DELL EMC

Technical Whitepaper

Deployment and Migration of Boot from SAN Configuration using Dell EMC OpenManage Enterprise version 3.3.1

Abstract

This technical whitepaper illustrates deployment of the boot from SAN configurations on servers and the migration of these deployed configurations to identical servers using OpenManage Enterprise.

March 2020

Revisions

Date	Description
March 10, 2020	Initial release

Acknowledgements

This paper was produced by the following:

Author: Sreejaya Thazhe Veedu

Support: Raghu Chozhan Viswanathan (InfoDev)

Table of contents

Executive summary

Configuring the newly added servers for a boot from SAN operation is often a repetitive and a time-consuming process in a data center.

Using Dell OpenManage Enterprise, the newly added systems can be configured easily to operate in a specific SAN protocol.

Dell OpenManage Enterprise optimizes this process for the following scenarios:

1. Configuration of servers to support Boot from SAN using iSCSI, FCoE or FC protocols.
2. Migration of workloads amongst identical servers in case of failures.

In this whitepaper, we describe the configuration of boot from SAN on a target server for the iSCSI and FC protocols using OpenManage Enterprise.

1 Boot from SAN operation using OpenManage Enterprise – basic requirements

The following requirements must be met to configure the newly added servers for a boot from SAN operation using OpenManage Enterprise:

- An active OpenManage Enterprise Advanced license is needed. For more information on OpenManage Licenses, see OpenmanageEnterprise Licensing Guide.
- For PowerEdge servers with iDRAC version lesser than 2.52.52.52, SMBv1 should be enabled in OpenManage Enterprise. For instructions on enabling SMBv1, refer the Openmanage Enterprise documentation

2 Configure boot from SAN operation using OpenManage Enterprise – overview

OpenManage Enterprise provisions the configuration of servers to support boot from SAN using iSCSI, FCoE or FC protocols using the ‘stateless’ computing concepts. It applies virtual identities like virtual iSCSI MAC address, user-defined iSCSI IQNs and iSCSI IP addresses. Similarly, in case of FCoE and FC protocols, OMEnterprise applies virtual identities such as FIP MAC address, virtual Worldwide Port Name to the target servers.

Virtual identities or user-defined identities are required to ensure that the LUNs on which the operating systems are installed are not physically attached or ‘tied’ to a target server. In the event of a server failure, these virtual identities can be quickly moved to another identical server with a minimal impact on operations.

OpenManage Enterprise uses the existing template deployment feature to accomplish the boot-from-SAN configurations on the target servers. Please refer the Deployment whitepaper for more details.

The following sections describe the configuration of Boot from SAN on a Target server for iSCSI and FC protocol using OMEnterprise.

3 Configure boot from SAN with the iSCSI protocol

The following steps are used to create an iSCSI SAN configuration.

Step 1: Create a base system.

A 'base system' is an existing server discovered in OME, which is already configured or is readied for a one-time boot from SAN configuration. The template derived from this system is treated as a 'golden' template and is used for deployment on the newly added servers.

Step 2: Capture template from the base system.

Step 3: Create and associate virtual identities to the template.

Step 4: Attach a Boot to Network ISO image for deployment.

Note: The ISO image can be customized to contain a ‘kickstart’ file so that the OS installation can go unattended.

Step 5: Deploy the template to the newly added servers.

3.1 Create a base system

System setup is an integral part of 'stateless' deployment. The CNA card of the base system must be configured to enable the iSCSI boot protocol which is essential for iSCSI boot from SAN. Disabling the **iSCSI parameters via DHCP** and **TCP/IP parameters via DHCP** allows OpenManage Enterprise to assign mandatory identities required for iSCSI boot.

Creation of a base system setup is a onetime manual task. This system setup must be done accurately as OpenManage Enterprise replicates this 'golden' configuration on equivalent devices and the success of further deployments depends on the accuracy of this configuration.

If the base system is not already setup for boot from SAN using iSCSI, follow the below mentioned configuration guidelines.

As an example, the base system is setup using the following hardware configuration:

- **Server used**: MX840c
- **CNA used**: QLogic QL41262HMKR.

Note: Different vendors have various methodologies to configure Boot from SAN. Refer to the vendor-specific documentation for more details.

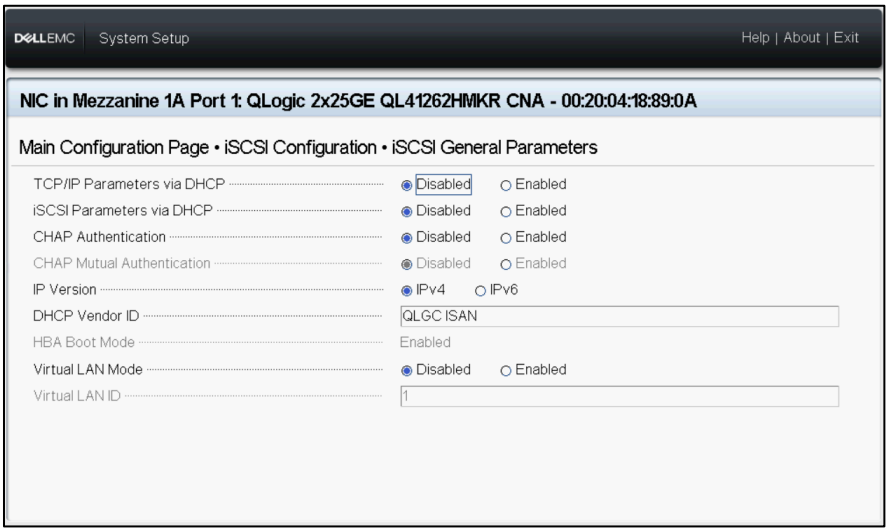
Note: Ensure that both the iSCSI initiator and the target are on the same network and can reach each other.

To configure the iSCSI boot parameters on the base system:

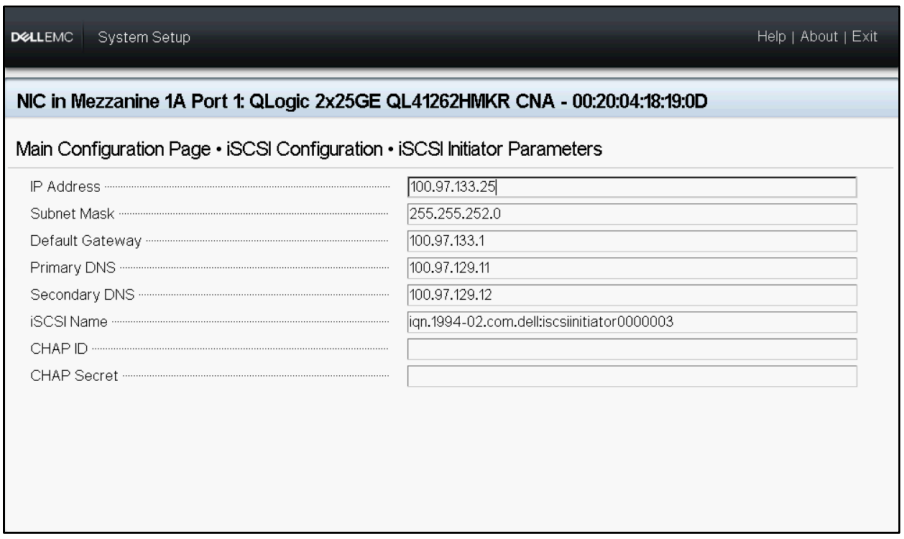
1. Configure Virtualization mode as NPAR under Device Level Configuration.

NPAR technology is implemented on modern Broadcom and QLogic CNAs which allows splitting a single physical NIC in to multiple NICs. Hence this configuration is vendor specific, see the documentation provided by the vendor for more details.

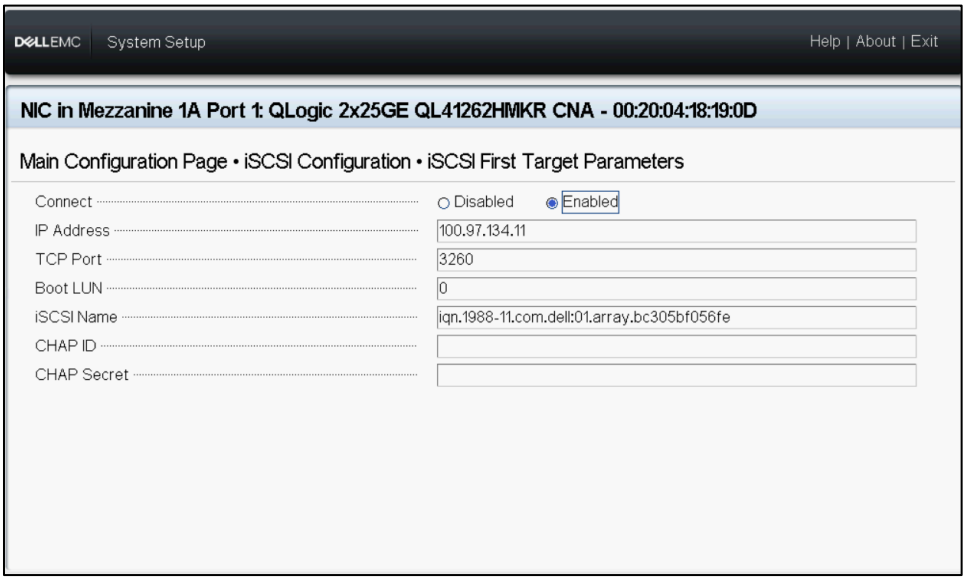
2. Set Boot Protocol as **UEFI iSCSI HBA** under **NIC Configuration**.
3. Enable **iSCSI Offload** mode under Partition 3 Configuration.
4. Set the iSCSI General Parameters for Static iSCSI Boot Configuration - Disable TCP/IP Parameters via DHCP and iSCSI Parameters via DHCP.



5. The iSCSI Initiator parameters contains the Initiator IP Address, iSCSI Name etc. These values are not assigned via DHCP, as the General parameters are set to static.



6. The iSCSI target parameters contain the Target IP address, Boot LUN, iSCSI Name etc. These values are not assigned via DHCP, as the General parameters are set to static.



7. Once the Initiator and Target iSCSI parameters are configured, the base system is then available for connection with the storage target LUN. However, this configuration uses the physical identities hardwired to the NIC card and the data is prone to loss in case of failure.

   OpenManage Enterprise, using ‘stateless’ computing, assigns virtual identities for each iSCSI parameters and ensures no identities are tied to the server.

3.2 Capture the base system template

In this step, a configuration template of the 'base' system is captured by OpenManage Enterprise. This template is used for setting up the target servers' system configuration after the necessary identity pool and target attributes required for booting from SAN are associated.

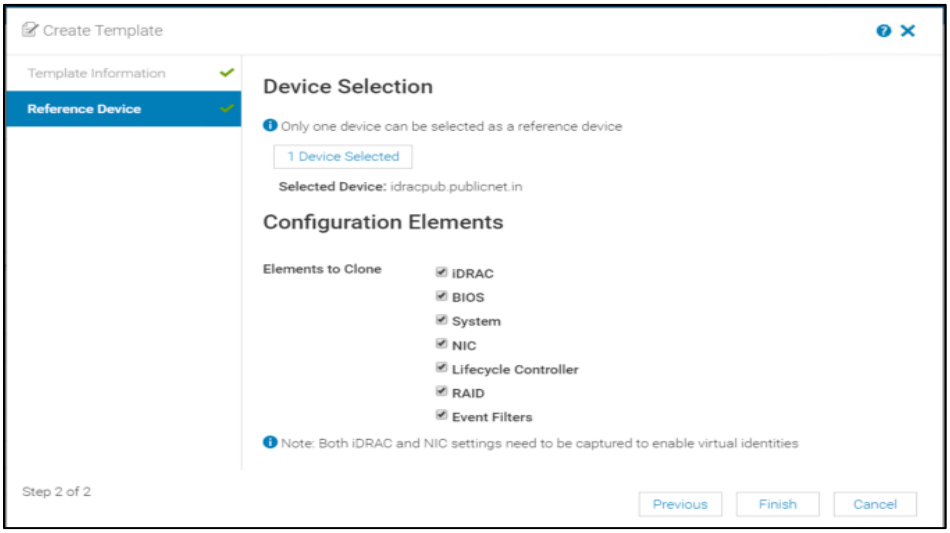
The below mentioned steps need to be followed for the capture the template of the base system:

1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Click **Create Template** and select **From Reference Device** to activate the Create Template wizard.
3. In the Template Information section enter a unique **Template Name**, add a **description** and for **Template Type** select the **Clone Reference Server** option. Click **Next**.
4. In the **Reference Device** section, click **Select Device** to select the device whose configuration properties must be used for creating the new template.

Note—Alternatively, you can select the target by entering the device name or service tag in the Advanced Filters dropdown.

---

5. In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. You can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.



6. Click **Finish**. A job is created. To view the progress and the execution history of the job, click the **Jobs** tab under **Monitor**, select the respective job, and click on the **View Details** on the right pane. Once the job is successfully completed, the 'base' system template is listed on the Deploy page (**Configuration** > **Deploy**).

3.3 Create an iSCSI-defined identity pool

An Identity Pool provides a collection of unique attribute values such as MAC Address, IP Address, WWPN, WWNN, and so on for Ethernet, iSCSI, FC, and FCoE. The physical hardwired identities are replaced by user defined initiator identities which help in keeping the data image of the LUN mobile and portable to another identical server in case of failure.

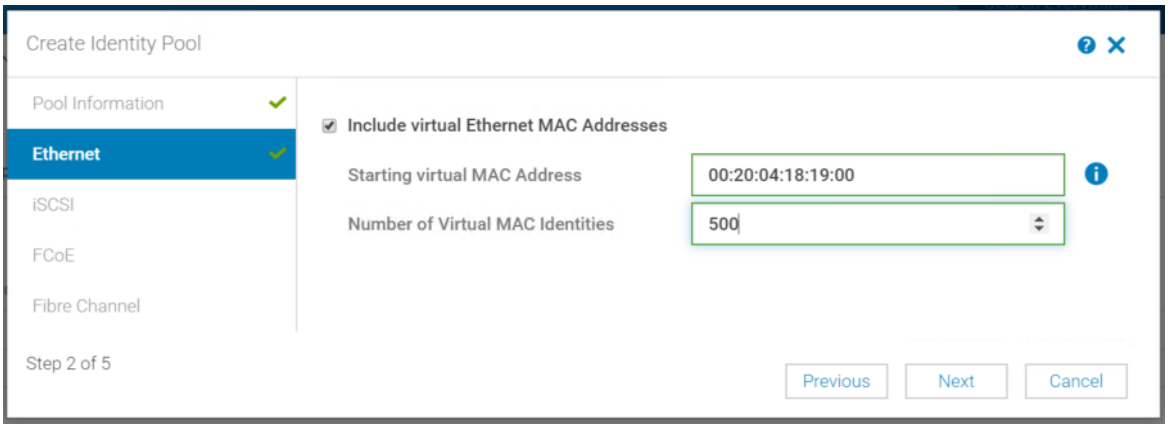
An iSCSI identity pool consists of the ethernet MAC address for the NIC port supporting ethernet functionality and the iSCSI MAC address for the NIC port/partition supporting the iSCSI boot protocol. Identity pool allows the user to provide the necessary attribute values required for iSCSI Boot from SAN.

OpenManage Enterprise allows the user to create an Identity pool with a range of identity attributes as desired, which is then automatically assigned to corresponding NICs during deployment.

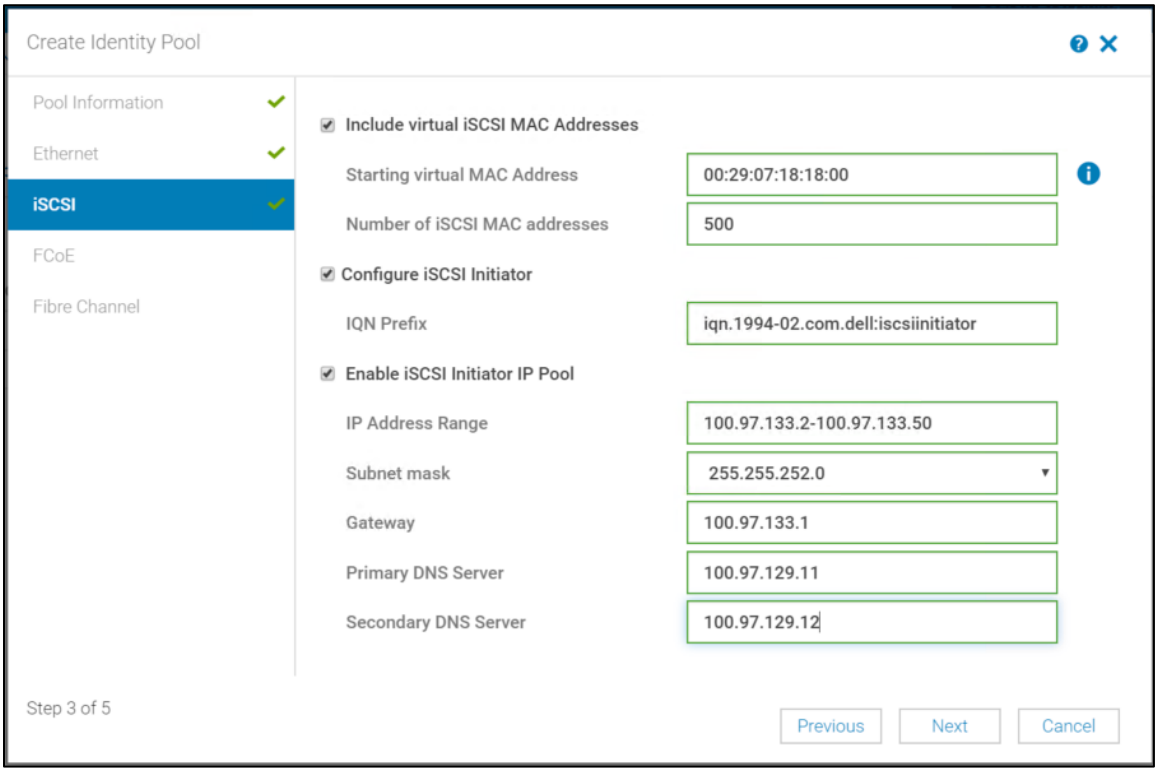
The below mentioned steps need to be followed to create an iSCSI-defined identity pool:

1. Go to the Identity Pools page by clicking **Configuration** > **Identity Pool**.
2. Click **Create** to activate the **Create Identity Pool** wizard.
3. On the Pool Information page, enter a unique P**ool Name** and **Description** (optional). Click **Next**.

4. On the **Ethernet** page of the wizard, select the **Include virtual Ethernet MAC Addresses** check box and enter a unique **Starting Virtual MAC address** and the range in **Number of virtual MAC Identities**. Click **Next**.



5. On the iSCSI page, Select the **Include virtual iSCSI MAC Addresses** check box and enter a unique **Starting Virtual MAC address** and a range for **Number of iSCSI MAC addresses**. Select the **Configure iSCSI Initiator** to enter the **IQN Prefix** and enable the **iSCSI Initiator IP Pool** check box and enter the range of **iSCSI initiator IP Pool** details.



6. Click **Next** and **Finish** to complete the identity pool creation. The Identity pool summary gives the details of the added Identity attributes.

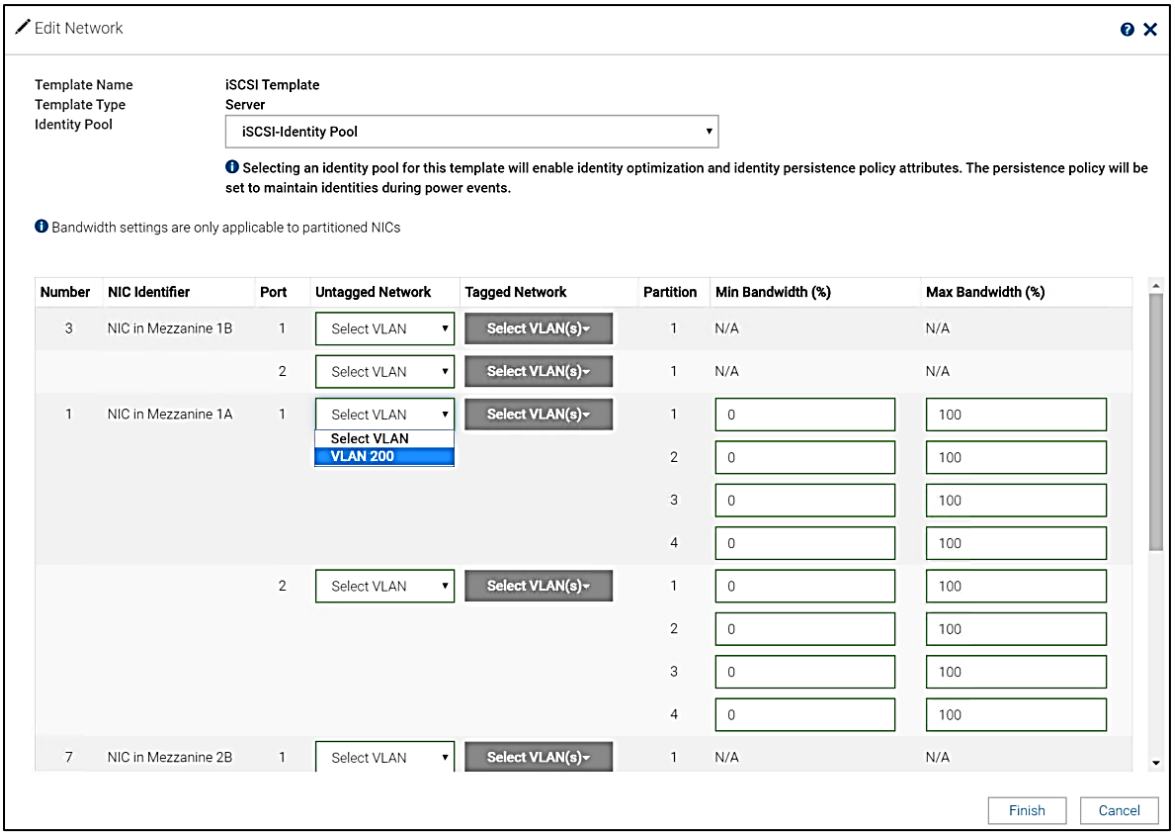
3.4 Associate the iSCSI-defined identity pool with the captured base system template

Identity pool association is a critical step in the 'stateless' deployment. In this step, the base system template is linked with the iSCSI identity pool, which would be applied to the target servers' NIC ports during deployment. Link establishment to SAN target using virtual identities keeps the data image of the LUN mobile and portable to another identical server in case of failure.

Note: Post deployment, the associated Identity pool is attached to the Server Template and cannot be modified.

The below mentioned steps must be followed to associate an identity pool to a template.

1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Select the base system template and click **Edit Network**.
3. Select the iSCSI Identity pool from the **Identity pool** dropdown.



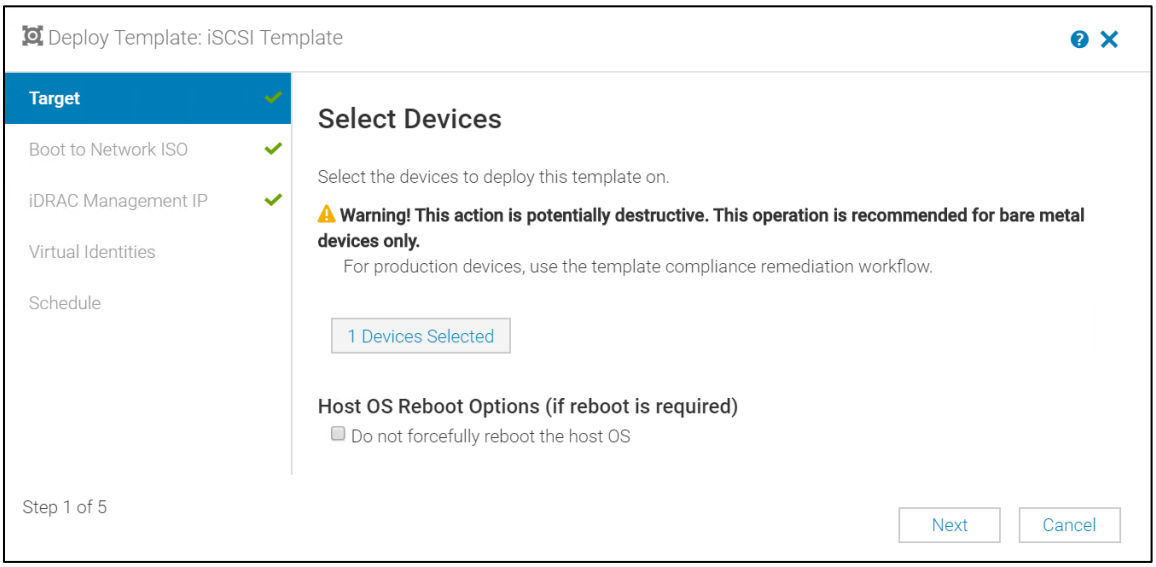
4. Click **Finish** to associate the iSCSI identity pool with the base system template.

3.5 Deploy the base system template

Deploying templates is the process of applying configuration settings to remote devices. In this step the captured base system template along with the associated Identity pool is deployed on the selected identical targets. The user can reserve the identities for the deployment and provide SAN boot target attribute values required to connect to the storage array.

Once the template is deployed, the target servers can be associated with the storage array and boot to the specified LUN successfully. The following steps need to be followed for deployment of a template on identical target devices:

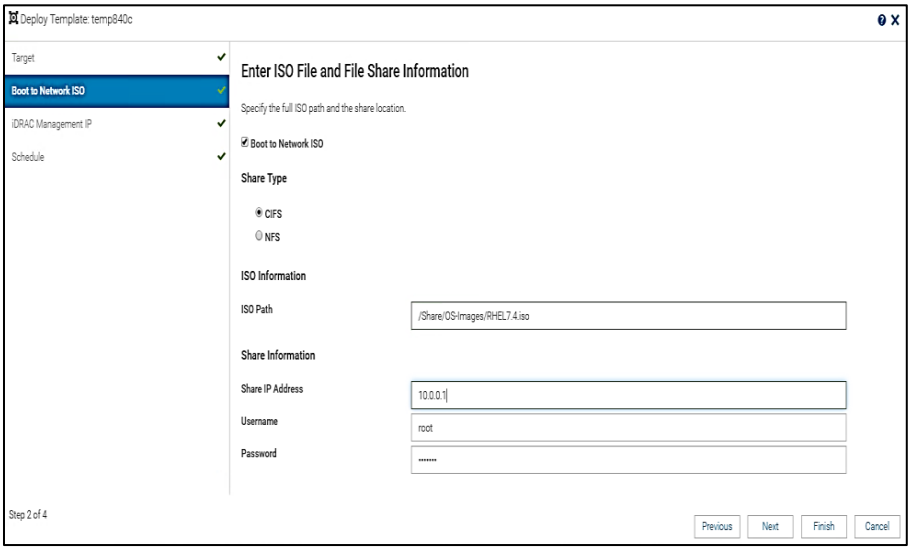
1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Select the created 'base' system template from the list and click on **Deploy Template** to activate the Deploy Template wizard.



3. Select one or more identical target devices on the Target page. Click **Next**.

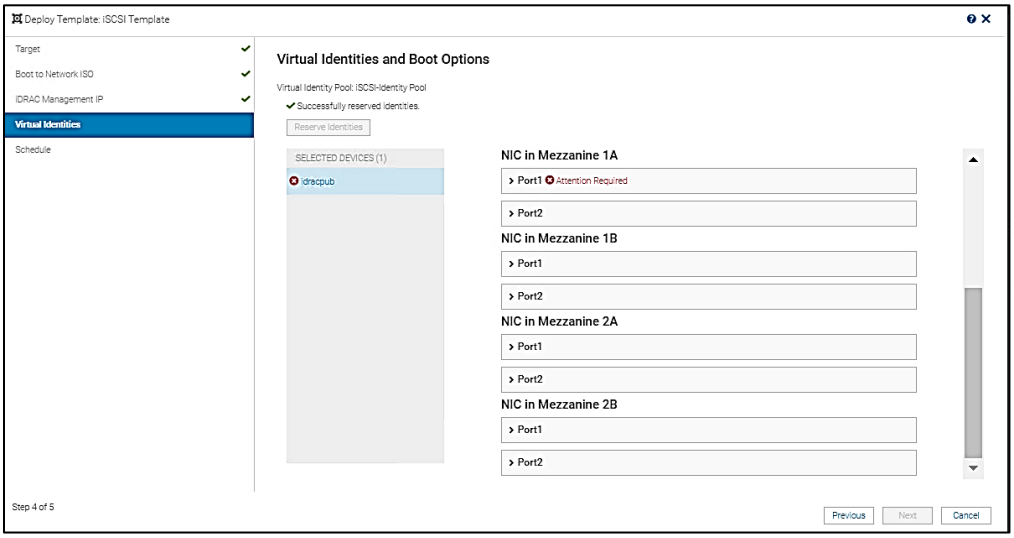
4. The **Boot to Network ISO** page allows you to install the specified OS post deployment.

    a. Select the Share type as CIFS/ NFS.
    b. Provide the path to the OS image in the ISO path input box in “/OS-Images/OS-file.iso” format.
    c. Provide the Share IP address and Credentials that can be accessed from OM Enterprise console.



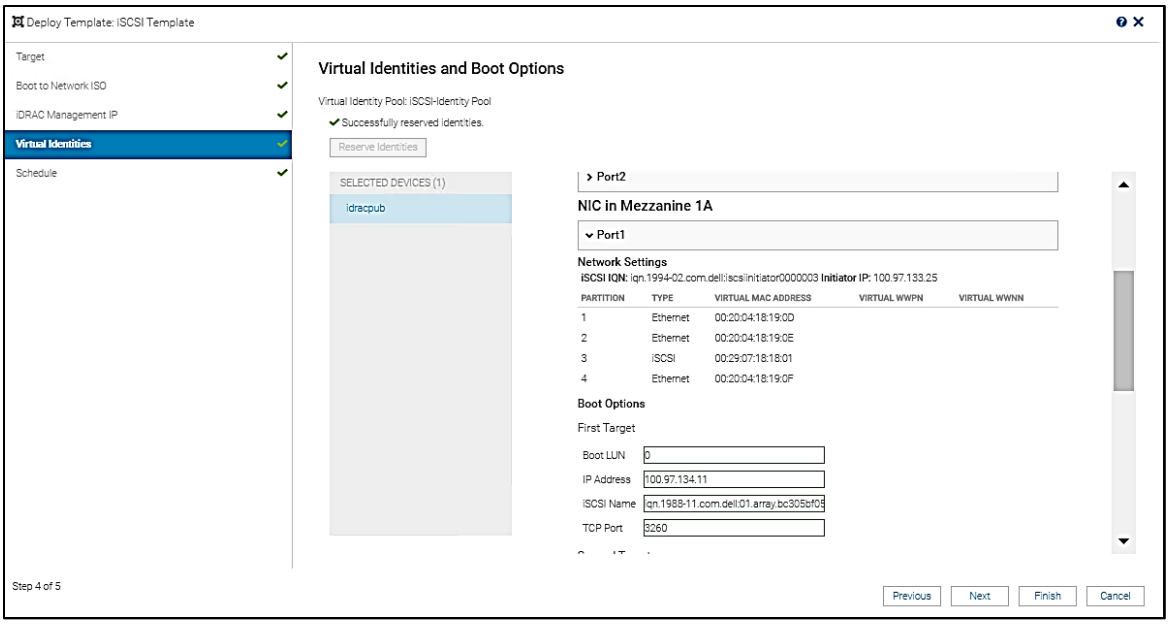
Note: Providing Boot to Network ISO is optional if the Storage LUN already has an Operating System installed.

5. Click **Next.** On the **Virtual Identities** page, click on **Reserve Identities**. The associated identities are reserved for each port of the NIC.



An ‘**Attention required**’ note is displayed against the port to which the target attributes should be added. Provide the **Storage array iSCSI Name**, **Boot LUN ID**, **Storage Controller iSCSI IP address**, and **TCP port number**.

Note: The target value should be provided only if the iSCSI parameters via DHCP was set as static in System setup.



With the completion of reserve identities, all the iSCSI supported NIC ports are intended to be auto assigned with virtual iSCSI MAC address, IQN and IP address. User can manually enter the first and second storage target array details.

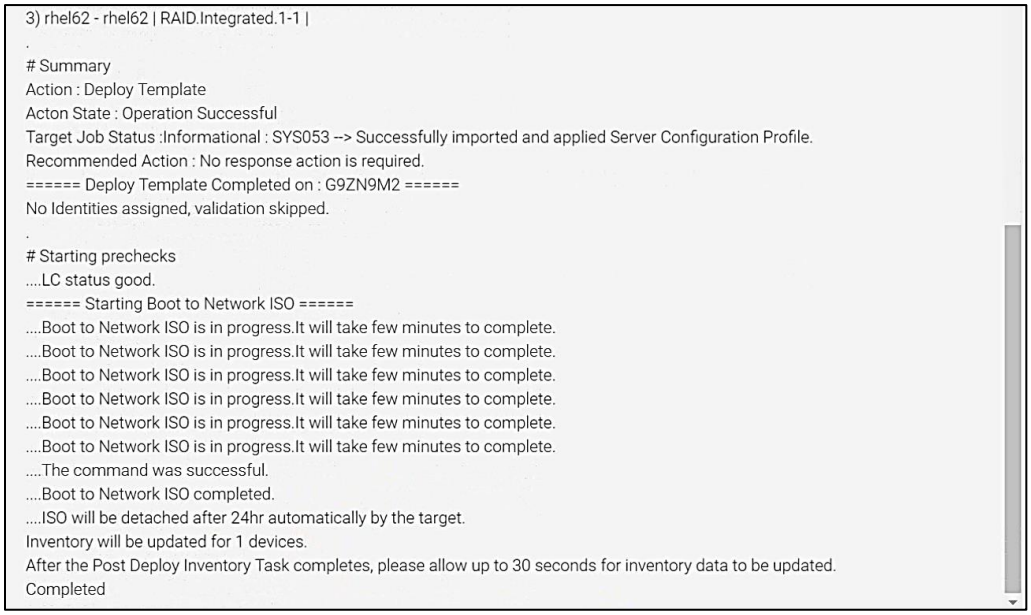
6. On the Schedule page, select the option **Run Now** to run the deployment job immediately or select a convenient date and time to schedule the deployment.

Note: After the completion of deployment job, the physical identities of the target server/s such as iSCSI MAC address, IP address, IQNs are replaced by the reserved virtual identities from the Identity pool.

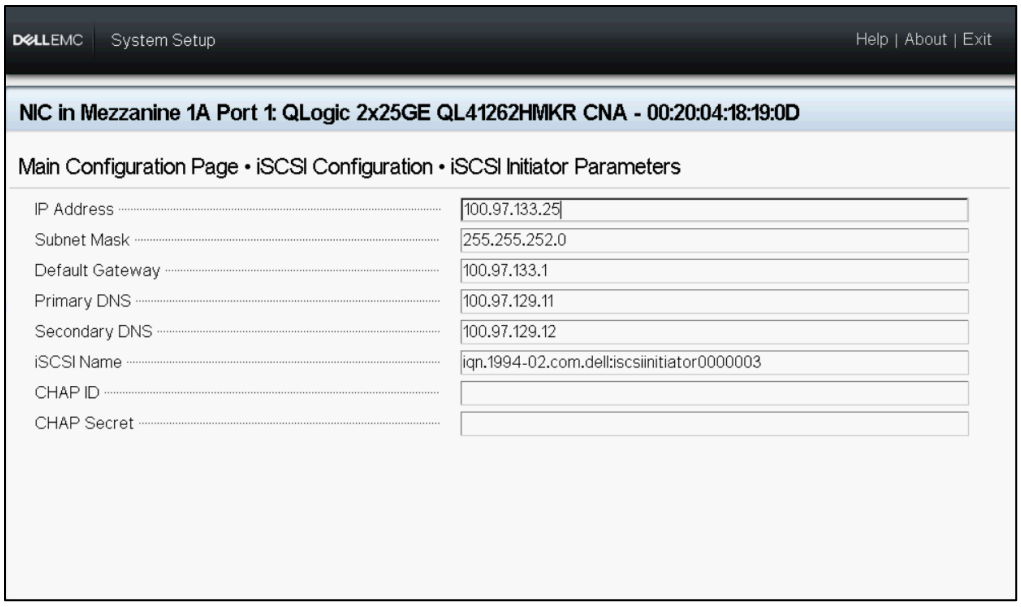
The benefit of the virtual Identities is to ensure that the LUN on which the Operating systems are installed is not physically attached or 'tied' to a target server. In case of failure, these virtual Identities can be moved to another identical server with a minimal impact on operations.

3.6 Boot to SAN via iSCSI

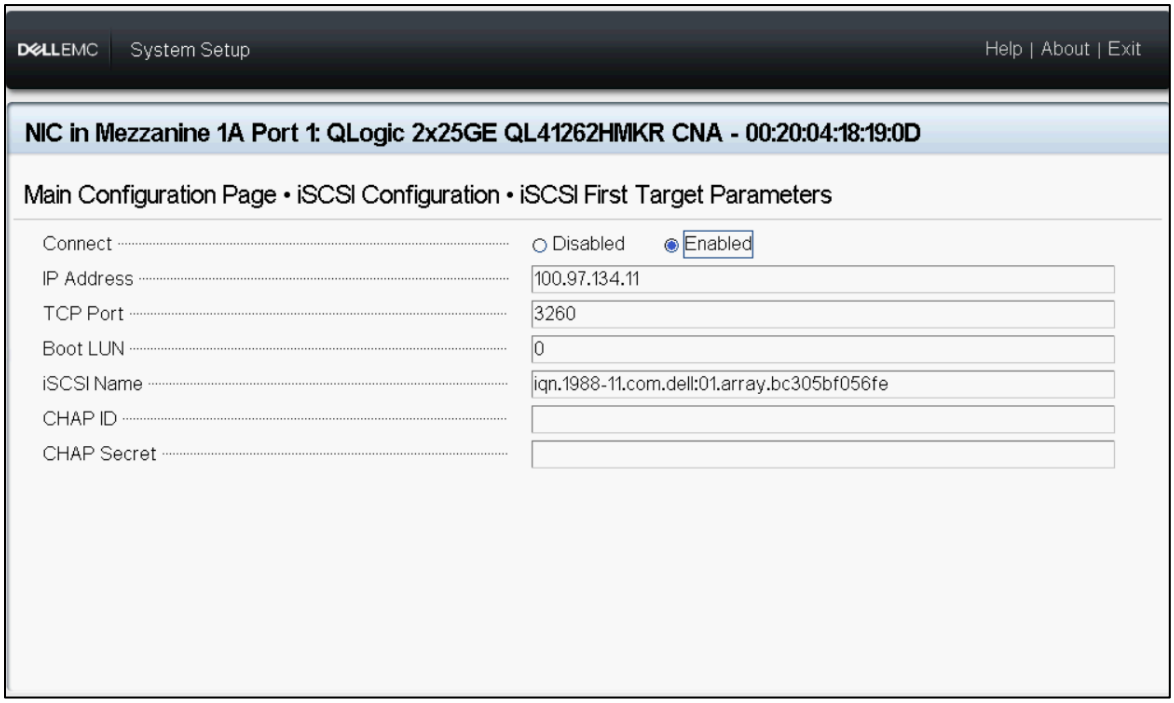
After a successful deployment of the base system template, the 'initiator' parameters from the identity pool are associated to the target server ports making them ready for an iSCSI boot from the associated ISO image. The progress of the Deployment job is displayed on the Task Execution page as shown below.



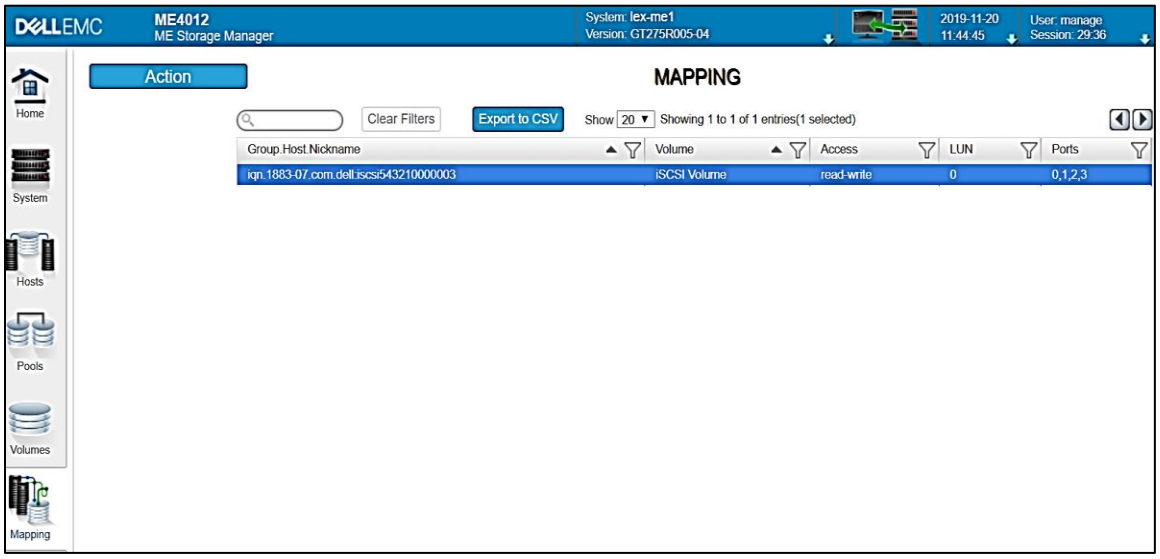
The iSCSI Initiator parameters such as the IP address and iSCSI Name, that had 0.0.0.0 values prior to deployment, are successfully associated with the attribute values from identity pool assignments after the base template deployment to be efficiently connected to the storage array.



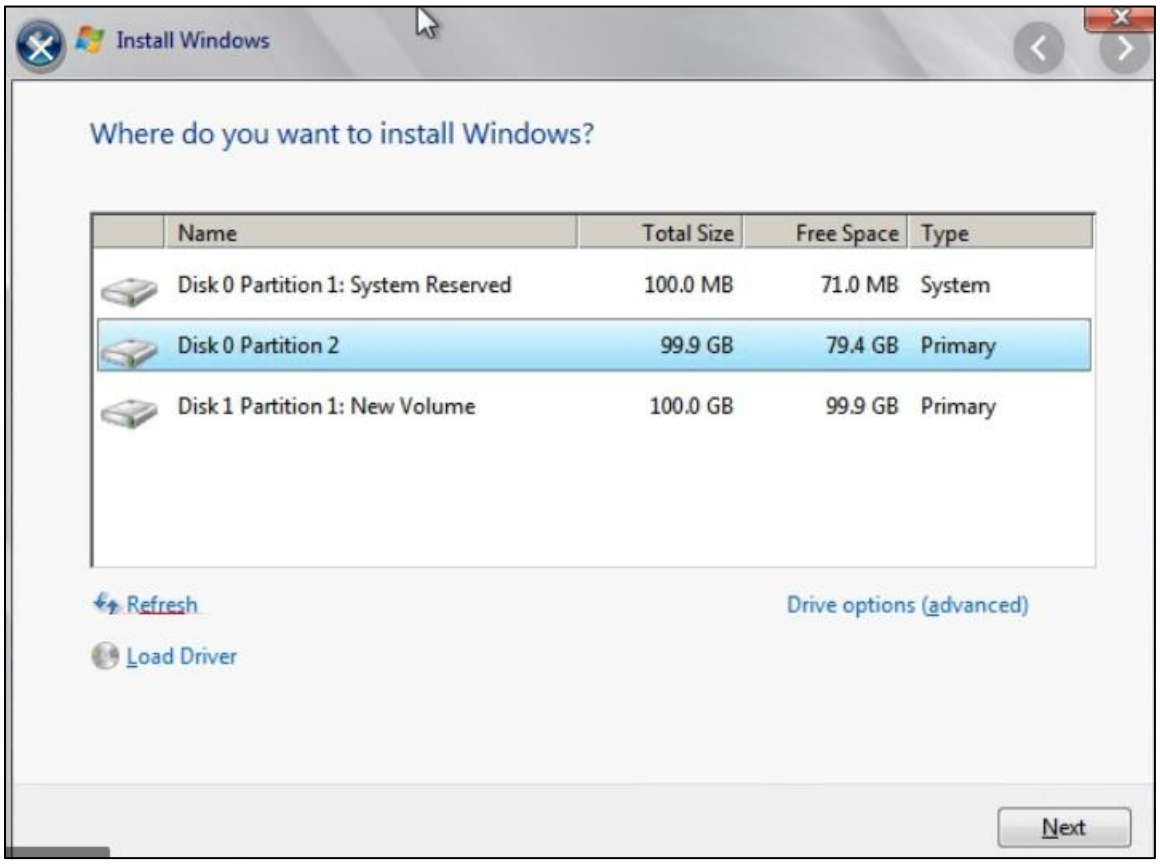
Similarly, the iSCSI target parameters such as the IP address and iSCSI Name, that had 0.0.0.0 values prior to deployment, are also successfully associated with the attribute values from identity pool assignments to be efficiently connected to the Initiator.



The Host is successfully discovered in the storage array and the volume with specified LUN ID is mapped to the host.



Server boots into the OS and the LUN is visible for installation.



4 Configuring servers for boot from SAN with FC Protocol

The following steps are used to create an FC SAN configuration.

Step 1: Create a base system.

A 'base system' is an existing server discovered in OME, which is already configured or is readied for a one-time boot from SAN configuration. The template derived from this system is treated as a 'golden' template and is used for deployment on the newly added servers.

Step 2: Capture template from the base system.

Step 3: Create and associate virtual identities to the template.

Step 4: Attach a Boot to Network ISO image for deployment.

Note: The ISO image can be customized to contain a ‘kickstart’ file so that the OS installation can go unattended.

Step 5: Deploy the template to the newly added servers.

4.1 Creation of a base system for a boot to SAN on the FC protocol

System setup is an integral part of 'stateless' deployment and is a onetime manual task. As OpenManage Enterprise replicates this 'golden' configuration on equivalent devices, the success of further deployments depends on the accuracy of this configuration.

If the base system is not already setup for boot from SAN using FC, follow the below mentioned configuration guidelines.

As an example, setting up the base system using the following hardware configuration:

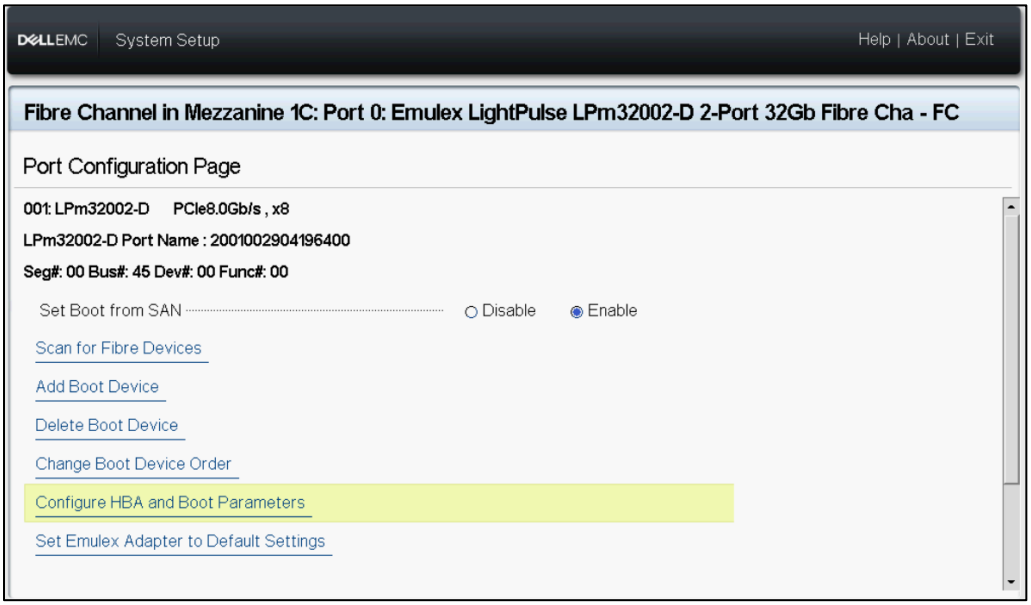
- **Server** used: MX840c
- **FC card** used: Emulex LightPulse LPm32002-D

Note: Different vendors have various methodologies to configure Boot from SAN. See the documentation provided by the vendor for more details.

Follow the below mentioned steps to configure the FC Boot parameters of the base system:

1. Enable the **Set Boot from SAN** on all the FC ports.

Note: The storage target WWPN is entered, and the Fiber devices are scanned manually. However, this section will be later automated by OpenManage Enterprise in deployment process.



2. Once the FC Target parameters are provided, the base system is now available for connection with the Storage Target LUN. However, this configuration uses the physical identities hardwired to the FC card, the data is prone to loss in case of failure.

OpenManage Enterprise uses ‘stateless’ computing to assign virtual identities for each FC Ports and ensures no identities are tied to the base system server

4.2 Capture the base system template

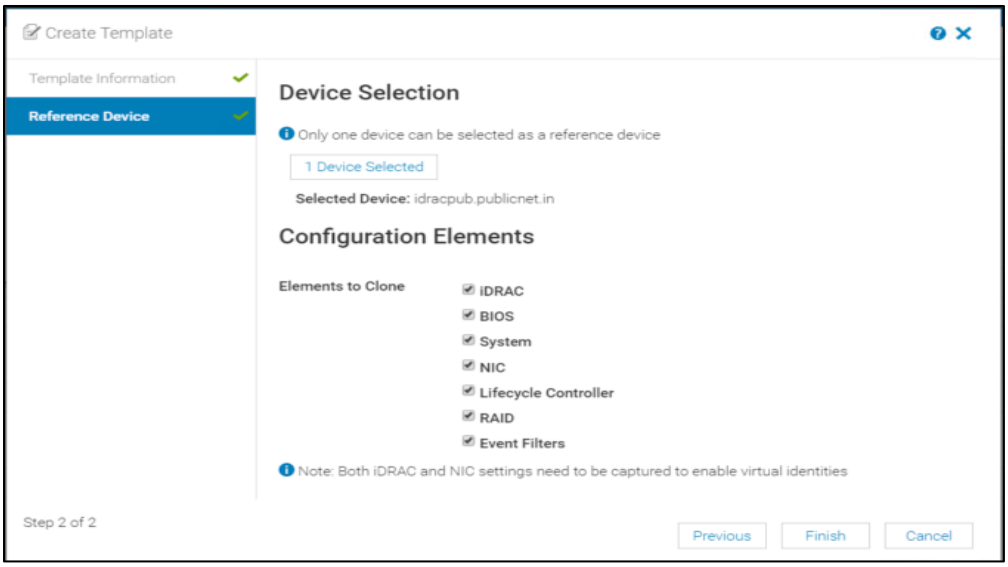
A template of the base system, which is specifically designated for use as prototype for setting up system configuration, is captured in OpenManage Enterprise. Using this 'golden' template, OpenManage Enterprise can associate the identity pool and target attributes required for booting from SAN on the target systems.

The below mentioned steps need to be followed for the capture the template of the base system:

1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Click **Create Template** and select **From Reference Device** to activate the Create Template wizard.
3. On the Template Information page, enter a unique **Template Name**, add a **description** and for **Template Type** select the **Clone Reference Server** option. Click **Next**.
4. On the **Reference Device** page, click **Select Device** to select the device whose configuration properties must be used for creating the new template.

Note—Alternatively, you can select the target by entering the device name or Service Tag in the Advanced Filters dropdown.

In the **Configuration Elements** section, select the check boxes corresponding to the device elements that must be cloned. You can select to clone the server properties such as iDRAC, BIOS, Lifecycle Controller, and Event Filters. By default, all elements are selected.



5. Click **Finish**. To view the progress of created job, click the **Jobs** tab under **Monitor**. Select the respective job and click on the **View Details** on the right pane to view the execution history of the job. A job is created. Once the job is successfully completed, the 'base' system template is listed in the Deploy page (**Configuration > Deploy**).

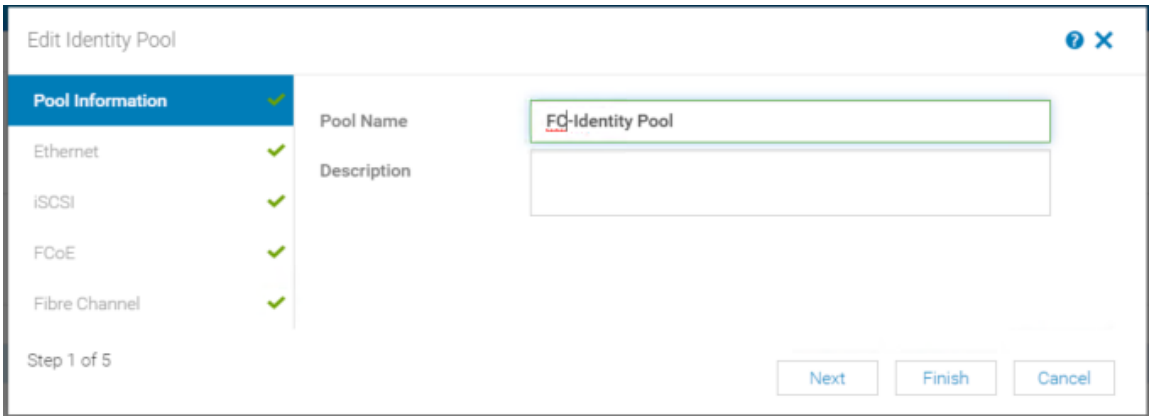
4.3 Create an FC-defined Identity pool

An Identity Pool provides a collection of unique attribute values such as MAC Address, IP Address, WWPN, WWNN, and so on for Ethernet, iSCSI, FC, and FCoE. The physical hardwired identities are replaced by user defined initiator identities which help in keeping the data image of the LUN mobile and portable to another identical server in case of failure.

OpenManage Enterprise allows the user to create an Identity pool with a range of identity attributes, which is then automatically assigned to corresponding NIC and FC port according to the available network protocol and settings during deployment.

The below mentioned steps need to be followed to create an FC-defined identity pool:

1. Go to the Identity Pools page by clicking **Configuration** > **Identity Pool**.
2. Click **Create** to activate the **Create Identity Pool** wizard.
3. On the Pool Information page, enter a unique P**ool Name** and **Description** (optional). Click **Next**.



4. On the **Fiber Channel** page of the wizard, select the **Include FC Identities** check box and enter a unique Postfix (6 Octets) and the range for the number of WWPN/WWNN Address. Click **Next**.

5. Click **Next** and **Finish** to complete the identity pool creation. The Identity pool summary displays the details of the added identity attributes.

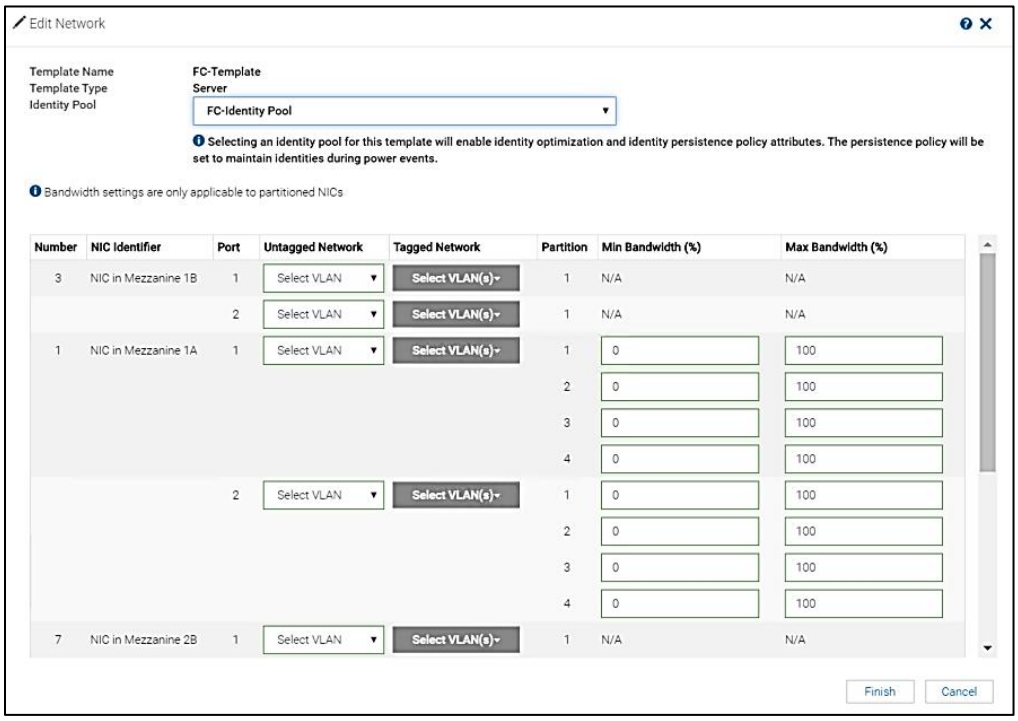
4.4 Associate an FC-defined identity pool to the captured base system template

Identity pool association is a critical step in the 'stateless' deployment. In this step the base system template is linked with the FC identity pool, which would be applied to the target servers' FC ports during deployment. Link establishment to SAN target using virtual identities keeps the data image of the LUN mobile and portable to another identical server in case of failure.

Note: Post deployment, the associated Identity pool is attached to the server template and cannot be modified.

The below mentioned steps must be followed to associate an FC-defined identity pool to a template.

1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Select the base system template and click **Edit Network**.
3. Select the FC Identity pool from the **Identity pool** dropdown.

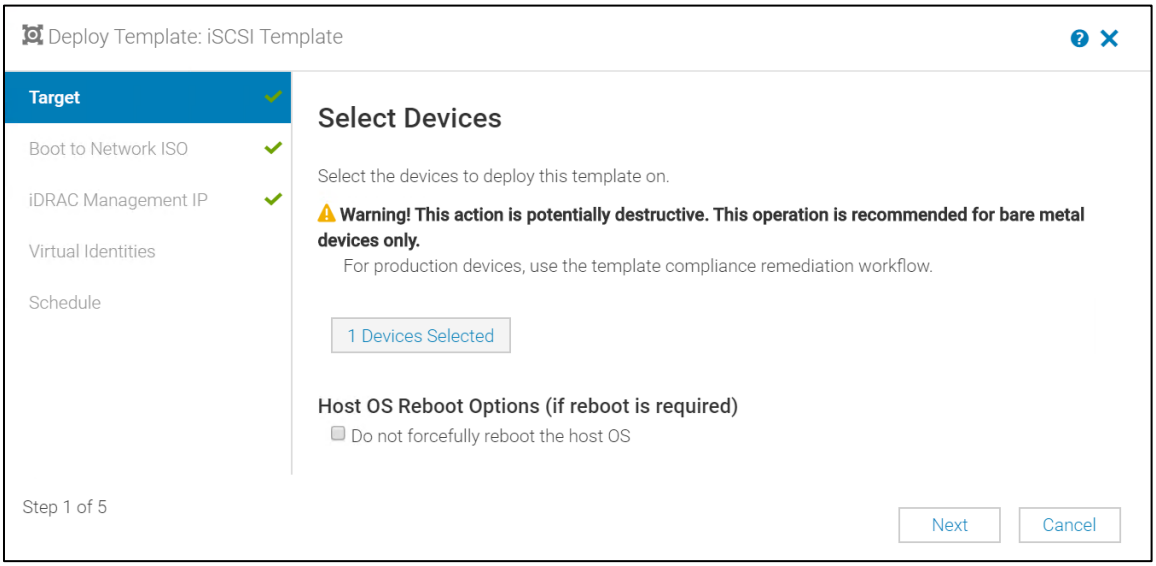


4.5 Deploy the base system template

Deploying templates is the process of applying configuration settings to remote devices. In this step, the captured base system template along with the associated Identity pool is deployed on the selected identical targets. The user can reserve the identities for the deployment and provide SAN boot target attribute values required to connect to the storage array.

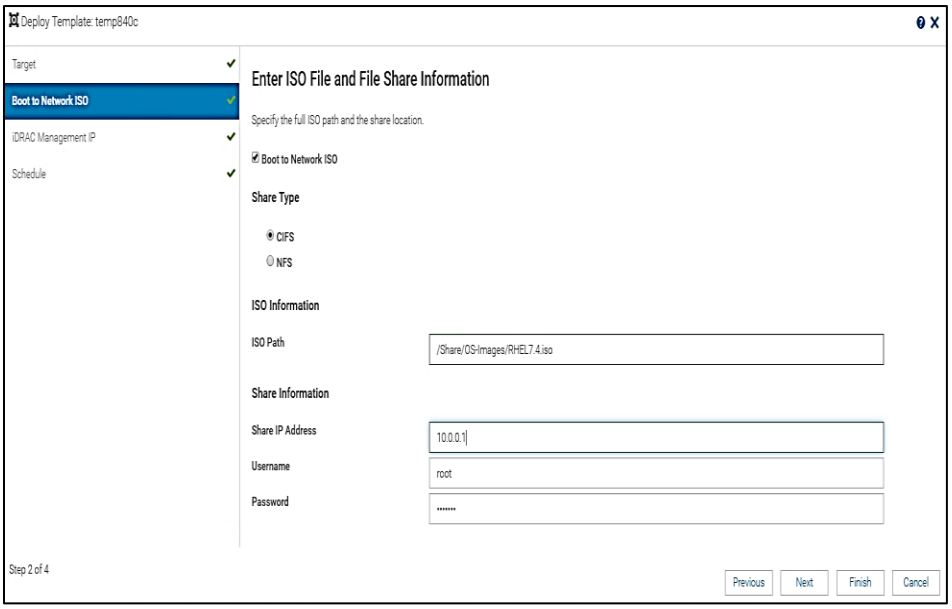
Once the template is deployed, the target servers can be associated with the storage array and boot to the specified LUN successfully. The following steps need to be followed for deployment of a template on identical target devices:

1. Go to the Deploy page by clicking **Configuration** > **Deploy**.
2. Select the created 'base' system template from the list and click on Deploy Template to activate the Deploy Template wizard.
3. Select one or more identical target devices on the Target page. Click **Next**.



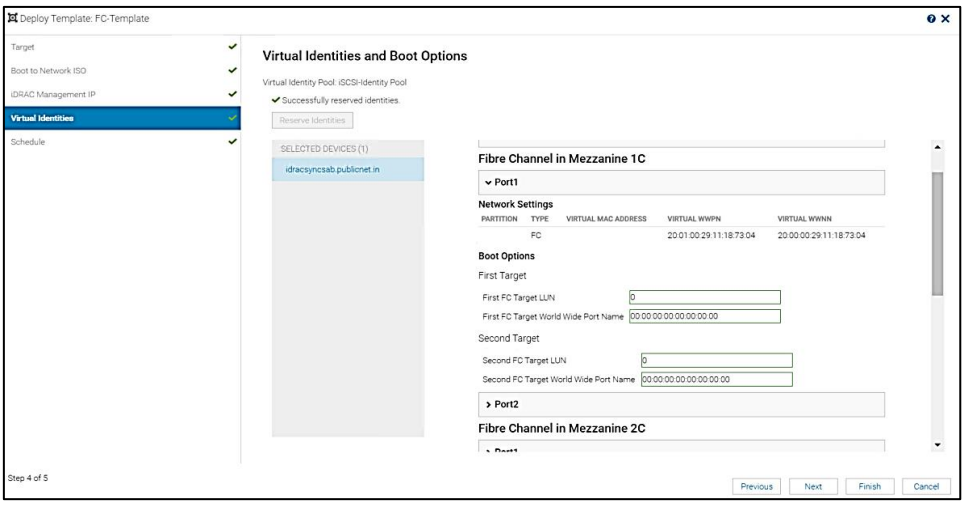
4. The **Boot to Network ISO** page allows you to install the specified OS post deployment.

a. Select the Share type as CIFS/ NFS.
b. Provide the path to the OS image in the ISO path input box in “/OS-Images/OS-file.iso” format.
c. Provide the Share IP address and credentials that can be accessed from the OpenManage Enterprise console.



Note: Providing Boot to Network ISO is optional if the Storage LUN already has an Operating System installed.

5. Click **Next.** On the **Virtual Identities** page, **Reserve Identities,** provide the storage array World Wide Port Name (WWPN) and Boot LUN.



Note: The FC initiator ports are intended to be auto assigned with virtual WWPN, user should manually enter the first and second storage target array details.

6. On the Schedule page, select the option **Run Now** to run the deployment job immediately or select a convenient date and time to schedule the deployment.

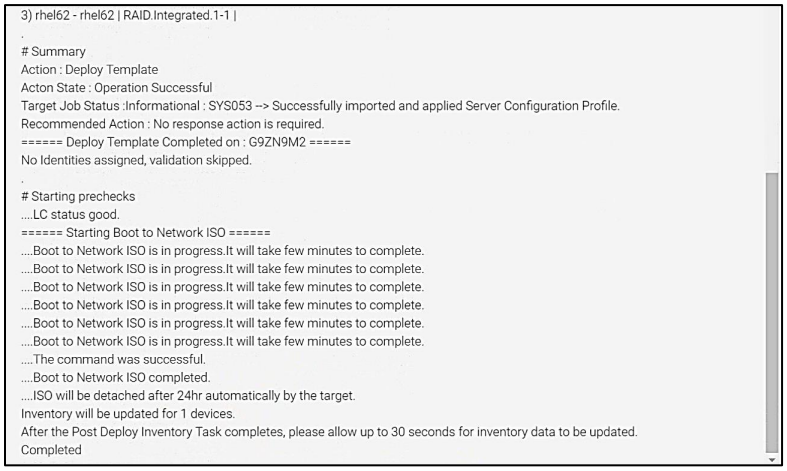
Note: After the completion of deployment job, the physical FC identities of the target server/s are replaced by the reserved virtual identities from the Identity pool.

The benefit of the virtual identities is to ensure that the LUN on which the operating systems are installed is not physically attached or 'tied' to a target server. In case of failure, these virtual Identities can be moved to another identical server with a minimal impact on operations.

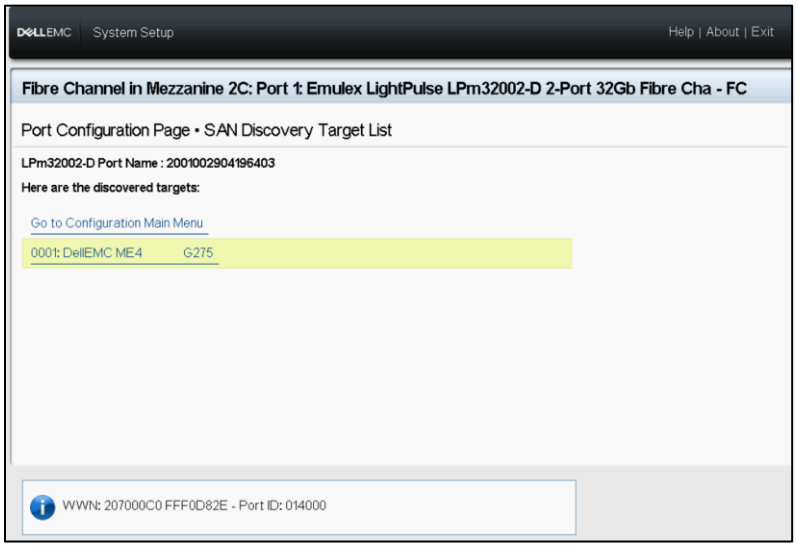
4.6 Booting to SAN via FC

Target systems are ready for an FC boot after a successful base system template deployment. When the deployment job completes the Initiator parameters (WWPNs) from the identity pool are associated to respective FC ports and the ISO image is associated for OS installation.

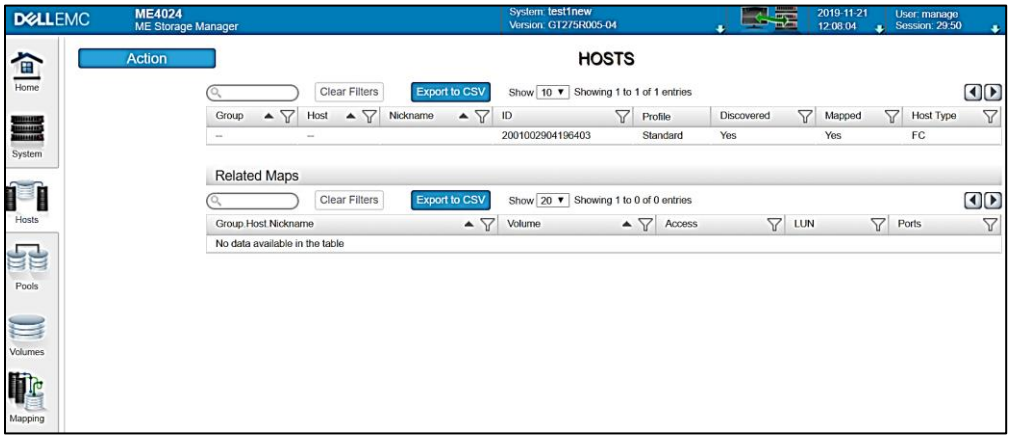
The progress of the Deployment job can be viewed on the Task Execution page.



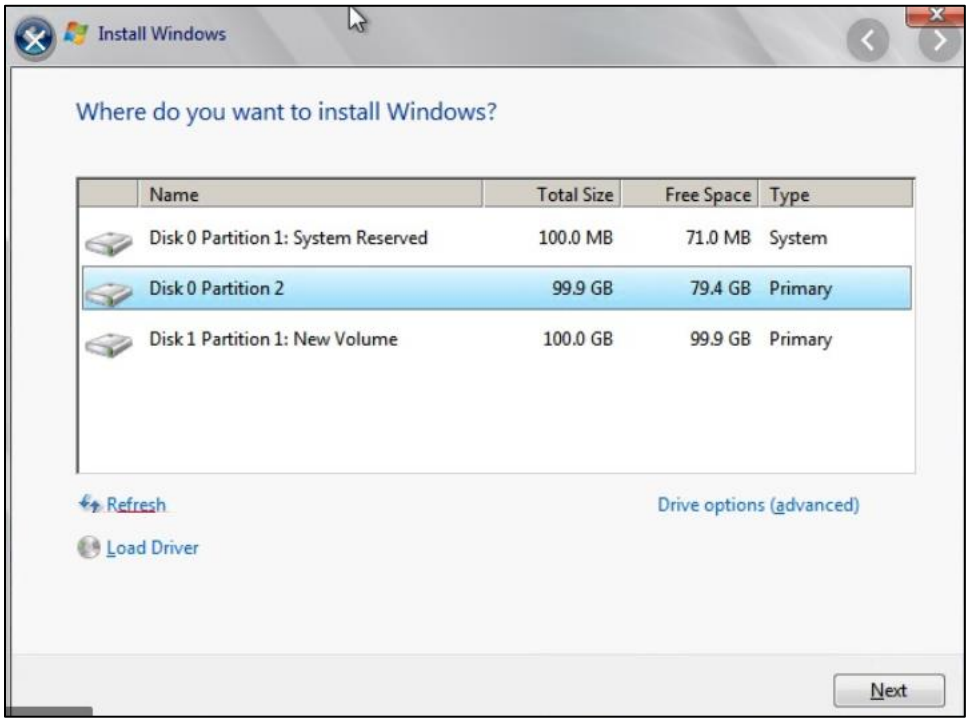
- The Storage Target is discovered for the specific FC port.



- The host is successfully discovered in the storage array and the volume with specified LUN ID is mapped to the host.



- The LUN is visible for OS installation.



5 Migration of Identities in OpenManage Enterprise

Migration is the process of removing the virtual identities from a failed server (source) and deploying them to an identical target server.

As explained in the previous topics, the identities assigned by OpenManage Enterprise are virtual and are not physically 'tied' to a server. In the event of a system failure, OpenManage Enterprise allows the user to migrate these assigned virtual identities to an identical server to boot from the attached storage with a minimal impact on operations.

Note: The new server which is selected for migration, should have an identical configuration to the source server for the success of migration process.

As part of the migration process, the identities assigned to the source server are first reclaimed and then deployed to the selected target server. Reclaiming is a process of removing the assigned identities from the source server so that no two servers are assigned the same identities. Post reclaim, the source server is powered off automatically by OpenManage Enterprise.

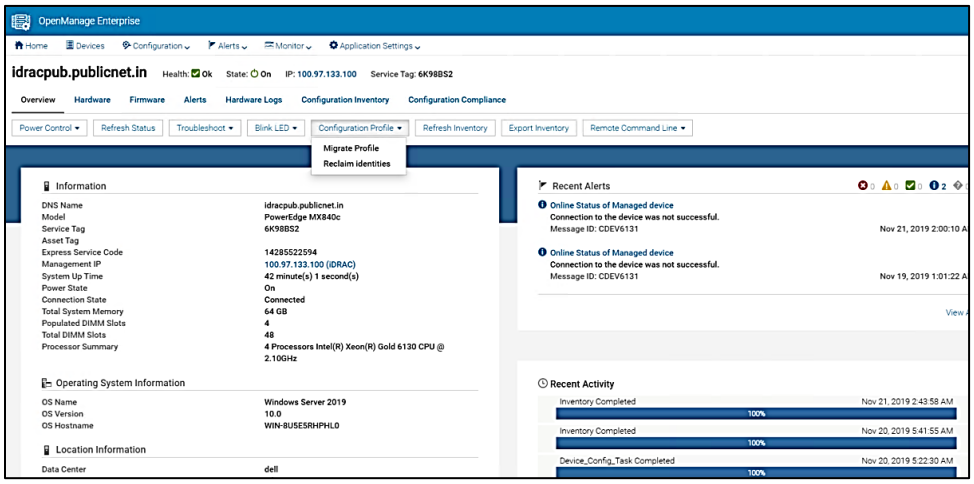
OpenManage Enterprise performs a seamless migration which results in the new target server booting into the same LUN containing the critical workload.

To explain the concept better, the migration of virtual identities from an MX840c server (source) on the following setup, is detailed.

- The sled is deployed with FC Identities and currently booted into ME array LUN via FC protocol containing some critical workload.
- An identical MX840c is the target server to which the profile is migrated.

To migrate the virtual identities the following steps must be followed:

1. Go to the Details page of the server on which the template is deployed.
2. Select Migrate Profile under Configuration Profile.



3. Select an identical target server to migrate the profile.
4. Uncheck Force migration.

Note: Force Migration is selected to forcefully remove the identities from the source server. When the source server is not reachable or is in a critical state, user can forcibly detach the assigned identities from the source server using this option.

5. Select the option **Run Now** if you wish to run the job immediately or the deployment can be scheduled. A 'migration' task is created.

Post the migration task, the source server is powered off. The identities are migrated to the new target server that will boot from the same LUN and operating system. The new target server boots into the Operating system residing in the LUN via FC protocol.