Managing Server Configuration by using Dell EMC OpenManage Essentials

This technical white paper describes the process of managing and replacing server configuration by using OME.

Dell EMC Engineering Team
February 2018

A Dell EMC Technical White Paper

Revisions

Date	Description
August 2017	Initial release
February 2018	Redfish Streaming Support Update

Contents

1. Configuration Baseline, compliance, and remediation

The configuration of a server in a production environment must be properly maintained to ensure availability of the server. These server configuration settings tend to be drifted over time because of various reasons. The Device Compliance Portal enables you to verify and ensure the compliance of multiple servers to a device configuration baseline that serves as a baseline. The compliance status indicates compliance status of device with respect to the associated baseline. The Device Compliance Portal also allows you to create baseline, and assign the required baseline to multiple production servers for establishing the compliance.

1.1 Prerequisites

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

1.1.1 Target server requirements

- For 12th generation PowerEdge servers, the minimum supported version of iDRAC is 1.57.57.
- For 13th generation PowerEdge servers, the minimum supported version of iDRAC is 2.0.
- For 14th generation PowerEdge servers, the minimum supported version of iDRAC is 3.00.00.00 and later.
- By default, the 'Server configuration for OpenManage Essentials' license is installed on the iDRAC. This is a separate license from the iDRAC license.
- iDRAC Enterprise or iDRAC Express license—this is a separate license from the 'Server configuration for OpenManage Essentials' license.

1.1.2 Redfish Streaming Support

With OpenManage Essentials version 2.4, the device configuration and deployment feature now makes use of iDRAC's Redfish Streaming interface.

- For PowerEdge servers, the minimum supported version of iDRAC is 2.50.50.50 and later for Redfish support.

With Redfish Streaming support available, the existing file share option becomes redundant. The file share can be disabled, as described in the later sections. It is highly recommended to upgrade iDRAC to the minimum supported version.

1.1.3 File share settings

The Device Configuration and Deployment feature now makes use of iDRAC's Redfish interface. However, for servers not having the minimum supported iDRAC version 2.50.50.50, it would require a staging area (file share). This section describes about the file share and setting up the file share.

1.1.3.1 File share overview

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

1.1.3.2 Setting up the file share

The file share settings must be entered in OME. The file share settings require a user name and a password. The user name and password of the OME user must have enough privileges to read and write files on the system. During a deployment or configuration task, the user name and password are sent to the remote targets to access the file share. Using an Administrator account is recommended.

1. Navigate to the **Configuration** portal.
2. In the left pane, under **Common Tasks**, click **File Share Settings**.
3. Type the user name and password of a user on the OME system that has necessary privileges to read and write files to the system.
4. If there are server devices being managed without having minimum supported iDRAC version 2.50.50.50, click the **Allow using file share for Device Configuration feature on server** check box. If iDRAC on all server devices has been upgraded to version 2.50.50.50 or later, you do not select this check.

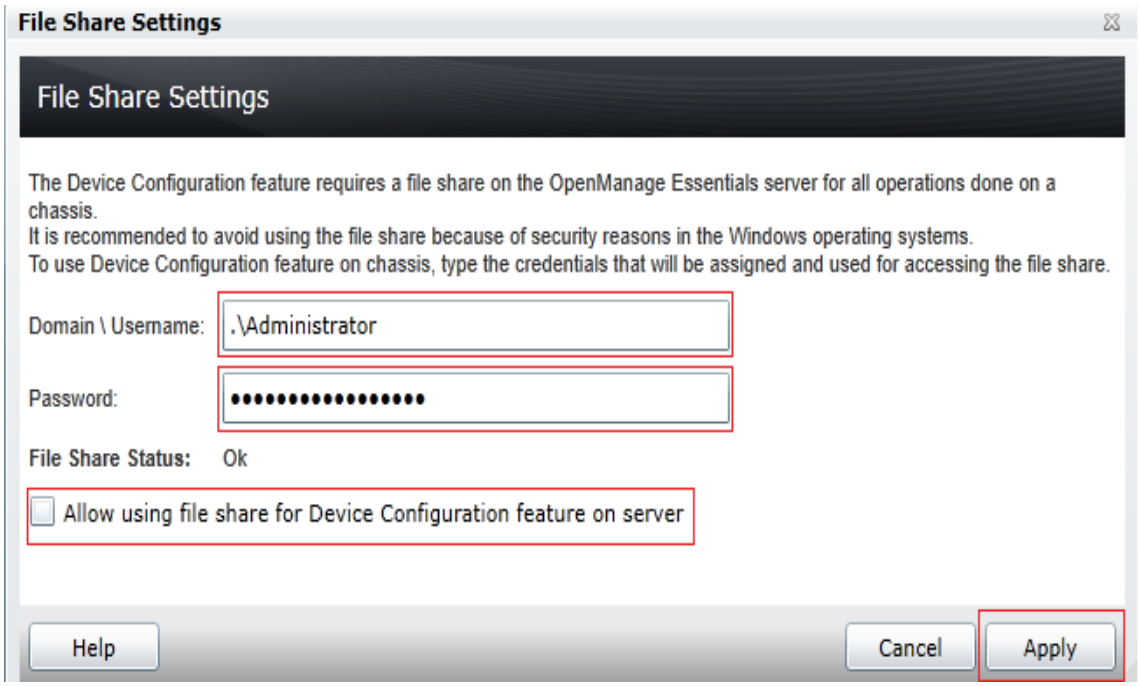

Figure 1 File share settings

5. Click **Apply** If the **Allow using file share for Device Configuration feature on server** check box is selected, a message is displayed to upgrade servers to latest firmware:

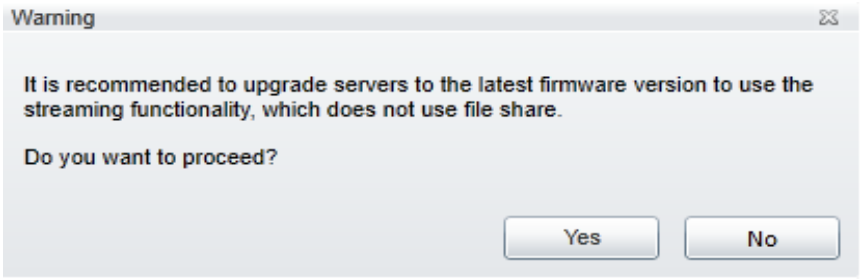

Figure 2 Firmware Warning

6. Click **Yes,** to continue to use file share.
7. After configuring the file share, at anytime later if check box is cleared, a message is displayed to indicate the configuration compliance of servers will be lost which have iDRAC version earlier than the minimum supported version of 2.50.50.50

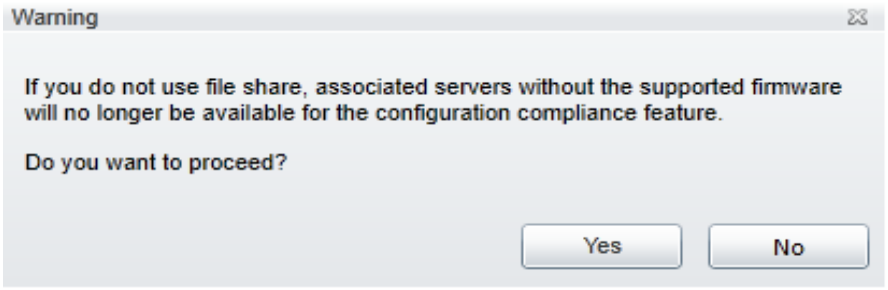

Figure 3 Compliance Warning

1.1.3 Setting up and running the configuration inventory

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

Note: Dell EMC Networking IOAs will not be listed for scheduled configuration inventory collection.

1.1.3.1 Modifying configuration inventory credentials and/or schedule

The configuration inventory schedule and credentials can be modified. The configuration inventory can be disabled if network or performance issues are observed. To modify the schedule and setting the credentials for the configuration inventory:

1. Navigate to the **Configuration** tab under the **Manage** tab.
2. In the left pane, under **Common Tasks**, click **Configuration Inventory Schedule**.
3. If the credentials have not been added, click **Add New Credential**.
    a. Type a unique description name.
    b. Type the user name 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**.

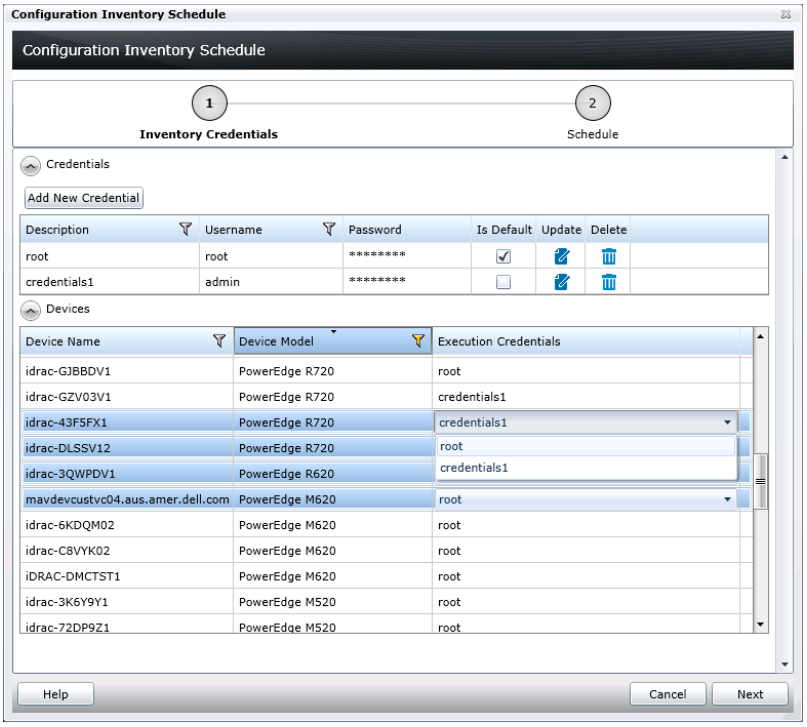

Figure 4 Configuration inventory credentials

5. Select the **Enable Configuration Inventory** check box.
6. Select 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** table. Double-click the execution history to view task information. Else, right-click the execution history, and then select **Details**.

1.1.3.2 Running configuration inventory per target

To get the current configuration inventory from a device:

- Click **Manage → Devices**.

- Right-click the target devices, pause the pointer over **Device Configuration**, and then select **Refresh Device Configuration Inventory**.

1.2 Creating Baseline

Understanding and creating baseline is necessary for using the configuration features. This section describes about creating a baseline from a reference device or from a file.

1.2.1 Baseline Definition

A baseline 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 baseline for specific use cases. A user can edit, clone, delete, or rename a baseline, or can use baseline to make device(s) complaint. A sample baseline must be cloned to deploy, or to use it for compliance.

1.2.2 Prerequisites

To create a baseline from a reference device, the device must meet the same requirements listed in the **Target Server requirements** section. To create a baseline, the server does not require a license.

1.2.3 Creating a baseline from a reference device

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

1.2.3.1 Creating a baseline from a reference device

- Click **Manage → Configuration**.
- In the left pane, under **Common Tasks**, click **Create Baseline**.
- Enter a unique name for the baseline.
- Select **Create from Device**.
- 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.

- Enter the execution credentials for the target server. The credentials must have the Administrator privileges on the target iDRAC.

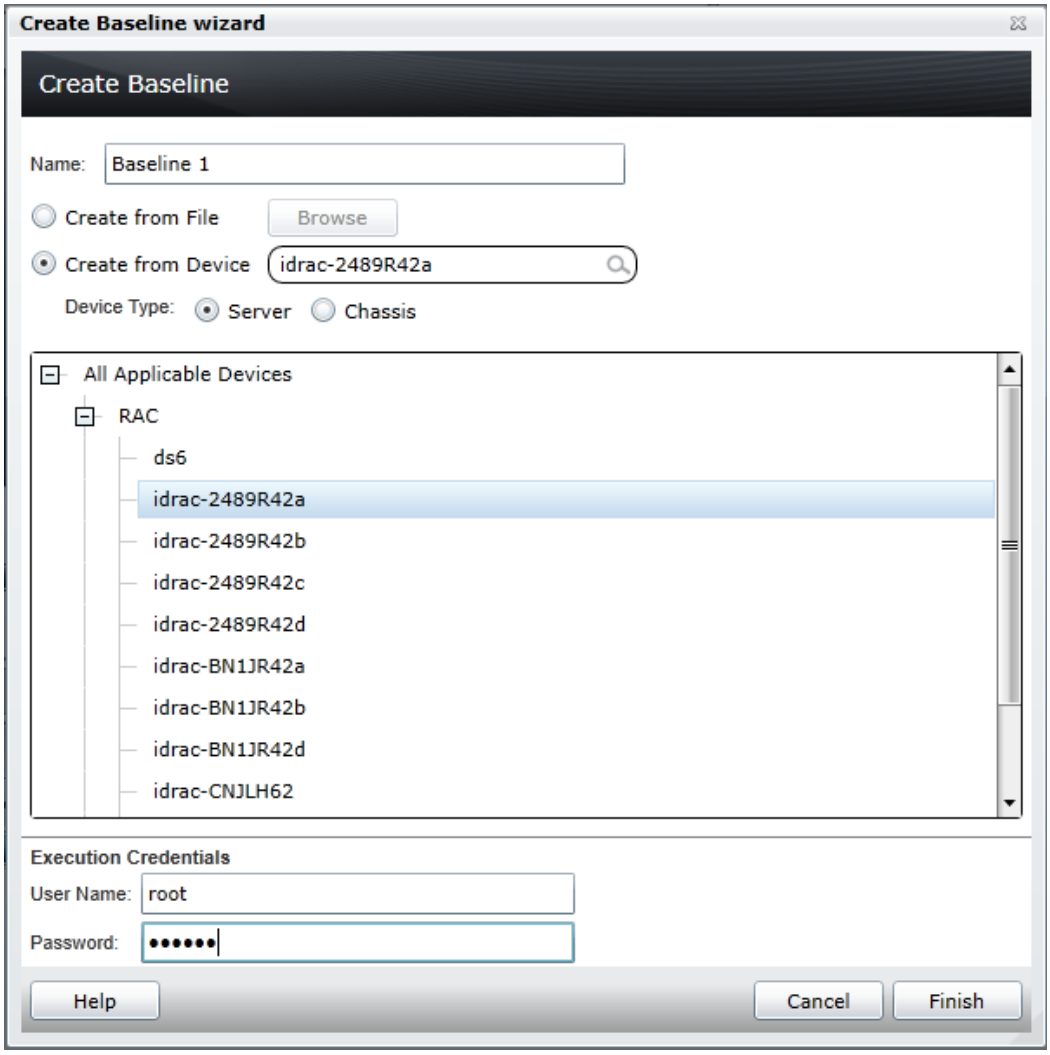

Figure 5 Create baseline from reference device wizard

- Click **Finish**, and then click **OK**.

A task is created when the wizard is closed. To view the created task, click the **Tasks** tab in the **Configuration** portal. To view the progress of the task, see the **Task Execution History** table. To view the execution history information, double-click the task execution history, or right-click the task execution history and, then select **Details**. Information about issues such as incorrect credentials is displayed.

If the task is successful, a template is created and displayed under **Server Baselines**.

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 the iDRAC credentials.

Note: Baseline template does not contain any destructive attributes (for example, Raid Foreign configuration, and Disk Physical state attributes).

1.2.4 Creating a baseline from an XML configuration file

This section describes about creating a baseline from an XML configuration file. A configuration XML is used for server templates. A configuration file can be obtained by exporting a template to file in OME. Configuration baseline files are also available from the Dell TechCenter.

1.2.4.1 File requirements

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

1.2.4.2 Creating a baseline from an XML file

- Click **Manage → Configuration**.
- In the left pane, under **Common Tasks**, click **Create Baseline**.
- Enter a unique name for the template.
- Select **Create from File**.
- Click **Browse**, and navigate to the file location.
- Select the file, and click **Open**.

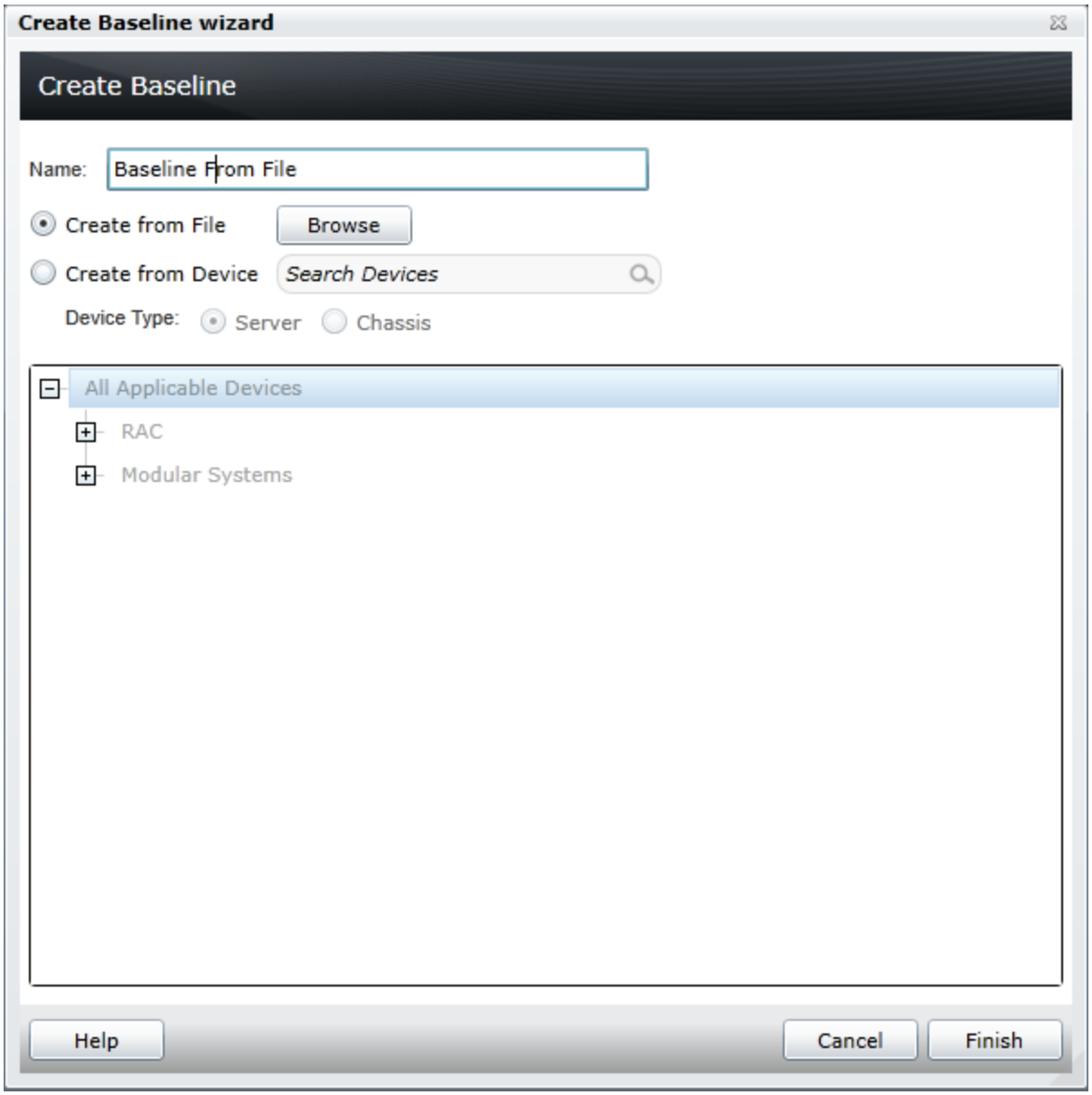

Figure 6 Create baseline from file wizard

- Click **Finish** to create the baseline. The baseline is added under **Server Baslines**.

1.3 Associating devices to a baseline

The configuration compliance detects drift of the device attributes from the baseline attributes. A process called configuration inventory gets configuration information (inventory) from all applicable devices and compares the inventory against an associated compliance baseline.

1.3.1 Prerequisites

- The file share must be configured (see the **How to set up the file share** section).
- The target devices must fulfill the minimum requirements for the deployment and configuration features (see the **Target server requirements** section).
- At least one user-created baseline (a cloned sample baseline is a user-created baseline).
- Configuration Inventory must be enabled, and the target device credentials must be provided.

1.3.2 Associating devices to a baseline

A device requires an associated compliance baseline for the device to have a compliance status in the compliance pie chart.

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

To set a compliance baseline for a device, you must associate the device to a baseline. A device may only have one associated baseline. To associate a device to a baseline:

1. Click **Manage** → **Configuration**.
2. In the left pane, under **Common** Tasks, click **Associate Devices to a Baseline**.
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 server requirements** section), and only those that are of the same device type as the baseline are displayed.

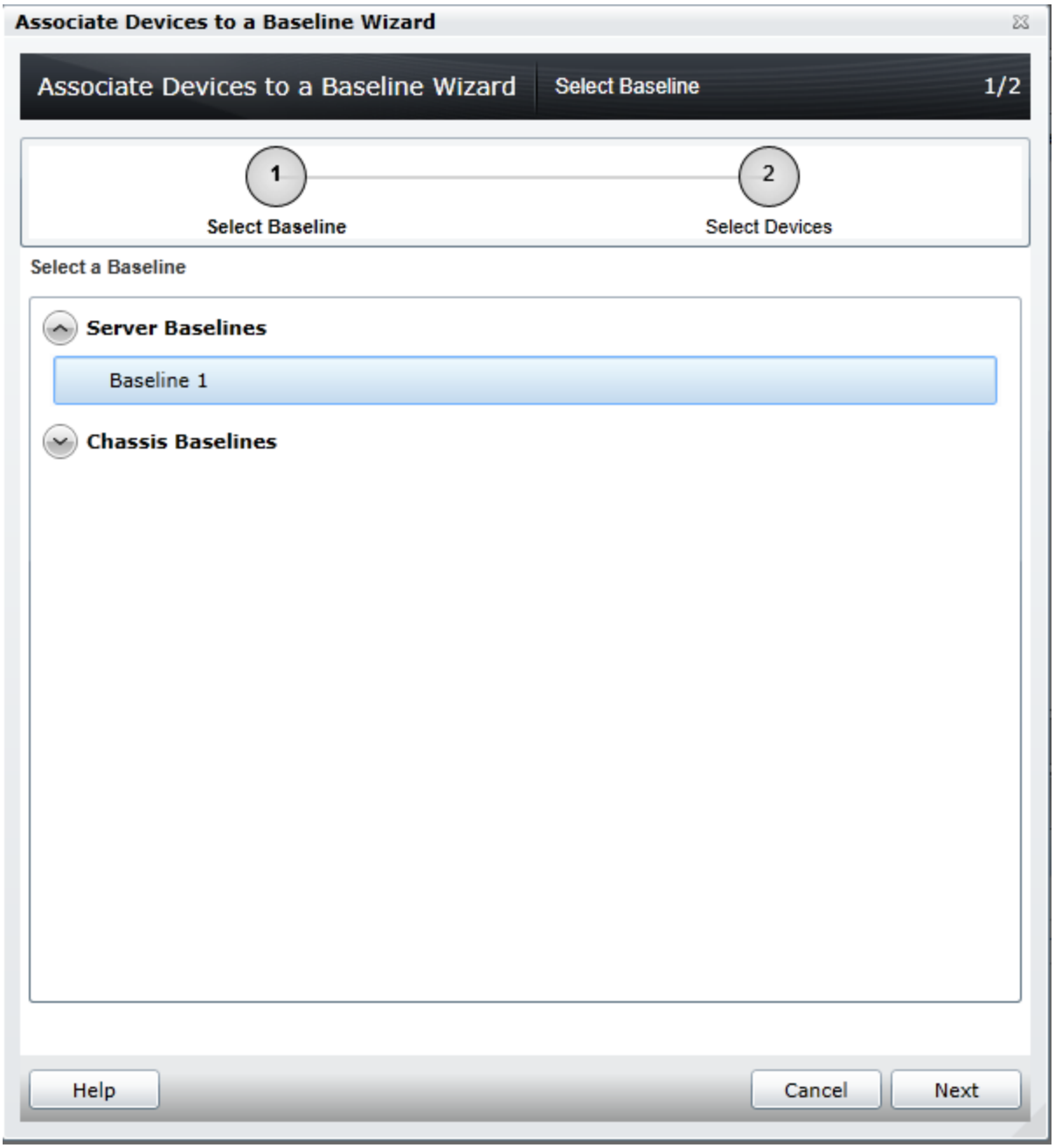

Figure 7 Associating devices to a Baseline (Baseline selection)

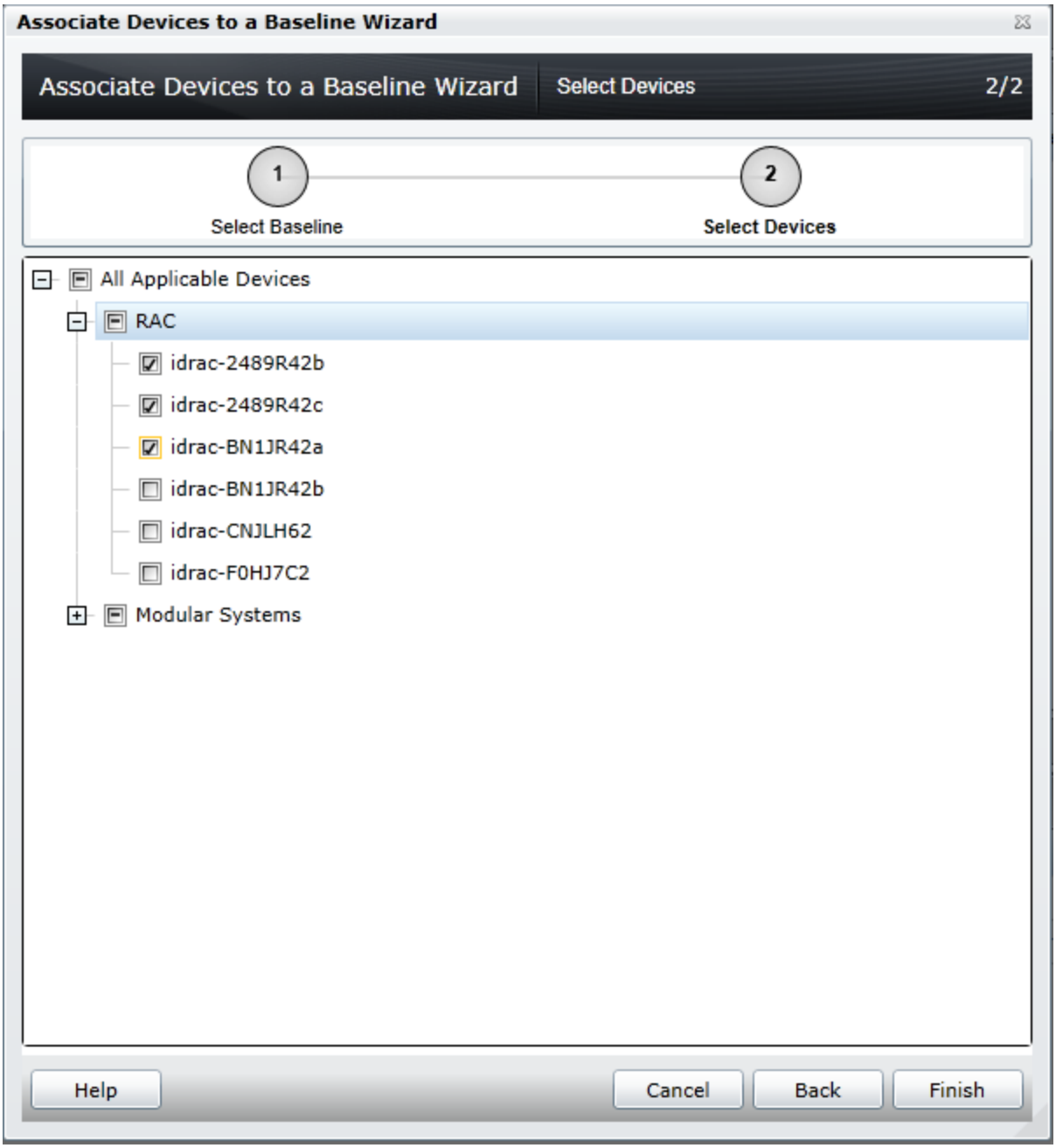

Figure 8 Associating devices to a Baseline (device selection)

1.3.6 Viewing and leveraging 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 Server requirements** section). Every eligible device is in one of the states. Clicking a slice of the pie chart displays 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.

- Compliant Devices
  - No action required
- Not Compliant Devices
  - Double-click the compliance row to view the differences between the associated baseline and the device inventory
  - Adjust the device settings, or associate to a different baseline, to make the device compliant
- Not Inventoried Devices
  - Inventory the device. See the **Setting up and running the configuration inventory** section.
  - Ensure the credentials of the target devices are correct
- Not Associated Devices
  - Associate the devices to a template. See the **Associating devices to a Baseline** section.
- Not Licensed Devices
  - Import a 'Server configuration for OpenManage Essentials' license in the device iDRAC license interface

1.4 Remediation

The devices which are not conforming to the associated baselines can be remediated to make them conform to the baseline configurations.

1.4.1 Prerequisites

- The file share must be configured (see **How to set up the file share** section).
- The target devices must fulfill the minimum requirements for the deployment and configuration features (see the **Target server requirements** section).
- At least one user-created baseline (a cloned sample baseline is a user-created baseline).
- Configuration Inventory must be enabled, and the target device credentials must be provided.
- At least one device should be non-compliant.

1.4.2 Making device(s) compliant

To make the devices compliant:

1. Click **Manage** → **Configuration**.
2. In the left pane, under **Common** Tasks, click **Make Device(s) Compliant**.
3. Enter a name for the task, and click **Next**.
4. Select one or more devices from **Top Devices** grid and click **Next**.
5. Select the **Server Reboot** check box, and click **Next**.

6. Set the schedule and provide credentials for the task.
7. Click **Next**.
8. Review the summary and click **Finish**.

Available reboot options:

- **Manual Server Reboot**: In this option, the server configuration changes are staged, and are applied when the server is manually restarted.
- **Automatic Server Reboot**: If the configuration changes require a reboot, the server is automatically restarted. In case of a reboot, first a graceful shutdown is attempted. If the graceful shutdown fails, a force shutdown is executed, and the server is forcibly restarted.

NOTE: The destructive and password attributes of the devices are not considered for compliance. Therefore, these attributes are not considered for the remediation task.

NOTE: The user configuration attributes will be successfully remediated only if the same user exists on the target devices. You cannot create a new user as the password attributes are not considered for remediation.

NOTE: The remediation task fails for the devices which are non-compliant due to the missing attributes. Clear the Deploy check box for the missing attributes in the corresponding baseline to make the devices compliant.

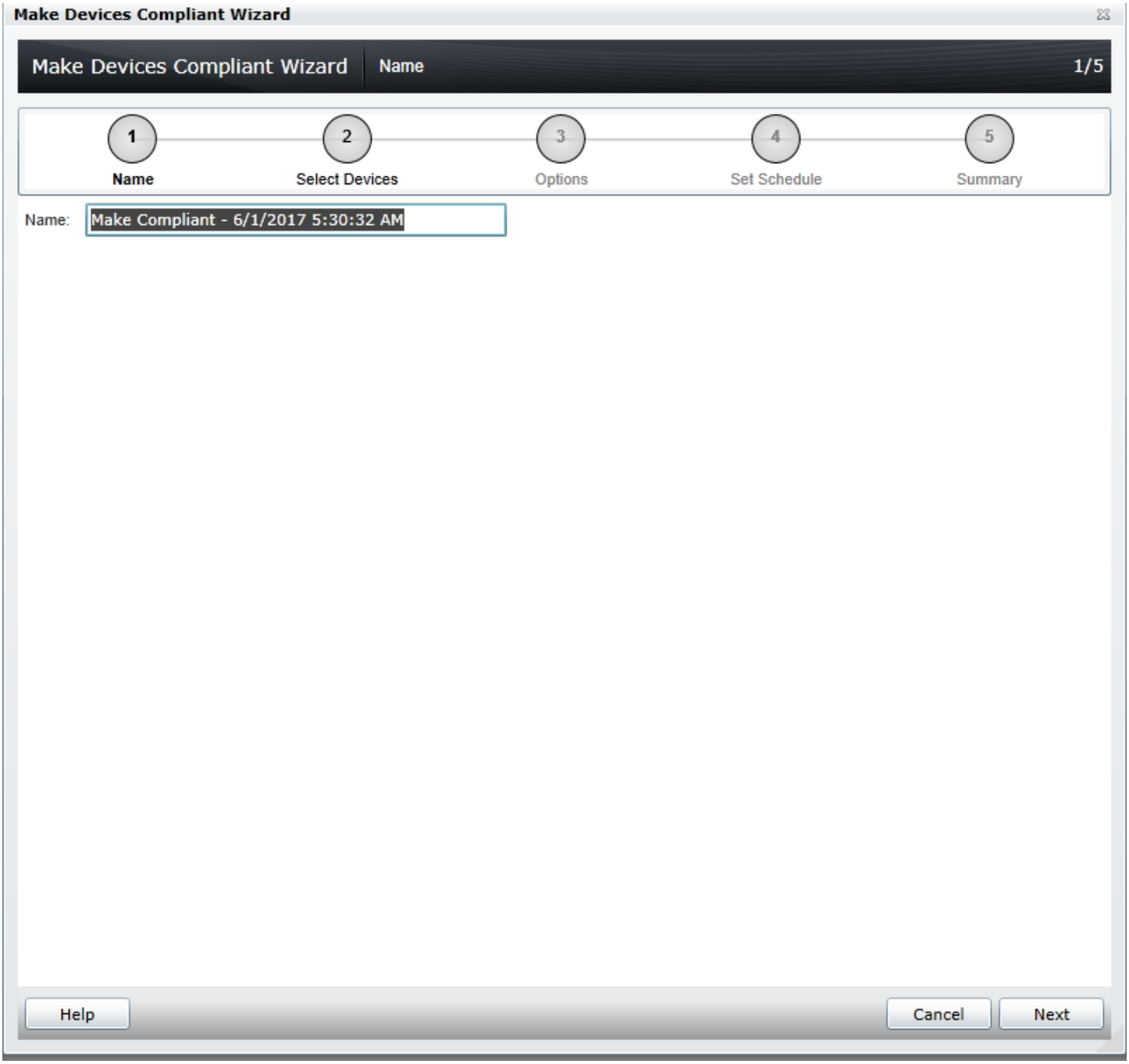

Figure 9 Making Device(s) Compliant Wizard

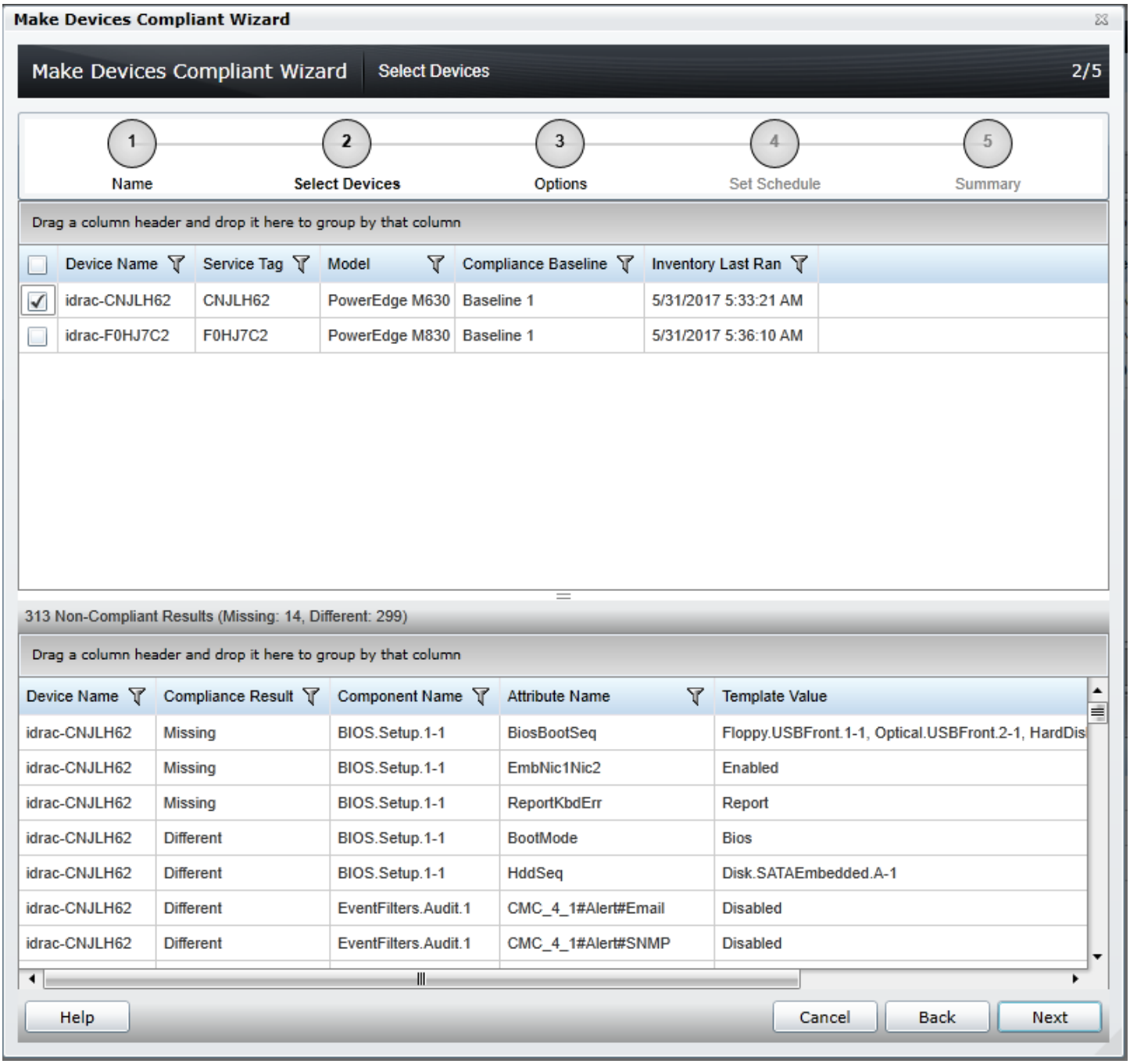

Figure 10 Making Device(s) Compliant Wizard (device selection)

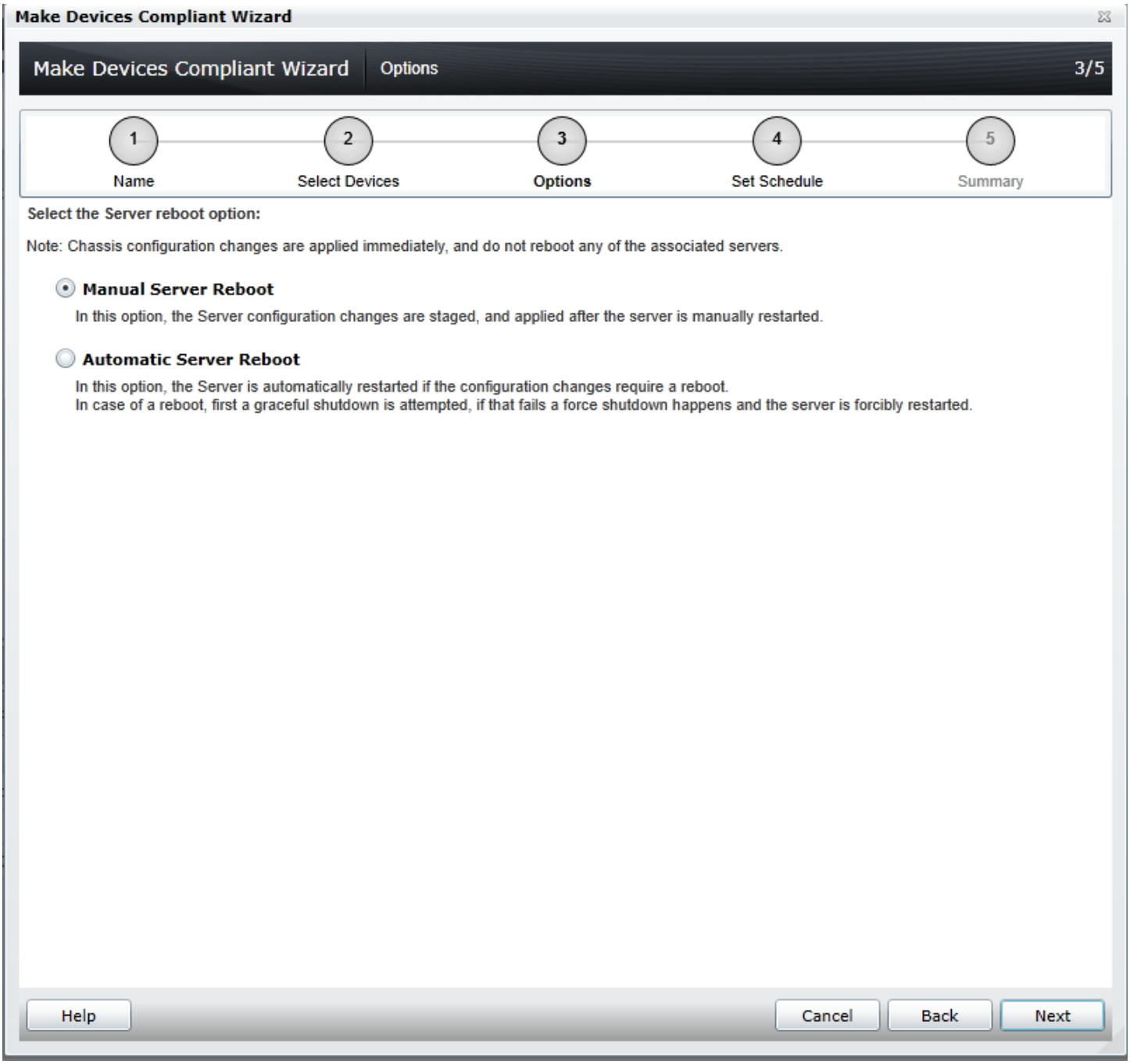

Figure 11 Making Device(s) Compliant Wizard (option selection)

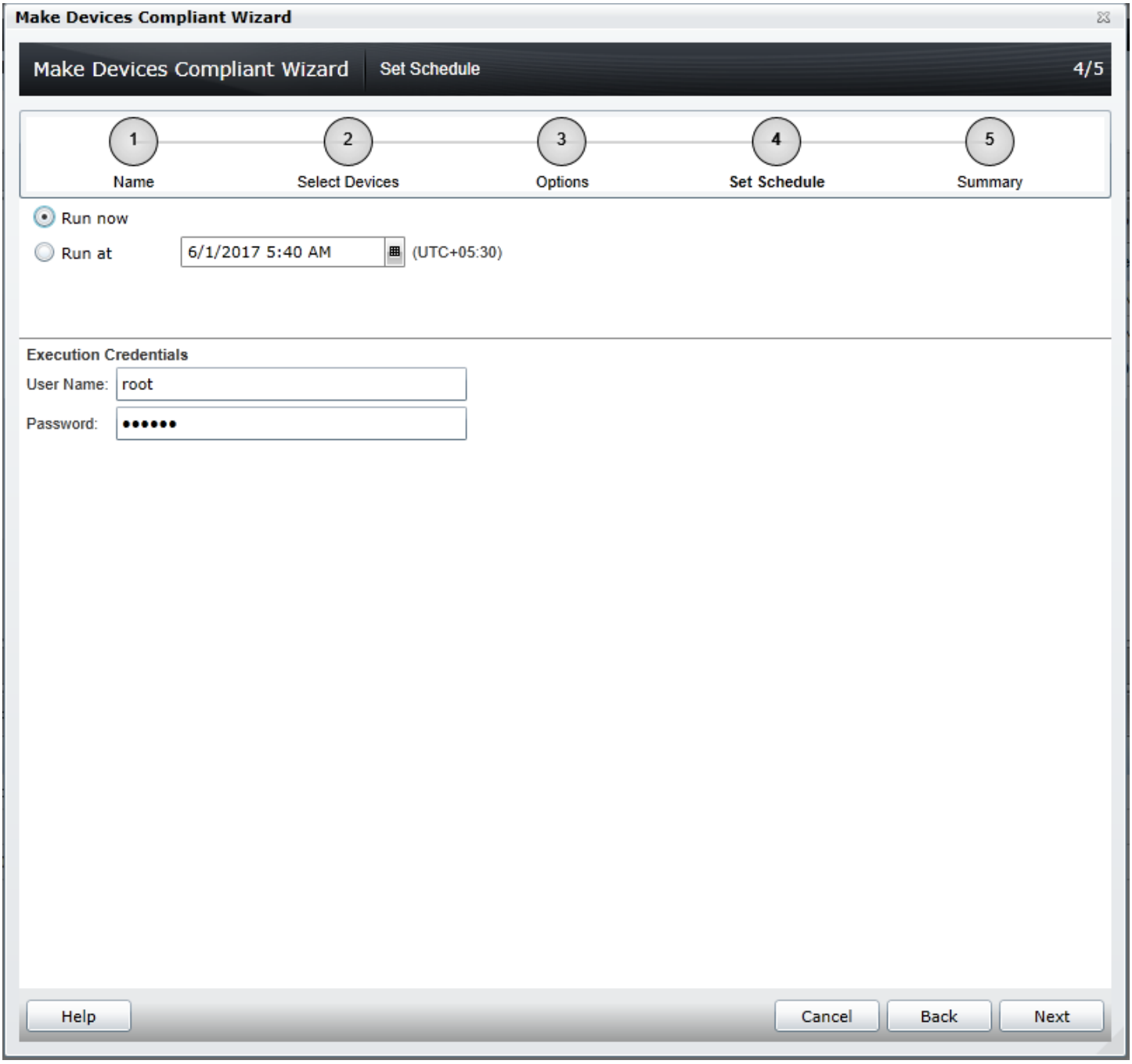

Figure 12 Making Device(s) Compliant Wizard (schedule and credentials)

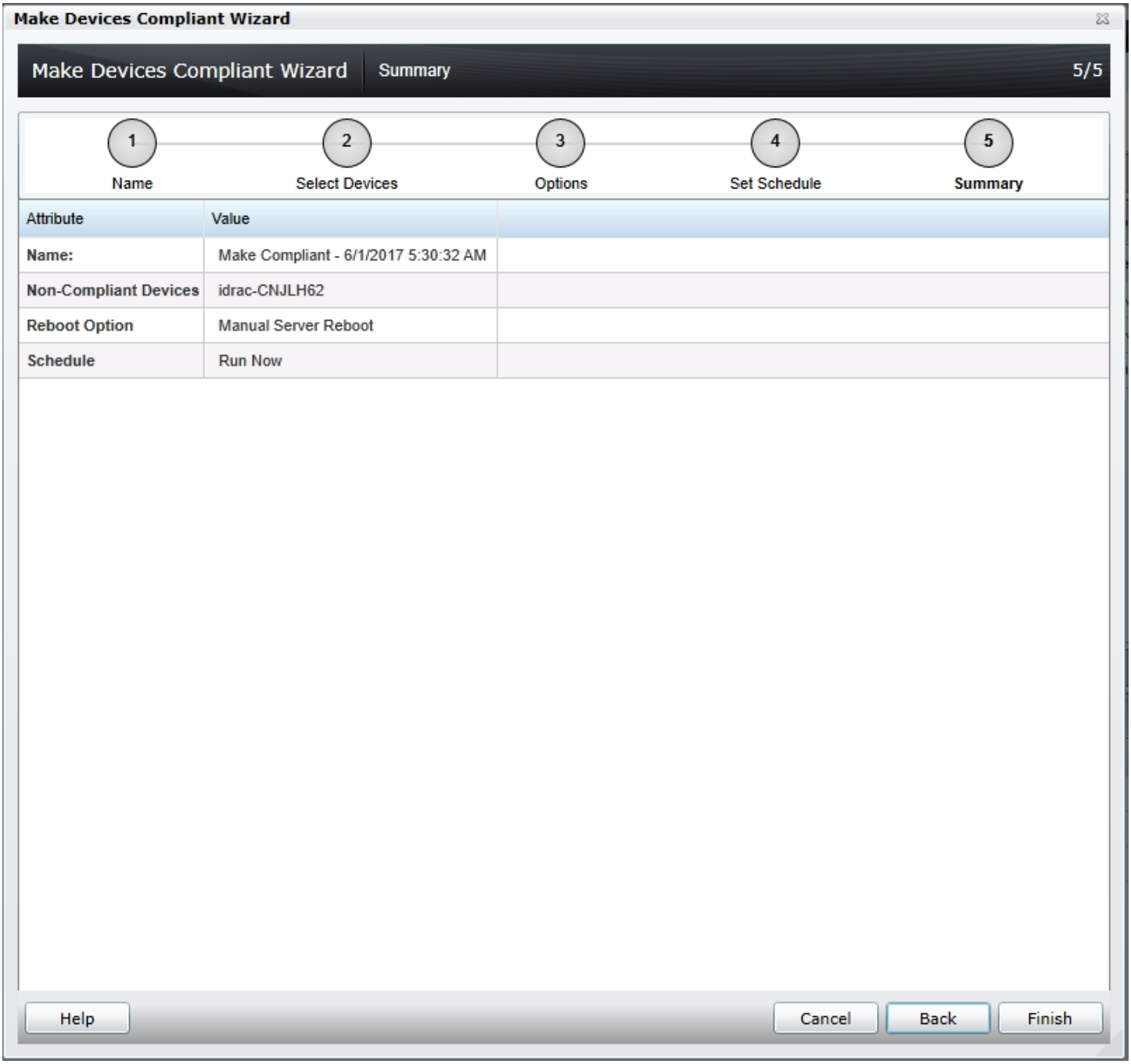

Figure 13 Making Device(s) Compliant Wizard (summary)

2. Server configuration: Backup and Replace

This feature is for the servers that are not deployed by OME by using a compute pool. You must be able to copy the profile (server configuration) of such systems and deploy the same on to a different system when the parent system is removed (deleted from OME and physically removed) for replacement.

2.1 Prerequisites

Before starting Server Backup and Replace feature, you must have configured following settings in OME:

- The file share must be configured (see the **How to set up the file share** section).
- The target devices must meet the minimum requirements for the deployment and configuration features (see the **Target server requirements** section).
- Configuration Inventory must be enabled, and the target device credentials must be provided.
- For replacing, the target server must be a part of the Repurpose and Bare-metal group.

2.2. Backed-up devices

This feature shows the backed-up servers in the OME user interface. This feature is available under **Manage → Configuration → Backed-Up Devices**. You can select each server, and the corresponding server attributes are displayed in the bottom grid. The server backup is created by OME after scheduling a configuration inventory, or when the you refresh the configuration inventory. On the **Backed-Up Devices** page, available right-click menu options are configuration inventory, replace server, and add/remove server from the Repurpose and Bare-metal group.

NOTE: The Backup and Replace feature is applicable only for servers.

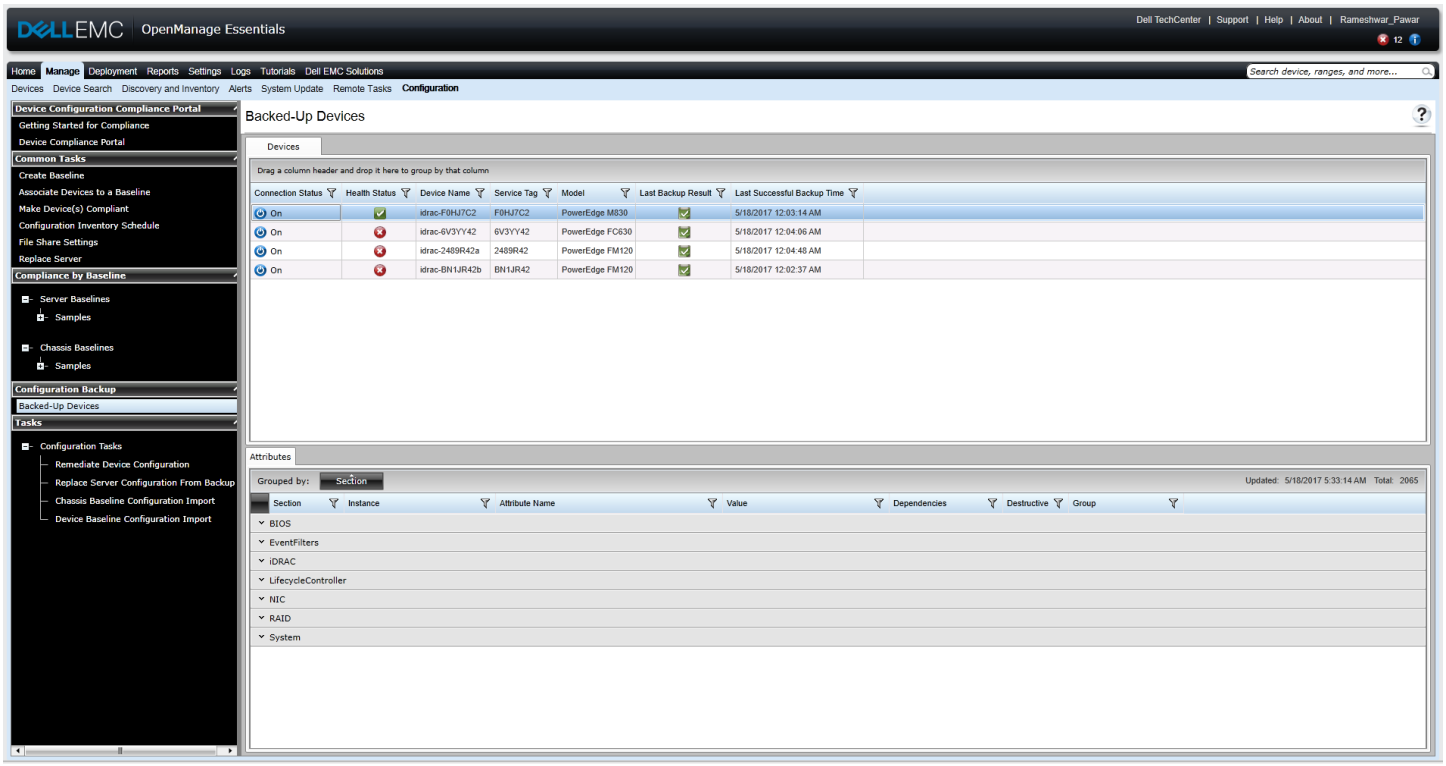

Figure 14 Backed-Up Devices

2.3. Replacing a server

This feature allows you to replace configuration from the source server to a target server. This feature's functionality is similar to the stateless server replacement. Using the Replace Server wizard, the user can create a configuration replace task. Before starting replace server wizard, source and target servers must be added to the Repurpose and Bare-metal group.

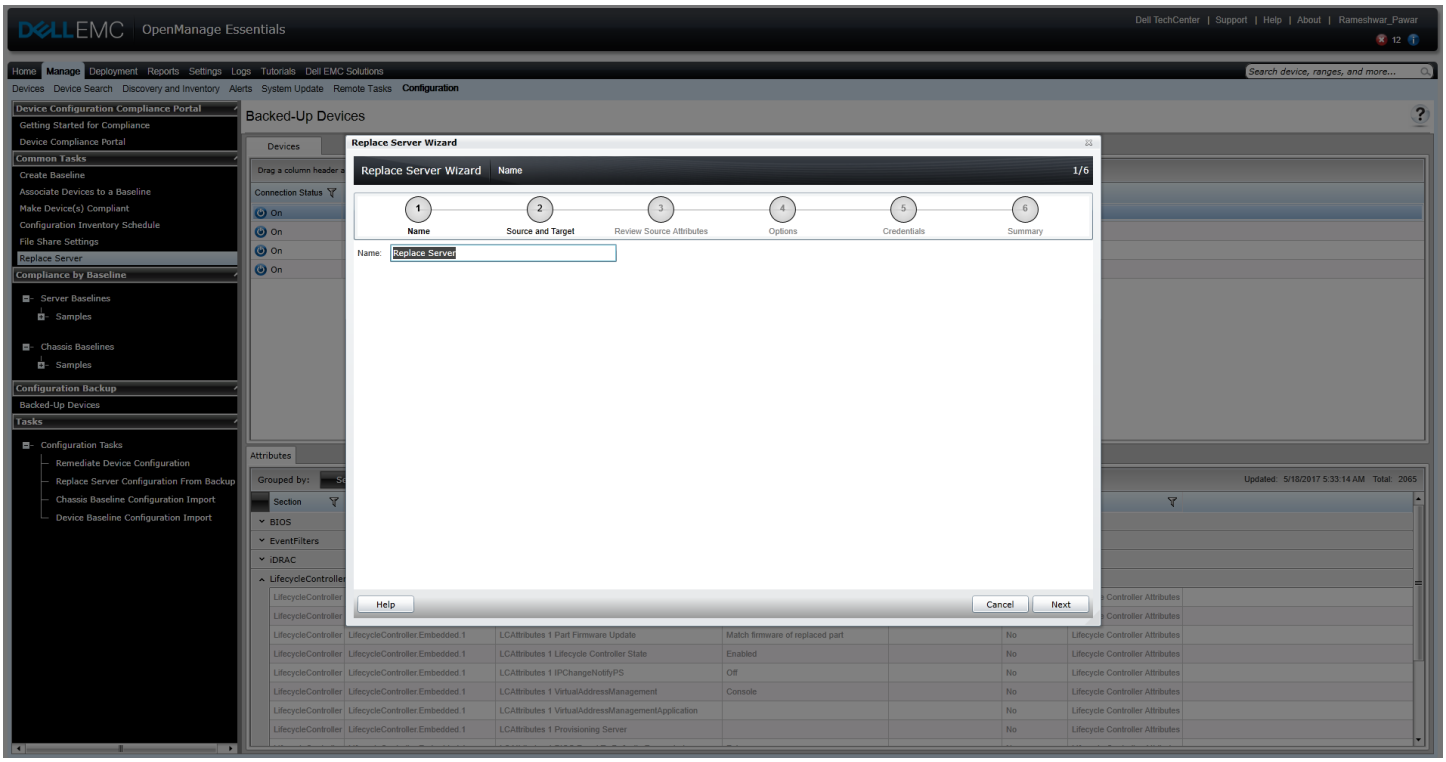

Figure 15 Replace Server (Task name)

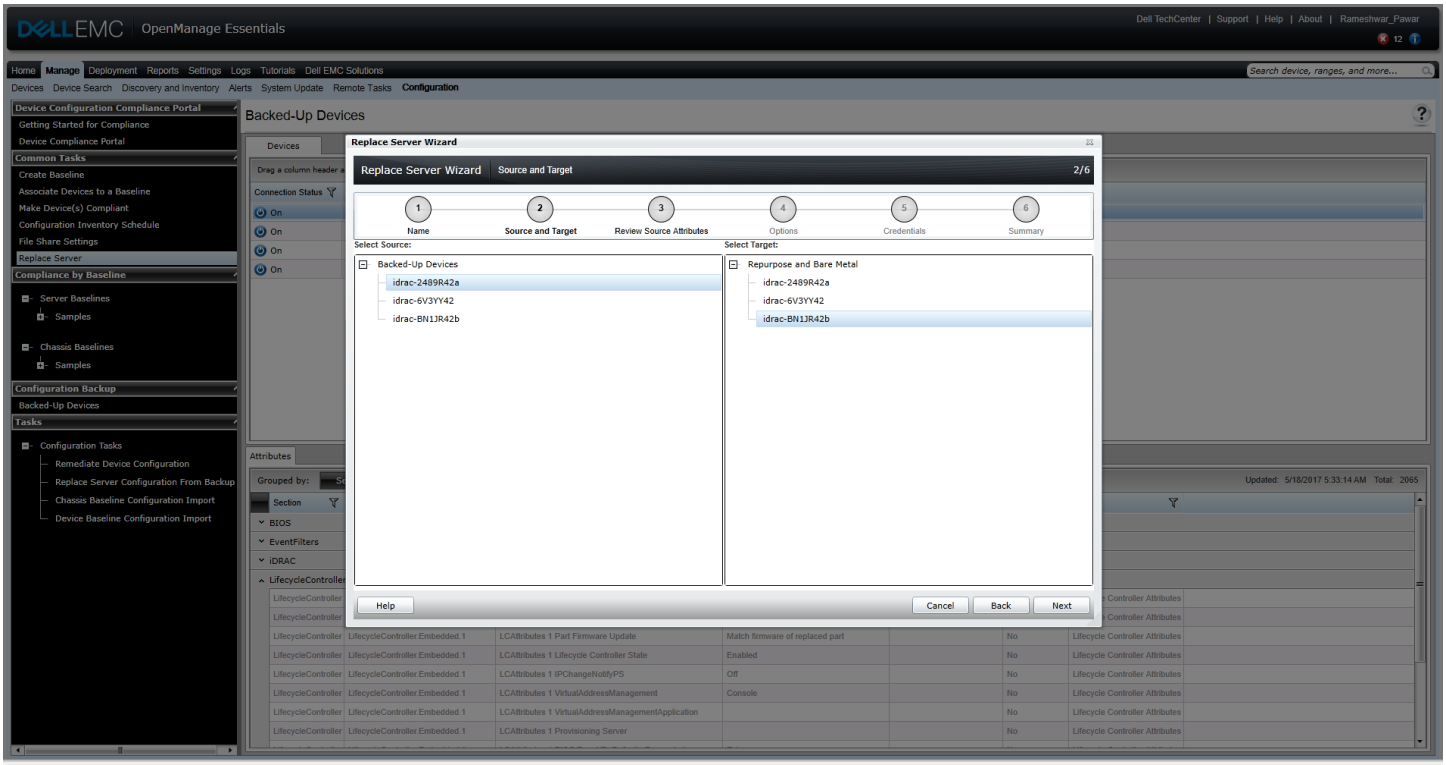

Figure 16 Replace Server (Source and Target Device Selection)

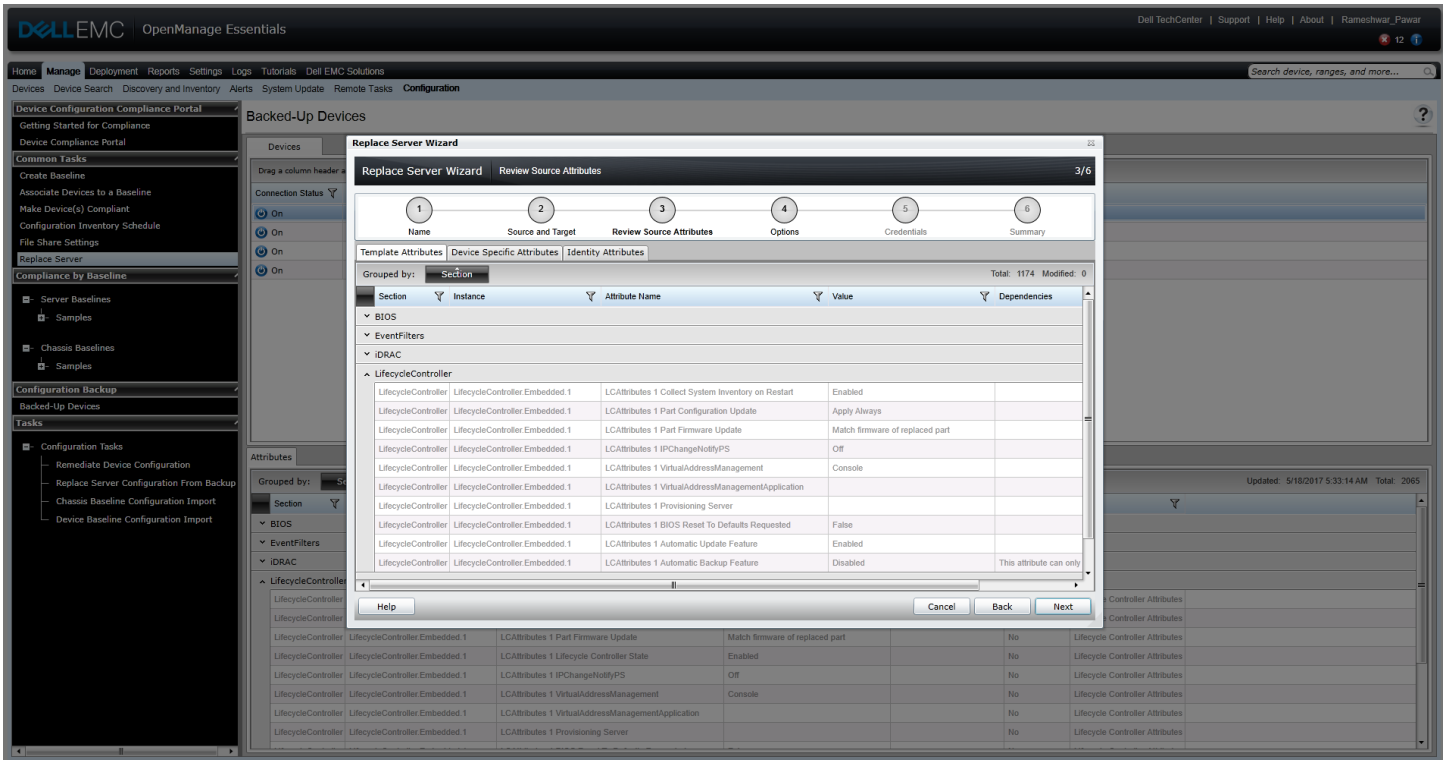

Figure 17 Replace Server(Source attribute review)

Options

- **Remove target from Bare-metal group**: After selection of this option, the target server is removed from the Repurpose and Bare-metal group after the Replace Server task completes successfully.

- **Deploy to target even if virtual identities cannot be removed from the source**: After selection of this option, even if few identities are not removed from the source server during the Replace Server task, the task will continue to remove the identities from the source target and are deployed on the target server.

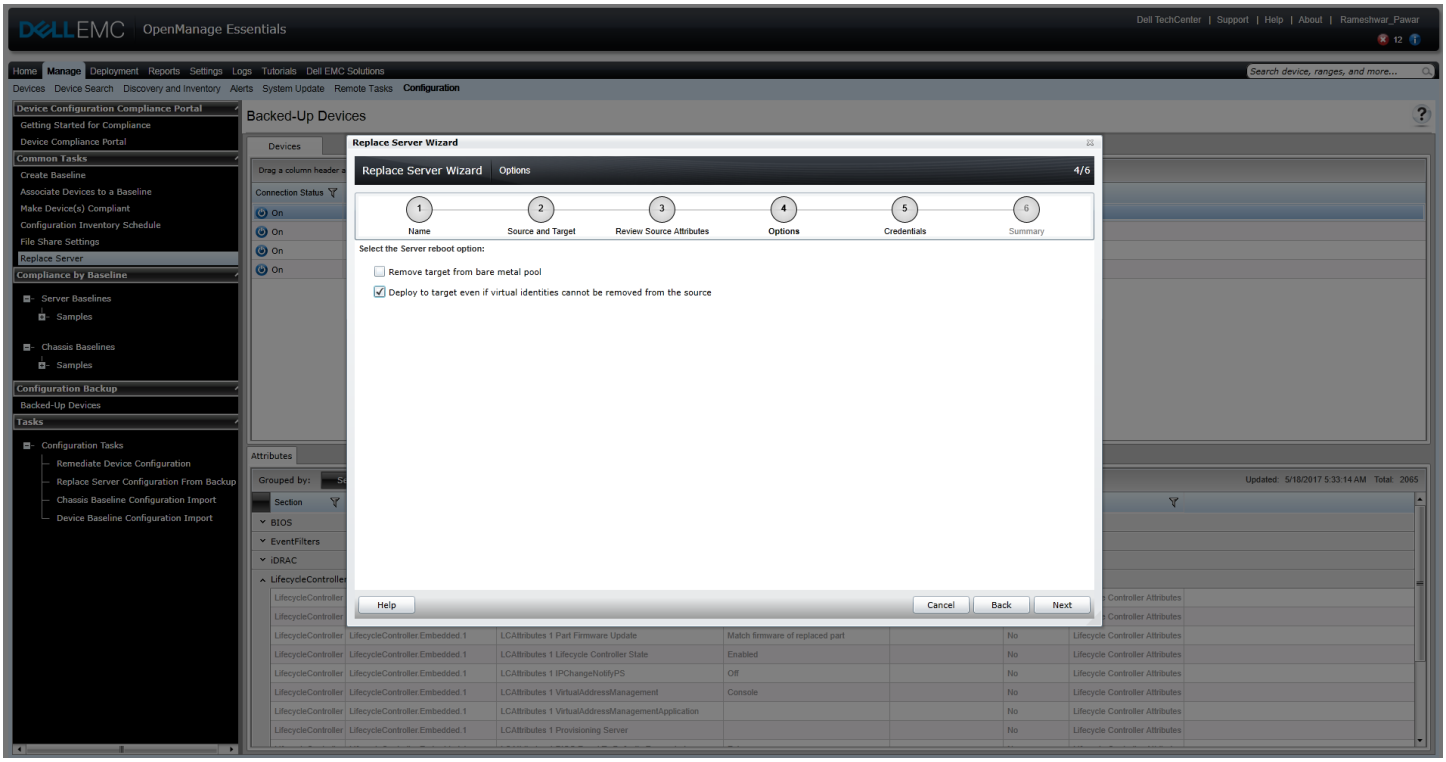

Figure 18 Replace Server(Option Selection)

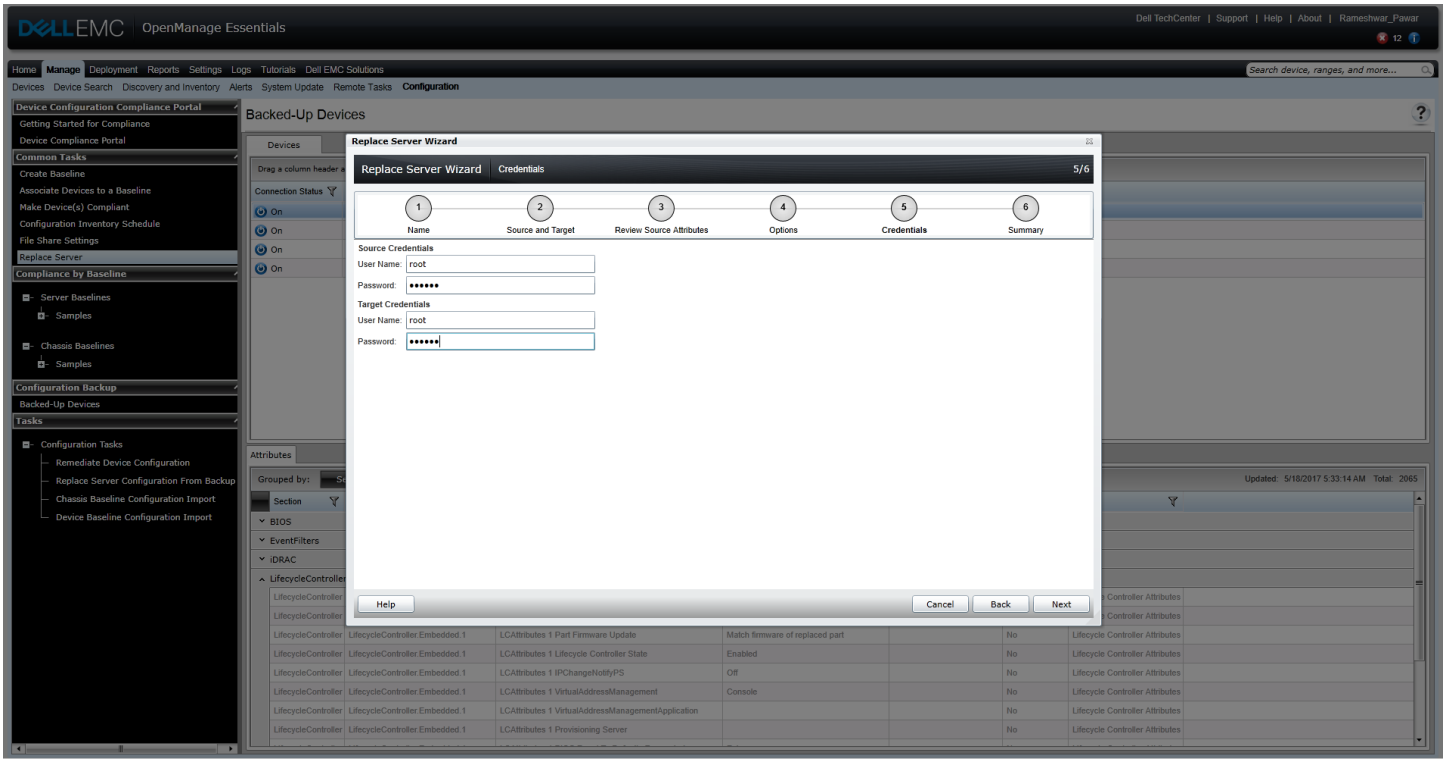

Figure 19 Replace Server(Source & Target Credentials)

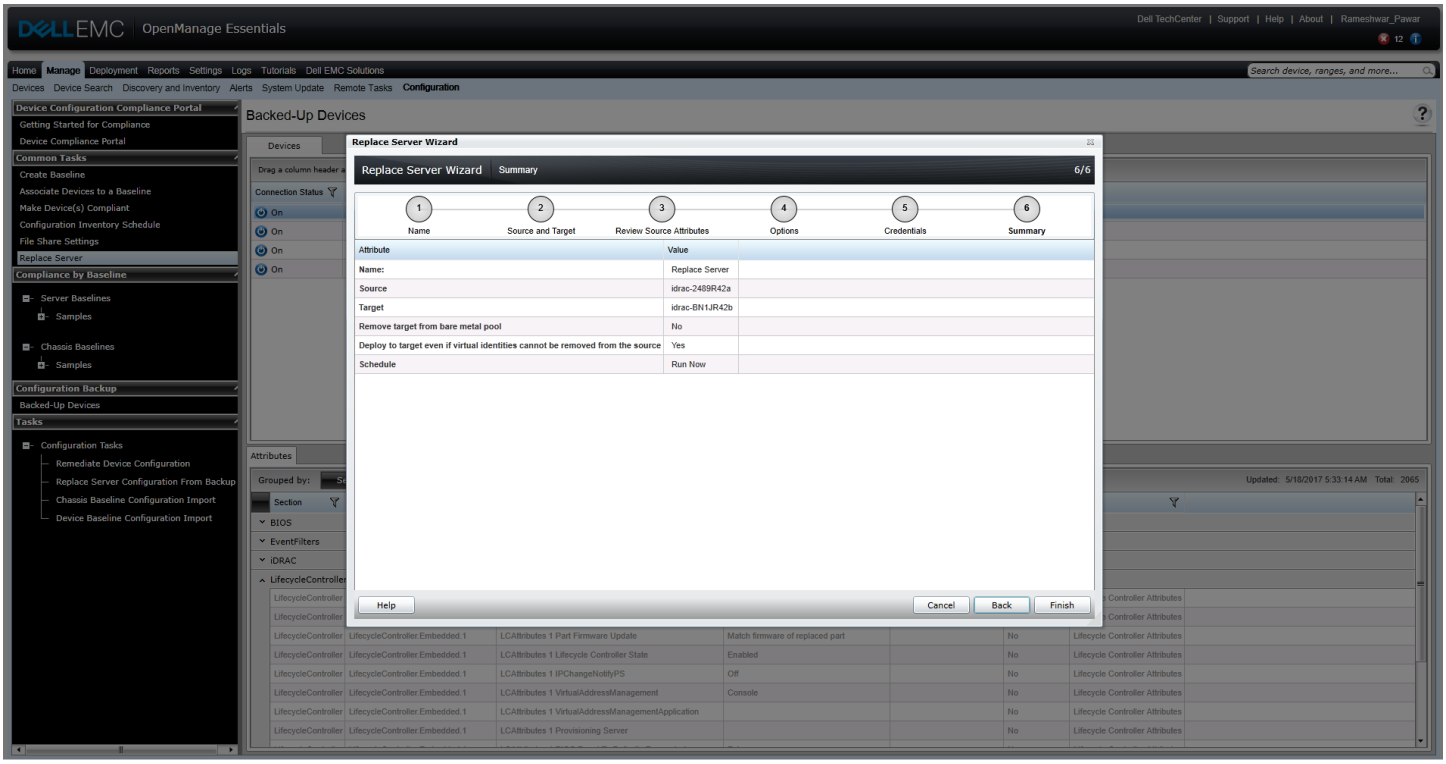

Figure 20 Replace Server(Review Summary)

Finally, the Replace Server task is run, and is displayed under the **Tasks → Replace Server Configuration from Backup** tab.

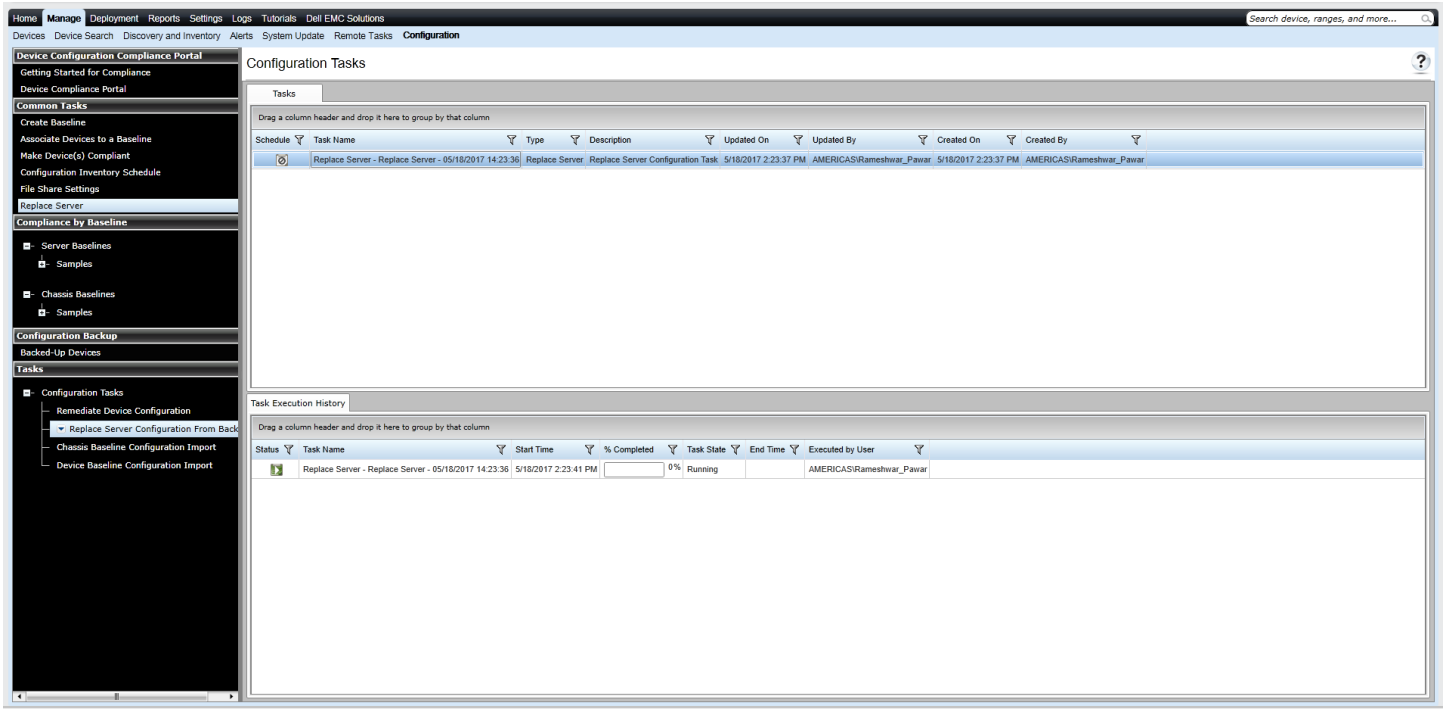

Figure 21 Replace Server(Task Execution)