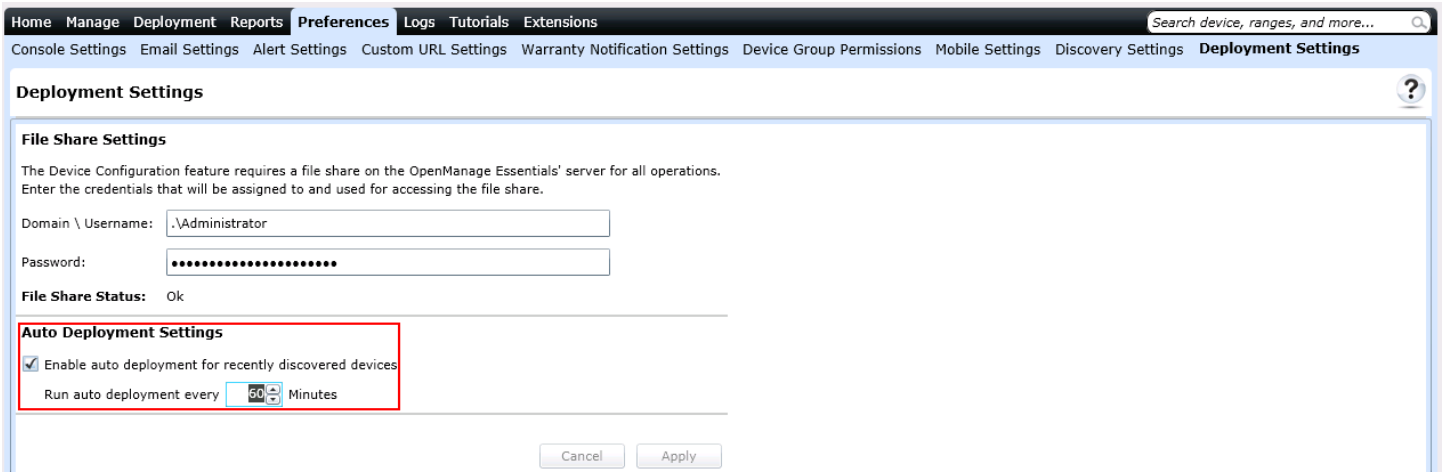

Figure 12 Auto deployment settings page

4. Click 'Apply'.

9 Deploy Network ISO Image

Deploying of a network ISO boots a server to an ISO image that is located on your network. This can be done independent, or in conjunction with a deployment task.

9.1 Deploy network ISO image requirements

1. Must meet all Deploy Template requirements (see the Target device requirements section).
2. If the 'Deploy Template' deploy option is checked, only server templates may be selected.

9.2 How to deploy network ISO image

1. Navigate to the 'Deployment' tab.
2. Click 'Deploy Template' (located in the left hand navigation under 'Common Tasks').
3. Enter a unique name for the task. A name is optional since a default name is supplied, but it is a generic name, and the same default name is always supplied. Selecting a name that is relevant to what is being deployed is suggested.
4. Check 'Boot to Network ISO' and uncheck 'Deploy Template'. Click 'Next'.

Note: Both 'Deploy Template' and 'Boot to Network ISO' can be selected. If both are selected, the 'Select Template' and 'Edit Attributes' tabs are added to the wizard. See the Deploy a template to servers section for a 'How to' on the 'Select Template' (above) and 'Edit Attributes' (above) tabs.

5. Enter ISO filename, Share IP, Share Name, Share username and Share password. Click 'Next'.

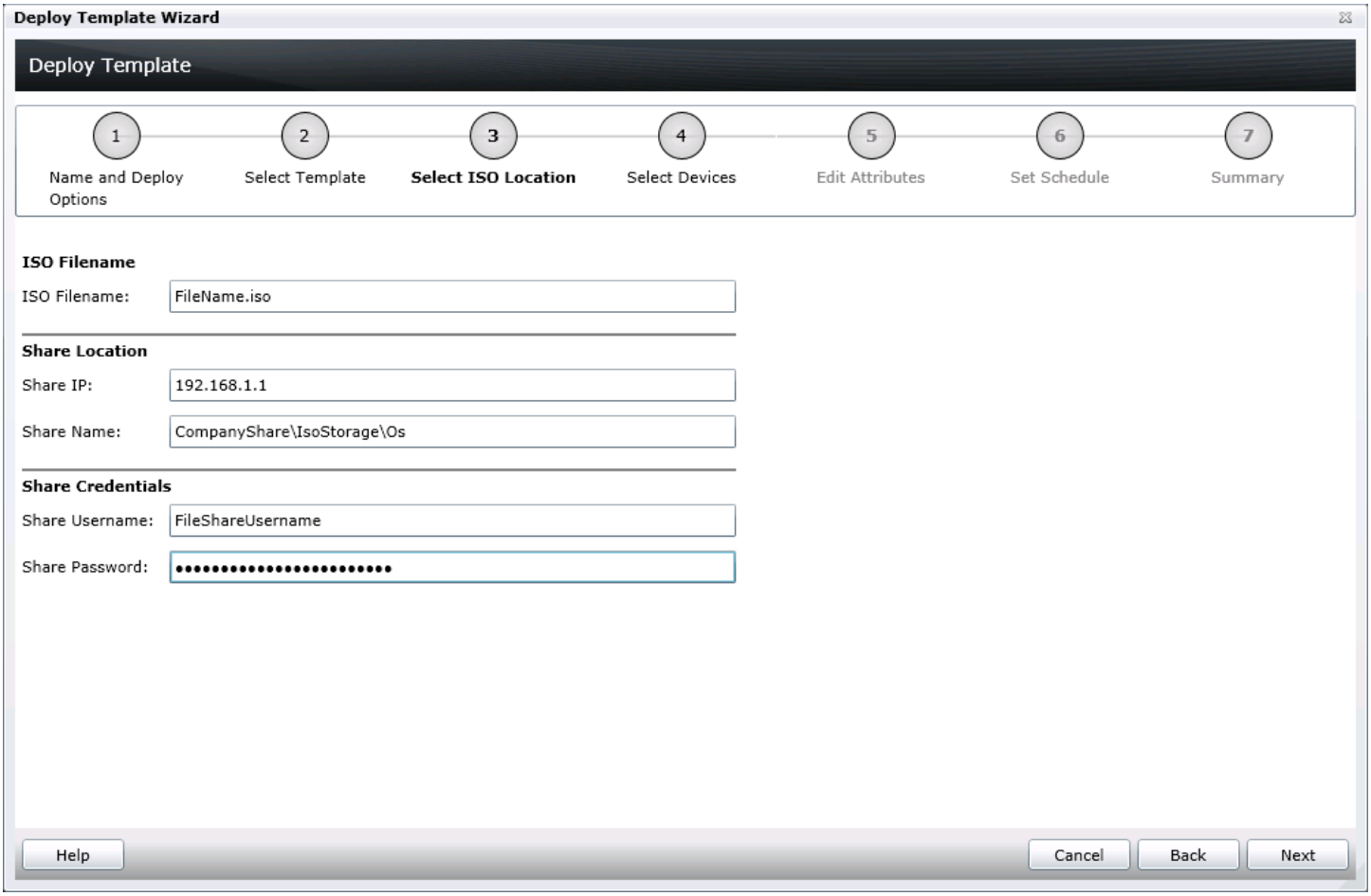

Figure 13 Select ISO location page

Note: The user must have full control to the share folder where the ISO is located. The share folder should be different than the file share used for deployment.

6. Select the target devices and click 'Next'.

Note: Only devices in the 'Repurpose and Bare Metal' device group may be selected. See the How to add devices to the 'Repurpose and Bare Metal' device group section to add devices to the device group.

7. Set the schedule of when the deploy template task will run. 'Run now' will run the task when the wizard is closed. 'Run at' will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have Operator or Administrator privileges on the iDRAC. Click 'Next'.
8. Review the task in the Summary pane and click 'Finish'.

10 Configuration Compliance

Configuration compliance detects drift of a device's attributes from a template's attributes. A process called 'configuration inventory' gets configuration information (inventory) from all applicable devices and compares the inventory against an associated compliance template.

10.1 Configuration compliance requirements

1. The file share must be configured (see the How to setup the file share section).
2. The target devices must meet the minimum requirements for the deployment and configuration features (see the Target device requirements section).
3. At least one user created template (a cloned sample template is a user created template).
4. Configuration Inventory must be enabled and the target device credentials must be provided.

10.2 How to setup and run the configuration inventory

The configuration inventory task collects the attribute information from all eligible devices. An eligible device is any device that meets the device configuration target requirements (see the Target device requirements section). The inventoried values are used to calculate the compliance of a device against the device's associated template.

10.2.1 Modify configuration inventory credentials and/or schedule

The configuration inventory schedule and credentials may be modified. The configuration inventory can be turned off if network or performance problems are encountered. The steps below describe how to modify the schedule and set the credentials for the configuration inventory.

1. Navigate to the 'Configuration' tab under the 'Manage' tab.
2. Click on 'Configuration Inventory Schedule' in the left hand navigation under 'Common Tasks'.
3. If credentials have not been added, click on the 'Add New Credential'.
   a. Enter a unique description name.
   b. Enter the username and password that the target devices will use.
   c. Select 'Default' for a credential to have discovered devices automatically assigned to the credential. One set of credentials must be assigned as the default.
4. Select the credentials for each device. Each device can have its own set of credentials. Click 'Next'.

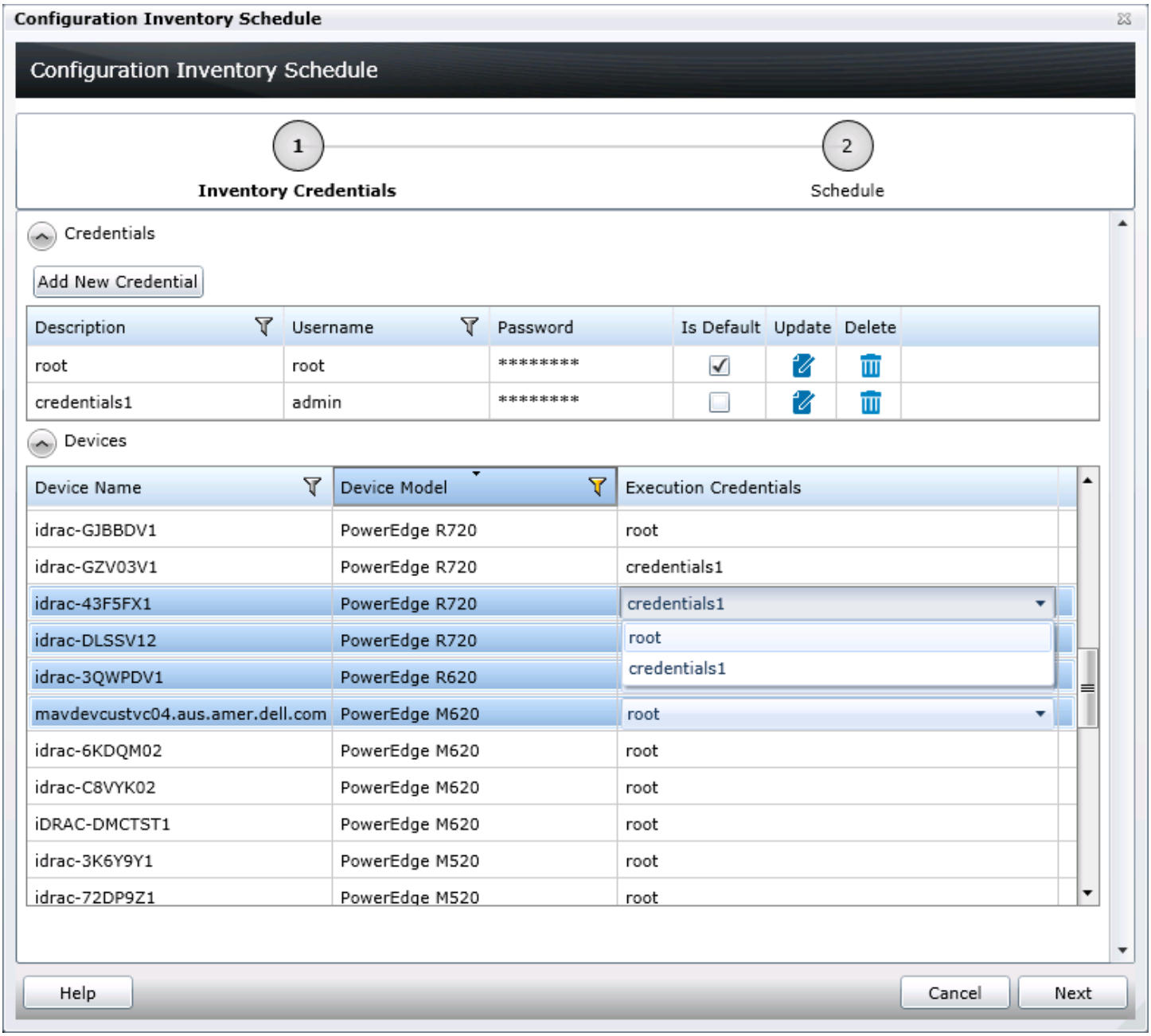

Figure 14 Configuration inventory credentials page

5. Make sure that 'Enable Configuration Inventory' is checked.
6. Choose a schedule – Either every week on given days at a given time or every day/hour interval.
7. Execution histories for the configuration inventory are displayed in the 'Task Execution History' grid. Double click on the execution history to view task details or right click on the execution history row and select details.

10.2.2 Run configuration inventory per target

To get the current configuration inventory from a device, do the following…

1. Navigate to the device tree ('Manage' -> 'Devices').
2. Select target devices and right click.
3. Hover over 'Device Configuration'.
4. Select 'Refresh Device Configuration Inventory'.

10.3 How to associate devices to a template

A device needs an associated compliance template for the device to have a compliance status in the compliance pie chart.

Note: Compliance does not include the device specific attributes of a template.

To set a compliance template for a device, you must associate the device to a template. A device may only have one associated template. To associate a device to a template, do the following…

1. Navigate to the 'Configuration' tab under the 'Manage' tab.
2. Click on 'Associate Devices to a template' in the left hand navigation under the 'Common Tasks' section.
3. Select a template and click 'Next'.
4. Select devices and click 'Finish'.

Note: Only devices that meet the device configuration requirements (see the Target device requirements section) and are of the same device type as the template are shown.

10.4 How to view and leverage the compliance report

The device compliance panel shows the configuration compliance status and state of all eligible devices (an eligible device is a device that meets the requirements in the Target device requirements section). Every eligible device is in one of the states below. Clicking a slice of the pie chart will show all the devices that have the selected pie slice's state. Device configuration compliance can be viewed in the 'Configuration' tab under the 'Manage' tab. The summary and pie chart have the following states. Actions required for the state are listed under each of the states below.

1. Compliant Devices
   a. No action required.
2. Not Compliant Devices
   a. Double click the compliance row to view differences between the associated template and the device's inventory.
   b. Adjust the device's settings or associate to a different template to make the device compliant.
3. Not Inventoried Devices
   a. Inventory the device. See the How to setup and run the configuration inventory section.
   b. Make sure the credentials for the target are accurate.

4. Not Associated Devices
   a. Associate the devices to a template. See the How to associate devices to a template section.
5. Not Licensed Devices
   a. Import a 'Server configuration for OpenManage Essentials' license in the device's iDRAC license interface.

11 Troubleshooting

11.1 Troubleshooting the file share

1. Check the file share status in OME.
   a. The file share status is at the bottom of the file share wizard and is in the 'Deployment Settings' preference.

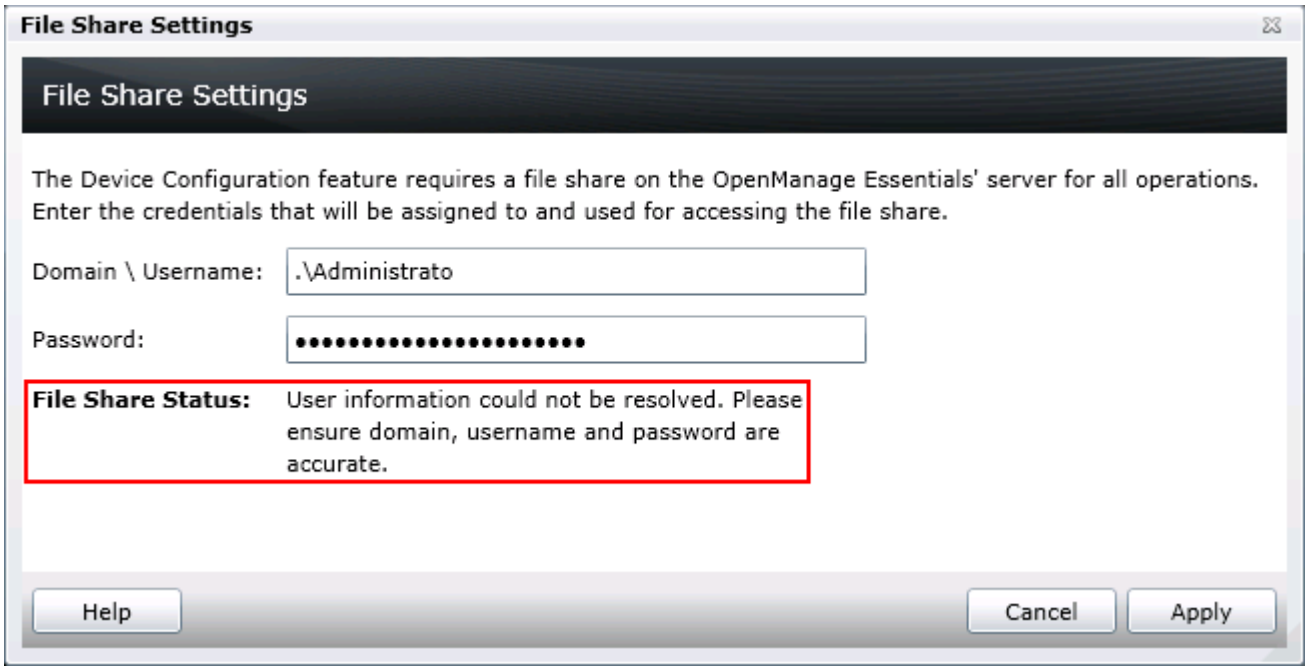

Figure 15 File share settings popup status

2. Check the username, domain and password in OME.
3. Check the share folder in Windows Explorer.
   a. Verify the 'ServerConfig' folder exists under the installation configuration folder (by default under 'Program Files\Dell\SysMgt\Essentials\configuration').
   b. Verify the folder is shared. Right click the folder, select 'Properties', select the 'Sharing' tab. The folder should be shared. The 'Advanced Sharing' permission settings should have the user entered in OME as the only user with permissions to the folder.

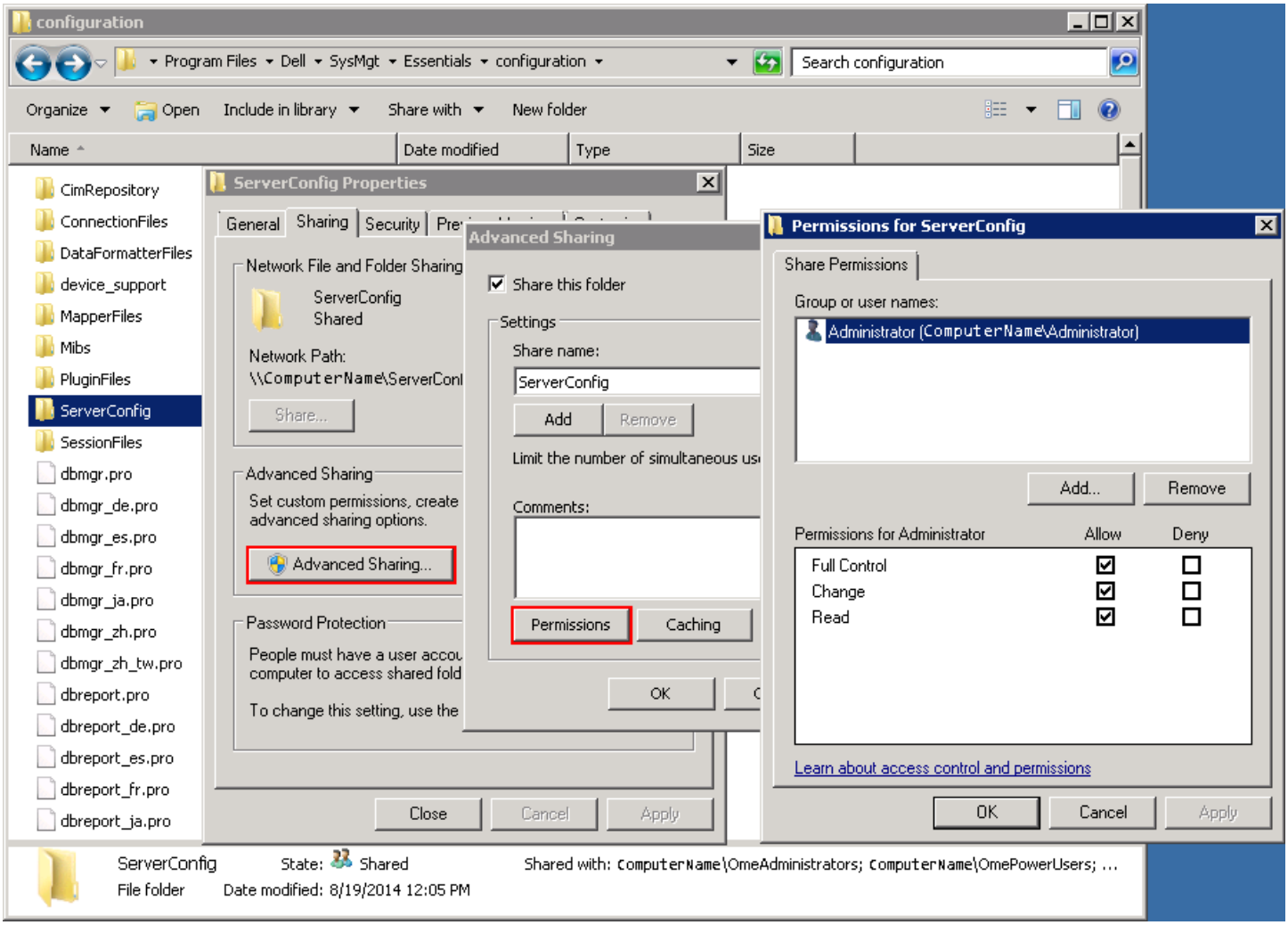

Figure 16 Advanced sharing tab of the 'ServerConfig' folder

4. Verify the share folder location using the 'net share' command.
   a. Open the command prompt and type 'net share'.
   b. A share with the name 'ServerConfig' should be in the network share list.

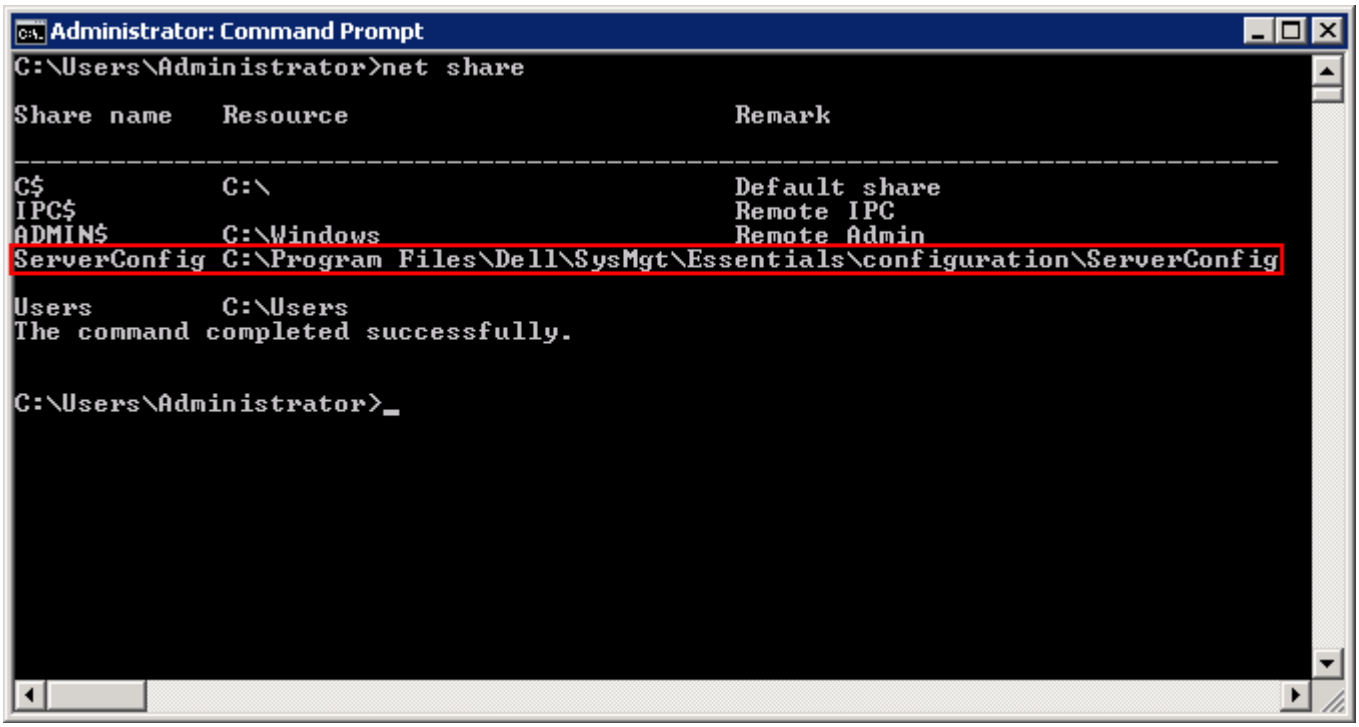

Figure 17 Net share command results

5. Check the user permissions in the 'User Accounts' window.

11.2 Troubleshooting creating a template

Troubleshooting creating a template from a reference device

1. Make sure the file share settings are correctly configured. See the How to setup the file share section or the Troubleshooting the file share section.
2. Run the task again. Right click the task or task execution history and select 'Run'.
3. The task execution may have an 'LC' code in the details. Review the 'LC' code in the iDRAC documentation. See the Additional resources section below.
4. Make sure the provided credentials have enough privileges to run the task (requires administrator privileges on the iDRAC/CMC).

Troubleshooting creating a template from a file

1. Make sure the file meets the file requirements in the File requirements section.
2. If you do not see the file you are looking for, make sure the file type is correct (in the file dialogue next to file name). The two options are .xml and .ini.

11.3 Troubleshooting deploying a template

The task execution history details provide troubleshooting information.

1. Check that the file share settings are entered correctly (see the Troubleshooting the file share section.
2. Double click the task execution history entry (or right click and select 'Details') to see the task execution history details. The 'Results' tab displays information on task activities and any errors that occurred. Errors with an 'LC' error code can be looked up in the iDRAC documentation (link in the Additional resources section). The details tab also contains the results of applying individual attributes.
3. If there is a 'cannot connect to server' error, make sure the target credentials are correct.
4. For a 'server is being configured' error, wait and retry later. If the task still fails, the server may need a reboot and/or iDRAC reset.
5. For a server reboot failure, reboot the server via the iDRAC interface.
6. If an attribute fails to be set, there may be an attribute dependency conflict. In some cases, re-running the task allows additional configuration settings to be applied to targets. For more details about attribute dependencies, refer to the attribute registry (link in the Additional resources section).
7. If the task does not complete, the task will timeout and exit after 30 minutes of inactivity. Rerun the task. A reboot and/or iDRAC reset may be necessary.

11.4 Troubleshooting auto deploying templates

Each time the 'Deploy Configuration to Undiscovered Devices' task runs, it looks for Service Tags in the 'Auto Deployment' list. The following situations may be encountered:

1. There are no Service Tags in the 'Auto Deployment' list. In this case, the task exits, and no entry is created in the task execution history grid for that run.
2. The task finds one or more Service Tags in the 'Auto Deployment' list for devices that have not been discovered by OME yet. In this case, a task execution history entry is created and it indicates why the Service Tag was not processed.
3. The task finds one or more Service Tags in the 'Auto Deployment' list for devices that have been discovered by OME. It creates tasks named 'Deploy Configuration to Undiscovered Devices - Task – timestamp' to deploy to those devices. In this case, an execution history entry is created and the entry specifies which Service Tags were processed for deployment.

If an error occurs in a task created for auto deployment to a device, troubleshooting for that error should be done as explained in the Troubleshooting the file share

4. Check the file share status in OME.
   a. The file share status is at the bottom of the file share wizard and is in the 'Deployment Settings' preference.

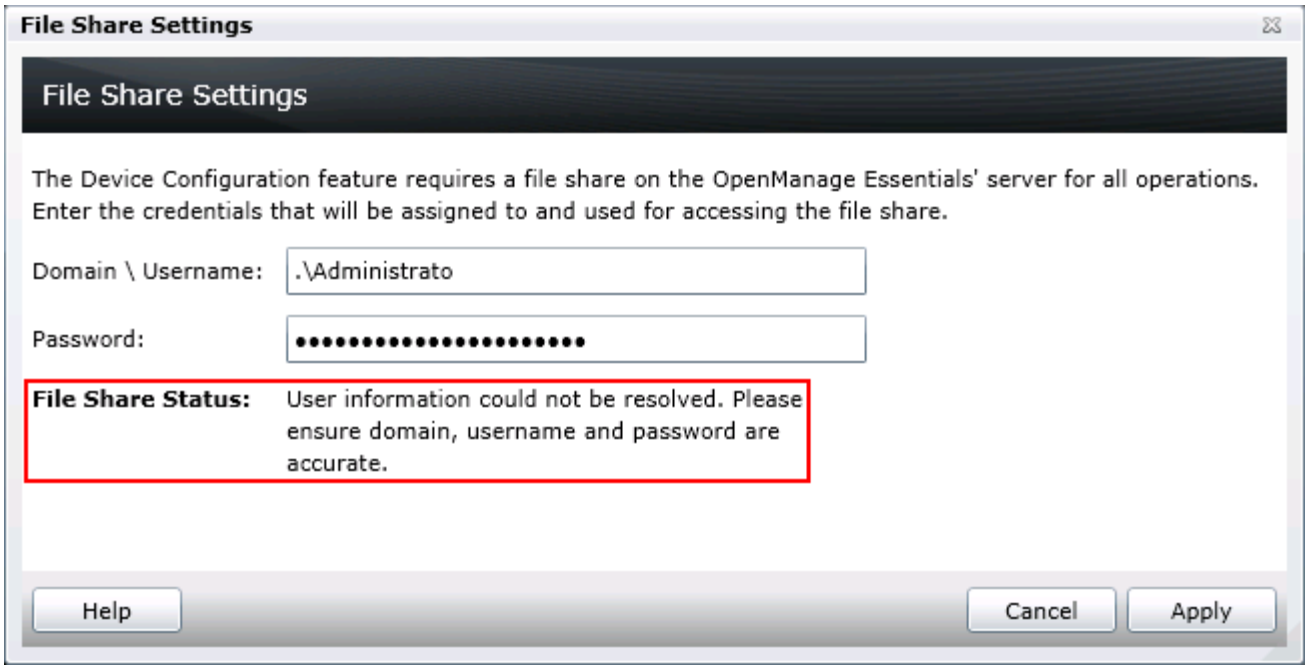

Figure 18 File share settings popup status

5. Check the username, domain and password in OME.
6. Check the share folder in Windows Explorer.
   a. Verify the 'ServerConfig' folder exists under the installation configuration folder (by default under 'Program Files\Dell\SysMgt\Essentials\configuration').
   b. Verify the folder is shared. Right click the folder, select 'Properties', select the 'Sharing' tab. The folder should be shared. The 'Advanced Sharing' permission settings should have the user entered in OME as the only user with permissions to the folder.

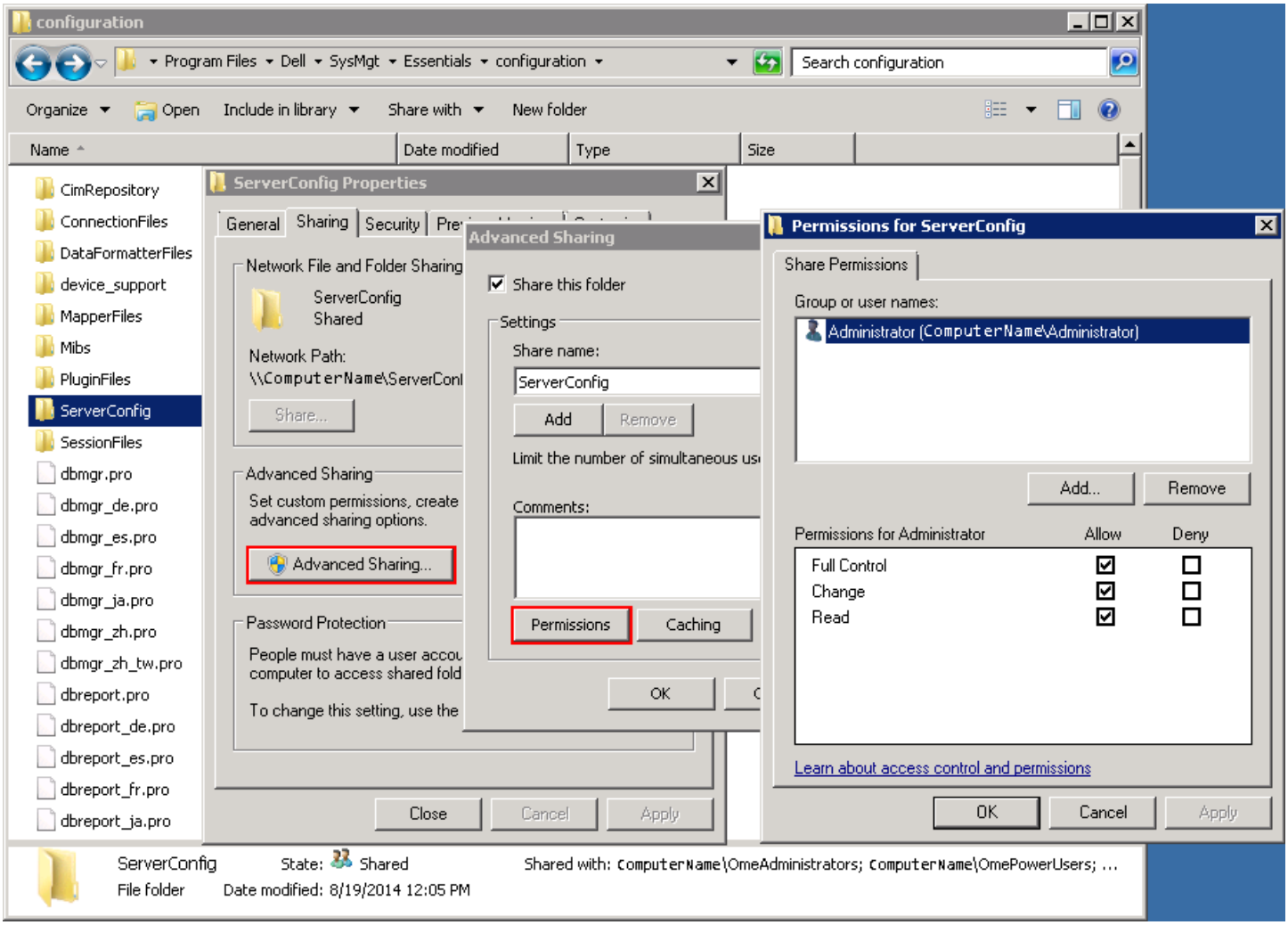

Figure 19 Advanced sharing tab of the 'ServerConfig' folder

7. Verify the share folder location using the 'net share' command.
   a. Open the command prompt and type 'net share'.
   b. A share with the name 'ServerConfig' should be in the network share list.

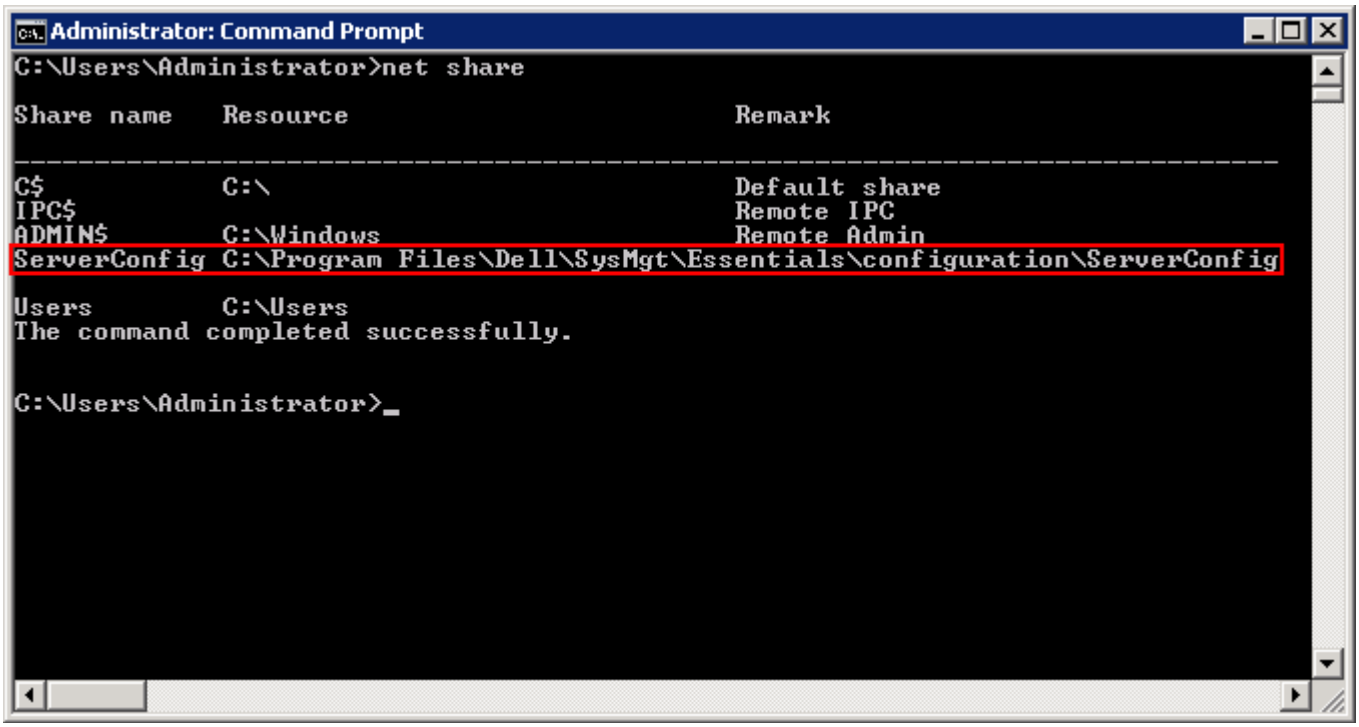

Figure 20 Net share command results

8. Check the user permissions in the 'User Accounts' window.

11.5 Troubleshooting creating a template

Troubleshooting creating a template from a reference device

5. Make sure the file share settings are correctly configured. See the How to setup the file share section or the Troubleshooting the file share section.
6. Run the task again. Right click the task or task execution history and select 'Run'.
7. The task execution may have an 'LC' code in the details. Review the 'LC' code in the iDRAC documentation. See the Additional resources section below.
8. Make sure the provided credentials have enough privileges to run the task (requires administrator privileges on the iDRAC/CMC).

Troubleshooting creating a template from a file

9. Make sure the file meets the file requirements in the File requirements section.
10. If you do not see the file you are looking for, make sure the file type is correct (in the file dialogue next to file name). The two options are .xml and .ini.

Troubleshooting deploying a template section. If a device was discovered but could not be deployed for some reason, that information is also recorded in the task execution history entry.

The task execution history details provide troubleshooting information.

1. Check that the file share settings are entered correctly (see the Troubleshooting the file share section.
2. Make sure the 'Deploy Configuration to Undiscovered Devices' task is enabled.
3. The service tags cannot match the service tag of a discovered device. To deploy to discovered devices see the How to deploy a template section.
4. Check if the 'Deploy Configuration to Undiscovered Devices' task has run recently. A task execution history is added every time the 'Deploy Configuration to Undiscovered Devices' task runs against auto deployment targets.

11.6 Troubleshooting deploying a network ISO

The task execution history details provide troubleshooting information.

If the network is unable to find the ISO share, check the following:

1. Verify the IP address in the share location.
2. Verify the path to the folder of the share.
   a. A common misconception is to put the share base folder in the share name area; however, the share base folder is for the full folder path. For example:
      i. Share: share\isos\linux File name: Ubuntu.iso (correct)
      ii. Share: share File name: isos\linux\Ubuntu.iso (incorrect)
3. Verify the user credentials for the file share.

If the task is unable to find the file, check the following:

1. Check the file name for correctness.
2. Check the path of the ISO.

11.7 Troubleshooting configuration compliance

If a device does not show in the pie chart, make sure it meets the device configuration requirements (see the Target device requirements section).

If a device was recently licensed and shows as 'unlicensed', refresh the inventory of the device by right clicking on the device in the device view under 'Manage' -> 'Devices' and selecting 'Refresh Inventory'. After the inventory is run, the device state should no longer be 'Not Licensed'.

If a device is shown in the pie chart, follow the states in the How to view and leverage the compliance report section.

If you believe the state of a device is incorrect, refresh the configuration inventory of the device (right click the device compliance entry and select 'Run Inventory Now').

A Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Dell Attribute Registry:
  http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx#attributereg

- Dell iDRAC7 with Lifecycle Controller 2 White Papers:
  http://en.community.dell.com/techcenter/systems-management/w/wiki/4317.white-papers-for-idrac7-with-lifecycle-controller-2.aspx

- Dell iDRAC Licensing:
  http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac.aspx#iDRAC7_licensing

- Dell LC Error Codes:
  http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx

- Dell OpenManage Essentials TechCenter page:
  http://en.community.dell.com/techcenter/systems-management/w/wiki/1989.openmanage-essentials.aspx