

# Server Hardware Provisioning and OS Deployment by using Dell EMC OpenManage Essentials

This technical white paper describes the process of provisioning the server hardware and deploying Operating System (OS) by using OME.

Dell EMC Engineering  
February 2018

## Revisions

Date	Description
September 2015	Initial release
July 2016	Added support for Dell EMC Networking IOAs
June 2017	Focus on servers with guidance on template editing
February 2018	Redfish streaming support update

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © February 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [2/6/2018] [Technical White Paper]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

# Contents

Revisions.....	2
Executive summary.....	6
1 Features discussed in this technical white paper.....	7
2 Preparing OME for device configuration .....	8
2.1 Target device requirements.....	8
2.2 Redfish streaming support.....	8
2.3 File share settings.....	9
2.3.1 File share requirement explanation .....	9
2.3.2 Setting up file share.....	9
3 Editing server configuration template in a guided manner.....	12
4 Understanding the differences between bare-metal and stateless deployments .....	13
5 Deploying the template in stateless environment.....	14
6 Replacing a server in stateless environment .....	15
7 Reclaiming virtual identities deployed by OME .....	16
8 Deploying the template to the bare-metal device.....	17
9 Configuring VLANs on server-facing ports of IOAs along with server deployment.....	18
10 Automating hardware configuration and operating system deployment (auto deploy) of recently ordered devices .....	19
11 Hardware setup for the stateless environment.....	20
12 Creating templates .....	21
12.1 Template definition .....	21
12.2 Requirements for creating the template .....	21
12.3 Creating the template from the reference device .....	21
12.3.1 Creating the template from the reference server .....	21
12.4 Creating the template from an XML configuration file .....	23
12.4.1 File requirements.....	23
12.4.2 Creating the template from the XML file.....	23
12.5 Guidance on template editing.....	25
12.5.1 Defining First Boot configuration .....	25
12.5.2 Updating network interface settings .....	27
12.6 Editing IOA VLAN Attributes in server template .....	29
13 Creating Virtual I/O pools .....	31
13.1 Virtual I/O pool definition .....	31

13.2	Types of identities.....	31
13.2.1	MAC address definition .....	31
13.2.2	World Wide Node Name (WWNN) definition .....	31
13.2.3	World Wide Port Name (WWPN) definition.....	32
13.2.4	IQN Definition .....	32
13.3	Creating the Virtual I/O pool .....	32
13.3.1	Creating an identity type definition from an import file .....	33
13.4	Increasing the size of Virtual I/O Pool .....	34
13.4.1	Increasing the size of start address based identity .....	34
13.4.2	Increasing the size of import based identity .....	34
13.5	Locking and unlocking the Virtual I/O pool .....	34
14	Creating compute pool .....	35
14.1	Compute pool Components.....	35
14.2	Creating the compute pool .....	35
14.3	Adding devices to the compute pool.....	35
15	Deploying compute pools .....	36
15.1	Deploying requirements.....	36
15.2	Deploying the compute pool .....	36
15.3	Compute pool lock .....	37
16	Deploying template to bare-metal devices .....	38
16.1	Prerequisites for deployment.....	38
16.2	Purpose and definition of the 'Repurpose and Bare-metal' device group.....	38
16.2.1	Adding devices to the "Repurpose and Bare-metal" device group .....	38
16.3	Deploying the template .....	39
16.3.1	Deploying the template to servers.....	39
16.3.2	Editing the device specific attributes of the deploy template task.....	40
17	Configuring VLANs on the server-facing ports of IOAs during template deployment on the server.....	42
17.1	Deploying the template to servers along with VLAN configuration of associated IOA ports.....	42
17.2	Editing the IOA VLAN attributes during server template deployment .....	43
18	Auto-deploying the templates.....	44
18.1	Auto deploy requirements.....	44
18.2	Setting up auto deploy of a template .....	44
18.2.1	Creating Service Tag CSV file .....	44

18.2.2	Setting up stateless auto deploy of the template to the server Service Tags .....	44
18.2.3	Setting up bare-metal auto deploy of the template to server Service Tags .....	45
18.2.4	Modifying the auto deployment settings .....	47
19	Deploying network ISO image .....	48
19.1	Deploying network ISO image requirements .....	48
19.2	Deploying network ISO image .....	48
20	Troubleshooting .....	50
20.1	Troubleshooting the file share .....	50
20.2	Troubleshooting the template creation .....	52
20.3	Troubleshooting the Virtual I/O pool creation .....	53
20.4	Troubleshooting the template deployment .....	53
20.5	Troubleshooting the auto deploying templates .....	54
20.6	Troubleshooting the network ISO deployment .....	55
21	Additional resources .....	56
22	Boot-from-SAN considerations .....	57
22.1	Boot-from-SAN by using iSCSI .....	57
22.2	Boot-from-SAN by using FC or FCoE .....	59

## Executive summary

With OpenManage Essentials (OME) version 2.4, basic and intuitive guidance is now provided to set up first restart and update network settings in a server configuration template. These are very common use cases intercepted in a server's life-cycle.

This technical white paper includes:

- Configuring VLANs on Dell EMC Networking IOAs included within server template deployment workflows.
- Stateless computing provides a powerful abstraction that allows workloads to seamlessly move from hardware to hardware and scale workloads. Maintaining a stateless environment and quickly responding to errors is difficult.
- The device configuration features (deploying bare-metal devices and auto deployment) have changed, and are important to understand in order to compliment the stateless feature set. Best practices and troubleshooting for the stateless and bare-metal deployment are also included.

# 1 Features discussed in this technical white paper

- Comprehensive use case examples for using OpenManage Essentials device configuration features
- Requirements and setup for using the features
- Create a template from a server
- Edit a server template to configure first restart and network settings
- Create a Virtual I/O pool
- Create a compute pool
- Deploy a compute pool
- Deploy a template to a server
- Deploy VLANs on server facing ports of IOAs during template deployment on the server
- Deploy a template to undiscovered devices by Service Tag (Auto Deploy)
- Deploy an ISO image from your network to the server

## 2 Preparing OME for device configuration

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

### 2.1 Target device requirements

- For 12th and 13th generation of PowerEdge servers, the minimum supported version of iDRAC is 2.30.30.30.
- For 14th generation PowerEdge servers, the minimum supported version of iDRAC is 3.00.00.00.

Additional requirements to enable Deploy operation on the server:

- Server configuration for OpenManage Essentials license installed on the iDRAC. This is a separate license from the iDRAC license.
- iDRAC Enterprise or iDRAC Express license. This is a different license from the 'Server configuration for OpenManage Essentials' license.

Target IOA requirements for VLAN configuration:

- Supported models:
  - > PowerEdge M I/O Aggregator
  - > PowerEdge FN410S
  - > PowerEdge FN410T
  - > PowerEdge FN2210S
- Supported modes:
  - > Standalone
  - > Virtual Link Trunk (VLT)
  - > Programmable MUX (PMUX)
- Supported versions of Dell EMC Networking OS firmware are 9.10.0.0, 9.10.0.1P10, 9.11.0.0, and 9.11.2.0.

### 2.2 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.



## 2.3 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.

### 2.3.1 File share requirement explanation

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

### 2.3.2 Setting up file share

The file share settings must be entered in OME. The file share settings require a username and a password of a user who has privileges to read and write files on the OEM system. During the deployment or 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. In the left pane, click **File Share Settings** under the **Common Tasks** section.
3. Type the user name and password in the **File Share Settings** dialog box.
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.

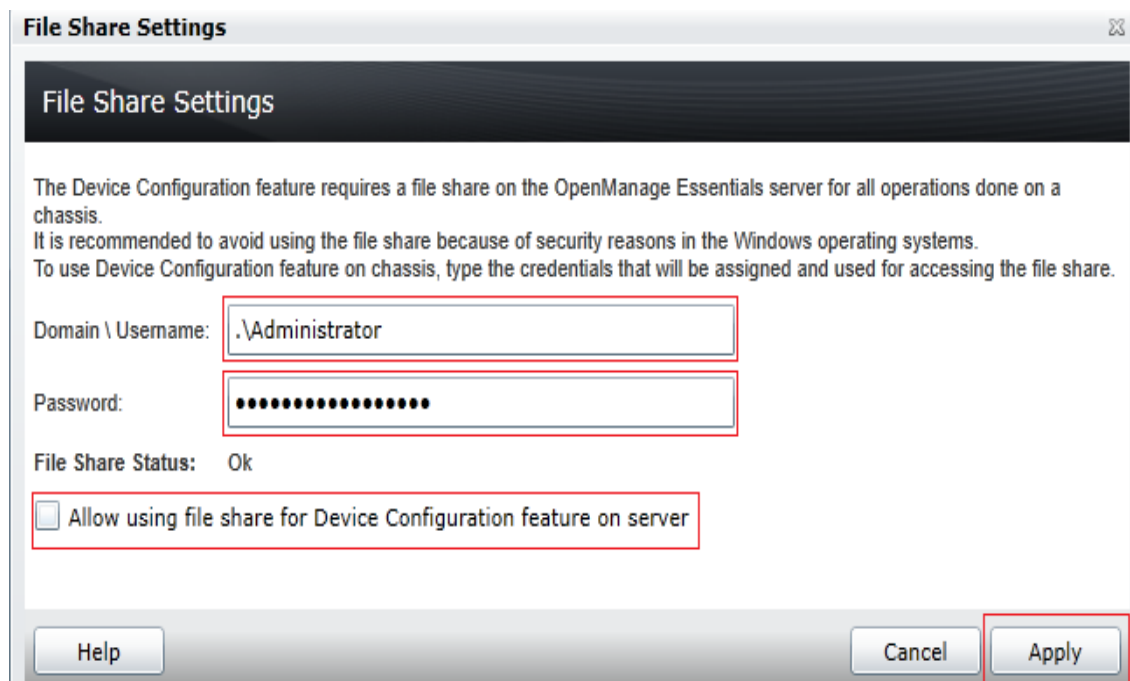


Figure 1 File share settings

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, if at later time the 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

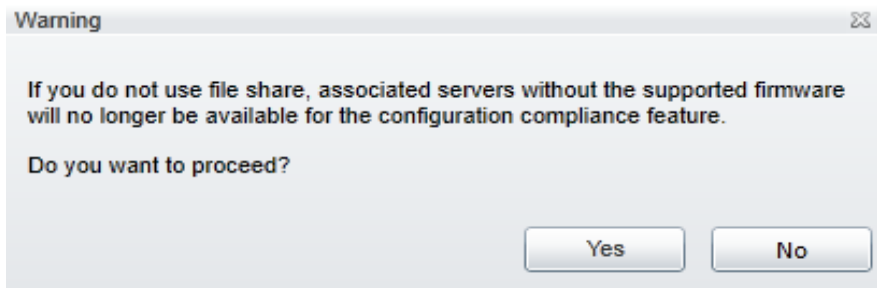


Figure 3 Compliance Warning

### 3 Editing server configuration template in a guided manner

Conventionally, editing the configuration template has been difficult in OME, as all the attributes are presented in one view. One must identify all the attributes to be edited to enable/disable a particular feature. To simplify most common use cases of a server's life cycle, guidance is provided in OME 2.4 to:

- Configure first boot
- Update network settings

User friendly controls are presented and can be used to configure a server template as per the requirements. The edited template can be saved without the necessity of a set of attributes that got added or updated. Also, such template can be deployed on intended target servers by using the existing workflows.

**Note:** Creating the template and deploying the template have requirements for the OME system and for the target devices.

- To review the requirements for creating the template, see [Requirements for creating a template](#).
- To use the guidance for editing the template, see [Guidance on template editing](#).
- To review the requirements for deploying the template, see [Deploy requirements](#).

## 4 Understanding the differences between bare-metal and stateless deployments

Bare-metal and stateless are the two methods of deployment available from OME version 2.1 onwards. The primary differentiator between these is who controls the virtual identities assigned to the device.

In bare-metal deployment, the user defines the identities and manually enters these into OME. This could also be considered manual identity deployment. The benefits of this is that the user can choose exactly which identity gets tied to each interface. The drawbacks are that the user must manually type this in and must also make sure not to reuse an identity on multiple interfaces. Also, for this mode, the use of compute pools is optional.

Stateless deployment allows the user to define a range of identities as a Virtual I/O pool, and then OME will manage the assignment of the pool and automatically assign identities from the pool to devices. This expedites the deployment process and removes the burden from the user for ensuring an identity is not accidentally reused. Compute pools are required for this mode.

## 5 Deploying the template in stateless environment

**Example use case**—you want to deploy and manage servers in a virtualized environment connected to a storage area network. You want the configuration of one well-formatted server deployed to other servers, and you want the servers to use virtual identities created from manageable virtual identity definitions.

To accomplish this use case:

1. Get the configuration from the device that is already configured and saved in OME as the template. See [Creating the template from the reference device](#).
2. Create the definitions of the identities you wish to deploy. This is accomplished in OME by creating a “Virtual I/O pool”. See [Creating Virtual I/O pools](#).
3. Create a deployment definition that describes what to deploy and what servers to deploy against. This is accomplished in OME by creating a “Compute Pool”. See [Creating compute pool](#).
4. Deploy the compute pool deployment definition to the target devices. See [Deploying the compute pool How to deploy](#).

**Note:** Creating a template and deploying a template have requirements for the OME system and the target devices.

- To review the requirements for creating a template, see [Requirements for creating a template](#).
- To review the requirements for deploying a template, see [Deploy requirements](#).

## 6 Replacing a server in stateless environment

**Example use case**—a server in your stateless environment experienced a hardware failure. You need to transfer the workload of the failing server to a new server.

Prerequisites:

- The source device must have been deployed from OME from a compute pool by using Virtual I/O.
- The target device must be in the same compute pool as the source.
  1. Add the target device to the 'Repurpose and Bare-metal' device group if not already. See [Adding devices to the "Repurpose and Bare-metal" device group](#).
  2. Add the target device to the compute pool of the source device if it is not already.
  3. Complete the replace server wizard to initiate the replace server task.
  4. Verify the task succeeded in the task execution history.

**Note:** The virtual identities of the source server are deployed to the target server during this operation. If OME is unable to connect to the source and physically remove the identities, it will lead to network conflicts later if it is reconnected to the network. The wizard will not be accessible if the prerequisites are not met.

## 7 Reclaiming virtual identities deployed by OME

**Example use case**—a production server with a specific workload needs retired, and you wish to reclaim all the virtual identities so OME can reuse these later.

Prerequisites:

The source device must have been deployed from OME by using a compute pool by using Virtual I/O.

1. Complete the reclaim identities wizard to begin the reclaim process.
2. Verify the task succeeded in the task execution history.

**Note:** It is possible to reclaim the identities for reuse in OME, whether or not the device is still visible in OME. However, if the device was already deleted from OME, the reclaim operation will not be able to physically remove the identities from the device, and if it were to be reconnected to the network in that case, it could result in network conflicts if the identities have been reused. The wizard will not be accessible if there are no deployed identities to reclaim.



## 8 Deploying the template to the bare-metal device

**Example use case**—based on your data center’s requirements, you configure all the settings of one server. You have a new bare-metal device or device you want to repurpose. You want to copy all of the settings of the configured device and apply them to bare-metal/repurpose device.

To accomplish this use case:

1. Get the configuration from the device that is already configured and save it in OME as a template. See [Creating the template from the reference device](#).
2. Add the target device (the bare-metal device) to the “Repurpose and Bare-metal” device group. See [Adding devices to the “Repurpose and Bare-metal” device group](#).
3. Deploy the template to the target device. See [Deploying the template](#).

**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 [Requirements for creating a template](#).
- To review the requirements for deploying a template, see [Deploy requirements](#).

## 9 Configuring VLANs on server-facing ports of IOAs along with server deployment

**Example use case**—you are using VLAN tagging in your networking infrastructure to control packet flow. Additionally, you are using specific VLANs to control communication with modular servers enforced by chassis IOAs. Based on your data center's needs, you configure all the settings of one modular server. You have a new bare-metal/repurpose modular server. You want to copy all of the settings of the configured modular server and apply them to a bare-metal/repurpose modular server along with the VLANs that you want to configure on connected ports of chassis IOAs.

To accomplish this use case:

1. Add the target server (the bare-metal device) to the “Repurpose and Bare-metal” device group. See [Adding devices to the “Repurpose and Bare-metal” device group](#).
2. Deploy the template to the target server along with the VLAN configuration of the associated IOA ports. See [Configuring VLANs on the server-facing ports of IOAs during template deployment on the server](#).

**Note:** Creating a template and deploying a template have requirements for the OME system and for the target devices. Additionally, associated chassis IOAs must be discovered in OME and should meet minimum requirements for the VLAN configuration step to succeed. See [Target device requirements](#).

- To review the requirements for creating a template, see [Requirements for creating the template](#).
- To review the requirements for deploying a template, see [Deploy requirements](#).

## 10 Automating 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 on devices discovered by OME, see [Deploying template to bare-metal devices](#).

To accomplish this use case:

1. Create a template from a configured device or sample template. See [Creating the template from the reference device](#).
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 [How to setup auto deploy of a template](#).
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 [Requirements for creating a template](#).
- To review the requirements for auto deploying a template, see [Auto deploy requirements](#).

## 11 Hardware setup for the stateless environment

This section covers the hardware setup and best practices for configuring an environment for stateless computing.

## 12 Creating templates

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

### 12.1 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 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.

### 12.2 Requirements for creating the template

To create a template from a reference device:

1. The file share must be configured. See [Setting up file share](#).
2. The device must meet the minimum requirements for the deployment and configuration features. See [Target device requirements](#). To create a template, a server does not require a license.

### 12.3 Creating the template from the reference device

This section describes how to create a template from a discovered device. The '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.

#### 12.3.1 Creating the template from the reference server

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Create Template** under **Common Tasks**.
3. In the **Create Template** dialog box, type 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 **Create from Device**.

6. Type the user credentials in **Execution credentials**.

**Note:** Type the administrator user name and password on the target iDRAC.

Figure 4 Create template from reference device wizard

7. Click **Finish**.
8. Click **Ok**. A task is created.
9. To view the created task, click the **Tasks** tab in the **Deployment**.
10. To view the progress of the task, look at the **Task Execution History** grid.
11. To view the details of execution history, double-click the task execution history entry, or right-click the task execution history entry.
12. Select Details. The information about the issues (such as incorrect credentials) is displayed. If the task is successful, the template is created and displayed in the **Server Templates** tree.
13. If the task is unsuccessful, right-click the task execution history or the task, and then click **Run**.

**Note:** Enter the iDRAC credentials to run the task again.

## 12.4 Creating the template from an XML configuration file

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

### 12.4.1 File requirements

XML files used for the template must meet the following requirements:

- Must be well formed
- Must contain at least one attribute

### 12.4.2 Creating the template from the XML file

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Create Template** under **Common Tasks**.
3. Type a unique name for the template.
4. Select **Create from File**.
5. Click **Browse** and browse to the file's location.
6. Select the file and click **Open**.

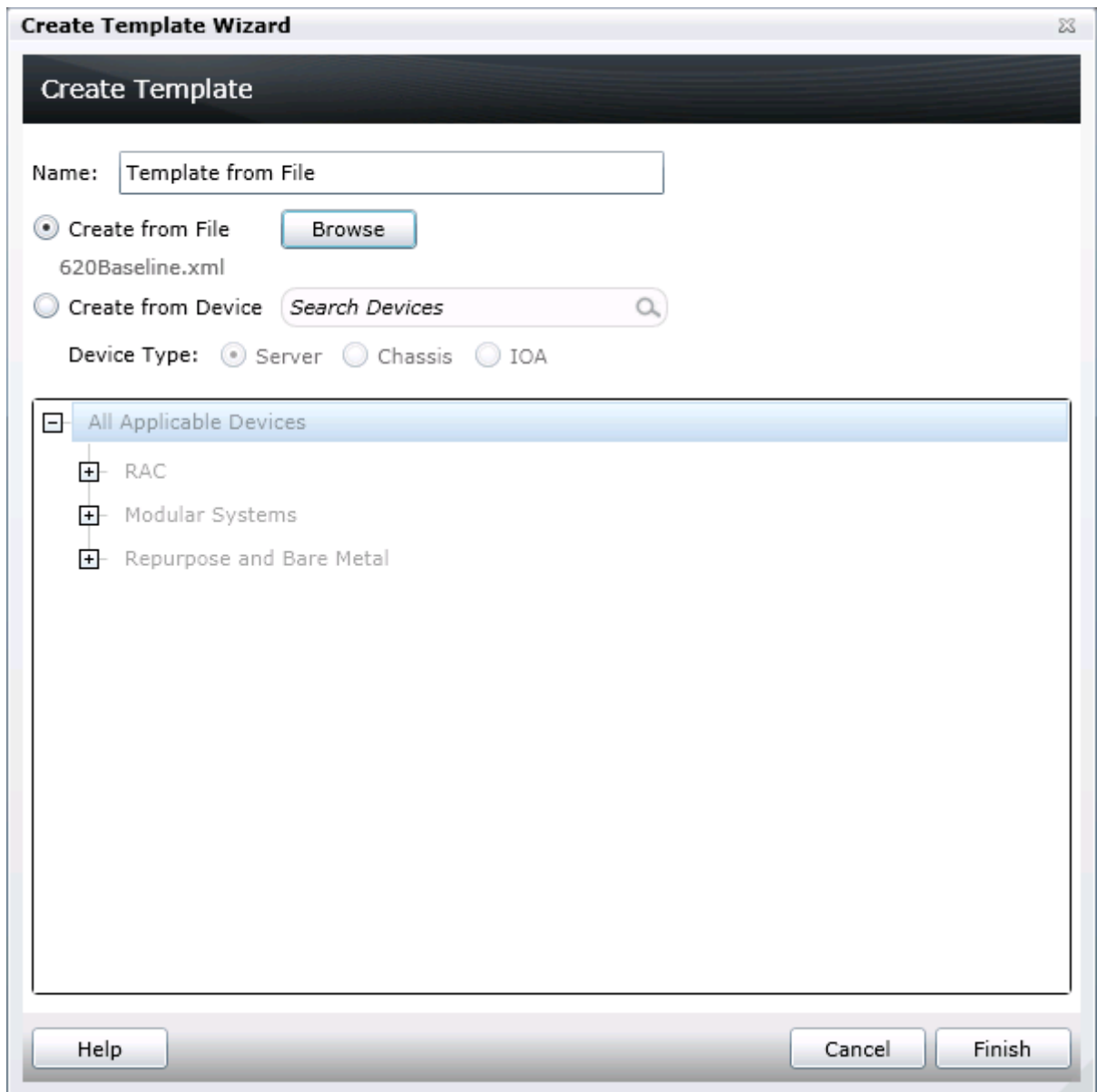


Figure 5 Create template from file wizard

7. Click **Finish** to create the template.
8. The template name is added to the **Server Templates** tree.



## 12.5 Guidance on template editing

The following section describes how to edit the server configuration template to enable or disable certain features. Supported use cases:

1. Configuring first boot settings.
2. Enabling/disabling partitioning on capable NICs.
3. Editing IOA VLAN attributes with respect to modular servers.

**Note:** Use case configuration options are derived based on the capabilities of the (template) source server. For example, if a FC card is not available in the server, FC boot cannot be configured in the template created from it.

Although support, templates that are created from file and edited using this workflow, might fail to deploy on identical targets. To have best results, it is recommended to use templates that are directly created from source server in OME.

### 12.5.1 Defining First Boot configuration

Using this section of template settings, the following boot parameters can be defined:

- Boot mode – UEFI or BIOS
- Boot type – hard drive (HDD), PXE, FC, or FCoE
- Boot sequence and hard drive sequence

Boot Type	BIOS Mode	UEFI Mode
Hard drive	✓	✓
PXE	✓	✓
FC	✓	✗
FCoE	✓	✗
iSCSI	✗	✗

Table 1 Supported boot types for selected boot mode

**Note:** FC and FCoE boot types require target storage controller WWPN and LUN ID to be provided for successful boot-up after deployment. Second storage target details can also be provided optionally while setting up FC boot.

To enable FCoE boot in the server template:

1. Navigate to the **Deployment** tab.
2. In the left-hand side navigation tree, select the template under **Templates → Server Templates**.
3. In the right corner of the screen, select **Boot and Network Configuration** tab.
4. Expand **First Boot Configuration** panel.
5. Select **FCoE** under **Select Boot Type**.
6. Provide target storage WWPN under **First Target WWPN**.
7. Provide target LUN Id under **First Target LUN Id**.
8. Click **Save** to make the changes to the template.

**Note:** While configuring first boot, boot mode cannot be changed in templates created from 13<sup>th</sup> generation of servers and onwards. This is a limitation as the profile XML provides boot sequence and other attributes for current boot mode only.

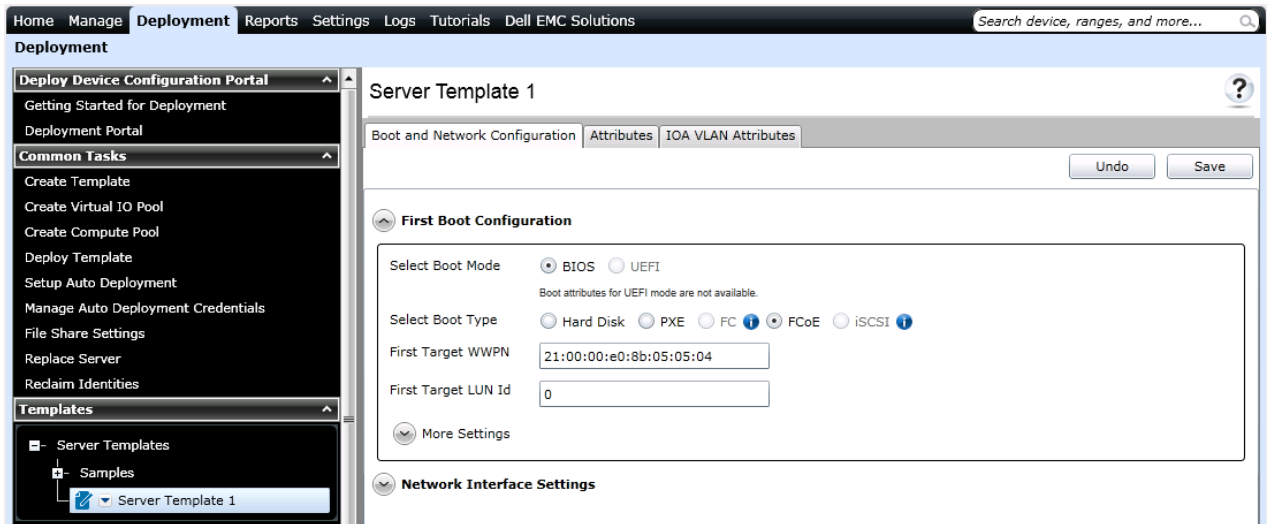


Figure 6 Configure FCoE boot in a server template

**Note:** For templates created from (and deployed to) 12<sup>th</sup> generation of servers or later running with older firmware, PXE boot in UEFI mode will not work. Nor will it get identified in the template if set so. To resolve the problem, update the iDRAC firmware to the latest version available.

After you configure the required boot type, if required, change the boot sequence and hard drive sequence also. Sequence changes are not allowed beyond the scope of the selected boot type when it cannot be satisfied.

For example, if the boot type is changed to FCoE, capable NIC instance (say, *Integrated NIC 1 Port 1 Partition 1*) available in the boot sequence will be automatically selected to be booted from (made first entry in the boot sequence). One can make another capable NIC instance (say, *Integrated NIC 2 Port 1 Partition 1*) as first entry in the boot sequence when required.

Do the following when you are clear about the desired end result:

1. Expand **More Settings** under **First Boot Configuration**.
2. Change **Boot Sequence** and/or **Hard Drive Sequence**.
3. Click **Save** to make the changes to the template.

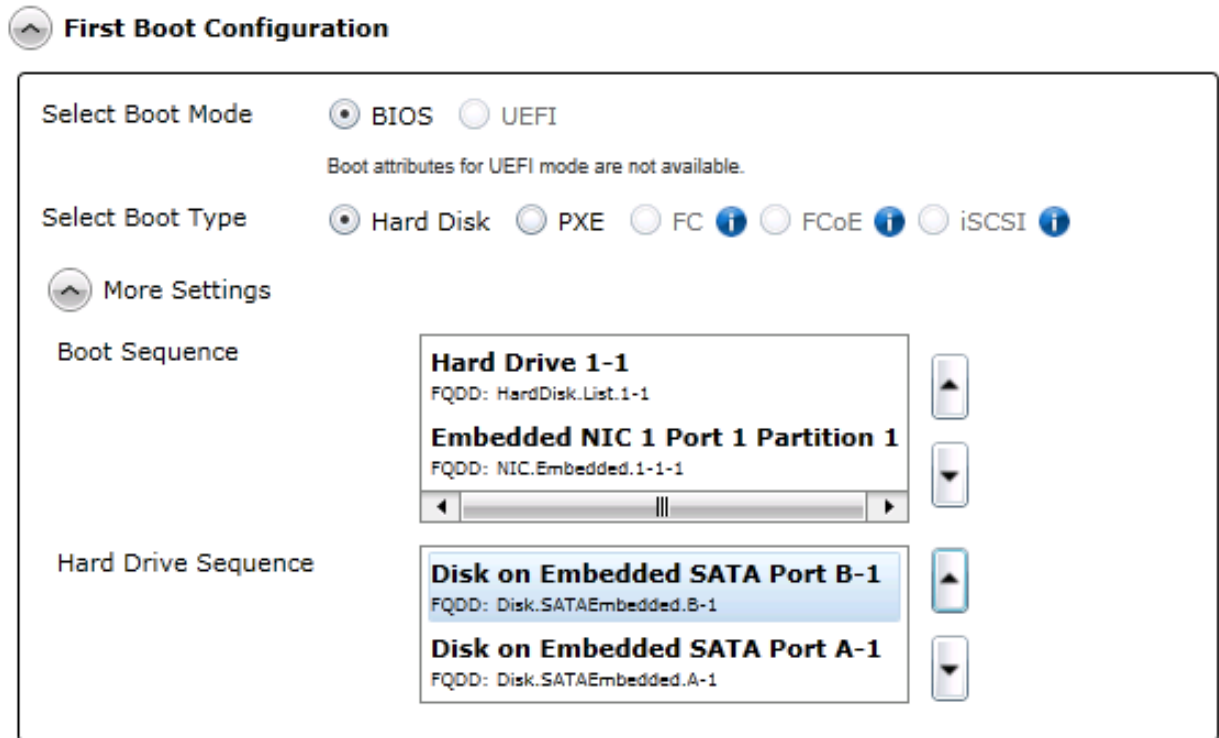


Figure 7 Change hard drive sequence

## 12.5.2 Updating network interface settings

Under the **Network Interface Settings** section, all network interfaces and Fiber channel cards that are available in (template) the source server are listed with following details:

- User friendly name with location
- Type of fabric: NIC, CNA, or FC
- Port layout
- Partitioning capability and option to enable/disable it
- Min/Max bandwidth allocation per partition
- IOA VLAN attributes corresponding to network ports (for modular server templates only)

Following use cases can be achieved by using this section of template settings:

- Enable or disable partitioning on capable cards
- Allocate minimum and maximum bandwidth for each partition
- Assign tagged VLANs and untagged VLAN per port

**Note:** Dual port card will always provide four partitions per port. However, Quad port card will always provide 2 partitions per port. Also, cards that can support more number of virtual functions per port than defined here, are not supported yet. However, if tried, template deployment might eventually fail. Example cards: Intel(R) 10GbE 2P X710-k bNDC, Emulex OCm14102-U5-D - F8:BC:12:FB:00:02, etc.

Follow these steps to enable partitioning and allocate minimum and maximum bandwidth per partition on a network interface card in the server template:

1. Navigate to the **Deployment** tab.
2. In the left pane select the template under **Templates**→**Server Templates**.
3. Select **Boot and Network Configuration** tab in the right side template details.
4. Expand **Network Interface Settings**.
5. Expand network interface card of your choice.
6. Select the **Enable** check box.
7. Select **Minimum Bandwidth (%)** and **Maximum Bandwidth (%)** for each partition of the port.
8. Click **Save** to make the changes to the template.

**Note:** During the deployment of edited templates, target server's iDRAC might restart multiple times depending on configuration template settings. For example, enabling partitioning on an un-partitioned network interface card.

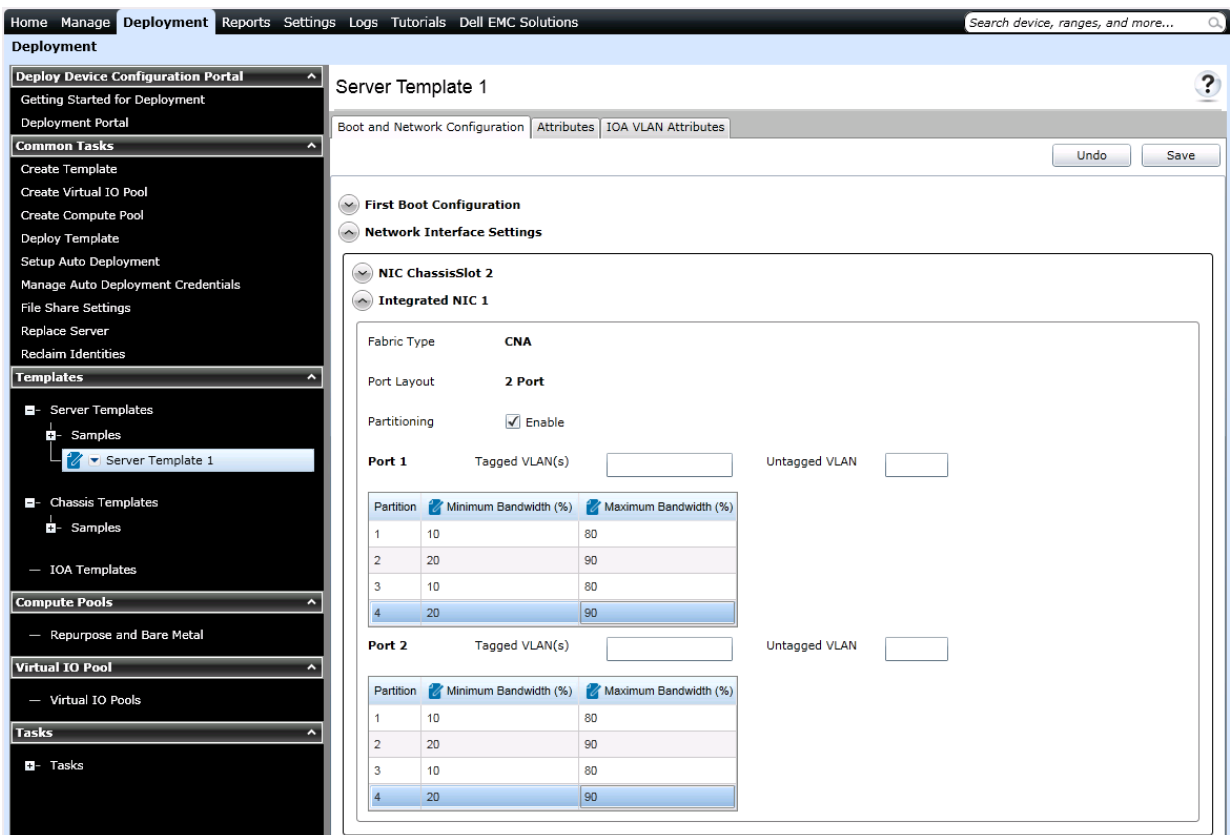


Figure 8 Enable partitioning on a network interface card

To assign tagged VLAN and untagged VLAN on corresponding IOA ports of server's network interface card:

1. Expand the required NIC.
2. Type the values in the **Tagged VLAN(s)** and **Untagged VLAN** boxes corresponding to **Port 1** and **Port 2**.
3. Click **Save** to make the changes to the template.

**Network Interface Settings**

**NIC ChassisSlot 2**

**Integrated NIC 1**

Fabric Type	<b>CNA</b>		
Port Layout	<b>2 Port</b>		
Partitioning	<input type="checkbox"/> Enable		
<b>Port 1</b>	Tagged VLAN(s)	<input type="text" value="2-100"/>	Untagged VLAN <input type="text" value="1"/>
<b>Port 2</b>	Tagged VLAN(s)	<input type="text" value="2-100"/>	Untagged VLAN <input type="text" value="1"/>

Figure 9 Assign tagged VLANs and untagged VLAN

## 12.6 Editing IOA VLAN Attributes in server template

This section describes how to edit and assign IOA VLAN attributes for a particular template created by using the modular server. To enable VLAN assignment on the server-facing ports of IOAs during the deployment of configuration template on sever:

**Note:** IOA VLAN Attributes will only be available with templates created by using modular servers.

1. Navigate to the **Deployment** tab.
2. Select the template under **Templates** → **Server Templates** in the upper-left corner.
3. Select **IOA VLAN Attributes** tab.
4. Type the values in the **Tagged VLAN(s)** and **Untagged VLAN** boxes corresponding to the ports that you need to configure.
5. Click **Save** to make the changes to the template.

Home

Manage

Deployment

Reports

Settings

Logs

Tutorials

Dell EMC Solutions

Search device, ranges, and more...

Deployment

Deploy Device Configuration Portal

Getting Started for Deployment

Deployment Portal

Common Tasks

Create Template

Create Virtual IO Pool

Create Compute Pool

Deploy Template

Setup Auto Deployment

Manage Auto Deployment Credentials

File Share Settings

Replace Server

Reclaim Identities

Templates

Server Templates

Samples

Server 1

Chassis Templates

Sample - FX2 Chassis

Sample - VRTX Chassis

Sample - M1000e Chassis

Server 1

Attributes

IOA VLAN Attributes

Undo

Save

Drag a column header and drop it here to group by that column

Total: 4 Modified: 2

Deploy	Modified	NIC	Fabric	Tagged VLAN(s)	Untagged VLAN
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-3-1	A1	1-100	101
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-4-1	A2	1-100	101
<input type="checkbox"/>	No	NIC.Integrated.1-1-1	A1		
<input type="checkbox"/>	No	NIC.Integrated.1-2-1	A2		

Figure 10 Edit IOA VLAN attributes

## 13 Creating Virtual I/O pools

Virtual I/O pools simplify identity management in the OME. This section describes how to create the Virtual I/O pool from a prefix definition or an import file. Also, about how to increase the size of Virtual I/O pool and lock or unlock the Virtual I/O pool.

### 13.1 Virtual I/O pool definition

The Virtual I/O pool is a definition of identity types that describe identities and determines the identities OME will generate. A Virtual I/O pool may contain identity definitions for different types of identities.

### 13.2 Types of identities

Virtual I/O pools may contain different identity type definitions. Identity types define the identity properties required for a specific network protocol. For example, Ethernet MAC address.

An identity type is defined by specifying the start address and the actual number of identities (except for IQN which is defined by an IQN seed string) or by importing identities from the file. All the generated identities of the specific identity type will begin with the provided start address. OME uses last 3 octets for generating the necessary number of Ethernet identities, and last 5 octets in case of WWNN and WWPNN identities for the same purpose. Imported identities must be unique and pass the restriction checks mentioned below. Imported identities are used as it is by OME.

#### 13.2.1 MAC address definition

MAC address is used to define virtual MAC address properties. It is recommended to define this in all the SAN types.

An example of MAC address is 00-14-22-01-23-45. Note that this will vary based on the environment and vendor HBA cards.

Restrictions: MAC address prefixes cannot be a multicast address. A multicast address is an address with a value of 1 in the least-significant bit of the first octet. (Therefore 01, 03, 0B etc. are not allowed).

Defined by:

- Start address
- Number of identities or imported identities

#### 13.2.2 World Wide Node Name (WWNN) definition

WWNN address is used to define virtual WWNN address properties. It is recommended to define this in FCoE and FC environments only.

For example, 21:00:00:e0:8b:05:05:04 is the identity for QLogic HBA card. Please note that this will vary based on the vendor HBA cards.

Restrictions:

WWN address prefixes require a NAA value of two, five or six. An NAA value (Network Address Authority) is a 4-bit field used to guarantee uniqueness of WW names. The NAA value is the first four bits of the address (so, the address must start with 2, 5 or 6).

Defined by:

- Start address
- Number of identities or imported identities

### 13.2.3 World Wide Port Name (WWPN) definition

WWPN address is used to define virtual WWPN address properties. It is recommended to define this in FCoE and FC environments only.

Restrictions:

WWPN address prefixes have the same NAA restrictions mentioned in the section above.

Defined by:

- Start address
- Number of identities or Imported identities

### 13.2.4 IQN Definition

IQN addresses are used to define virtual IQN addresses. It is recommended to define this in iSCSI environments only.

An example for IQN is: *iqn.2001-09.com.example:mystorage.disk1.test1.abc*

Restrictions:

- Value cannot be empty

Defined by:

- IQN seed string or imported identities

## 13.3 Creating the Virtual I/O pool

The Virtual I/O pool can be created from the deployment portal. The Virtual I/O pool may contain an identity definition for each identities. Multiple definitions for a single identity type is not allowed. The Virtual I/O pool may contain identity types defined by combination of start address along with necessary number and/or import files. To create the Virtual I/O pool:

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Create Virtual I/O pool** under **Common Tasks**.
3. Type the unique name (and optionally a description), and then click **Next**.
4. Type the MAC address, number of identities, and then click **Next**.



5. Type the WWNN address and number of identities if the stateless environment is FC or FCoE or clear the **Include Fiber Channel WWNN Identities in the Pool** check box, and then Click **Next**.
6. Type the WWPN address and number of identities if the stateless environment is FC or FCoE or clear the **Include Fiber Channel WWPN Identities in the Pool** check box, and then Click **Next**.
7. Type an iSCSI IQN string if the stateless environment is iSCSI. Otherwise, clear the **Include IQN Identities in the Pool** check box, and then click **Next**.
8. Review and click **Finish**.

Figure 11 Defining WWNN identities by start address and size

### 13.3.1 Creating an identity type definition from an import file

An identity type may be defined by using an import file. This section covers the file requirements and how to import the identities from a CSV file.

#### 13.3.1.1 File Requirements

The imported file must meet the following requirements:

- The file must have a CSV extension.
- Identity types are limited to 10,000 imported identities. Any identity over this count will be discarded.
- The CSV file must have a column title. The title may be any name.
- Imported items must meet the requirements in the [Types of identities](#) section above.

### 13.3.1.2 Importing identities from a CSV file

To import identities from a file:

1. Under the **Create Virtual I/O Pool** in the identity type screen (example **Ethernet Identities** screen) click **Import from file**
2. Click **Import**.
3. In the import dialog box, click **Import**.
4. Select a file.
5. Wait for the import to finish (progress bar shows the status).
6. Review results and close the results.
7. (Optional) import additional files (repeat steps 3—6).
8. Click **Close**.

The imported identities may be viewed in this wizard by clicking the **View** button in the **Create Virtual I/O pool** wizard.

## 13.4 Increasing the size of Virtual I/O Pool

While assigning or deploying identities, a Virtual I/O pool may run out of identities. The number of identities in a Virtual I/O pool may be increased. This section describes how to increase the size of a Virtual I/O pool.

### 13.4.1 Increasing the size of start address based identity

To increase the number of identities for an identity defined by a start address, increase the number of identities. This can be done by editing the Virtual I/O pool and increasing the number of identities field.

### 13.4.2 Increasing the size of import based identity

To increase the number of identities for an identity defined by an import file, import more identities by using file. The import operation does not overwrite the previous identities and is an additive operation. To know how to import identities to a Virtual I/O pool, see [Import identities from a CSV file](#).

## 13.5 Locking and unlocking the Virtual I/O pool

The lock state of the Virtual I/O pool is determined by the lock state of all the compute pools associated to that Virtual I/O pool. A locked Virtual I/O pool cannot change the identity type definitions or imported identities of the Virtual I/O pool. To unlock the Virtual I/O pool, unlock all the locked compute pools associated to the Virtual I/O pool. The Compute Pool Summary page is useful for sorting by Virtual I/O pool and the lock state. It is suggested to perform this only if you plan about redeploying to call devices in the previously locked compute pools.

## 14 Creating compute pool

Compute pools provide the method to group a set of similar devices for deployment and pre-configure the settings which will be applied to them. The pool can be recalled at the deployment time to simplify the deployment process.

Compute pools are required for Virtual I/O.

Compute pools are visible in the deployment portal and under the main device tree under the repurpose and bare-metal group.

### 14.1 Compute pool Components

The compute pool definition includes several optional components:

- **Template:** The template will define the attributes which will be available to deploy. After defining for a compute pool, the template cannot be reused for another compute pool.
- **Network ISO:** Defines the network ISO to deploy for the compute pool
- **I/O Assignment type:**
- **User defined I/O:** The user will define the I/O attributes manually, this will operate like bare-metal deployment
- **Automatic I/O:** The virtual identities are filled by OME for the selected attributes and identities are managed.
- **Devices:** Defines the devices that are part of the pool. Note that device can be a member of only one pool.

### 14.2 Creating the compute pool

Type or select information in Create Compute Pool. The compute pool will be available in the compute pool navigation.

**Note:** This action only defines the pool in OME. The task will not be created or any settings will not be applied to the device. You must deploy the compute pool to apply this definition.

- Most of the steps in the wizard are optional while creating the compute pool. However, the required components will be enforced before the deployment.

### 14.3 Adding devices to the compute pool

Right-click a compute pool to add or remove devices from a pool. You can add devices to the compute pool even when locked.

## 15 Deploying compute pools

Deploying the compute pool is required to actually apply the settings in the pool definition to one or more devices in the pool.

### 15.1 Deploying requirements

- The file share must be configured. See [Setting up file share](#).
- The target devices must meet the minimum requirements for the deployment and configuration features. See [Target device requirements](#).
- The target devices must be added to the Repurpose and Bare-metal device group. See [Adding devices to the “Repurpose and Bare-metal” device group](#).
- At least one user-created template (a cloned sample template is a user-created template). The compute pool must have been created already by using the create compute pool action. See [Deploy requirements](#) for more information on general deployment requirements.

### 15.2 Deploying the compute pool

1. Right-click a compute pool to open the Deploy Template wizard for the pool.
2. Ensure the compute pool is selected as a deploy target.
3. Ensure the compute pool is selected as the deploy target.
4. The template defined by the pool should be pre-selected.
5. The IO assignment for the pool should be pre-selected. Note for stateless management, the setting should be on automatic IO assignment with a Virtual I/O pool selected.
6. Select the devices you want to deploy. This will be limited to devices already included in the pool definition.
7. You can optionally edit device specific attributes. If you have already defined the attribute settings during pool creation, then this will not be needed.
8. You can optionally assign identities and view them. This option is available on the identity attributes tab available only when virtual IO is being used. This action will reserve identities even if the wizard is later cancelled. If you do not need to see the identities before deployment, this step can be skipped because the task will automatically do the assignment if identities are not already reserved.

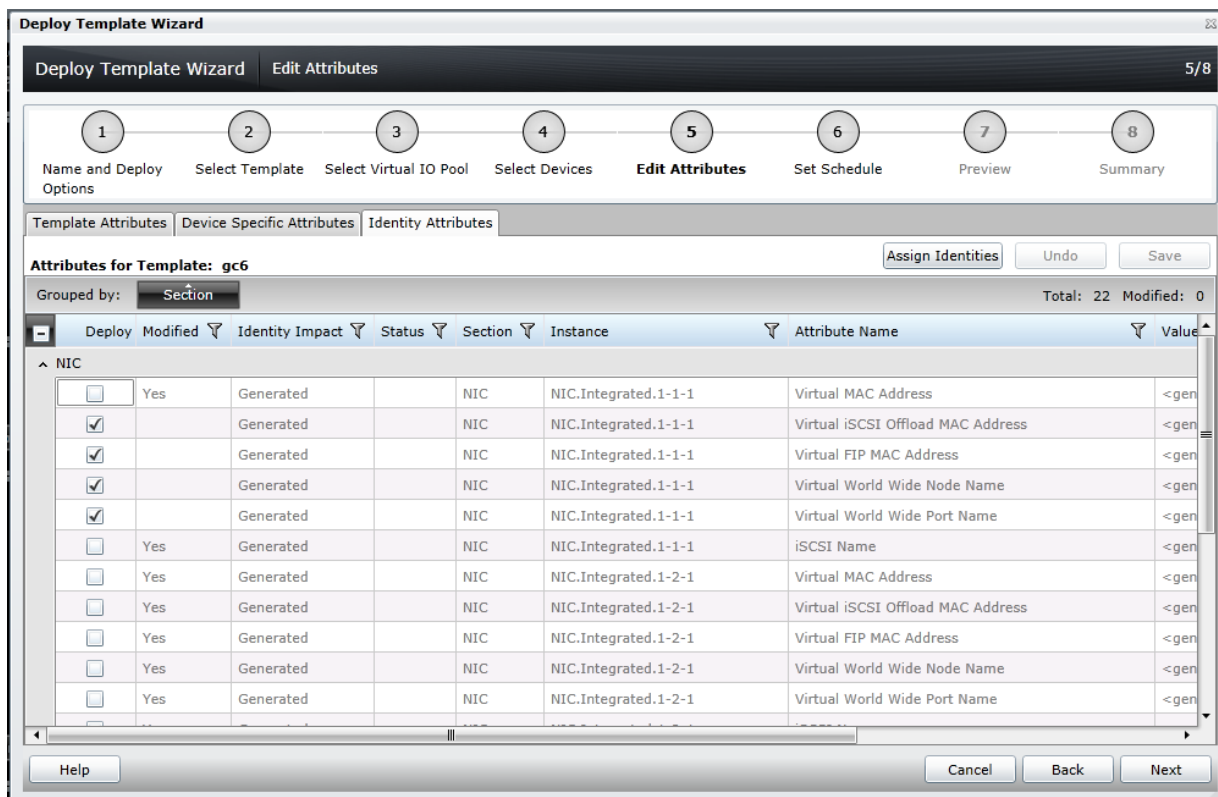


Figure 12 Assign identity attributes

9. Define the task start time.
10. You can optionally preview the task results. This will simulate the deploy action and show the results, when the task is executed.
11. After completing the wizard, the task will be created and scheduled for running.
12. You should verify the task result by reviewing the task execution history for the task after it is executed.

## 15.3 Compute pool lock

After creation of first deployment task, the pool will become locked preventing the pool definition from being edited. The lock will affect the pool definition itself, the pool template, and the linked IO pool.

The purpose of the lock is to ensure the pool definition is not unintentionally altered after it has active deployments.

**Note:** you can still add and remove devices from the pool when it is locked.

It is possible to unlock the pool which will also unlock the template and I/O pool and re-enable editing.

## 16 Deploying template to bare-metal devices

This section describes how to deploy the template by using manual IO which was introduced in OME 2.0. For stateless deployment, see [Deploying the compute pool](#), and its prerequisite sections.

Deploying templates is the process of sending and applying configuration settings to remote devices. A template may contain a configuration settings for one or more specific functional areas, or a full device configuration. To deploy the template, you must first create the template. The template is crucial to the success of the deploy task. You confirm the device for creating the template from is configured exactly how you wish to deploy it when you create the template. To create a template, see [Creating templates](#).

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. If there is a need and some configuration settings have to be changed from what has been captured when template was created, make sure to update those while reviewing the template. Update the respective attributes and remember to save the changes.

### 16.1 Prerequisites for deployment

1. The file share must be configured. See [Setting up file share](#).
2. The target devices must meet the minimum requirements for the deployment and configuration features. See [Target device requirements](#).
3. The target devices must be added to the Repurpose and Bare-metal device group. See [Adding devices to the 'Repurpose and Bare-metal' device group](#).
4. At least one user-created template (a cloned sample template is a user-created template).

### 16.2 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. Add devices to this group only 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.

#### 16.2.1 Adding devices to the "Repurpose and Bare-metal" device group

1. Navigate to the **Deployment** tab.
2. In the left pane, under **Deploy Device Configuration Portal**, click **Deployment Portal**.
3. Click the **Repurpose and Bare-metal Devices** tab.
4. In the lower-right corner of the grid, click **Modify Devices**.
5. Check the target devices in the message displayed. The target devices must be discovered and the target server must have the Server configuration for OpenManage Essentials license.
6. Click **Ok**.

**Note:** Only devices that satisfy the deploy requirements appear in the device selection. To review the requirements, see the Prerequisites for deployment section.

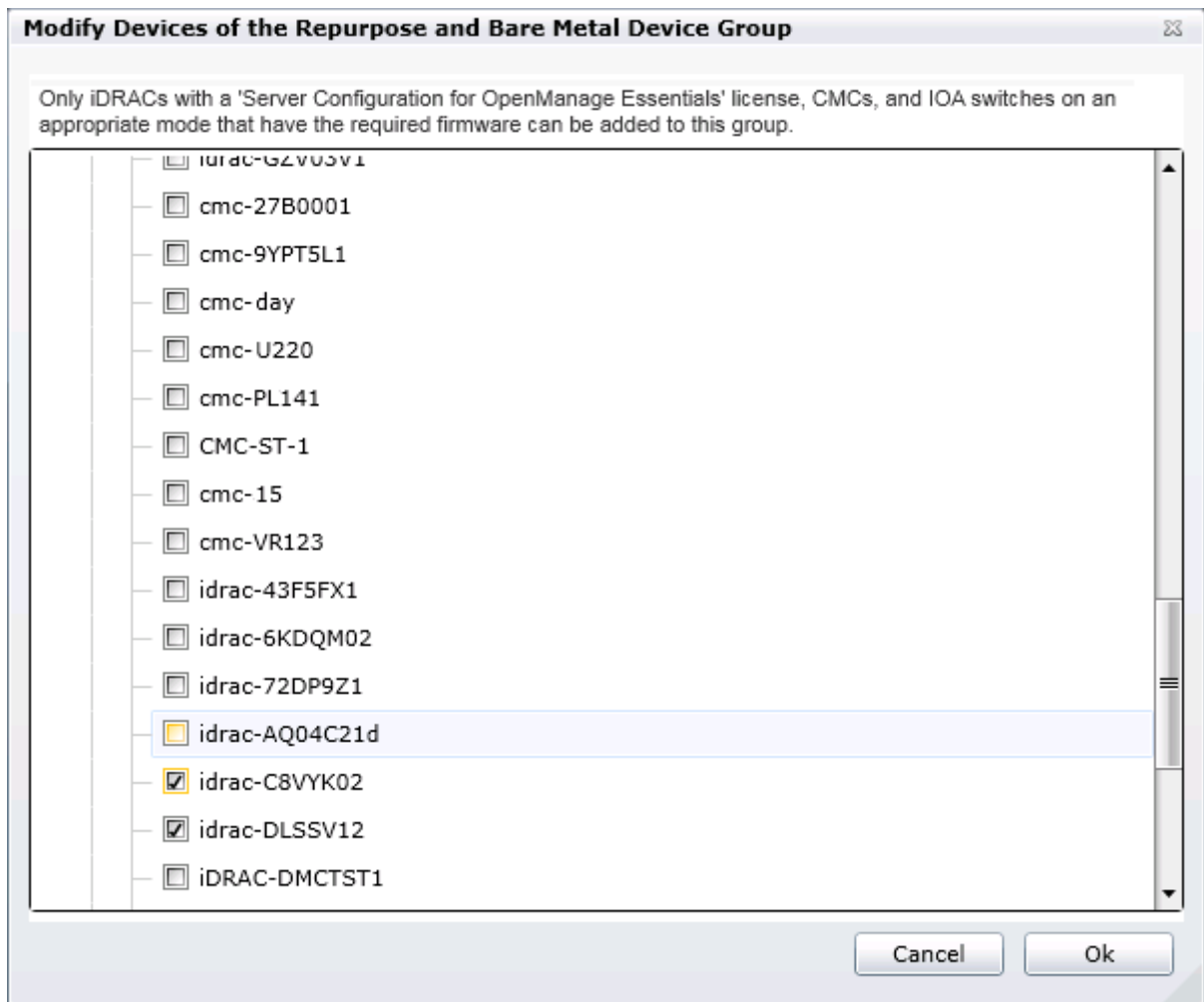


Figure 13 Modify repurpose and bare-metal device group popup

## 16.3 Deploying the template

This section describes how to deploy the template to servers, chassis and IOAs.

### 16.3.1 Deploying the template to servers

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Deploy Template** under **Common Tasks**.
3. Type a unique name for the task. The 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. Select **Deploy Template**, and then click **Next**.
5. Select the template to be deployed on the target server or iDRAC, and then click **Next**.
6. Select the target devices, and then click **Next**.

**Note:** Only devices in the **Repurpose and Bare-metal** device group and match the device type of the selected template may be selected. To add the devices to the device group, see [Adding devices to the 'Repurpose and Bare-metal' device group](#).

1. Enter the system-specific attributes for each target device and click **Next**.

**Note:** 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 information, see [Editing the device specific attributes of the deploy template task](#).

2. Set the schedule when the deploy template task runs. **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 the Operator or Administrator privileges on iDRAC.
3. Click **Next**.
4. Review the task in the **Summary** pane and click **Finish**.
5. Review the message. The deploy action can be destructive. It is important you review and understand the template you are deploying.

### 16.3.2 Editing the device specific attributes of the 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 side and displays the device specific attributes for the selected device in the right side grid.

To edit the attributes:

1. In the left pane, select a device.
2. Click **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 EMC Attribute Registry** site.
4. Click **Save**.
5. Repeat for each device.

**Note:** OME will automatically rediscover the target server whenever a new static IP address is deployed after the deployment finishes successfully. A new discovery range will be added when required.



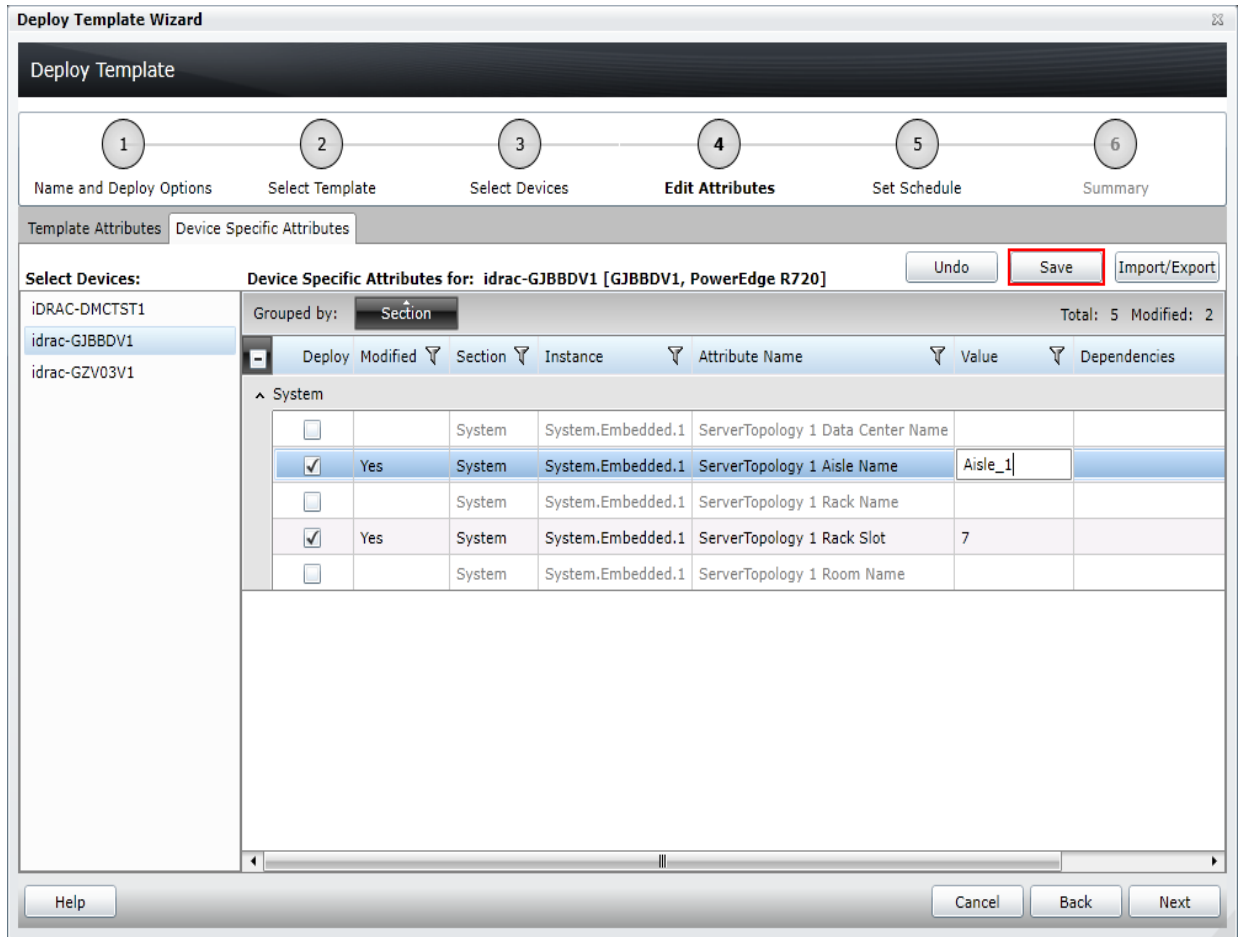


Figure 14 Edit attributes pane

Alternatively, you can import and export the grid file to edit. You may want to export/import if you have a more number of devices with a large number of device-specific attributes. The device-specific attributes grid can be exported based on 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](#)). The grids will be populated with the import data. The UI logs will report any problems with format or values of the import file.

## 17 Configuring VLANs on the server-facing ports of IOAs during template deployment on the server

This section describes how to configure VLANs on the server-facing ports of IOAs during template deployment on target servers.

### 17.1 Deploying the template to servers along with VLAN configuration of associated IOA ports

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Deploy Template** under **Common Tasks**.
3. Enter a unique name for the task. A name is optional since a default name is displayed, 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. Select **Deploy Template** and click **Next**.
5. Select the template to be deployed on the target server or iDRAC, and then click **Next**.
6. Select the target devices, and then click **Next**.

**Note:** Select the devices that are only in the Repurpose and Bare-metal device group, and device that match the device type of the selected template. See [Adding devices to the 'Repurpose and Bare-metal' device group](#) to add devices to the device group.

7. Click **IOA VLAN Attributes** tab to edit the IOA VLAN attributes for the selected template. For more information, see [Editing IOA VLAN Attributes in server template](#).

**Note:** IOA VLAN attributes are applicable to templates created from modular servers only. For selected modular servers during server template deployment, the VLANs will also be configured on the IOA ports facing the server NIC ports.

8. 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 information, see [Editing the device specific attributes of the deploy template task](#). Click **Next**.
9. Set the schedule 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. Enter IOA Credentials if deployable IOA VLAN attributes are present. The credentials must be valid for all target devices and must have the Operator or Administrator privileges on the iDRAC.
10. Click **Next**.
11. Set the schedule after the Deploy Template task is run.

**Note:** Fields to enter the 'IOA Credentials' will be displayed in the compute pool and auto-deploy deployment workflows as well if deployable IOA VLAN attributes are present with the template.

12. Review the task in the **Summary** pane, and then click **Finish**.
13. Review the message.

**Note:** The deploy action can be destructive. It is important you review and understand.

## 17.2 Editing the IOA VLAN attributes during server template deployment

During template creation from a modular server, IOA VLAN attributes are automatically added and linked to the server template. After configuring, these attributes are used to configure VLANs on the IOA ports that are facing the server NIC ports. If the template being deployed has IOA VLAN attributes, those will appear in the 'Edit Attributes' page of the deploy wizard. The 'Edit Attributes' page has 'IOA VLAN Attributes' tab that lists all available attributes for the selected template. To edit the IOA VLAN attributes:

1. On the **Edit Attributes** page, click **IOA VLAN Attributes** tab.
2. Select **Deploy** on the attributes that you want to deploy.
3. Type the values in **Tagged VLAN(s)** and **Untagged VLAN**.
4. Click **Save**.

Deploy Template Wizard

Deploy Template Wizard Edit Attributes 5/8

1 Name and Deploy Options 2 Select Template 3 Select Virtual IO Pool 4 Select Devices 5 Edit Attributes 6 Set Schedule 7 Preview 8 Summary

Template Attributes IOA VLAN Attributes Device Specific Attributes

IOA VLAN Attributes for Template: Server 1 Undo Save

Drag a column header and drop it here to group by that column Total: 4 Modified: 2

Deploy	Modified	NIC	Fabric	Tagged VLAN(s)	Untagged VLAN
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-3-1	A1	1-100	101
<input checked="" type="checkbox"/>	Yes	NIC.Integrated.1-4-1	A2	1-100	101
<input type="checkbox"/>	No	NIC.Integrated.1-1-1	A1		
<input type="checkbox"/>	No	NIC.Integrated.1-2-1	A2		

Help Cancel Back Next

Figure 15 Edit IOA VLAN attributes

## 18 Auto-deploying the templates

Auto deploying the templates applies to all the attribute values of the templates to the device, after it is 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. For instructions to create a template, see [Creating templates](#).

**Note:** Auto deploy is only for devices that have not been discovered by OME. To deploy on devices discovered by OME, see [Creating templates](#).

### 18.1 Auto deploy requirements

To add auto deployment entries, the following requirements must be met:

- Must have a template to deploy. See [Creating the template from the reference device](#).
- Must meet all device configuration target device requirements. See [Target device requirements](#).
- Target Service Tags cannot match a Service Tag of a discovered device.
- A CSV file with the Service Tags. See [Create a Service Tag CSV file](#).

### 18.2 Setting up auto deploy of a template

This section describes how to set up auto deployment of a template by using Service Tags. Also, describes how to create and format the auto deployment CSV file and the auto deployment wizard.

#### 18.2.1 Creating Service Tag CSV file

To create a CSV file containing the target Service Tags to be deployed:

- Must have a column named **ServiceTag**.
- Each Service Tag must match Dell EMC standards for Service Tags.
- Service Tags may not match the Service Tag of a discovered device in OME.

	A
1	ServiceTag
2	ABCDEFGF
3	HY3912B
4	A123456
5	VNX189W

Figure 16 Format of an example CSV file.

#### 18.2.2 Setting up stateless auto deploy of the template to the server Service Tags

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Setup Auto Deployment** under **Common Tasks**.
3. Select the target compute pool, and then click **Next**.
4. Review the selected template, and then click **Next**.

5. Review the selected Virtual I/O pool, and then click **Next**.
6. Click the **Import** to import the csv file that contains the Service Tag or node ID. The imported Service Tags or node IDs must be compatible with the type of template selected in the step above.
7. Browse to the location where the file is saved, select the file, and then click **Open**. All the Service Tags in the file will be imported and listed in OME. The **Import Summary** window is displayed.
8. Review and click **Ok**. Click **Next**.
9. (optional) Enter the unique attributes per Service Tag. For more information, see [Editing the device specific attributes of the deploy template task](#). Note that virtual identities may be reviewed, but may not be assigned. Assignment occurs when the device is discovered.
10. Click **Next**.
11. 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. If no credentials exists yet, at least one (a default set of credentials) must be created. Do the following. Else, go to the last step in this section.
  - i. Click **Add New Credential**.
  - ii. Type a description for the credential set (the description text is displayed in the credential selection page).
  - iii. Type the username and password.
  - iv. Click **Finish**.
12. Review the task in the Summary pane and click **Finish**.
13. All the Service Tags/node IDs that were imported are listed in the **Auto Deployment** tab.
14. 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 compute pool 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 the task to view the task details. Task execution history entries can be found in the task execution history grid. Double-click on task execution history entry to view the task execution history details.

### 18.2.3 Setting up bare-metal auto deploy of the template to server Service Tags

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Setup Auto Deployment** under **Common Tasks**.
3. Select **Deploy Template**, and then 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 then 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, and then click **Next**.

7. (optional) Enter the unique attributes per Service Tag. For details, see [Editing the device specific attributes of the deploy template task](#).
8. Click **Next**.
9. 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. If no credentials exists yet, at least one (a default set of credentials) must be created. Follow these steps, otherwise go to last step.
  - i. Click **Add New Credential**.
  - ii. Type a description for the credential set (the description text is displayed in the credential selection page).
  - iii. Type the username and password.
  - iv. Click **Finish**.

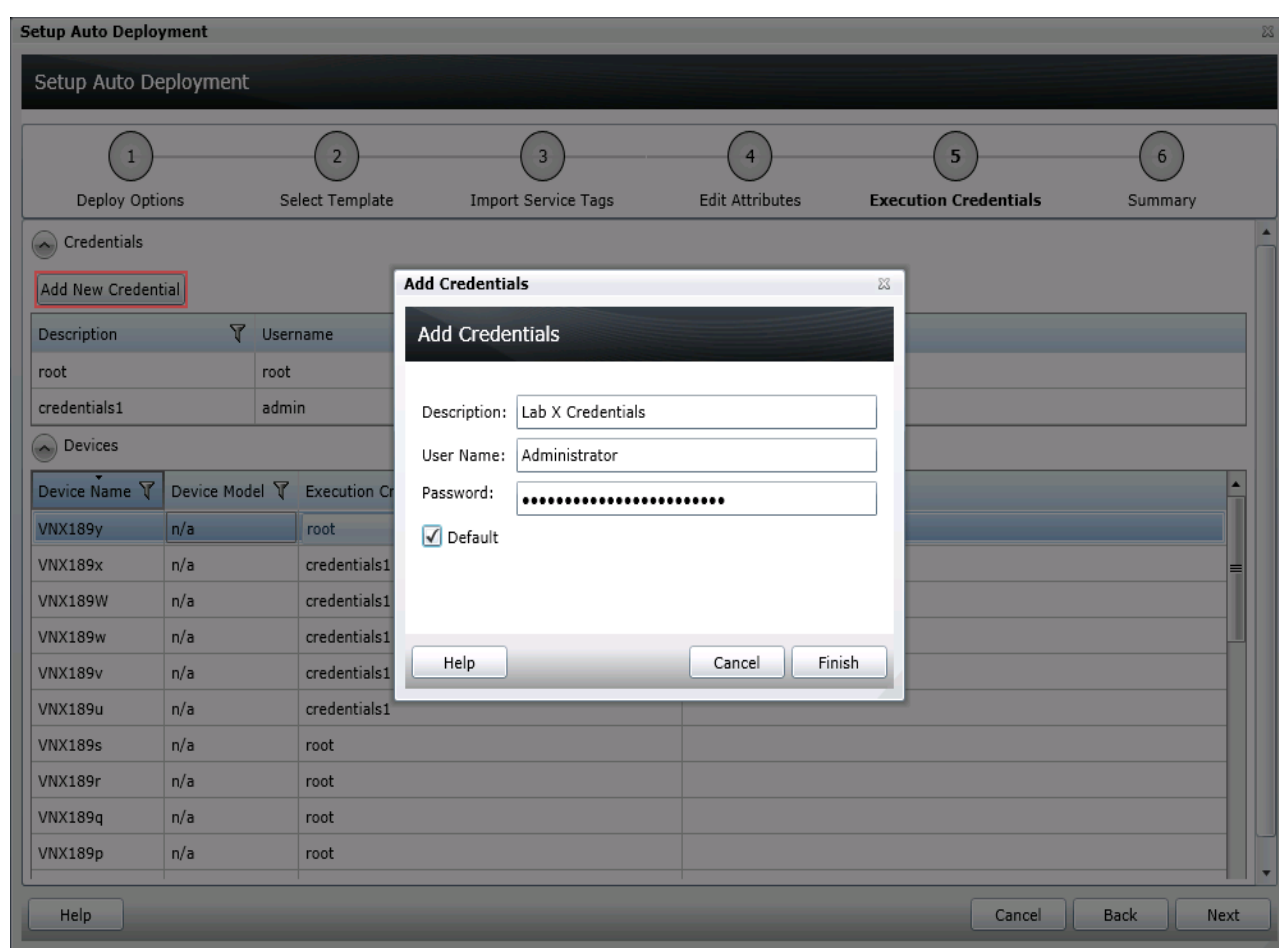


Figure 17 Auto deployment target credentials page

10. Review the task in the **Summary** pane, and then click **Finish**.
11. All the Service Tags that were imported are listed in the **Auto Deployment** tab.
12. 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.

## 18.2.4 Modifying the auto deployment settings

By default, the Deploy Configuration to Undiscovered Devices task runs after 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:

1. Under the **Preferences** tab, navigate to the **Deployment Settings** tab.
2. Select or clear 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 by using the numeric control. The number is the minute interval that the **Deploy Configuration to Undiscovered Devices** task will run.

The screenshot shows the 'Deployment Settings' page in the Dell EMC OpenManage Essentials interface. The left-hand navigation pane lists various settings categories, with 'Deployment Settings' currently selected. The main content area is divided into two sections. The top section, 'File Share Settings', includes a text description about file share requirements and fields for 'Domain \ Username' (set to '.\Administrator') and 'Password'. Below this, the 'File Share Status' is 'Ok', and a checkbox 'Allow using file share for Device Configuration feature on server' is checked. The bottom section, 'Auto Deployment Settings', is highlighted with a red rectangular box. It contains a checked checkbox 'Enable auto deployment for recently discovered devices' and a configuration for the task interval: 'Run auto deployment every' followed by a numeric spinner set to '60' and the unit 'Minutes'. At the bottom right of the page, there are 'Cancel' and 'Apply' buttons.

Figure 18 Auto deployment settings page

4. Click **Apply**.

## 19 Deploying network ISO image

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

### 19.1 Deploying network ISO image requirements

- Must meet all Deploy Template requirements. See [Target device requirements](#).
- If the **Deploy Template** option is selected, only server templates can be selected.

### 19.2 Deploying network ISO image

1. Navigate to the **Deployment** tab.
2. In the left pane, click **Deploy Template** under **Common Tasks**.
3. Type 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. Select the **Boot to Network ISO** check box and clear the **Deploy Template** check box.
5. 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. For deploying the template and editing the attributes, see [Deploying the template to the servers](#).

6. Enter ISO filename, Share IP, share name, share username and share password, and then click **Next**.



**Deploy Template Wizard**

**Deploy Template**

1 Name and Deploy Options   2 Select Template   **3 Select ISO Location**   4 Select Devices   5 Edit Attributes   6 Set Schedule   7 Summary

**ISO Filename**

ISO Filename:

---

**Share Location**

Share IP:

Share Name:

---

**Share Credentials**

Share Username:

Share Password:

Figure 19 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.

7. Select the target devices and click **Next**.

**Note:** Only devices in the **Repurpose** and **Bare-metal** device group may be selected. To add the devices to the group, see the [Adding devices to the 'Repurpose and Bare-metal' device group](#).

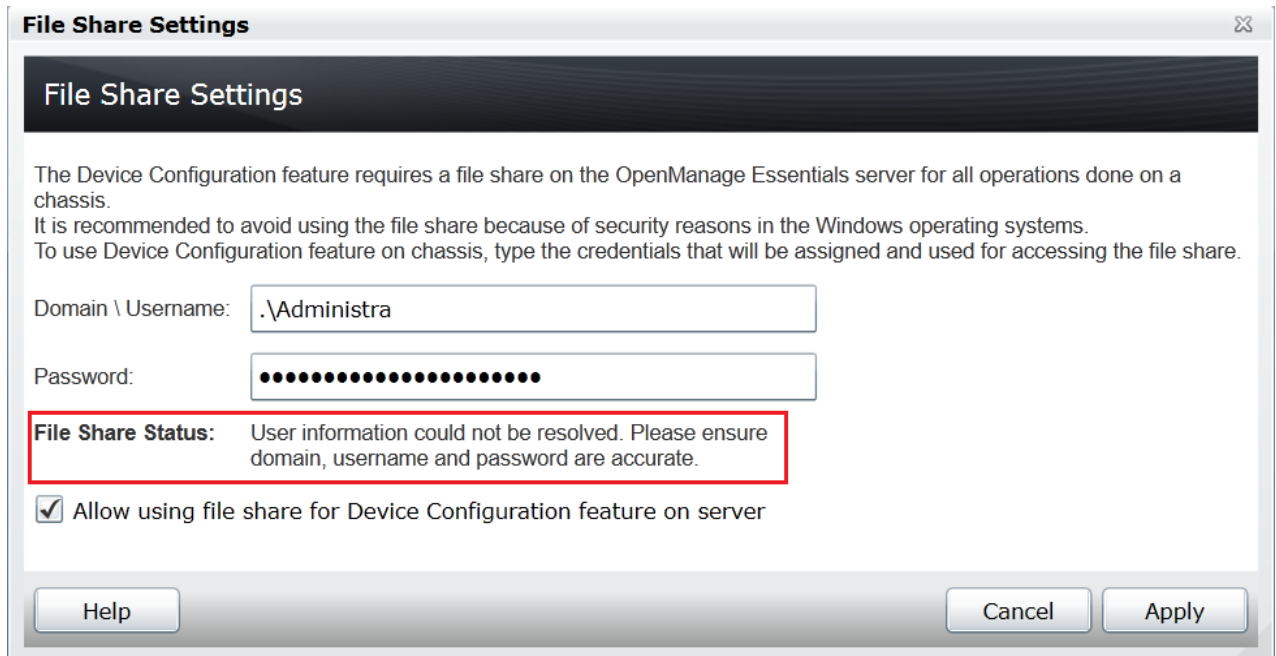
8. Set the schedule of when the deploy template task will run. **Run now** will run the task when the wizard is closed. **Run at** will run the task on the selected future date. Enter the credentials for all target devices. The credentials must be valid for all target devices and must have the Operator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

## 20 Troubleshooting

### 20.1 Troubleshooting the file share

1. Check the file share status in OME.

Note: The file share status is at the bottom of the file share wizard and under the **Deployment Settings** preference.



**File Share Settings**

**File Share Settings**

The Device Configuration feature requires a file share on the OpenManage Essentials server for all operations done on a chassis.  
It is recommended to avoid using the file share because of security reasons in the Windows operating systems.  
To use Device Configuration feature on chassis, type the credentials that will be assigned and used for accessing the file share.

Domain \ Username: .\Administra

Password: .....

**File Share Status:** User information could not be resolved. Please ensure domain, username and password are accurate.

☒ Allow using file share for Device Configuration feature on server

Help Cancel Apply

Figure 20 File share settings status

2. Check the username, domain and password in OME.
3. Check the share folder in Windows Explorer.

Verify the **ServerConfig** folder exists under the installation configuration folder (by default under **Program Files\Dell\SysMgt\Essentials\configuration**).

Verify the folder is shared. Right-click the folder, select **Properties**, and navigate to the **Sharing** tab. The folder must be shared. The **Advanced Sharing** permission settings must have the user entered in OME as the only user with permissions to the folder.

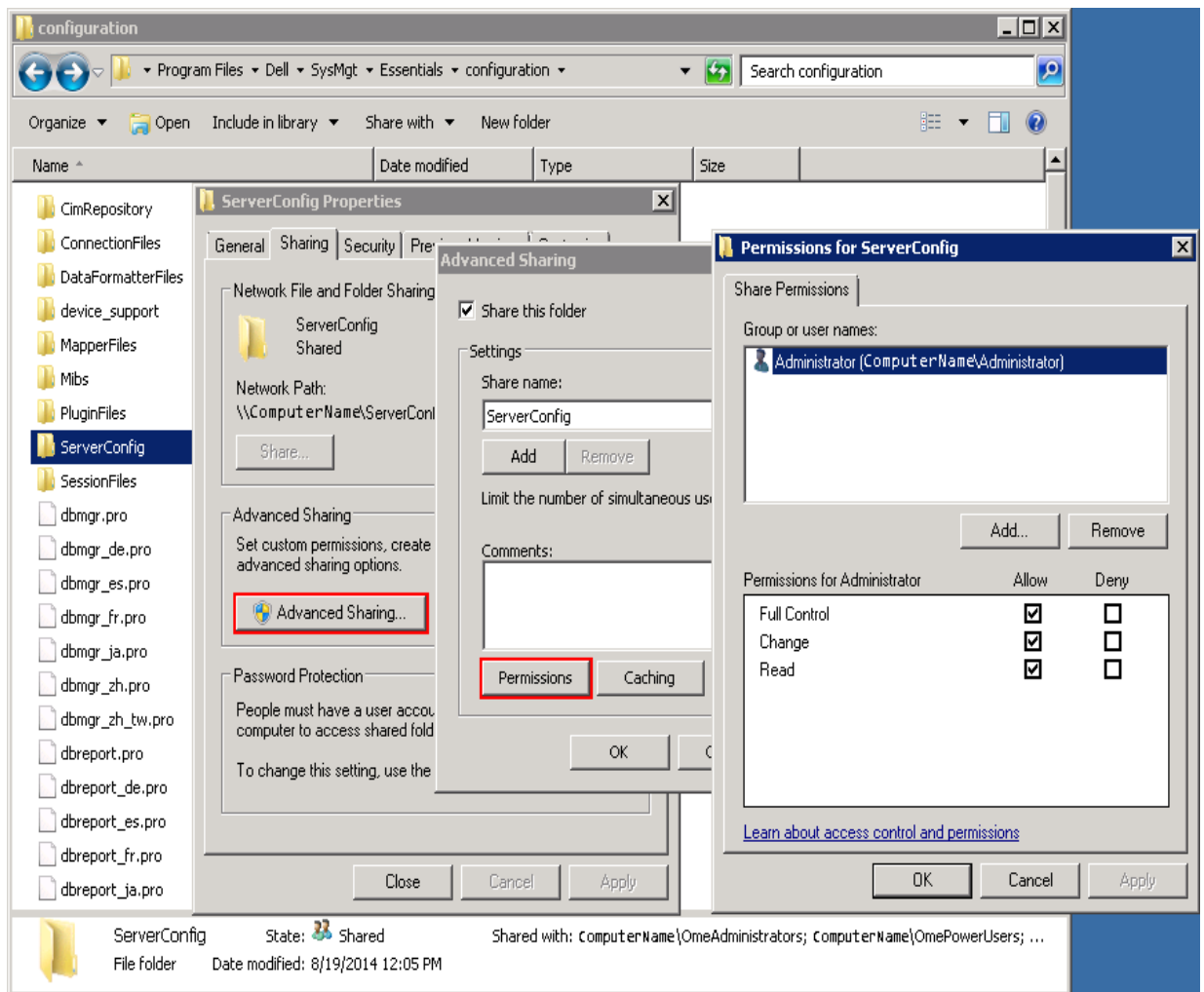
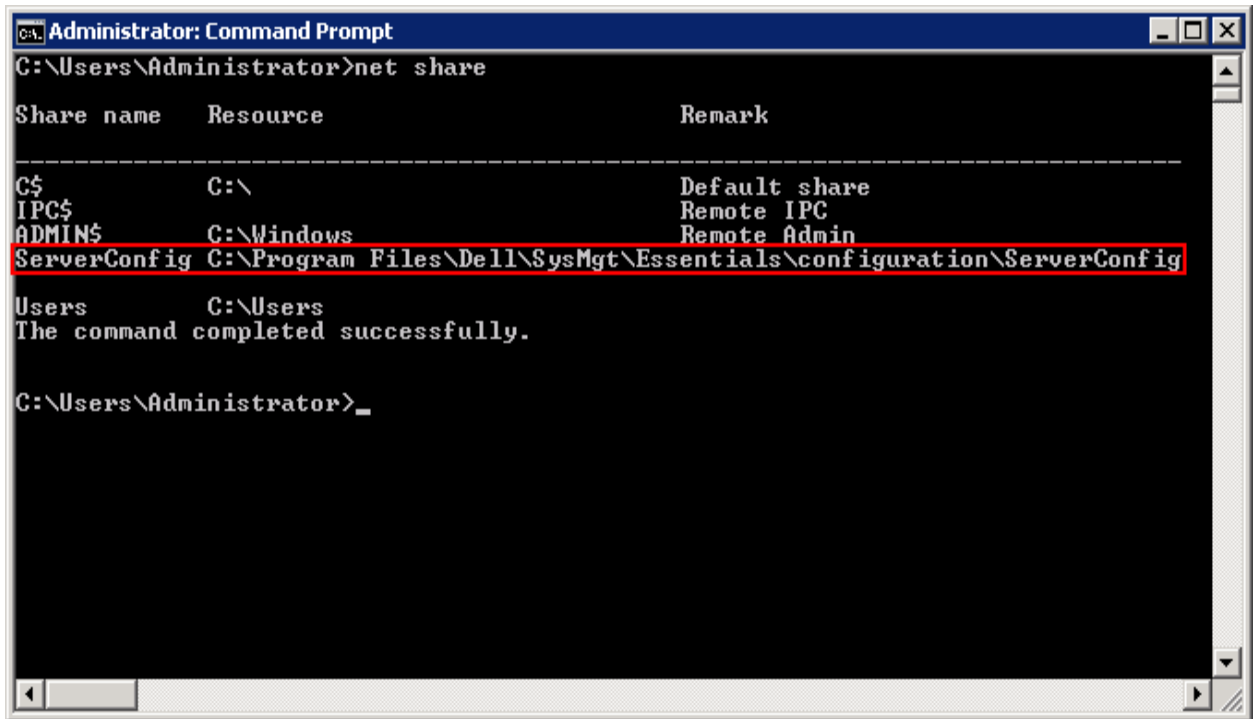


Figure 21 Advanced sharing tab of the **ServerConfig** folder

- Verify the share folder location by using the `net share` command.
- Open the command prompt and type `net share`.
- A share with the name **ServerConfig** should be in the network share list.



```
Administrator: Command Prompt
C:\Users\Administrator>net share

Share name      Resource                                Remark
-----
C$              C:\                                    Default share
IPC$            C:\                                   Remote IPC
ADMIN$          C:\Windows                           Remote Admin
ServerConfig    C:\Program Files\Dell\SysMgt\Essentials\configuration\ServerConfig
Users           C:\Users
The command completed successfully.

C:\Users\Administrator>
```

Figure 22 Net share command results

- Check the user permissions in the **User Accounts** window.

## 20.2 Troubleshooting the template creation

Troubleshooting creating a template from a reference device:

- Make sure that the file share settings are correctly configured. See [Error! Reference source not found.Troubleshooting the file share](#).
- Run the task again. Right-click the task or task execution history and select **Run**.
- The task execution may have an **LC** code in the details. Review the **LC** code in the iDRAC documentation. See [Additional resources](#)
- Make sure that the provided credentials have enough privileges to run the task (requires administrator privileges on the iDRAC).
- Make sure that the minimum firmware version requirement is met by the reference device.

Troubleshooting creating a template from a file:

- Make sure the file meets all the requirements. See [File Requirements](#).
- 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 available options are .xml, .ini, and .txt.

## 20.3 Troubleshooting the Virtual I/O pool creation

Troubleshooting the creating or editing an identity type:

- Make sure the identity type definition meets the requirements for that identity type. See [Types of identities](#).
- If you cannot edit a Virtual I/O pool, it is likely locked. To unlock it (and enable editing) see [Locking and unlocking the Virtual I/O pool](#).
- If a Virtual I/O pool runs out identities to assign, a warning message appears during the assignment process in the deploy wizard. The size of a Virtual I/O pool can be increased. See [Increasing the size of the Virtual I/O Pool](#).

## 20.4 Troubleshooting the template deployment

The task execution history details provide troubleshooting information.

- Redfish Streaming related messages are shown in case of any error with it.
- If the file share is used for servers, ensure that settings are entered correctly. See [Troubleshooting the file share](#).
- 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. See [Additional resources](#). The details tab also contains the results of applying individual attributes.
- If there is **cannot connect to server** error, make sure the target credentials are correct.
- If there is **server is being configured** error, wait and retry later. If the task still fails, the server may need a restart and/or iDRAC reset.
- If there is server restart failure, restart the server through the iDRAC interface.
- 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 the attribute registry in [Additional resources](#).
- If the task is not completed, the task will timed out and exit after 30 minutes of inactivity. You need to execute the task again. The restart and/or iDRAC reset may be necessary.

## 20.5 Troubleshooting the auto deploying templates

Whenever the **Deploy Configuration to Undiscovered Devices** task is executed, it looks for Service Tags in the **Auto Deployment** list. The following situations may be observed:

- 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.
- 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.
- 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, to troubleshoot the error, see [Troubleshooting the file share](#).

## 20.6 Troubleshooting the network ISO deployment

The task execution history details provide the troubleshooting information.

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

- Verify the IP address in the share location.
- Verify the path to the folder of the share.

A common misconception is to put the share base folder in the share name area; however, the share base folder is used for the full folder path.

**Correct:**

Share: share\isos\linux

File name: Ubuntu.iso

**Incorrect:**

Share: share

File name: isos\linux\Ubuntu.iso

Check the user credentials for the file share.

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

- Check the file name for correctness.
- Check the path of the ISO.

## 21 Additional resources

[Support.dell.com](http://support.dell.com) is focused on meeting your needs with proven services and support.

[DellTechCenter.com](http://delltechcenter.com) is an IT Community where you can connect with Dell EMC Customers and Dell EMC employees for the purpose of sharing knowledge, best practices, and information about Dell EMC products and installations.

Referenced or recommended Dell EMC publications:

- Dell EMC Attribute Registry:  
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx#attributereg>
- Dell EMC iDRAC7 with Lifecycle Controller 2 Technical White Papers:  
<http://en.community.dell.com/techcenter/systems-management/w/wiki/4317.white-papers-for-idrac7-with-lifecycle-controller-2.aspx>
- Dell EMC iDRAC Licensing:  
[http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac.aspx#iDRAC7\\_licensing](http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.dell-remote-access-controller-drac-idrac.aspx#iDRAC7_licensing)
- Dell EMC LC Error Codes:  
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx>
- Dell EMC OpenManage Essentials TechCenter page:  
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1989.openmanage-essentials.aspx>



## 22 Boot-from-SAN considerations

The template attributes include the attributes to support Boot-from-SAN operations. Boot-from-SAN functionality may run over iSCSI, FC, or FCoE connections. The Boot-from-SAN operations attributes include the attributes for both initiators and targets.

Regardless of the protocol being used, the storage (target) hardware and software must be setup, configured, and available on the network. It is beyond the scope of this document to address this topic, as these procedures are usually vendor-specific.

Irrespective of the protocol, confirm the below actions for the storage (target) hardware and software:

- Setup
- Configuration
- Availability on the network

For a device to boot-from-SAN, its attributes need to be configured correctly. During the manual identity assignment, the operator sets all the attributes to the appropriate values. During OME's auto identity assignment, OME uses the Virtual I/O pool associated with the Compute Pool to set applicable Initiator identity attributes associated with Boot-from-SAN operations. If you need to change the Target attributes for Boot-from-SAN operations (For example, if you need to use the different target), the operator has to make those changes manually.

### 22.1 Boot-from-SAN by using iSCSI

The following attributes apply to Boot-from-SAN operations by using iSCSI:

#### Initiator Attributes

##### General iSCSI Attributes

```
iScsiOffloadMode
TcpipViaDHCP
IscsiViaDHCP
DhcpVendId
ChapAuthEnable
ChapMutualAuth
LnkUpDelayTime
LunBusyRetryCnt
IpVer
IpAutoConfig
TcpTimestamp
WinHbaBootMode
```

## Initiator-Specific iSCSI Attributes

**VirtIscsiMacAddr**  
IscsiInitiatorIpAddr, IscsiInitiatorIpv4Addr, IscsiInitiatorIpv6Addr  
IscsiInitiatorSubnet  
IscsiInitiatorSubnetPrefix  
IscsiInitiatorGateway, IscsiInitiatorIpv4Gateway, IscsiInitiatorIpv6Gateway  
IscsiInitiatorPrimDns, IscsiInitiatorIpv4PrimDns, IscsiInitiatorIpv6PrimDns  
IscsiInitiatorSecDns, IscsiInitiatorIpv4SecDns, IscsiInitiatorIpv6SecDns  
**IscsiInitiatorName**  
IscsiInitiatorChapId  
IscsiInitiatorChapPwd  
IscsiVlanMode  
IscsiVlanId  
SecondaryDeviceMacAddr  
UseIndTgtPortal  
UseIndTgtName

## Related Attributes

BiosBootSeq  
BootOption  
VirtualizationMode

## Target Attributes

### General Target iSCSI Attributes

IscsiTgtBoot  
ConnectFirstTgt                      ConnectSecondTgt  
FirstHddTarget

### Target-Specific iSCSI Attributes

FirstTgtIpVer	SecondTgtIpVer
FirstTgtIpAddress	SecondTgtIpAddress
FirstTgtTcpPort	SecondTgtTcpPort
FirstTgtIscsiName	SecondTgtIscsiName
FirstTgtBootLun	SecondTgtBootLun
FirstTgtChapId	SecondTgtChapId
FirstTgtChapPwd	SecondTgtChapPwd

Of the preceding iSCSI attributes related to boot-from-SAN, the only ones assigned by OME, for automatic identity assignment, are the **VirtIscsiMacAddr** and **IscsiInitiatorName** attributes (highlighted above). A value for the **VirtIscsiMacAddr** attribute is obtained using the “Ethernet Identities” definition specified for the Virtual I/O pool, and a value for the **IscsiInitiatorName** attribute is obtained using the “iSCSI IQN Identities” definition given for the Virtual I/O pool.

OME 2.1 has the following limitation regarding iSCSI boot-from-SAN and auto-assignment of identity values from a Virtual I/O pool:

Support is only provided for the assignment of iSCSI IP addresses by DHCP, which is specified via the following two attributes and corresponding values:

<code>TcpipViaDHCP</code>	"Enabled"
<code>IscsiViaDHCP</code>	"Enabled"

Due to this restriction, Virtual I/O pools don't have a provision for assigning IP addresses, subnet, or gateway values for iSCSI.

## 22.2 Boot-from-SAN by using FC or FCoE

The following attributes apply to Boot-from-SAN operations by using FC or FCoE:

### Initiator Attributes

- `VirtWWN`
- `VirtWWPN`
- `VirtFIPMacAddr`

### Target Attributes

#### General Attributes

- `FCoEOffloadMode`
- `FCoETgtBoot`
- `ConnectFirstFCoETarget`
- `FCoELnkUpDelayTime`
- `FCoELunBusyRetryCnt`
- `FCoEFabricDiscoveryRetryCnt`
- `FCoEBootScanSelection`
- `BootOrderFirstFCoETarget`
- `BootOrderSecondFCoETarget`
- `BootOrderThirdFCoETarget`
- `BootOrderFourthFCoETarget`
- `FirstFCoEWWPNTarget`
- `FirstFCoEBootTargetLUN`

#### Target-Specific Attributes

- `FirstFCoEFCFVLANID`
- `FCoEFirstHddTarget`

In the above FC/FCoE attributes related to boot-from-SAN, the attributes assigned by OME, for automatic identity assignment, are the `VirtWWN`, `VirtWWPN`, and `VirtFIPMacAddr` attributes. A value for the `VirtWWN` attribute is obtained by using the FCoE Node Name Identities definition specified for the Virtual I/O pool, a value for the `VirtWWPN` attribute is obtained using the FCoE Port Name Identities definition specified for the Virtual I/O pool, and a value for the `VirtFIPMacAddr` attribute is obtained by using the "Ethernet Identities" definition given for the Virtual I/O pool.