Advanced Server Configuration in Dell EMC OpenManage Enterprise 3.0

Abstract

This technical paper describes the functionality for server configuration management in Dell EMC OpenManage Enterprise 3.0 for device deployment and configuration activities.

January 2019

Revisions

Date	Description
January 2019	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC system management engineering team:

Author(s): **Reg Stumpe, Pushkala Iyer, Rakesh Ayolasomyajul, Matthew Maze, and David Sisson**

Contents

Revisions....2
Acknowledgements....2
Executive summary....5
1 Introduction to server configuration in OpenManage Enterprise 3.0....6
1.1 Configuration Elements....6
1.1.1 Templates in OpenManage Enterprise....6
1.1.2 Identities in OpenManage Enterprise....6
1.1.3 VLAN-based networks in OpenManage Enterprise....7
1.2 Deployment in OpenManage Enterprise....7
1.3 Typical Server Configuration Scenario....7
2 Templates in OpenManage Enterprise....8
2.1 Template Structure....8
2.2 Template Operations....8
2.2.1 Create Template....8
2.2.2 Setup Identity Pool and Network Settings....8
2.2.3 Modify template properties in OpenManage Enterprise....9
2.2.4 Deploy Template....11
2.2.5 Export Template....14
2.2.6 Clone Template....15
2.2.7 Delete Template....15
3 Identity Pools in OpenManage Enterprise....16
3.1 Purpose and usage of Identity Pools in OpenManage Enterprise....16
3.2 Identity States in OpenManage Enterprise....17
3.3 Identity Pool Structure....17
3.3.1 Ethernet Identities....17
3.3.2 iSCSI Identities....18
3.3.3 FCoE Identities....20
3.3.4 Fibre Channel (FC) Identities....21
3.3.5 Address constraints....21
3.4 Identity Pool operations....21
3.4.1 Create Identity Pool....22
3.4.2 Modify Identity Pool....22
3.4.3 Review Identity Pool Summary and Usage....22
3.4.4 Delete Identity Pool....23
3.4.5 Export Identity Pool....23

3.5 Identity Pool Planning and Strategy 23
4 VLAN-based networks 25
4.1 VLAN-based network structure and usage 25
4.2 VLAN-based network operations 25
4.2.1 Create VLAN-based network 25
4.2.2 Modify VLAN-Based Network 25
4.2.3 Export VLAN-Based Network 26
4.2.4 Delete VLAN-Based Network 26
5 Troubleshoot templates and Identify Pools in OpenManage Enterprise 27
A Technical support and resources 28

Executive summary

OpenManage Enterprise 3.0 is the logical follow-on to the existing OpenManage Essentials (OME) console or its predecessor OpenManage–Tech Release. While OpenManage Enterprise 3.0 can be used for monitoring and simple task execution on managed servers, it also has advanced features for server configuration. This technical white paper explains key terminology, constructs, and typical use cases for server configuration.

1 Introduction to server configuration in OpenManage Enterprise 3.0

The current configuration of a server is represented as several individual elements—called configuration attributes. For a typical server, there are several hundred such attributes, and it can be quite overwhelming to tune all different aspects. OpenManage Enterprise 3.0 has features that make it easy for a user to capture configuration from a “reference” server (that is, server for which all aspects have been correctly set up and fine-tuned) and replicate that configuration to one or more target servers. Some of the configuration element values need to be different on the different targets. OpenManage Enterprise 3.0 has features that ensure the configuration captured from a source server is correctly replicated to a target, while ensuring that the configuration elements that need disparate values are populated correctly.

1.1 Configuration Elements

1.1.1 Templates in OpenManage Enterprise

The configuration management and compliance operations provided in OpenManage Enterprise 3.0 provide the capability to manage and control the configuration of the devices in a network. A template is a set of system configuration settings referred to as attributes. A template may contain a small set of attributes for a specific purpose, or all the attributes for a full system configuration. OpenManage Enterprise provides several options for creating templates:

- Some pre-canned templates for specific purposes.
- A template can be created by importing a Server Configuration Profile (SCP) file into the OpenManage Enterprise appliance. The SCP file can be captured from a server by using the 1x1 iDRAC GUI (Graphical User Interface), or exported by OpenManage Essentials (OME), or OpenManage Enterprise.
- Most frequently, templates are created by getting the current system configuration from a server on the network (referred to in OpenManage Enterprise as a “Reference Server”).
- Templates may also be cloned (copied) and edited. This applies to all templates, whether built-in, imported, or created from a reference device.

1.1.2 Identities in OpenManage Enterprise

Some of the attributes which are typically included in a template are referred to as Identity attributes. Identity attributes identify a device and distinguish it from all other devices on the network. Because identity attributes must uniquely identify a device, it is imperative that each device has a unique network identity. Otherwise, inter-device network communications cannot function properly.

Devices come with unique manufacturer-assigned Identity values pre-installed (such as a factory-assigned MAC address). Those identities are fixed and never change. However, devices can assume a set of alternate identity values, called a “virtual identity”, and function on the network by using that identity, as if the virtual identity were its factory-installed identity. The use of virtual identity is the basis for Stateless operations.

OpenManage Enterprise provides management support for “virtual identities”. Just like factory-installed identities, virtual identities must also be unique on the network. Using virtual identities enables OpenManage Enterprise to support operations such as shifting (migrating) a full device configuration—including its virtual identity—from one server to another. In other words, a virtual identity can be removed from one device and assigned to a different device (for example, in case the original device stops working or requires maintenance).

1.1.3 VLAN-based networks in OpenManage Enterprise

VLAN-based networks refers to individual VLANs and/or VLAN ranges used for a specific purpose. These networks are configured by using the Networks tab on the Configuration page. VLAN-based networks are used when specifying network settings for templates.

1.2 Deployment in OpenManage Enterprise

Deployment is the process of applying a full or partial system configuration on a specific target device. In OpenManage Enterprise, templates are the basis for all deployments. Templates contain the system configuration attributes that get sent to the target device. The iDRAC on the target device applies the attributes contained in the template and restarts the device if necessary.

Often, templates contain virtual identity attributes. As mentioned earlier, identity attributes mush have unique values on the network. Identity Pools facilitate the assignment and management of unique virtual identities.

1.3 Typical Server Configuration Scenario

The system administrator sets up a reference server, fine tuning it as required. For example, the server may be setup for high performance computing, access to the host front USB disabled for security purposes, and power capped to a certain value. These settings could be configured from BIOS or via the iDRAC GUI or any other interface. The system administrator may then want to propagate this configuration to one or more target servers. This could be achieved by capturing a template from the source server by using OpenManage Enterprise. The system administrator could be selective about which aspects or components are included in the template. If all aspects of the template are included, some identity attributes need specific values assigned before the template is deployed to the multiple targets. The system administrator can use OpenManage Enterprise to set up an identity pool, and assign identities prior to deployment.

2 Templates in OpenManage Enterprise

2.1 Template Structure

- A template is a collection of various configuration elements, organized into different aspects or components. Viewing a template as an XML file shows this structure.
- A very short example is shown below. This shows the value of one attribute in the LifecycleController component.
- A template typically contains several hundred attributes in different components.
- The template was extracted from a PowerEdge MX740c server.

```
<SystemConfiguration TimeStamp="Tue ... 02:28:10 2018" ServiceTag="PFSTMB2"
Model="PowerEdge MX740c">
<Component FQDD="LifecycleController.Embedded.1">
       <Attribute
Name="LCAttributes.1#CollectSystemInventoryOnRestart">Enabled</Attribute>
</Component>
</SystemConfiguration>
```

2.2 Template Operations

2.2.1 Create Template

In OpenManage Enterprise 3.0, a Template can be created in one of the following two methods:

Extract template from a reference server—Enables you to create a template from reference device, and then capture a “clone” of the configuration from the server or chassis. You can select one device from which to extract the template, and then select the components that must be included in the template (the choice of components is only available for server templates).

Import template from a file—You have a template that is already extracted by some means earlier, and can import the template into OpenManage Enterprise. The “Import from File” option must be selected.

2.2.2 Setup Identity Pool and Network Settings

Identity Pools provide sets of values that can be used for virtual identity attributes for deployment. For example, MAC addresses, iSCSI MAC/IQNs/Initiator IPs, FCoE FIP MAC/WWPN/WWNN, FC WWPN/WWNN, which can be reserved and assigned for deployment.

After a template is created, an Identity Pool can be associated with it by using the “Edit Networking” option. The Identity Pool is then used to get identity values whenever the template is deployed to a target device. An identity pool can be associated with one or more templates. Identity pools are explained in detail in Identity Pools in OpenManage Enterprise.

The “Edit Networking” option can also be used to configure networking properties (for example, VLANs and bandwidth) with the NIC configuration that is associated with a template. The VLANs are used to configure the server-facing ports of supported Dell EMC networking IOMs for compute sleds in either an MX7000 chassis, M1000e, or VRTX chassis.

2.2.3 Modify template properties in OpenManage Enterprise

OpenManage Enterprise offers two methods to modify templates—a Guided Edit and an Advanced Edit.

The Guided Edit offers a simplified view of the server configuration attributes. These are a few of the BIOS, Boot, Networking, and Storage configuration.

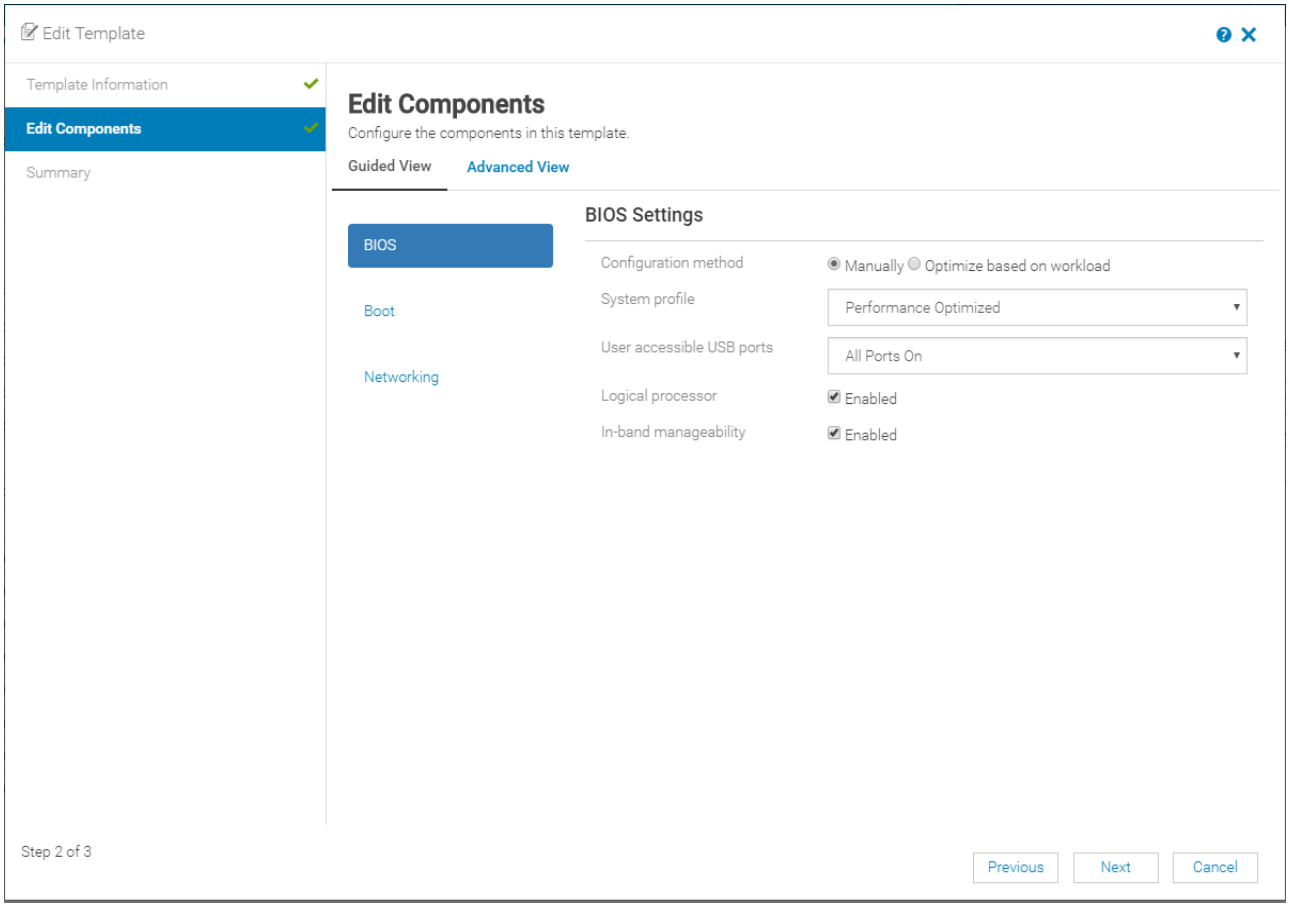

Figure 1 Edit template in OpenManage Enterprise—the Guided view (This screen varies depending on the template definition)

Basic BIOS specification—Enables the administrator to configure key basic BIOS attributes. This will include, for example, Workload Profile (options for power or performance settings for environments such as HPCC, Low Latency, Virtualization, Database, and Software defined storage), System Profile, Logical Processor or Hyper threading, In-band manageability interface, and User Accessible USB ports.

- Boot specification—Select among common boot options.
- Boot mode—BIOS or UEFI
- Secure boot configuration—Secure Boot (enabled/disabled), Secure Boot mode, and Secure Boot policy
- Boot sequence retry—Enabled or disabled
- Boot sequence—You can re-order the boot sequence.
- Networking specification—You can edit the networking specification to specify an optional I/O Identity Pool to associate with the template, the logical networks (untagged and tagged VLANs) to associate with each port, and the minimum/maximum bandwidth with any associated partitions.

- If the port has been configured for boot (PXE, iSCSI, FCoE), it is displayed on the GUI. For FCoE boot, you can configure attributes such as First FCoE WWPN target and boot LUN, and FCoE FCF VLAN ID (for Intel).
- If an FC HBA is present and has been configured for FC boot in the template being edited, you can configure the FC attributes such as First and second target WWPN and LUN ID.
- Storage specification—You can configure one or more virtual drive properties (with a name, size, RAID level or layout, stripe size, read policy, and Write policy) and the selection of associated physical drives (status, name, capacity, and media type).

The advanced edit provides you with a raw edit of the different attributes in an SCP file organized in a hierarchical manner.

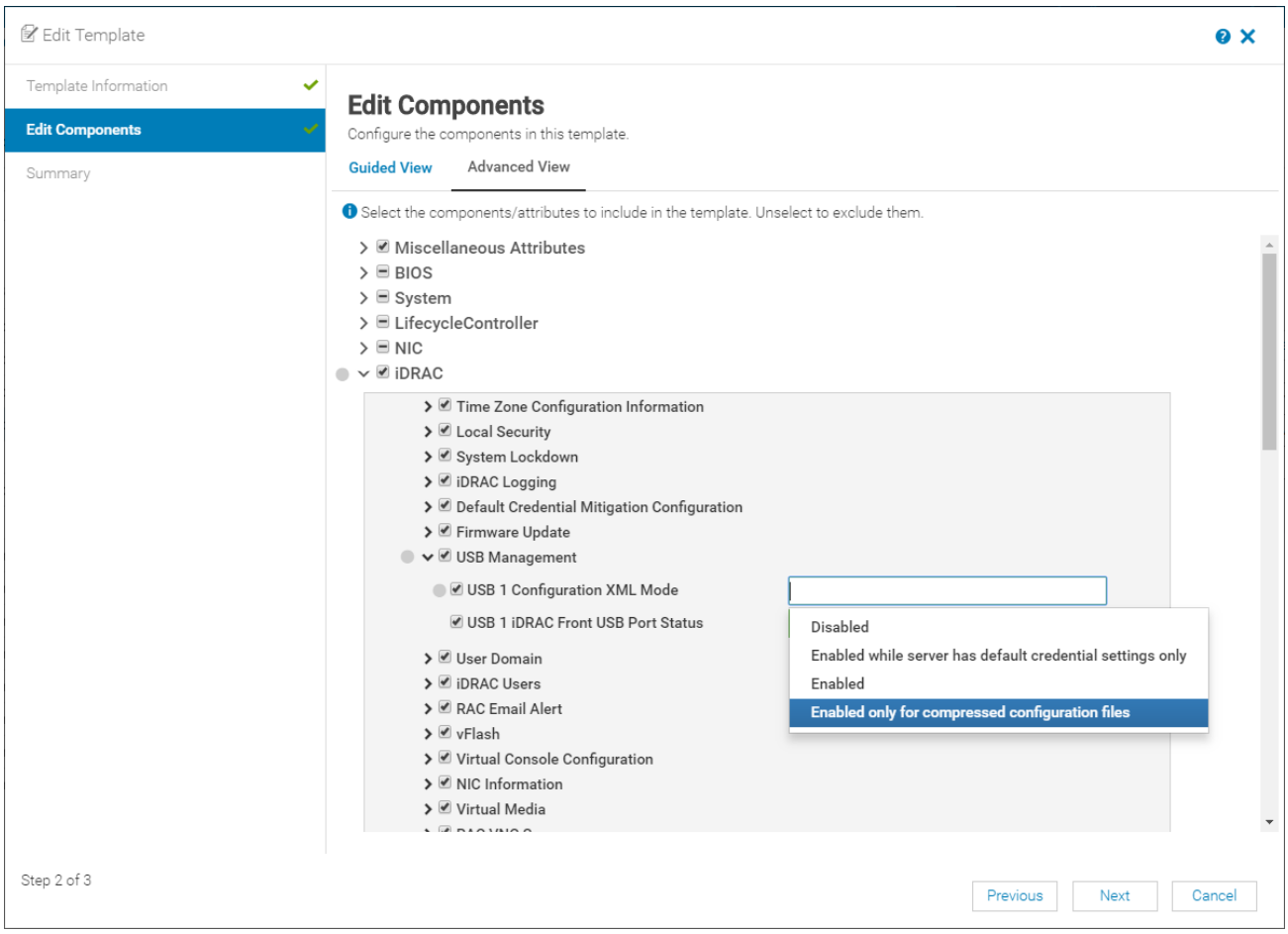

Figure 2 Edit template in OpenManage Enterprise—the Advanced view (This screen varies depending on the template definition)

2.2.4 Deploy Template

Template deployment has various steps and options. These are all displayed on the Deploy Template wizard. The Deploy Tempalte wizard has four or five steps, depending on whether or not an Identity Pool is associated with the Template being deployed. The steps in a Deploy Template wizard are:

Step: Target
The first step is to select the deployment targets—one or more target devices may be selected. Clicking the Select button displays a list of devices which may be selected as targets. In OpenManage Enterprise, only targets with a valid enterprise license can be selected for deployment. Those without that license will not be listed.

Some configuration changes require the target device to be restarted. By default, a 'force' restart is performed, which implies that the device is shut down without warning or waiting. Normally, the target devices expect the deployment and can be restarted as needed. However, if a 'graceful' shutdown is required when reboot is necessary, it can be indicated by selecting the **Do not forcefully reboot** check box in this dialog box.

Step: Boot to Network ISO
This step is optional. Iit provides a mechanism to boot the target device from a Network ISO image file after the new configuration has been deployed to it. If selected, the page prompts for share type, path, and access values for the ISO file. After deployment, the target will be booted from the specified ISO (if possible). The following screen shot shows this step when 'Boot to Network ISO' is indicated:

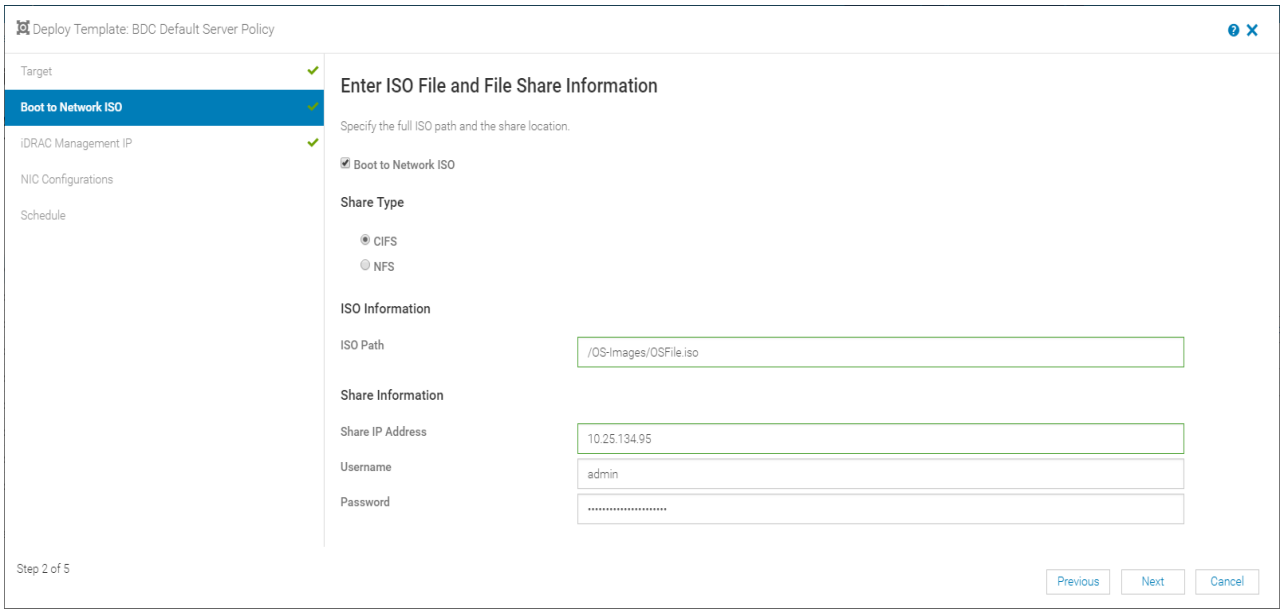

Figure 3 Boot to network ISO file share

Note that the 'Boot to Network ISO' setting applies to all target devices selected in the Target step—either they all boot from the same ISO image file, or none of them boot from an ISO image file.

Step: iDRAC Management IP
This step provides a mechanism for managing the iDRAC management IP address on the target devices. The options available are as follows:

Don't change IP settings—This is the default selection, which implies that the iDRAC IP management settings currently on the target devices will not be changed (that is, the deployment configuration will not include those attributes).

Set as DHCP—If this option is selected, the deployment configuration for each target device will specify that its iDRAC management IP address must be obtained from a DHCP server.

Set static IP for each device—If this option is selected, the deployment configuration for each target device will specify that its iDRAC management IP address is to be a static IP address. The page displays a list showing the name, model, and chassis name of each selected target device. The required static IP address must be entered for each target device.

Step: NIC Configurations
This step is only displayed when the selected tempate has an Identity Pool associated with it. It is used to reserve values from the template's assigned Identity Pool. This step is also used to set any target-specific attributes that are applicable—such as boot option attributes.

Initially, the only thing displayed on this page is an "Assign Identities" button. This button must be clicked to reserve values from the Identity Pool for this template. The types of numbers of identities that must be reserved depends on the template configuration. For example, identities are reserved for all ports and partitions defined in the template configuration.

After the Assign Identities button is pressed and identity values are reserved for all the target devices, details of the results are displayed as shown in the screen shot in Figure 4.

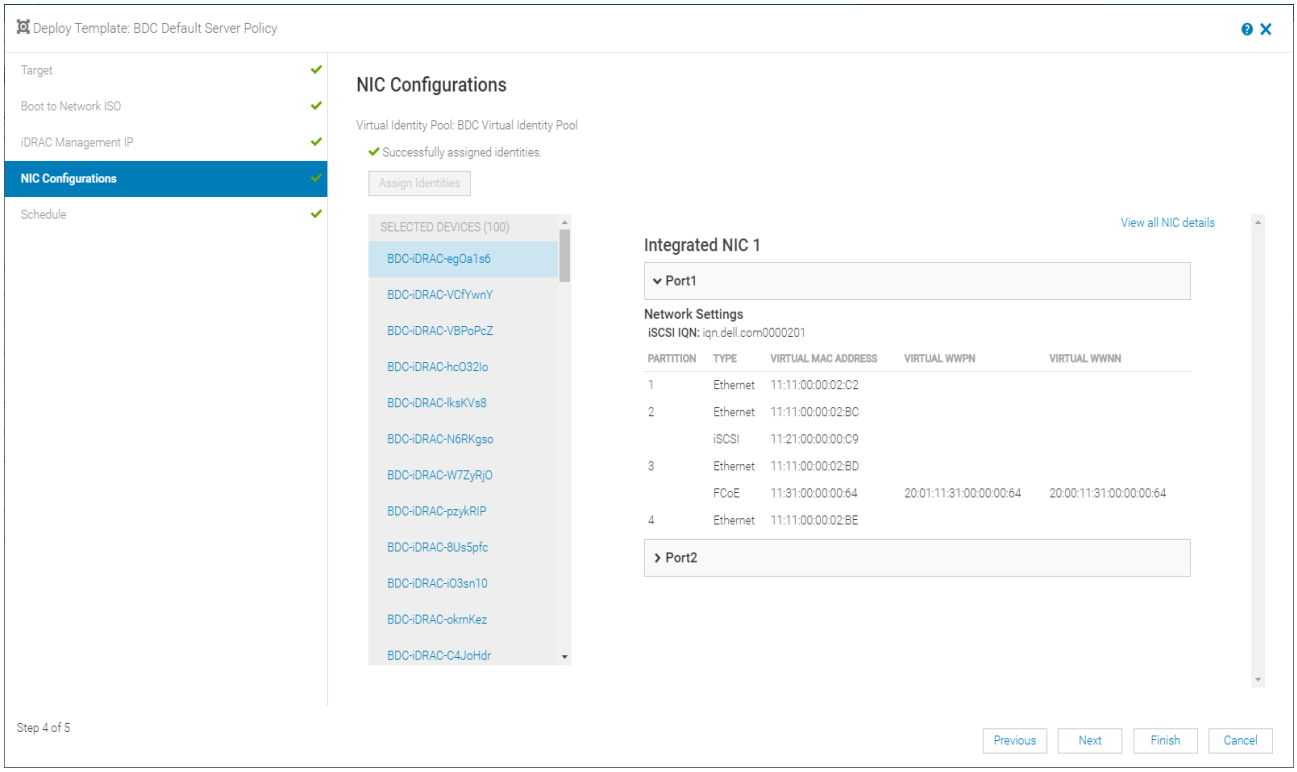

Figure 4 NIC configuration (post assign identities)

Observe that identity reservation results are displayed on a per-target basis. The list on the left includes each target device and the table on the right shows the identities and boot options for the selected device. To view a concise table of all identities reserved for the selected device, click **View all NIC details**.

Figure 4 shows only reserved identities because no Boot Options were applicable to the selected template. Boot options are configuration attributes that may require to be customized for different target devices, and are usually attributes which specify a boot device for a target device. This page allows different target devices to be configured to boot from different boot locations as required. Boot option attributes may apply to iSCSI, FCoE, or FC. Figure 5 shows a case where Fibre Channel boot options are applicable:

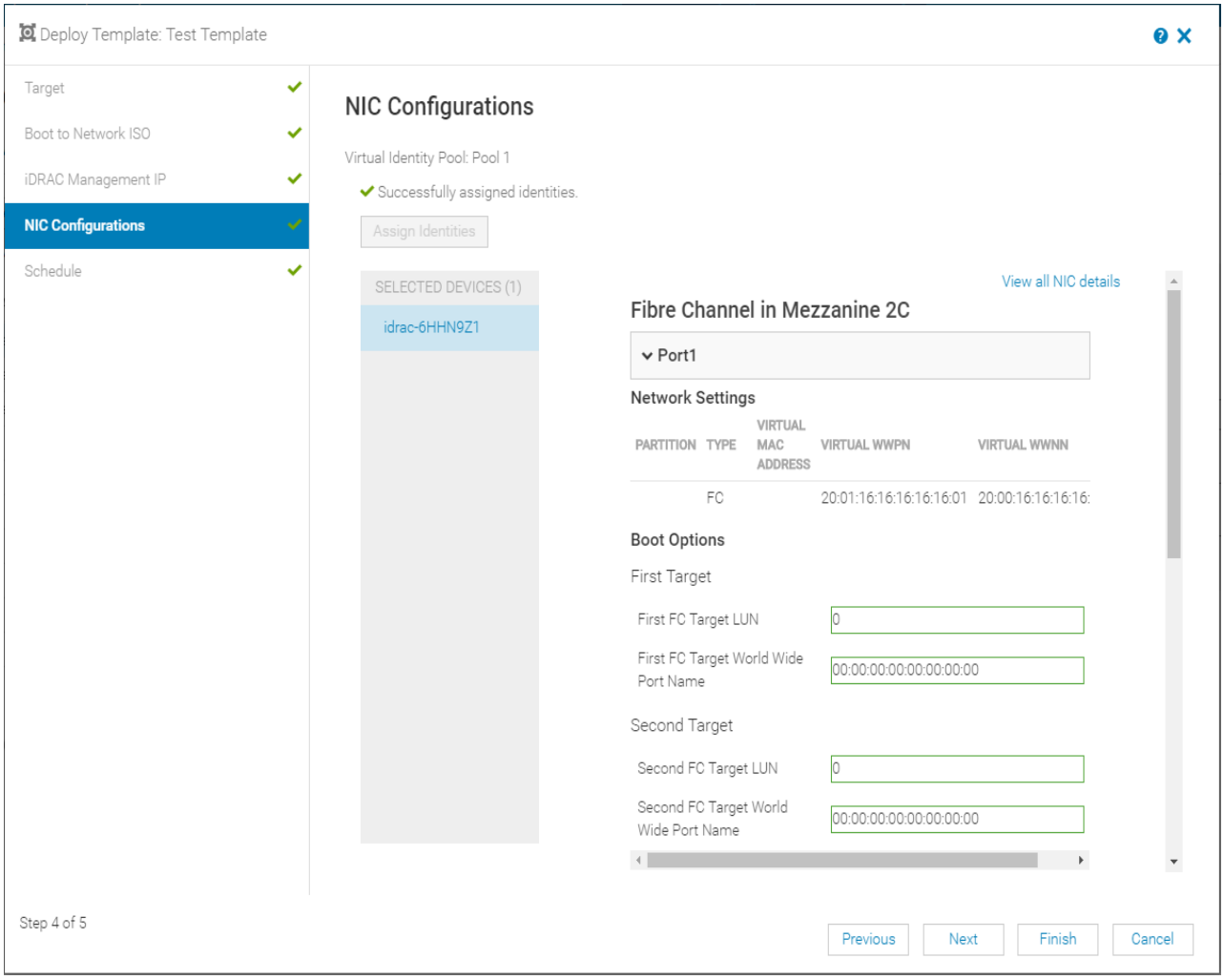

Figure 5 Fibre channel boot options

Step: Schedule

The final step, whether or not the template has an Identity Pool associated with it, is to specify when the deployment task must run. The default option is “Run Now”, if that is what is required, the wizard can be completed before getting to this step. Else, specific date and time can be specified. The deployment task will automatically start at the specified date and time.

Whether run immediately or sometime in the future, details from the deployment task can be seen by doing the following:

1. On the OpenManage Enterprise menu, click **Monitor → Jobs**.
2. Select the appropriate “Deploy Template” job.
3. Click **View Details**.

2.2.5 Export Template

A template created in OpenManage Enterprise can be exported to a file that is available to you on your file system. The exported template is in XML format. An advanced user, who knows exactly what attributes to change, could use this option to modify the content of the template and use it for deployment.

2.2.6 Clone Template

OpenManage Enterprise comes with some pre-canned templates. If you want to deploy any of these sample templates, the sample templates must be cloned first. The user may also use the clone option to make a copy of an existing template and edit it.

2.2.7 Delete Template

If a template is no longer required in OpenManage Enterprise, you can delete it. Deleting a template that has identities will cause the reserved identities (identities awaiting deployment) to be cleared and no longer show as reserved in the associated Identity Pool. Assigned identities (identities currently deployed to devices) will not be reclaimed.

3 Identity Pools in OpenManage Enterprise

This section provides detailed information about Identity Pools and their structure.

3.1 Purpose and usage of Identity Pools in OpenManage Enterprise

OpenManage Enterprise uses Identity Pools to manage the set of values that can be used as virtual identities for discovered devices. OpenManage Enterprise controls the assignment of virtual identity values, selecting values for individual deployments from pre-defined ranges of possible values. This allows the customer to control the set of values which can be used for identities, and means that the customer doesn't have to enter all needed identity values with every deployment request, or remember which values have or have not been used. Identity Pools make configuration deployment and migration much easier to manage.

Identity Pools are used in conjunction with the template deployment operations. They provide sets of values that can be used for virtual identity attributes for deployment.

After a template is created, an Identity Pool may be associated with it. Doing this specifies the Identity Pool to use to get identity values whenever the template is deployed to a target device. The same Identity Pool can be associated with (used by) any number of templates. Only one Identity Pool can be associated with a template.

Note— An Identity Pool can be associated with a template by clicking the **Edit Network** button on the **Configuration → Deploy** page.

An Identity Pool does not have to be associated with each template. However, if a template doesn't have an Identity Pool associated with it, OpenManage Enterprise cannot assign a virtual identity to target devices when the template is deployed. If a virtual identity cannot be assigned to a device, OpenManage Enterprise cannot perform some operations that would otherwise be supported (such as profile creation and migration).

If an Identity Pool is specified for a template, OpenManage Enterprise automatically uses virtual identities for management operations involving that template.

To initiate deployment of a template to a target device, you select a template (on the **Configuration → Deploy** page) and click the **Deploy Template** button. A template can be deployed whether or not an Identity Pool has been specified for it. In other words, templates can be deployed with or without a virtual identity. However, as mentioned above, if a template is deployed without a virtual identity, some configuration management operations cannot be done.

One of the steps in the **Deploy Template** wizard, when a template has an Identity Pool specified for it, is to "Assign Identities". This step reserves values from the associated Identity Pool for all virtual identity attributes needed by the template.

Each template will have specific virtual identity needs, based on its configuration. For example, one template may have iSCSI configured. Therefore, it will require appropriate virtual identities for iSCSI operations. Another template may not have iSCSI configured, but may have FCoE configured. Therefore, it will require virtual identities for FCoE operations but not for iSCSI operations.

3.2 Identity States in OpenManage Enterprise

As part of its virtual identity management functionality, OpenManage Enterprise tracks usage information for each possible virtual identity that can be generated from the sub-pools in an Identity Pool. Each virtual identity that can be generated from an Identity Pool may be in one of the following states:

Unused—Indicates that the virtual identity value is not being used by any device (as far as OpenManage Enterprise can tell) and is available for reservation for deployment.

Reserved—Indicates that the virtual identity value is reserved for deployment to a target device. Once OpenManage Enterprise deploys the identity to the target device, and confirms that it was successfully applied on the device, it will change its state to Assigned.

Assigned—Indicates that the virtual identity value was deployed to a target device and OpenManage Enterprise confirmed that the value was successfully applied on that device.

The following list shows when identity state may change:

- **Available-Reserved**—When the “Assign Identities” button in the Deploy Template wizard is pressed.
- **Available-Assigned**—If a task gets a system configuration (such as when creating a template) and a device is using a virtual identity defined in an Identity Pool. This is not expected to occur very often.
- **Reserved-Available**—After canceling out of the Deploy Template wizard (once the cleanup task runs).
- **Reserved-Assigned**—After deploying an identity to a target device and getting confirmation that it was successfully applied on the device. If a task gets a system configuration (such as when creating a template) and a device is using a virtual identity defined in an Identity Pool. This is not expected to occur very often.
- **Assigned-Available**—After running Reclaim Identity on a device (so it returns to using its factory-assigned identity).

3.3 Identity Pool Structure

This section discusses the composition of an Identity Pool. Each Identity Pool must have a unique name, and may have a description. In addition, each Identity Pool can contain values to use for generating virtual identities for one or more of the following protocols:

- `Ethernet Identities`
- `iSCSI Identities`
- `FCoE Identities`
- `Fibre Channel (FC) Identities`

An Identity Pool may be thought of as a collection of one or more sub-pools—one for Ethernet, one for iSCSI, and so on. An Identity Pool only requires to include sub-pools which are applicable for its intended use. Identity information for each type of sub-pool is discussed in the later sections of this technical white paper.

3.3.1 Ethernet Identities

Ethernet identities refers to the configuration attributes that provide a unique virtual identity for Ethernet operations on a network. The Ethernet page of the Identity Pool wizard is used to define a sub-pool to use for generating unique Ethernet virtual identities. Because OpenManage Enterprise executes on an Ethernet network, most every Identity Pool will have to specify values for generating Ethernet virtual identities. The following values are specified to define a sub-pool for generating unique Ethernet virtual identities:

```
Starting Virtual MAC Address, Count
```

The Identity Pool wizard allows the entry of a starting Virtual MAC address and a pool size (that is, the number of MAC addresses in the pool, up to a maximum size of 5,000 addresses).

Note—A valid MAC address, using hexadecimal digits, must be supplied. The wizard has a tool tip which shows acceptable formats. The range cannot include any broadcast MAC addresses (that is, where the second digit in the first octet in the address is odd (1, 3, 5, 7, 9, B, or D)).

3.3.2 iSCSI Identities

iSCSI identities refers to the configuration attributes that provide a unique virtual identity for iSCSI operations on a network. The iSCSI page of the Identity Pool wizard is used to define a sub-pool to use for generating unique iSCSI virtual identities. iSCSI can be used for connection to iSCSI-based storage and/or for booting from an iSCSI-based repository. These activities may require virtual MAC addresses, a name, and/or IP addresses—a sub-pool can be specified for each of these. The following values are specified to define applicable sub-pools for generating an iSCSI virtual identity:

```
Starting Virtual MAC Address, Count
```

This pool functions the same as the Virtual MAC Address identities for Ethernet (and has the same value constraints), but is reserved for generating only iSCSI virtual identities. An iSCSI virtual MAC address is required whenever deploying a template in which iSCSI operations are enabled (either for an iSCSI connection or for iSCSI boot).

```
IQN Prefix
```

The IQN Prefix value is used when iSCSI is configured for booting. In this case, the target device needs to configure an iSCSI initiator, and the initiator requires a unique name for its virtual identity. The Identity Pool wizard accepts a prefix to use for generating unique iSCSI IQNs for the target device to use. When an iSCSI IQN is needed, it will add a unique string to the end of the specified prefix.

> The official IQN format is: `iqn.yyyy-mm.naming-authority:unique name`
>
> It is recommended that the specified IQN prefix at least begin with "`iqn.`" to avoid name rejection by a NIC. Think of OpenManage Enterprise as supplying "`unique name`".

It is a best practice to always specify an IQN Prefix when configuring an Identity Pool to include iSCSI MAC addresses. Although an IQN is only required when iSCSI boot is configured, it is likely that some templates that configure iSCSI will also require an iSCSI IQN. Therefore, it is best to just enter a prefix when the Identity Pool is defined. This prevents an error later in the Deploy Template wizard when an IQN is required but no prefix is specified in the Identity Pool.

Unlike other ranges (for MAC addresses and IP addresses), the iSCSI IQN is just a text name. It is not a limited resource. OpenManage Enterprise adds a seven-digit numerical suffix to the prefix specified in the wizard. Thus, every IQN pool can generate up to 10 million unique IQNs (minus one).

```
IP Address Range, Subnet Mask, Gateway, Primary DNS, Secondary DNS
```

These iSCSI Initiator IP settings are only used when iSCSI is configured for booting, and when iSCSI Initiator configuration via DHCP is disabled. When iSCSI Initiator configuration via DHCP is enabled, all of these values are obtained from a designated DHCP server.

The IP Address Range and Subnet Mask fields are used to specify a pool of IP addresses that OpenManage Enterprise can assign to a device for it to use in its iSCSI Initiator configuration. Unlike the MAC address pools, a count is not specified for the IP Address Range. Instead, the IP Address Range may be specified as a range of specific addresses (a starting address and an ending address) or as a subnet (using either CIDR notation or the Subnet Mask field). A maximum of 64,000 IP addresses are allowed in a pool.

The Identity Pool wizard in OpenManage Enterprise 3.0 supports only IPv4 address ranges. The following range formats are allowed:

- `startIP-endIP`
  The wizard is picky; it doesn't allow any spaces around the dash!
  This format requires a Subnet Mask to be selected.
- `subnet/CIDR`
  No Subnet Mask is applicable with this format.
- `subnet`
  This format requires a Subnet Mask to be selected.

Gateway, Primary DNS, and Secondary DNS are neither identity values nor used as a pool. They don't have to be unique on the network (and usually aren't unique), but they do serve a couple of purposes related to identity management. Therefore, they are included on the iSCSI page in the wizard:

- When specified, OpenManage Enterprise uses these values when deploying a template (rather than using the values originally contained in the template).
- When specified, OpenManage Enterprise will not assign those values from the IP address pool (if they fall within the specified IP address range). That is, they serve as exclusions from the specified IP address range (when applicable).

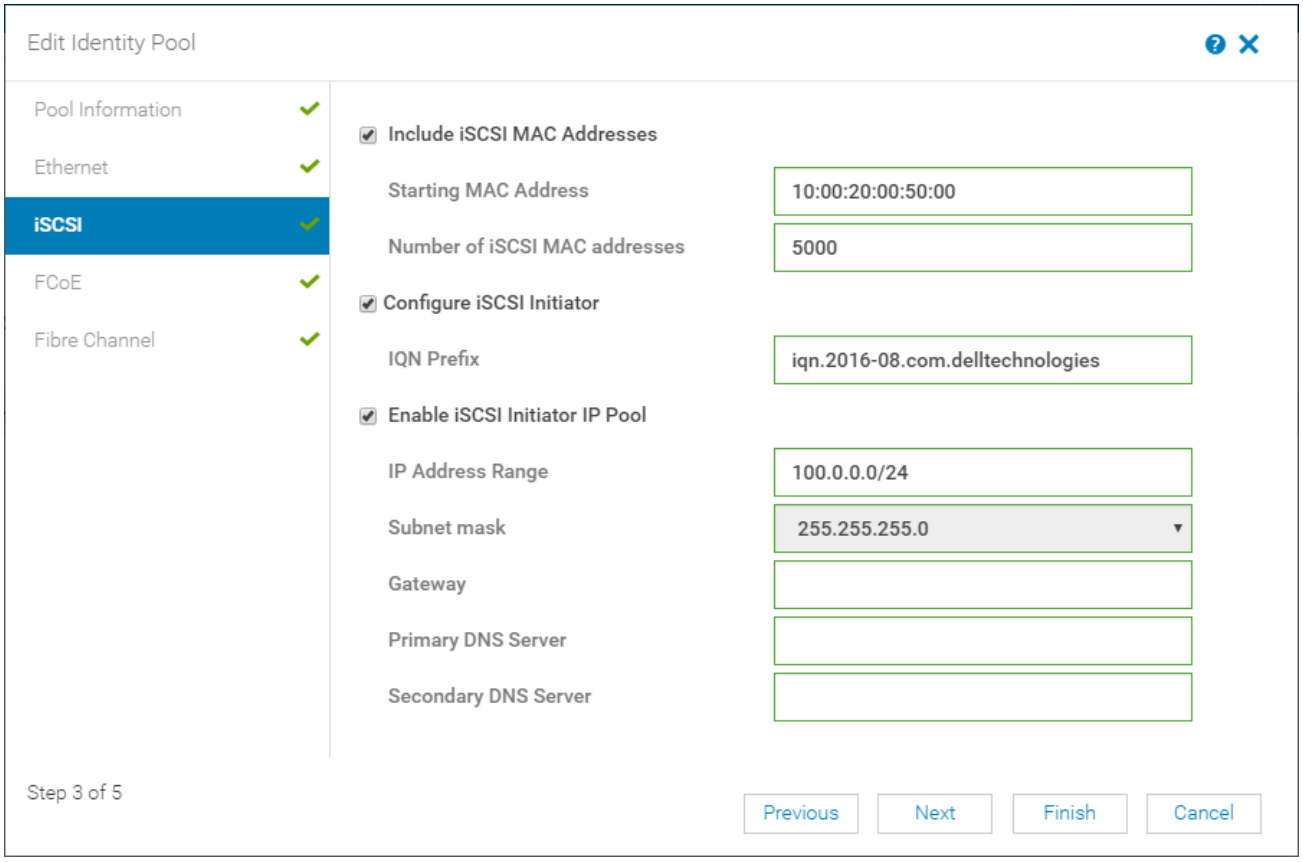

Figure 6 Identity pool wizard iSCSI section

3.3.3 FCoE Identities

FCoE identities refers to the configuration attributes that provide a unique virtual identity for FCoE operations on a network. The FCoE page of the Identity Pool wizard is used to define a sub-pool to use for generating unique FCoE virtual identities. The generated identities are used for booting from an FCoE-based repository. The following values are specified to define a sub-pool for generating unique FCoE virtual identities:

- `Starting Virtual MAC Address, Count`

  This pool functions the same as the Virtual MAC Address identities for Ethernet (and has the same value constraints), but is reserved for FCoE identities only. An FCoE virtual MAC address is required whenever deploying a template in which FCoE operations are enabled.

FCoE provides Fibre Channel support on an Ethernet network. The endpoints use Fibre Channel addressing, but data packets (containing FC payloads) traverse an Ethernet network. Therefore, FCoE requires both virtual MAC addresses, for sending packets on the Ethernet network, and virtual FC addresses (that is, virtual WWNN and virtual WWPN values), for Fibre Channel operations by the endpoints.

OpenManage Enterprise generates all necessary FCoE virtual identities using the FCoE Virtual MAC Address range specified for a pool. It can do this because MAC addresses are 6-octet values and FC addresses are 8-octet values. OpenManage Enterprise uses the FCoE Virtual MAC Address range to generate unique MAC virtual addresses for the Ethernet virtual identity. It also uses that range to generate unique virtual WWNN

and virtual WWPN addresses for the FC virtual identity. It does this by prepending a two-octet prefix to each possible address in the MAC address range (0x2000 for virtual WWNN addresses and 0x2001 for virtual WWPN addresses). As a result, customers do not have to specify address pools for FC virtual WWNN and WWPN addresses.

3.3.4 Fibre Channel (FC) Identities

FC identities are virtual identities required by a device to support virtual FC operations. The FC page of the Identity Pool wizard is used to define a sub-pool to use for generating unique FC virtual identities. The following values are specified to define a sub-pool for generating unique FC virtual identities:

- Starting Postfix and Count

As mentioned earlier, Fibre Channel requires 8-octet virtual WWNN addresses (for nodes) and virtual WWPN addresses (for ports on a node). In OpenManage Enterprise, the Identity Pool wizard page for defining an FC virtual identity pool has a starting postfix value, which takes a 6-octet value, and a count. Like it does for generating unique FC virtual WWNN and WWPN addresses for FCoE (as discussed above), OpenManage Enterprise prepends a two-octet prefix to each 6-octet value defined by the Postfix and Count values entered for a pool. The same prefixes are used as were indicated for FCoE.

Note that the Starting Postfix value is NOT a MAC address, even though it happens to be a 6-octet value. It is merely a 6-octet value; OpenManage Enterprise prepends two prefix octets, as mentioned above, in order to generate valid 8-octet FC WWNN and WWPN addresses. This approach means that the customer only has to specify one range (from which OpenManage Enterprise will generate values as if there were two FC address pools).

3.3.5 Address constraints

Identity addresses within and across Identity Pools cannot overlap. For example:

- The MAC addresses that can be generated by sub-pools for Ethernet, iSCSI, and FCoE cannot overlap with each other, either within one pool or in different Identity Pools.

- The FC addresses that can be generated by sub-pools for FC and FCoE cannot overlap with each other, either within one pool or in different Identity Pools. Both FCoE sub-pools and FC sub-pools generate FC virtual WWNN and WWPN addresses which could conflict with each other.

In each case, the Identity Pool wizard will report an error if it finds an address overlap within a pool or between pools. Note that since FCoE pools generate both virtual MAC addresses and virtual FC addresses (virtual WWNN and virtual WWPN), they have two possibilities for range conflict, both within or across Identity Pools.

3.4 Identity Pool operations

- This section discusses the functionalities provided by OpenManage Enterprise for managing Identity Pools.
- Identity Pools are created and managed via the Identity Pool portal. This page displays a list of identity pools, provides buttons for creating and managing identity pools, and identity pool summary and usage information.
- The Identity Pool portal page lists the current set of Identity Pools.
- If a single Identity Pool is selected, summary and usage information is displayed for it at the bottom of the page, and it can be edited, exported, or deleted.

- If multiple Identity Pools are selected, Delete is the only operation allowed.

3.4.1 Create Identity Pool

The Create Identity Pool wizard is used to create a new Identity Pool. Click **Create** on the **Identity Pools** portal page (**Configuration → Identity Pools**). Each Identity Pool must have a unique name and may specify sub-pools for Ethernet identities, iSCSI identities, FCoE identities, and/or FC identities as necessary. An Identity Pool can even be created without any sub-pools. It wouldn't be usable for deployment, but could be edited later to include sub-pool definitions.

See the Identity Pools in OpenManage Enterprise section for details about the different types of identities and sub-pools that can be configured for an Identity Pool.

It is important to remember that because a template can be associated with at most one Identity Pool, that Identity Pool must define sub-pools for all protocols which templates associated with the pool may need. Most templates will need Ethernet MAC addresses for virtual Ethernet identity, so a sub-pool for Ethernet MAC addresses will usually be required. Remember also that each port on each NIC may need a virtual Ethernet MAC address, so plan the pool size accordingly.

Other than that, each installation will need to determine whether or not their devices will require virtual identities for iSCSI, FCoE, or FC, and configure sub-pools accordingly.

3.4.2 Modify Identity Pool

The Edit Identity Pool wizard is used to view or make changes to previously-created Identity Pools. Click **Edit** on the **Identity Pools** portal page (**Configuration → Identity Pools**) This wizard is the same as the **Create Identity Pool** wizard, except that a couple constraints may apply to sub-pool definitions.

If an Identity Pool has either Reserved or Assigned virtual identities, then the following restrictions apply to sub-pools already defined for the Identity Pool:

- For all sub-pools that generate MAC address virtual identities (Ethernet, iSCSI, and FCoE), if the Identity Pool defines a sub-pool for the protocol, and that sub-pool contains Reserved or Assigned virtual identities, then the Starting MAC Address designated for that sub-pool cannot be changed and its Count can only be increased. This constraint is made so that Reserved and Assigned virtual identity values don ot drop out of an Identity Pool.

- An equivalent constraint applies to sub-pools that generate FC address virtual identities (FCoE and FC). Here too, if the sub-pool contains Reserved or Assigned identities then the Starting Address cannot be changed, and the Count can only be increased.

3.4.3 Review Identity Pool Summary and Usage

This section of the page displays summary information for the last Identity Pool that was selected (or unselected) in the Identity Pool list (even if it is no longer selected). This is essentially the same information that is displayed if the Identity Pool is opened for editing.

This section of the page displays usage information for the last Identity Pool that was selected (or unselected) in the Identity Pool list (even if it is no longer selected). Usage information can be displayed for Ethernet identities, iSCSI identities, FCoE identities, or Fibre Channel (FC) identities. For the selected identity type, the display shows the number of identities in the pool, the number of identities that are in use, and a list

containing each Reserved or Assigned identity (available identities are not displayed). See the Identity States in OpenManage Enterprise section for more info about identity states and their meanings.

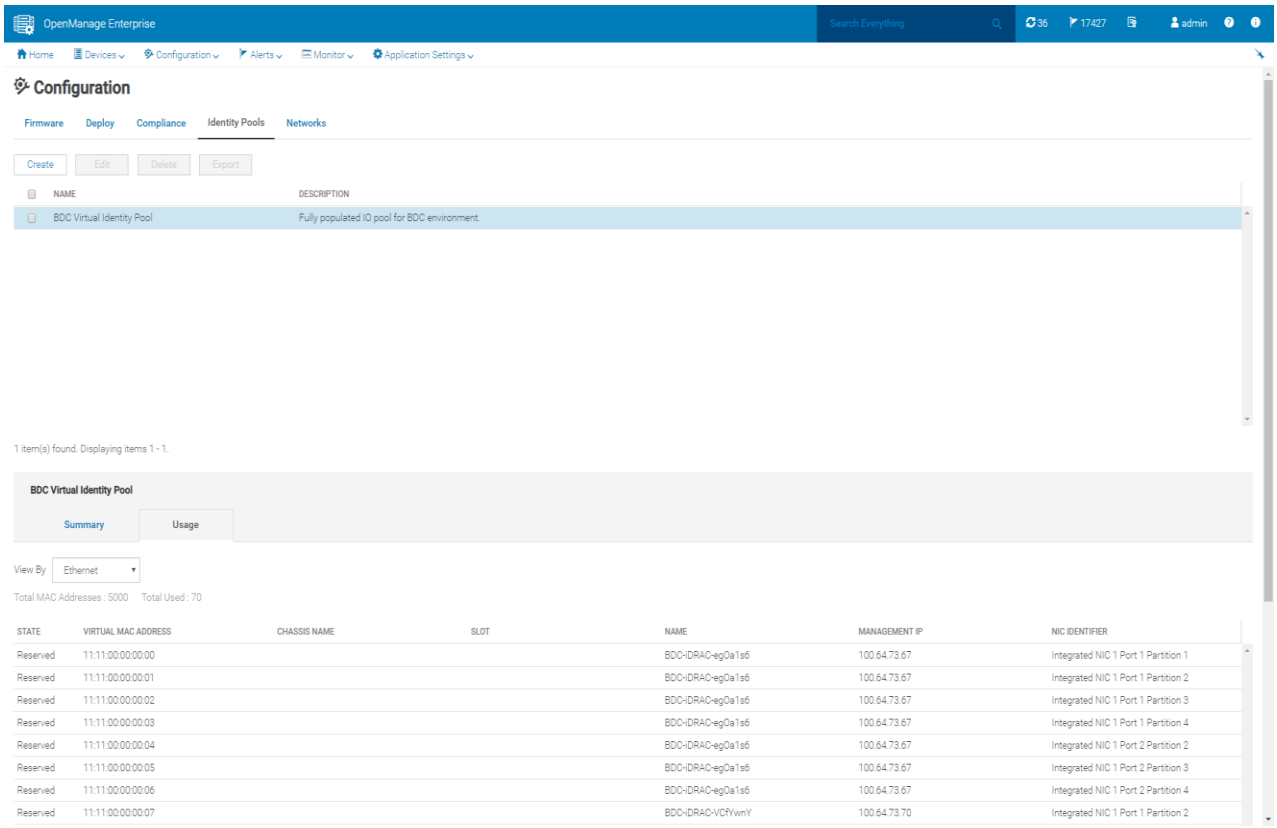

Figure 7 Identify Pool usage

3.4.4 Delete Identity Pool

This operation deletes one or more identity pools. Identity Pools where one or more sub-pools contain Reserved or Assigned virtual identity values cannot be deleted.

3.4.5 Export Identity Pool

The Identity Pool portal also provides the ability to export an Identity Pool definition (including all sub-pool definitions) to a CSV file.

3.5 Identity Pool Planning and Strategy

OpenManage Enterprise supports the creation of multiple Identity Pools. Here are some things to consider when deciding whether to create a single Identity Pool for all template deployments to use, or to create different Identity Pools for different purposes.

- An Identity Pool does not need to specify a sub-pool for each different protocol. However, a template can be associated with at most one Identity Pool, so identities for all protocols enabled in a template need to come from the Identity Pool associated with the template. Else, the Assign Identities step in the Deploy Template wizard will fail.

- Identity range addresses specified in one Identity Pool cannot overlap identity range addresses in another Identity Pool (or even in the same Identity Pool), irrespective of protocol.

- This rule applies based on address type. For example, MAC addresses. MAC address ranges are specified for Ethernet identities, iSCSI Initiator identities, and FCoE identities. A MAC address range in one Identity Pool (regardless of the protocol) cannot overlap with any other MAC address range, either in the same Identity Pool or in a different Identity Pool.

- When any identities in a sub-pool of an Identity Pool are Reserved or Assigned, the only change allowed to those sub-pools is to increase their size. The starting address cannot be changed and the count cannot be reduced.

Each Identity Pool definition should include a sub-pool for each type of virtual identity expected to be enabled in the Templates with which the Identity Pool will be associated.

- Most Identity Pools will need an Ethernet sub-pool, for use as virtual MAC addresses for network communications. Each NIC port usually requires a virtual MAC address. If partitioning is enabled, each partition could require a virtual MAC address (unless Ethernet is disabled on the partition).

- If an Identity Pool will be associated with templates where iSCSI could be enabled, either for connections or for booting, then an iSCSI identity range for MAC addresses should be specified. If iSCSI may be enabled for booting, then an IQN prefix and an IP range should also be specified (unless it is known for certain that every template to be used for deployment will specify that iSCSI Initiator settings be obtained from a DHCP server).

- If an Identity Pool will be associated with templates where FCoE could be enabled, then an FCoE identity range should be specified.

- If an Identity Pool will be associated with templates that may have Fibre Channel host bus adapter, then a range should be specified for Fibre Channel (FC) identities.

Each installation should determine the number of identity pools, sub-pools per Identity Pool, and sub-pool sizes that best fit their needs.

4 VLAN-based networks

4.1 VLAN-based network structure and usage

VLAN-Based Networks refers to individual VLANs and/or VLAN ranges used for a specific purpose. These networks are configured via the Networks tab on the Configuration page. VLAN-Based Networks are used when specifying network settings for Templates.

4.2 VLAN-based network operations

4.2.1 Create VLAN-based network

The following information may be specified for each VLAN-Based Network:

Name—A unique name for the network.

Description—An optional description of the network.

VLAN ID—The VLAN, or range of VLANs, to use for the network. A VLAN ID can apply to at most one VLAN-based Network. An error is displayed is VLAN IDs in different VLAN-Based Networks overlap. On the Template Network Settings page, Networks that have one VLAN can be selected for either tagged or untagged networks; Networks that specify a VLAN range can only be selected in tagged networks. See the “Setup Idenitty Pool and Network Settings” section for additional details.

Network Type—The intended purpose of the network. Possible values are as follows:

```
General Purpose (Bronze)
General Purpose (Silver)
General Purpose (Gold)
General Purpose (Platinum)
Cluster Interconnect
Hypervisor Management
Storage – iSCSI
Storage – FCoE
Storage – Data Replication
VM Migration
VMware FT Logging
```

4.2.2 Modify VLAN-Based Network

If the VLAN ID field for a VLAN-Based Network is changed, it can affect Template network settings.

- If VLAN ID is changed from a single value to a different single value, it will change the VLAN used by any templates which include that network.
- If VLAN ID is changed from a single value to a range, that Network will be dropped from Untagged Network entries in applicable templates.

4.2.3 Export VLAN-Based Network

This operation creates a CSV-format file containing the network info (excluding the Network Type).

4.2.4 Delete VLAN-Based Network

This operation deletes one or more VLAN-based Networks. Note that doing this may affect template configurations where that network is specified. A warning is displayed to indicate that this will happen, but there’s no easy way to see which templates will be affected. The deleted networks are just dropped from the network settings information of the affected templates.

5 Troubleshoot templates and Identify Pools in OpenManage Enterprise

This section lists a few things that you can check when any issues are run into when working with Templates and Identity Pools.

- The OpenManage Enterprise appliance has a built-in CIFS share and uses SMB 2 as the minimum default version. Some earlier iDRAC firmware versions are unable to access the CIFS share. If template extraction fails with an “Unable to access share” error, you can try to extract the template again, after setting the SMB version to 1.
- While assigning identities, it is possible that the pool does not contain the required number of identities or the right kind of identities. In this case, the you must edit the Identity Pool and expand it appropriately, or add the right type of identities.
- OpenManage Enterprise has a TUI (Text User Interface) from which the log levels of the services can be changed to “Debug”. You can then restart services from the TUI. After this is done, repeating any failing operation causes detailed debug logs to be generated, and they can be exported by using the Monitor → Audit Logs → Export Console Logs feature. After logs for the erroneous situation have been collected, the user should remember to reset the log levels back and restart services.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Referenced or recommended Dell publications:

Deployment and Managing Configurations with Dell OpenManage Enterprise 3.0