Optimizing I/O Identity and Applying Persistence Policy on Network and Fibre Channel Adapters

This white paper explains how to achieve optimized I/O Identity configuration on the 13th generation Dell PowerEdge servers. The white paper also explains the Persistence of virtual addresses, initiator and storage target settings on the network and fibre channel adapters.

Dell Engineering
September 2014

Authors

Sai Prasad Bale

Ajeesh Kumar

Nagaveni C

Table of contents

Executive summary

This white paper explains how you can reduce the downtime during an XML configuration of the I/O Identity attributes using the I/O Identity Optimization feature and advantages of using Persistence Policy to control adapter behavior for virtual address and initiator and target settings on the network and fiber channel adapters in the 13th generation PowerEdge servers.

1 Introduction

The I/O Identity feature available on iDRAC with Lifecycle Controller on the 11th and 12th generation Dell PowerEdge server, enables you to configure the I/O Identity of the network and fiber channel devices and overlay hardware MAC address of the adapters with virtual addresses. You can also configure the required set of initiator and target setttings based on the internal data center configuration. The main advantage of the I/O Indentity feature is that it provides the flexbililty in deploying rapid reconfiguration of system workloads to another system.

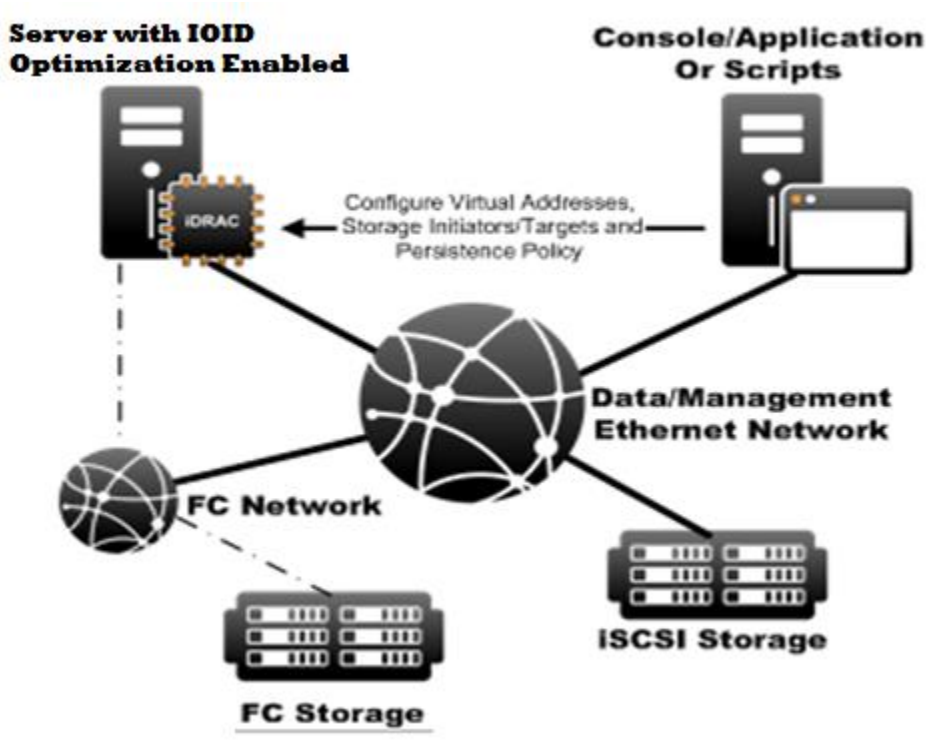


Figure 1 – High Level Architecture Diagram

However, the I/O Identity solution available on the 11th generation servers has the following drawbacks:

- Virtual addresses are volatile and lost if the adapter loses power during a power reset of the host.
- Storage Initiator and Target Settings are always persisted which are actually desired to be volatile.
- Host reboots at least twice while reconfiguring thevirtual address, initiator and target settings attributing to a higher down time.

The I/O Identity Optimization and Persistence Policy feature available on the 13th generation PowerEdge servers addresses the drawbacks listed above.

Optimization of Configuration: On the 11th and 12th generation PowerEdge servers, the XML configuration of NIC/FCHBA attributes would require a minimum of two host reboots – one to apply the configuration using Lifefcycle Controller Remote Services and a another to load the adapters with the setting. On the 13th generation PowerEdge servers, using I/O Identity Optimization, you can minimize the down time by reducing the the number of host reboots to one.

Persisting Virtual Addresses, Initiator and Target Configuration Settings: On the 11th and 12th generation PowerEdge servers, the persistence of virtual addresses and other initiator target settings are dependent on the hardware design. The different network and fibre channel vendors, implemented the behavior based on the power event performed on the host system. On the 13th generation PowerEdge servers, the Persistence policy feature available on iDRAC enables you to modify the policy settings to persist or clear the configuration values on the adapters during a server power cycle.

2 I/O Identity Optimization

The IO Identity feature was introduced in 11G and consists of the ability to get and set various virtual address attributes for NIC Ports and Partitions and iSCSI/FCoE initiators and for FC HBA ports and FC initiators. As explained in the introduction, the existing IO Identity implementation follows a 2 step process i.e Configure and Boot. Using the IO Identity Optimization feature, configure of IO Identity will reduce the whole process of "Configure and Boot" by 50 percent.

2.1 IO Identity Attributes

The following is the list of I/O Identity attributes that you can configure using the I/O Identity Optimization xml configuration:

Table 1: List of I/O Identity attributes

Attribute	NIC/CNA Personality	FC HBA
Virtual Addresses		
VirtMacAddr	NIC Port, NIC Partition	N/A
VirtIscsiMacAddr	ISOE	N/A
VirtFIPMacAddr	FCoE Initiator	N/A
VirtWWn	FCoE Initiator	FC Port Initiator
VirtWWPn	FCoE Initiator	FC Port Initiator
iSCSI InitiatorSettings		
IscsiInitiatorIpAddr	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv4Addr	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv6Addr	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorSubnet	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorSubnetPrefix	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorGateway	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv4Gateway	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv6Gateway	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorPrimDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv4PrimDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv6PrimDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorSecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv4SecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv6SecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorName	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorChapId	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorChapPwd	ISOE, NIC Port, NIC Partition	N/A
iSCSI Storage Target Settings		
ConnectFirstTgt	iSCSI Target	N/A
FirstTgtIpAddress	iSCSI Target	N/A
FirstTgtTcpPort	iSCSI Target	N/A
FirstTgtBootLun	iSCSI Target	N/A
FirstTgtIscsiName	iSCSI Target	N/A
FirstTgtChapId	iSCSI Target	N/A
FirstTgtChapPwd	iSCSI Target	N/A
FirstTgtIpVer	iSCSI Target	N/A
ConnectSecondTgt	iSCSI Target	N/A
SecondTgtIpAddress	iSCSI Target	N/A
SecondTgtTcpPort	iSCSI Target	N/A
SecondTgtBootLun	iSCSI Target	N/A
SecondTgtIscsiName	iSCSI Target	N/A
SecondTgtChapId	iSCSI Target	N/A

SecondTgtChapPwd	iSCSI Target	N/A
SecondTgtIpVer	iSCSI Target	N/A
FCoE Storage Target Setting		
FCoEBootScanSelection	FCoE Target	FC Target
FirstFCoEWWPNTarget	FCoE Target	FC Target
FirstFCoEBootTargetLUn	FCoE Target	FC Target
FirstFCoEFCFVLANId	FCoE Target	FC Target
FCoETgTBoot	FCoE Target	FC Target
FC Storage Target Setting		
BootScanSelection	N/A	FC Target
FirstFCTargetConnect	N/A	FC Target
FirstFCTargetWWPN	N/A	FC Target
FirstFCTargetLUN	N/A	FC Target
SecondFCTargetConnect	N/A	FC Target
SecondFCTargetWWPN	N/A	FC Target
SecondFCTargetLUN	N/A	FC Target

2.2 Supported Vendors

I/O Identity Optimization and Persistence Policy features are available in most of the supported network and fibre channel adapters on the 13th generation PowerEdge server. The supported vendors are:

- Broadcom
- Intel
- Emulex
- QLogic

2.3 Work flow for configuring the attribute using the IO Identity Optimization feature

This section gives the list of user interaction with idrac and sequecne ofsteps to be followed in order to configure Io identity attributes using IO Identity Optimization feature. Section explains racamd, WS-MAN and GUI work flows.

The following section provides the steps to configure the I/O Identity attributes using the I/O Identity Optimization feature.

1. Enabling I/O Identity Optimization

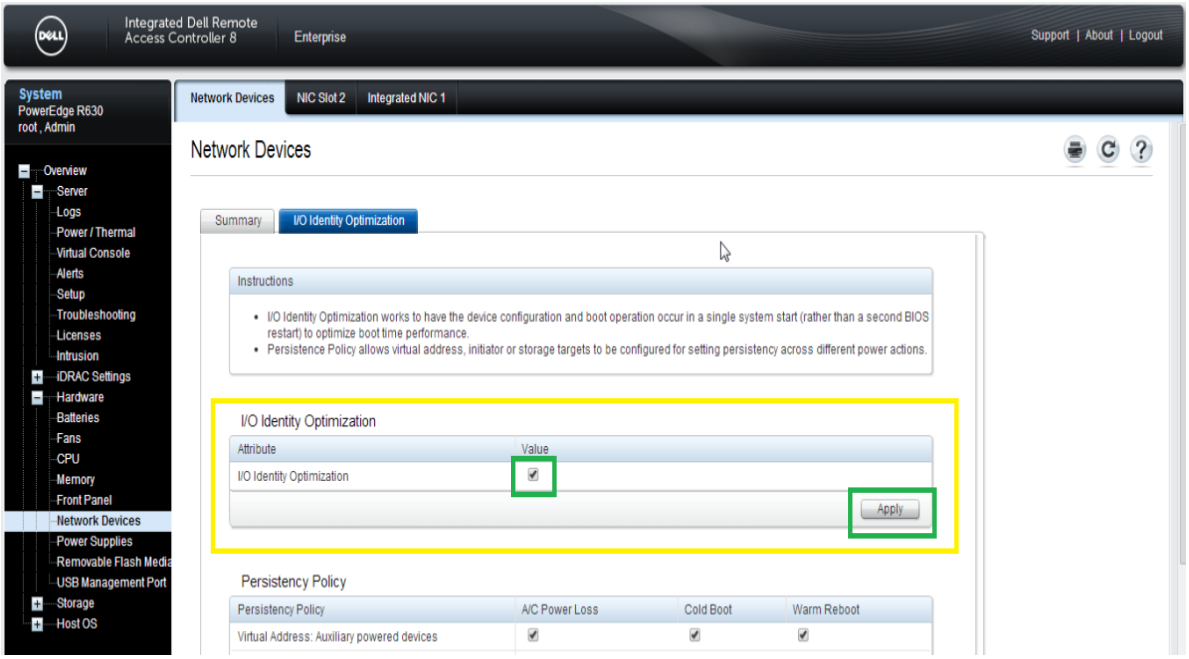
It is mandatory to enable the **I/O Identity Opmtization** feature to achieve boot optimization while configuring the attributes. To enable the feature, use any of the following interfaces:

RACADM

```
racadm set iDRAC.IOIDopt .IOIDOpt Enabled
```

iDRAC GUI

- Login to the iDRAC GUI.
- Click **Hardware**-> **Network Devices**-> **I/O Indetity Optimization**.
- Select the **I/O Identity Optimization** check box and click **Apply**.



WS-MAN Figure 1 Enabling I/O Identity Optimization

```
winrm i Apı                                                vscim/1/cim-
schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCARDS
ervice+Name=DCIM:iDRACCARDService+SystemCreationClassName=DCIM_ComputerSys
tem+SystemName=DCIM:ComputerSystem -u:root -p:calvin -
r:https://10.94.xx.xx/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic
@{TARGET="iDRAC.Embedded.1";AttributeName="IOIDOpt.1#IOIDOptEnable";Attrib
uteValue="Enabled"}
```

2. Exporting the configuration xml file

RACADM

Use the following RACADM commands to export the network and fibre channel device configurations:

Export the xml configuration to a CIFS share:

```
racadm get -f file -t xml -u myuser -p mypass -l
//<cifs_share_ip>/share
```

Export the xml configuration to a NFS share:

```
racadm get -f file -t xml -l <nfs_share_ip>:/myshare
```

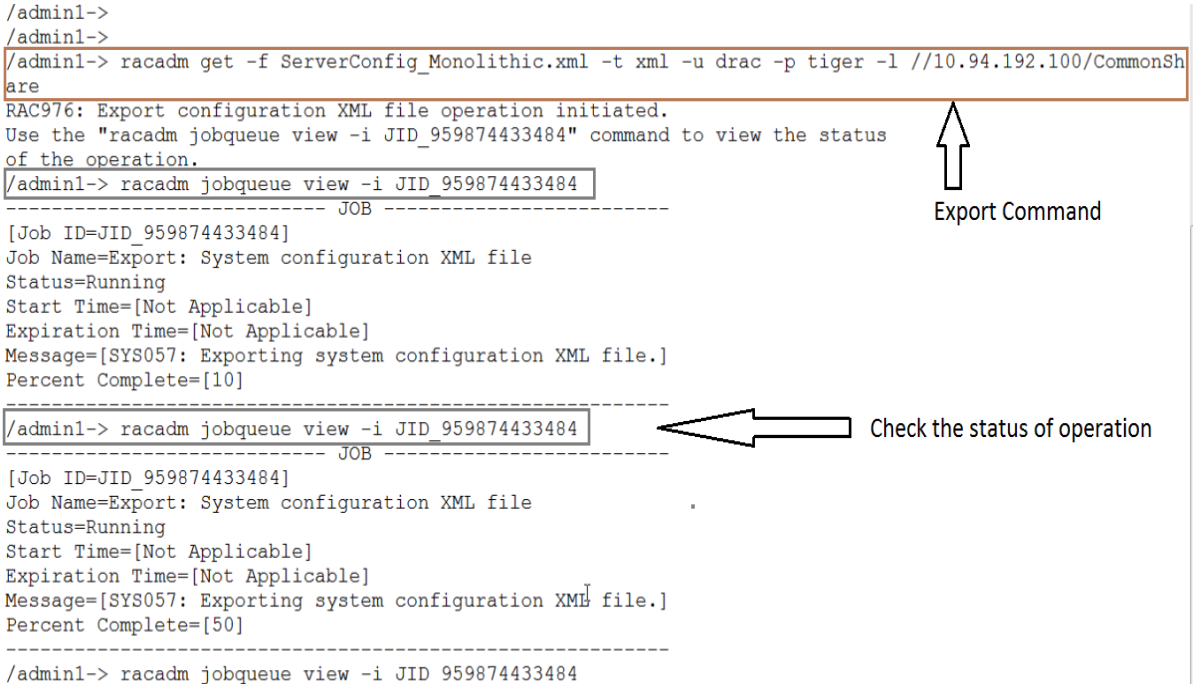


Figure 2 – Export Config xml file using RACADM

WS-MAN

Below WS-MAN command can also be used for exporting the xml configuration

```
winrm i ExportSystemConfiguration
"http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_LCService?CreationClassName=DCIM_LCService+SystemN
ame=DCIM:ComputerSystem+Name=DCIM:LCService+SystemCreationClassName=DCIM_C
omputerSystem" -u:root -p:calvin -r:https://10.94.xx.xx/wsman -
encoding:utf-8 -a:basic -SkipCNcheck -SkipCAcheck
@{IPAddress="10.94.xx.xx";ShareName="CommonShare";ShareType="2";UserName="
xxxx";Password="yyyyy";FQDD="iDRAC.Embedded.1";ImportOptions="0";FileName=
"test.xml"}
```

3. Chaning the required I/O Identity attributed in the exported XML file

Manually edit any of the IO Identity attributes listed in Table 1 in the exported XML file on the share.Attributes will be grouped into FQDD which are mapped to a particular Port or Partition of a NIC or Fibre Channel adapter. In case, the attribute you wanted to configure is commented using "<!--" and "-->", uncomment the attribute by removing "<!--" , "-->" and edit to the desired value which you wanted to configure as shown in the Figure 4.

Note: Make sure that you edit only the attributes listed in Table 1 for the optimization to occur.

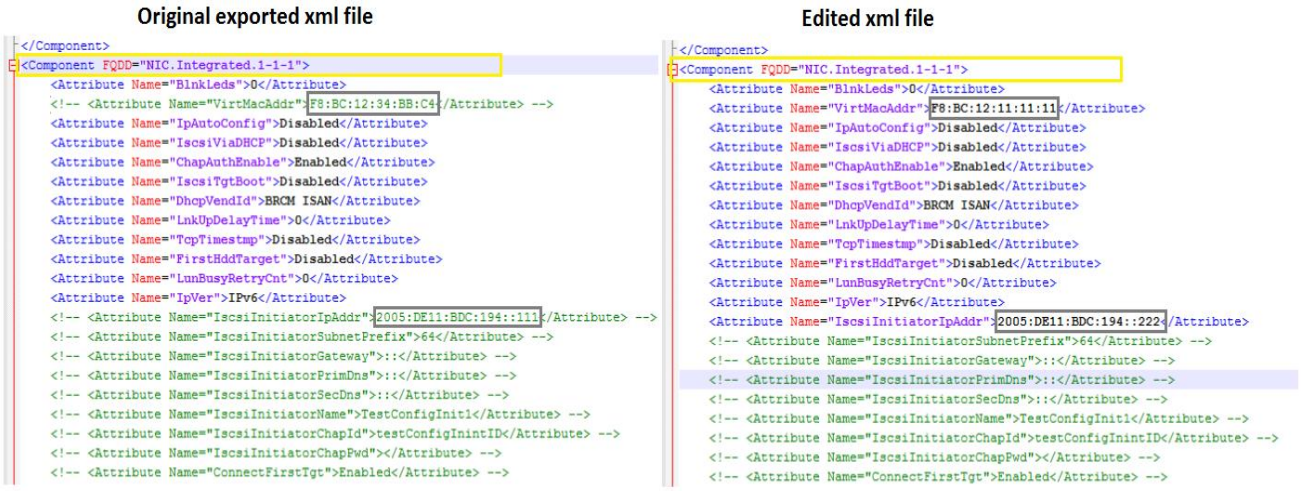


Figure 3 – Edit the Config xml file

4. Importing the edited xml file

After you have completed changing ther required attributes in the exported XML file, use the following command to import the XML file:

RACADM :

Configure a RAC from an XML configuration file located on a remote CIFS share.

```
racadm set -f myfile.xml -t xml -u myuser -p mypass -l
//<cifs_share_ip>/myshare
```

Configure a RAC from an XML configuration file located on a remote NFS share.

```
racadm set -f myfile.xml -t xml -l <nfs_share_ip>:/myshare
```

The set command above returns the job ID as the output.The host reboots after the import process starts and the edited attribute value is displayed as Pending value. See Figure 6.

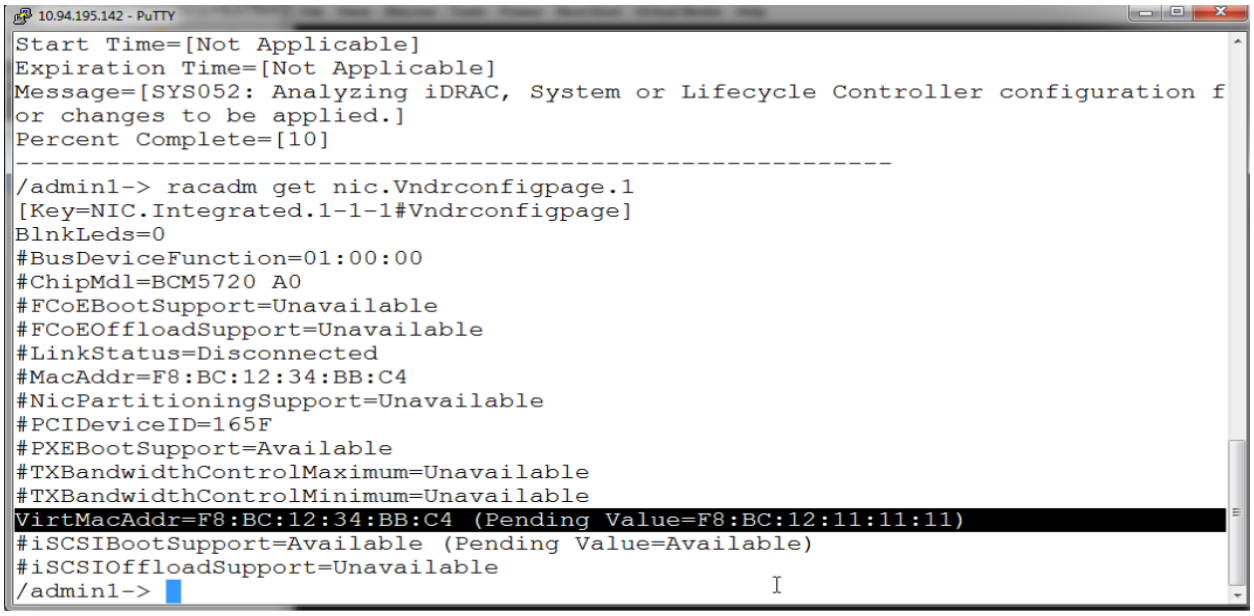


Figure 5 – Edit the Config xml file

WS-MAN :

Import the configuration xml file with the below WS-MAN command.

```
winrm i ImportSystemConfiguration
"http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_LCService?CreationClassName=DCIM_LCService+SystemN
ame=DCIM:ComputerSystem+Name=DCIM:LCService+SystemCreationClassName=DCIM_C
omputerSystem" -u:root -p:calvin -r:https://10.94.xx.xx/wsman -
encoding:utf-8 -a:basic -SkipCNcheck -SkipCAcheck
@{IPAddress="10.94.xx.xx";ShareName="CommonShare";ShareType="2";UserName="
xxxx";Password="yyyyy";FQDD="iDRAC.Embedded.1";ImportOptions="0";FileName=
"test.xml"}
```

5. Completing the job

After the import xml job completes successfully, the configured values are applied to the selected devices. You can check the status of the job by using RACADM command, WS-MAN command and iDRAC GUI.

RACADM :

```
racadm jobqueue view –i <jobid>
```

WS-MAN :

```
winrm g http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/DCIM_Lifecyclejob?__cimnamespace=root/dcim+InstanceID=<jobid>
-u:root -p:calvin -r:https://10.94.xx.xx/wsman -encoding:utf-8 -a:basic
-SkipCNcheck -SkipCAcheck
```

iDRAC GUI :

Click **Server-> Job Queue**

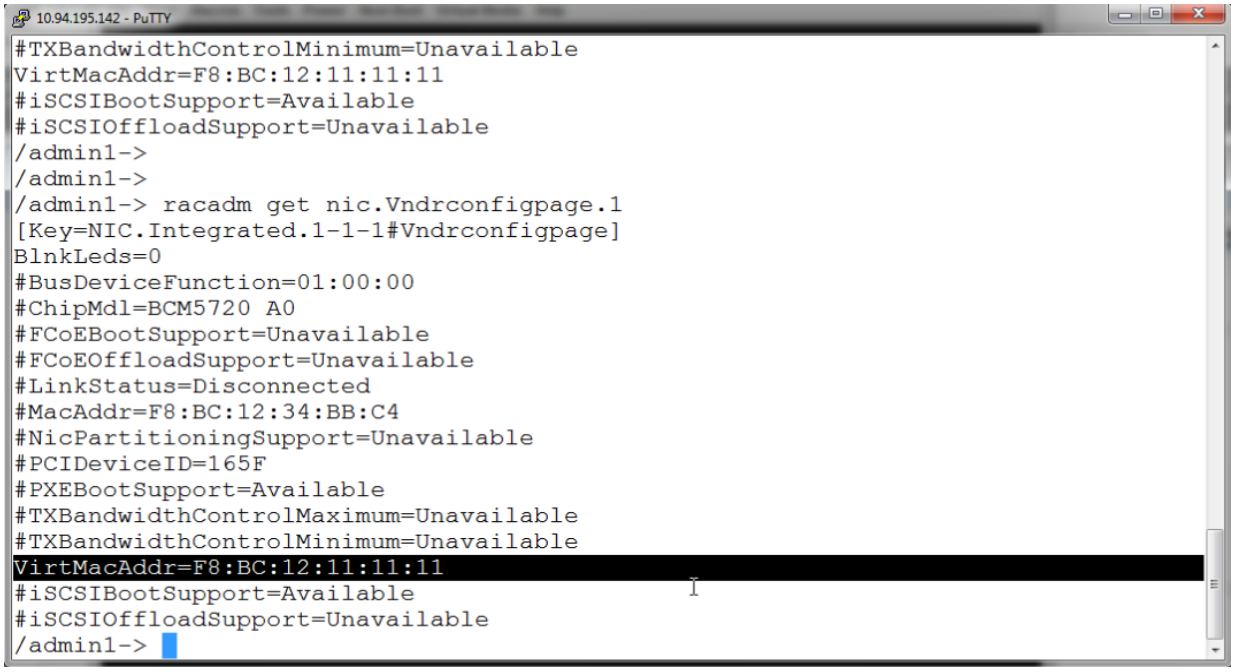


Figure 6.a – Configured parameter values once the import operation completes – racadm command

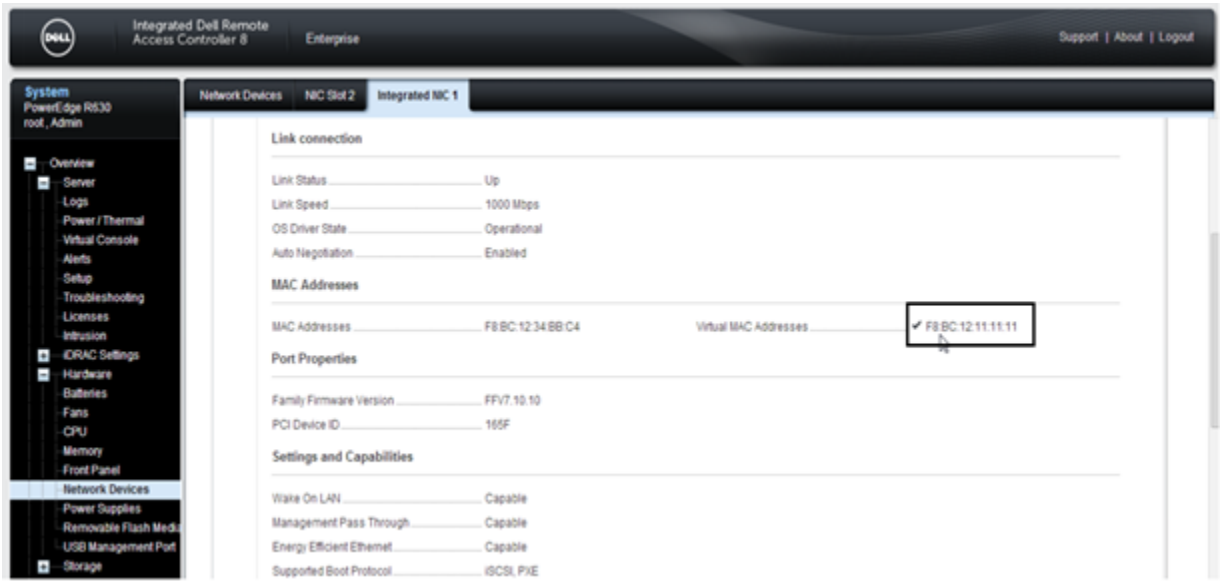


Figure 6.b – Configured parameter values once the import operation completes – iDRAC GUI

```
C:\Users\: xyz \Desktop>winrm e http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_NICView -u:"root" -p:"calvin"
ocationCheck -encoding:utf-8 ¼a:basic

DCIM_NICView
    AutoNegotiation = 2
    BusNumber = 1
    ControllerBIOSVersion = 1.33
    CurrentMACAddress = F8:BC:12:11:11:11
    DataBusWidth = 0002
    DeviceDescription = Integrated NIC 1 Port 1 Partition 1
    DeviceNumber = 0
    EFIVersion = 16.4.11
    FCoEOffloadMode = 3
    FCoEWWNN
    FQDD = NIC.Integrated.1-1-1
    FamilyVersion = FFV7.10.10
    FunctionNumber = 0
    InstanceID = NIC.Integrated.1-1-1
    LastSystemInventoryTime = 20140328065927.000000+000
    LastUpdateTime = 20140328075919.000000+000
    LinkDuplex = 1
    LinkSpeed = 3
    MaxBandwidth = 0
    MediaType = Base T
    MinBandwidth = 0
    NicMode = 3
    PCIDeviceID = 165F
    PCISubDeviceID = 1f5b
    PCISubVendorID = 1028
```

Figure 6.c – Configured parameter values once the import operation complets – check with WSMAN command

6. Verifying on the host

You can verify the change in virtual addresses on the host using the following commands:

On systems running Windows:
At the command prompt, type `ipconfig/all`

On systems running Linux:
At the command shell, type `ipconfig`.

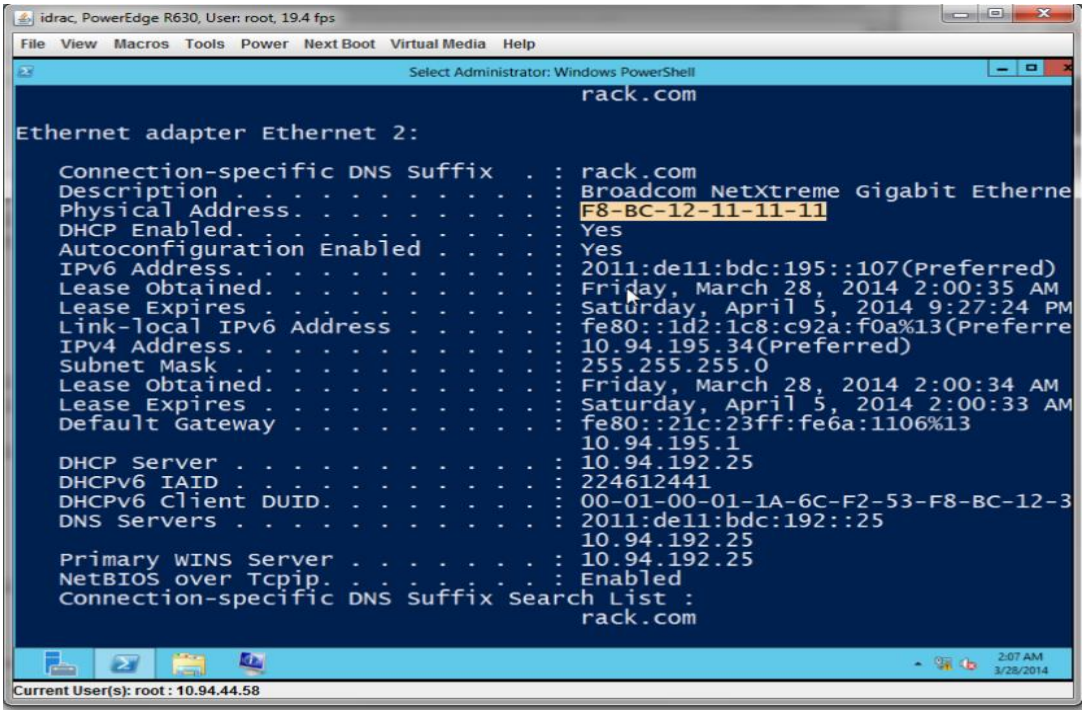


Figure 8 – Configured Virtual address from Windows HOST OS

3 Persistence Policy

On the 11th and 12th generation PowerEdge servers, the persistence behavior of the configuration values for the NIC/FB HBA devices differs based on the device type (auxillary/non-auxillary) and system reboot method (ac power cycle/ warm boot/cold boot). The virtual addresses are lost when the network and fibre channel adapters are powered off. Also, because of the persistence of the Initiator and Target settings in the adpaters during system reboots, you cannot set policies on the workload. In such a scenario, you must manually reconfigure the XML config file for all the adapters.

The Persistence Policy feature available on the 13th generation PowerEdge servers, enables you to control the volatility and persistence of virtual addresses, initiator and target settings for all NIC/FBA devices with different power cycles.

The Persistence Policy contribution attributes are:

- VirtualAddressAux Powered Persistence Policy
- Virtual Address Non-Aux Powered Persistence Policy
- Initiator PersistencePolicy
- StorageTargetPersistencePolicy

  The above policy settings can be configured to one or more of below values.

  - None
  - Warm Reset
  - Cold Reset
  - AC Power Loss

- If a policy is set or selected for any of the power event, after performing the selected power event, the parameters related to that particular policy will persist or reconfigure to the already configured values.
- If a set policy is cleared for any of the power events, the policy returns to the default state after perfoming the event..

Note: All the NDCs and LOMs are Auxiliary Powered devices.

The table below explains the behavior of the configured persistence policy settings on host power cycles.

	Persistence Policy Value							
	None	**ACPowerLoss**	**ColdReset**	**ColdReset, ACPowerLoss**	**WarmReset**	**WarmReset, ACPowerLoss**	**WarmReset, ColdReset**	**WarmReset, ColdReset, ACPowerLoss**
Virtual Address persistence policy for Aux Powered devices	On AC/Cold/Warm Reset, clear all the Virtual Addresses on Aux powered devices	Only on AC Power cycle, Persist all the Virtual Addresses otherwise clear it to default on Aux powered devices	Only on Cold Reset, Persist all the Virtual Addresses otherwise clear it to default on Aux powered devices	Only on Cold/AC Reset, Persist all the Virtual Addresses otherwise clear it to default on Aux powered devices	Only on Warm Reset, Persist all the Virtual Addresses otherwise clear it default on Aux powered devices	Only on Warm/AC Reset, Persist all the Virtual Addresses otherwise clear it to default on Aux powered devices	Only on Warm/Cold Reset, Persist all the Virtual Addresses otherwise clear it to default on Aux powered devices	On Warm/Cold/AC Reset, Persist all the Virtual Addresses on Aux powered devices
Virtual Address persistence policy for Non-Aux Powered devices	On AC/Cold/Warm Reset, clear all the Virtual Addresses on Non-Aux powered devices	Only on AC Power cycle, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	Only on Cold Reset, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	Only on Cold/AC Reset, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	Only on Warm Reset, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	Only on Warm/AC Reset, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	Only on Warm/Cold Reset, Persist all the Virtual Addresses otherwise clear it to default on Non-Aux powered devices	On Warm/Cold/AC Reset, Persist all the Virtual Addresses on Non-Aux powered devices
Initiator persistence policy	On AC/Cold/Warm Reset, clear all Initiator configuration settings to default	Only on AC Power cycle, Persist all the Initiator configuration settings otherwise clear it to default	Only on Cold Reset, Persist all the initiator configuration settings otherwise clear it to default	Only on Cold/AC Reset, Persist all the initiator configuration settings otherwise clear it to default	Only on Host Warm Reset, Persist all the initiator configuration settings otherwise clear it to default	Only on Host Warm/AC Reset, Persist all the initiator configuration settings otherwise clear it to default	Only on Host Warm/Cold Reset, Persist all the initiator configuration settings otherwise clear it to default	On Warm/Cold/AC Reset, Persist all the initiator configuration settings.
Storage Target persistence policy	On AC/Cold/Warm Reset, clear all Storage Target configuration settings to default	Only on AC Power cycle, Persist all the Storage Target configuration settings otherwise clear it to default	Only on Cold Reset, Persist all the Storage Target configuration settings otherwise clear it to default	Only on Cold/AC Reset, Persist all the Storage Target configuration settings otherwise clear it to default	Only on Host Warm Reset, Persist all the Storage Target configuration settings otherwise clear it to default	Only on Warm/AC Reset, Persist all the Storage Target configuration settings otherwise clear it to default	Only on Host Warm/Cold Reset, Persist all the Storage Target configuration settings otherwise clear it to default	On Warm/Cold/AC Reset, Persist all the Storage Target configuration settings.

3.1 I/O Identity Optimization and Persistence Policy using the iDRAC RACADM interfaces

1. Type the following command to check the I/O Identity Optimization and Persistence Policy status:

```
racadm get iDRAC.IOIDopt
```

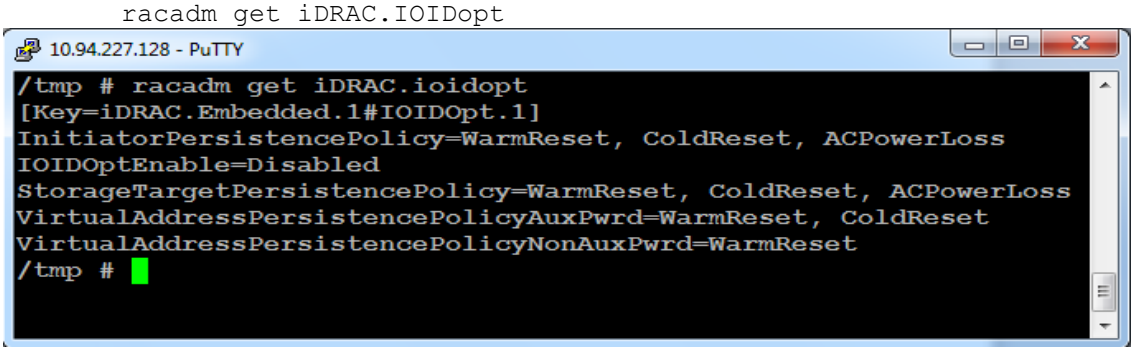


Figure 9 – I/O Identy Optimization in default state shown with racadm command

2. Use the following RACADM commands to set the policies:

- To set **VirtualAddressPersistencePolicyAuxPwrd** Persistence Policy:
  `racadm set iDRAC.IOIDopt.VirtualAddressPersistencePolicyAuxPwrd ColdReset`

- To set **VirtualAddressPersistencePolicyNonAuxPwrd** Persistence Policy:
  `racadm set iDRAC.IOIDopt.VirtualAddressPersistencePolicyNonAuxPwrd ColdReset`

- To set the **InitiatorPersistencePolicy**:
  `racadm set iDRAC.IOIDopt. InitiatorPersistencePolicyPolicy ColdReset`

- To set **StorageTargetPersistencePolicy**:
  `racadm set iDRAC.IOIDopt. StorageTargetPersistencePolicy ColdReset`

3.2 I/O Identity Optimization and Persistence Policy using iDRAC WS-MAN interface

1. Type the following commands to set the Virtual Address Persistence Policy for Auxillary Powered devices:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCARDSer
vice+Name=DCIM:iDRACCARDService+SystemCreationClassName=DCIM_ComputerSystem+
SystemName=DCIM:ComputerSystem -u:root -p:calvin -
r:https://10.94.xx.xx/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic
@{TARGET="iDRAC.Embedded.1";AttributeName="IOIDOpt.1#VirtualAddressPersisten
cePolicyAuxPwrd";AttributeValue="WarmReset,ColdReset,ACPowerLoss"}
```

2. Type the following commands to set the Virtual Address Persistence Policy for Non-Auxillary Powered devices:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCARDSer
vice+Name=DCIM:iDRACCARDService+SystemCreationClassName=DCIM_ComputerSystem+
SystemName=DCIM:ComputerSystem -u:root -p:calvin -
r:https://10.94.xx.xx/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic
@{TARGET="iDRAC.Embedded.1";AttributeName="IOIDOpt.1#VirtualAddressPersisten
cePolicyNonAuxPwrd";AttributeValue="WarmReset,ColdReset,ACPowerLoss"}
```

3. Type the following command to set the Initiator Persistence Policy:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCARDServ
ice+Name=DCIM:iDRACCARDService+SystemCreationClassName=DCIM_ComputerSystem+Sy
stemName=DCIM:ComputerSystem -u:root -p:calvin -r:https://10.94.xx.xx/wsman -
SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic
```

```
@{TARGET="iDRAC.Embedded.1";AttributeName="IOIDOpt.1#InitiatorPersistencePoli
cy ";AttributeValue="WarmReset,ColdReset,ACPowerLoss"}
```

4. Type the following command to set the Storage Target Persistence Policy:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCARDServ
ice+Name=DCIM:iDRACCARDService+SystemCreationClassName=DCIM_ComputerSystem+Sy
stemName=DCIM:ComputerSystem -u:root -p:calvin -r:https://10.94.xx.xx/wsman -
SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic
@{TARGET="iDRAC.Embedded.1";AttributeName="IOIDOpt.1#StorageTargetPersistence
Policy ";AttributeValue="WarmReset,ColdReset,ACPowerLoss"}
```

3.3 Setting I/O Identity Optimization and Persistence Policy using iDRAC GUI interface.

a. **iDRAC in a default state**

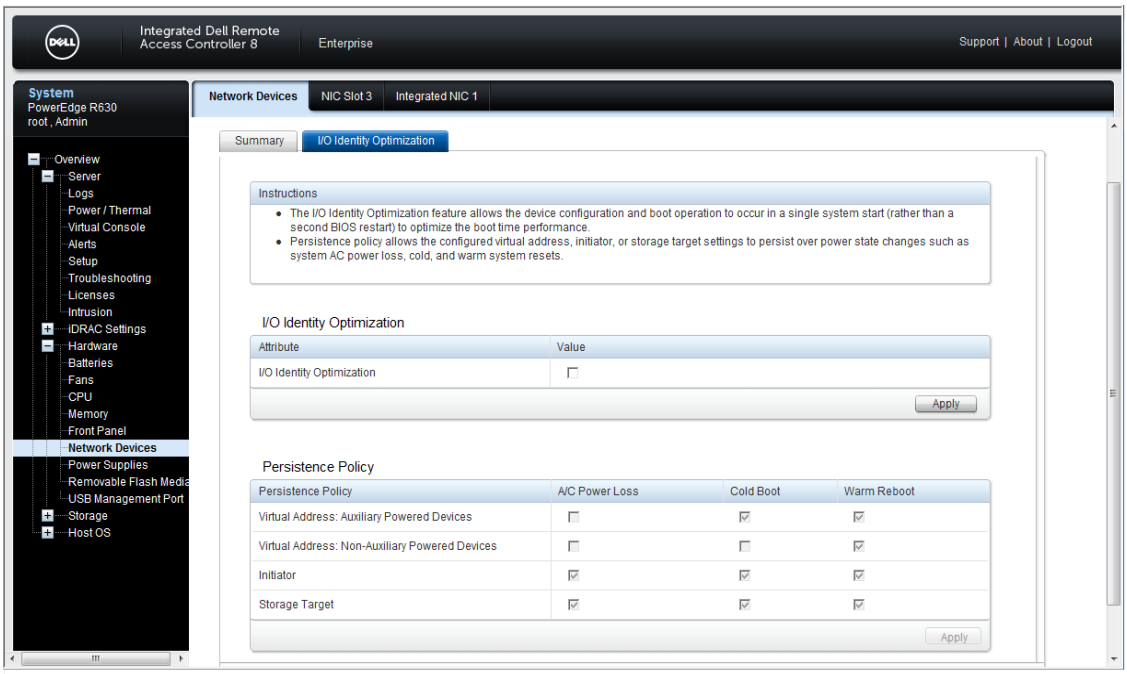


Figure 10 – I/O Identy Optimization in default state shown from iDRAC GUI

b. How to enable I/O Identity Optimization and Persistence Policy through iDRAC GUI

I/O Identity Optimization can be Enabled or Disabled by clicking on the checkbox provided under I/O Identity Optimization attribute and click on apply button provided under this attrubute.
Similarly Persistence policy for Virtual address, Initiator and Target can be set by clicking on the checkboxes provided under persistence policy for different power events and click on apply button provided under persistence policy table. Refer the Figure 11.

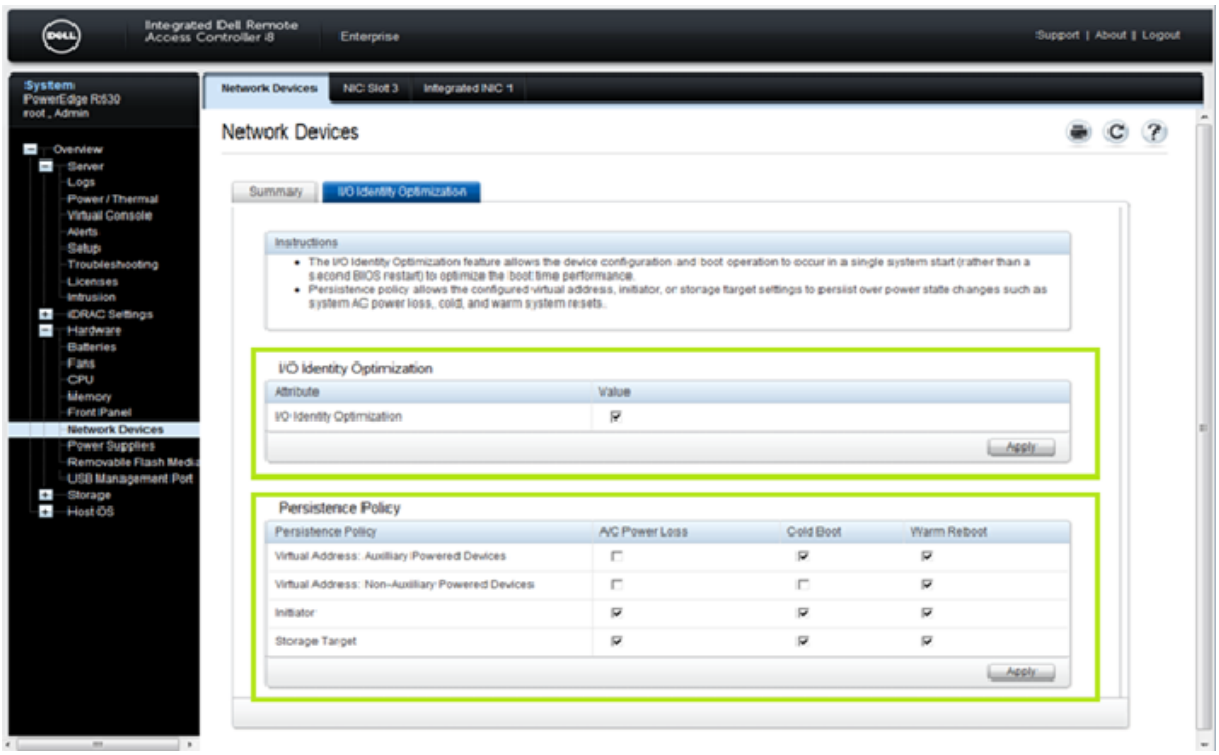


Figure 11 – I/O Identity Optimization and Persistence Policies from iDRAC GUI

3.3 Work Flow Example of Persistence Policy

The following workflow explains how virtual addresses of auxillary powered devices persist or reconfigure and reset back to hardware MAC address over different cold reboots.

1) Enable I/O Identity Optimization and select the cold boot for the virtual address auxillary powered devices.

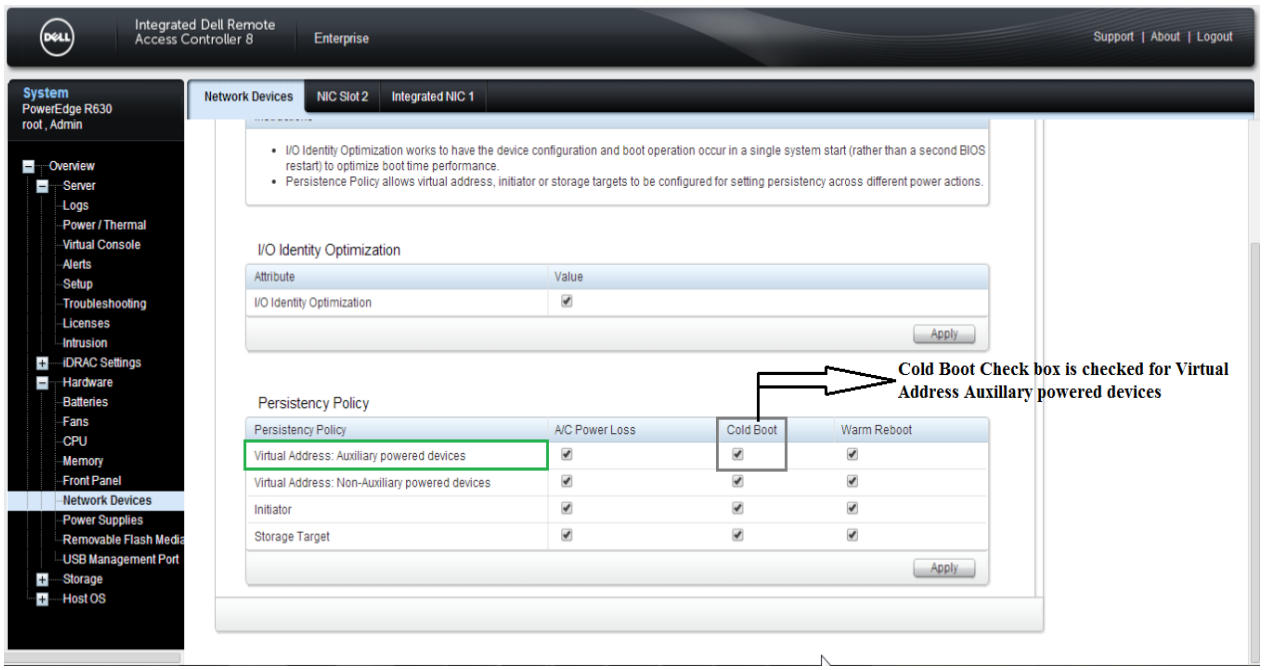


Figure 12 – Check the check box of Virtual Address Auxillary Powered devices for cold Boot.

2) Type the following RACADM command to perform a cold boot of the host.
   `racadm serveraction powercycle`
3) After the cold boot is completed, export the XML file.
4) You will notice that the configured virtual MAC address does not revert back to the hardware MAC address during a cold boot. The MAC addresses remain in the configured state and the virtual MAC addresses persist over cold boot.

Before Cold Boot

```
</Component>
<Component FQDD="NIC.Integrated.1-1-1">
    <Attribute Name="BlnkLeds">0</Attribute>
    <!-- <Attribute Name="VirtMacAddr">F8:BC:12:11:11:11</Attril
    <Attribute Name="IpAutoConfig">Disabled</Attribute>
    <Attribute Name="IscsiViaDHCP">Disabled</Attribute>
    <Attribute Name="ChapAuthEnable">Enabled</Attribute>
    <Attribute Name="IscsiTgtBoot">Disabled</Attribute>
    <Attribute Name="DhcpVendId">BRCM ISAN</Attribute>
    <Attribute Name="LnkUpDelayTime">0</Attribute>
    <Attribute Name="TcpTimestmp">Disabled</Attribute>
    <Attribute Name="FirstHddTarget">Disabled</Attribute>
    <Attribute Name="LunBusyRetryCnt">0</Attribute>
```

After Cold Boot Completes

```
</Component>
<Component FQDD="NIC.Integrated.1-1-1">
    <Attribute Name="BlnkLeds">0</Attribute>
    <Attribute Name="VirtMacAddr">F8:BC:12:11:11:11</Attribute>
    <Attribute Name="IpAutoConfig">Disabled</Attribute>
    <Attribute Name="IscsiViaDHCP">Disabled</Attribute>
    <Attribute Name="ChapAuthEnable">Enabled</Attribute>
    <Attribute Name="IscsiTgtBoot">Disabled</Attribute>
    <Attribute Name="DhcpVendId">BRCM ISAN</Attribute>
    <Attribute Name="LnkUpDelayTime">0</Attribute>
    <Attribute Name="TcpTimestmp">Disabled</Attribute>
    <Attribute Name="FirstHddTarget">Disabled</Attribute>
    <Attribute Name="LunBusyRetryCnt">0</Attribute>
```

Figure 13 – Comapare Virtual MAC Address of Integrated NIC Before Cold Boot and After Cold Boot

Note: You can check the parameter values using RACADM, WS-MAN, or iDRAC GUI. For more information, see Figure 7.a , 7.b and 8.

5) After I/O Identity Optimization is enabled, clear the cold boot option for virtual address auxillary powered devices.

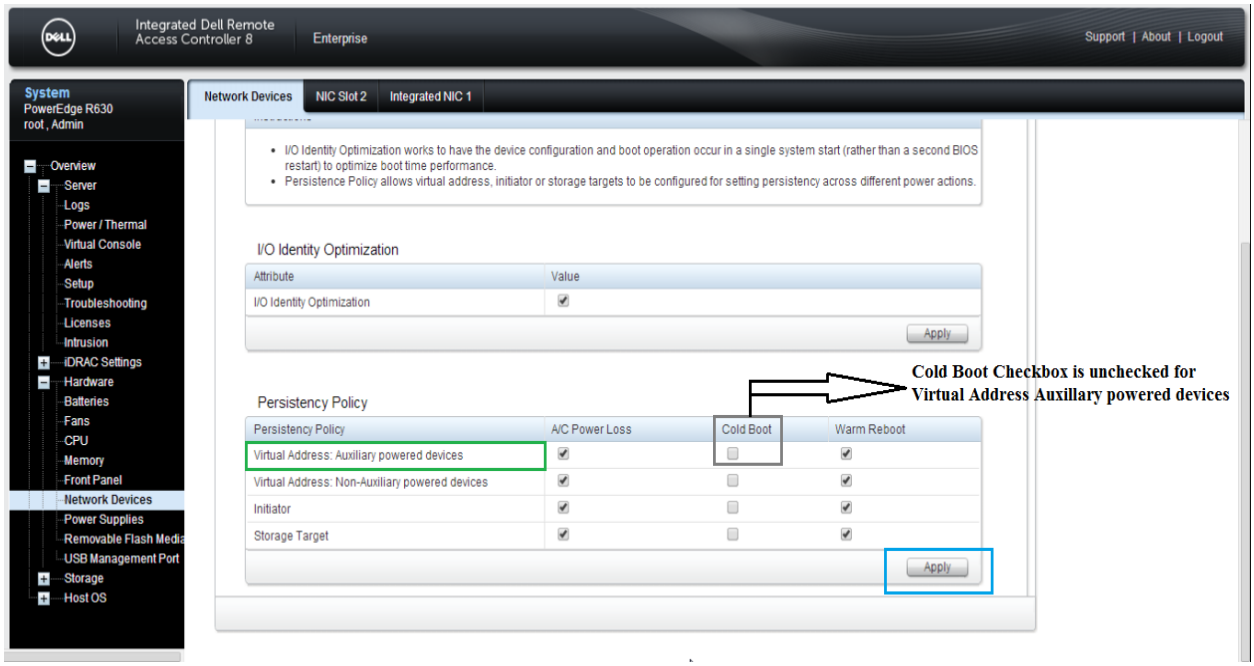


Figure 14 – Uncheck the check box of Virtual Address Auxillary Powered devices for cold Boot.

After the cold boot process completes, the virtual MAC address changes from the configured value to the hardware MAC address value . In Figure 15 shows the comaprision of virtual MAC address before performing cold boot operation and after completing cold Boot operation.

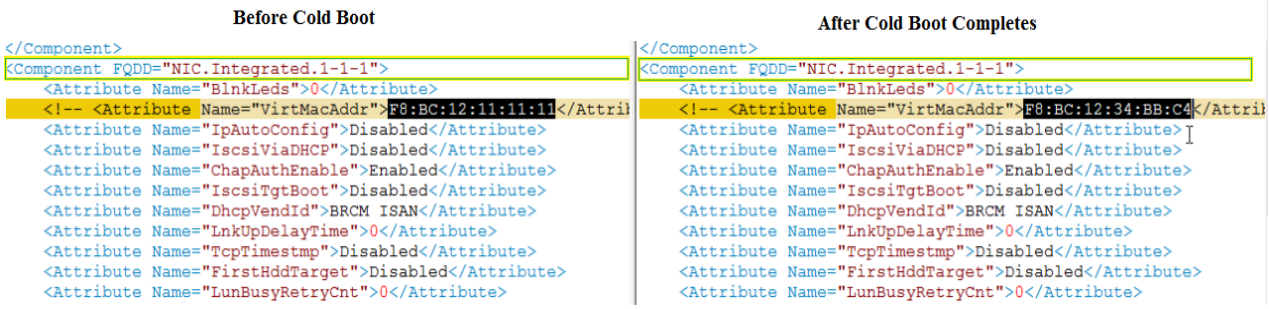


Figure 15 – Comapare Virtual MAC Address of Integrated NIC Before Cold Boot and After Cold Boot

Note: You can use RACADM or iDRAC GUI to check the virtual MAC address changed value. For more information, see Figure 7.a and Figure 7.b.

- Similar to the cold boot operation, Virtual address auxillary powered devices persist or reconfigure virtual MAC addresses and reset to its default hardware MAC address over Warm Boot and AC powercycle.
- Virtual address non-auxillary powered devices also works in same way as virtual address auxillray powered devices for different power events such as Warm Boot, Cold Boot and AC power cycle.

- Initiators and storage target parameters also persist the parameter values and reset to its default state depending on power cycle selected or cleared for different power event. Initiators and Storage target default values are provided in the tables below.

iSCSI Initiator	Default Values in Ipv4 mode	Default Values in IPv6 mode
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	ValueCleared	ValueCleared
IscsiInitiatorChapId	ValueCleared	ValueCleared
IscsiInitiatorChapPwd	ValueCleared	ValueCleared

Table 2: Initiator Default Values

iSCSI Storage target Attributes	Default Values in IPv4 mode	Default Values in IPv6 mode
"ConnectFirstTgt"	Disabled	Disabled
"FirstTgtIpAddress"	0.0.0.0	::
"FirstTgtTcpPort"	3260	3260
"FirstTgtBootLun"	0	0
"FirstTgtIscsiName"	ValueCleared	ValueCleared
"FirstTgtChapId"	ValueCleared	ValueCleared
"FirstTgtChapPwd"	ValueCleared	ValueCleared
"ConnectSecondTgt"	Disabled	Disabled
"SecondTgtIpAddress"	0.0.0.0	::
"SecondTgtTcpPort"	3260	3260
"SecondTgtBootLun"	0	0
"SecondTgtIscsiName"	ValueCleared	ValueCleared
"SecondTgtChapId"	ValueCleared	ValueCleared
"SecondTgtChapPwd"	ValueCleared	ValueCleared

Table 3: Storage Target Default Values

FCoE Target Attributes	Default Values
FCoEBootScanSelection	Disabled
FirstFCoEWWPNTarget	00:00:00:00:00:00:00:00
FirstFCoEBootTargetLUN	0
FirstFCoEFCFVLANID	00:00:00:00:00:00:00:00
FCoETgTBoot	0

Table 4: FCoE Target Default Values

FC Target Attributes	Default Values
BootScanSelection	Disabled
FirstFCTargetWWPN	00:00:00:00:00:00:00:00
FirstFCTargetLUN	0
SecondFCTargetWWPN	00:00:00:00:00:00:00:00
SecondFCTargetLUN	0

Table 4: FC Target Default Values