

ESXi deployment using Dell EMC OpenManage Integration for VMware vCenter (OMIVV) and deployment best practices

Abstract

Dell EMC OpenManage Integration for VMware vCenter (OMIVV) supports ESXi deployment on bare-metal servers. This technical white paper illustrates the process of an ESXi installation and best practices to follow during the deployment process.

January 2021

Revisions

Date	Description
January 2021	Initial release

Acknowledgments

This paper was produced by the following:

Authors:

Kavyashree Ramakrishna - Test Engineer2, Server, and Infrastructure Solutions

Anand Changegowda – Software Senior Engineer, Server, and Infrastructure Solutions

Atanu Sikder - Software Senior Engineer, Server, and Infrastructure Solutions

Support: Swapna M, Technical Content Developer 2, Information Development

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

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

Copyright © January 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Re	visions	5	2
Ac	knowle	edgments	2
Co	ntents		3
Те	rminolo	ogy	5
Ex	ecutive	e summary	6
1	Introd	duction	7
2	Bare-	-metal discovery	8
	2.1	Auto discovery	8
	2.2	Manual discovery of bare-metal servers	8
	2.2.1	Single node discovery	9
	2.2.2	Multiple nodes discovery without exclusion	9
	2.2.3	Multiple nodes discovery with exclusion	11
	2.3	Discovery jobs	12
	2.4	Discovery performance	12
3	Creat	te an ISO Profile	13
	3.1	Deploy an ISO profile	14
	3.2	Select installation target	14
	3.3	Select Host Credential Profile	16
	3.4	Configure network	18
4	Best	practices for OS deployment	21
	4.1	Customized ISO images	21
	4.2	Lifecycle Controller busy	21
	4.3	Disconnected network interfaces	22
	4.4	First boot disk selection	23
	4.5	Correct boot sequence	25
	4.6	Boot sequence enablement	26
	4.7	Virtual Disk should be created for controller (PERC or BOSS)	26
	4.8	In Multi-NIC environment, selection of right OMIVV network selection is important	27
	4.9	OMIVV does not support software controller	28
	4.10	Ensure while providing static network details, valid network details are entered	28
	4.11	Minimum requirements for ESXi installation	28
	4.12	vCenter license for adding host to vCenter after deployment	29
	4.13	OMIVV does not support installation of ESXi on virtual machine	29
	4.14	Ensure that OMIVV license for host is available	29

5

4.15	ESXi password requirements	29
4.16	Port information for ESXi installation	29
4.17	ESXi deployment failure	29
4.18	When NPAR is enabled on target node and disabled in System Profile, ESXi deployment fails	30
4.19	Sometimes MAC address is populated during ESXi deployment	30
4.20 mainte	After ESXi deployment, OMIVV fails to add ESXi host to vCenter or failed to add host profile or enter enance mode is failed for host	30
4.21	After performing ESXi deployment, host is either disconnected or not responding state	30
4.22 netwo	Deployment job times out when network interface card (NIC) of OMIVV is not connected to the ESXi host rk	30
4.23	General failure	30
4.24	Inaccessible network shares (OSD47, OSD17)	31
4.25	Auto discovered systems are displayed without model information in Deployment wizard	31
4.26	Server pending reboot	31
4.27	Boot order is not guaranteed in UEFI mode	31
4.28	Host credential profile having AD credentials are not listed in deployment page	31
4.29 versio wizard	Even though ESXi deployment is successful, inventory fails when selected ISO profile has ESXi 6.5 (or ean of the set in deployn n) image and host credential profile have different or no ESXi password other than which is set in deployn the set is a set in deployn the set in deployn the set in deployn the set in the set is a set in deployn the set in the set in the set is a set in the set in the set is a set in the set is a set in the set is a set in the set in the set is a set is a set in the set is a set is a set in the set is a set in the set is a set is a set in the set is a s	arlier nent 32
4.30	After performing an ESXi deployment, existing iDRAC jobs are not in seen	32
4.31	After performing upgrade to latest version, scheduled ESXi deployment job fails	32
4.32	Discovered user used during bare-metal discovery is disabled after performing ESXi deployment	32
4.33	ESXi deployment is blocked when secure boot is enabled	32
4.34	Deployment fails when other OS (RHEL or WINDOWS) is previously installed	32
Conclu	usion	33

Terminology

Terminology	Description
OMIVV	OpenManage Integration for VMware vCenter
iDRAC	Integrated Dell Remote Access Controller
UEFI	Unified Extensible Firmware Interface
OS	Operating System
SATA	Serial Advanced Technology Attachment
OOB	Out-of-band
CIFS	Common Internet File System
NFS	Network File System
BIOS	Basic Input/Output System
FC	Fiber Channel
MAC	Media Access Control
BOSS	Boot Optimized Storage Solution
NVMe	Non-Volatile Memory Express
SSD	Solid State Drive
CPU	Central Processing Unit
HDD	Hard Disk Drive
RAID	Redundant Array of Independent Disks
USB	Universal Serial Bus
NIC	Network Interface Controller
AHCI	Advance Host Controller Interface
RAM	Random Access Memory
SD	Secure Digital
DHCP	Dynamic Host Configuration Protocol
FQDN	Fully Qualified Domain Name
DNS	Domain Name System
PERC	PowerEdge RAID Controller

Executive summary

OpenManage Integration for VMware vCenter (OMIVV) provides an ability to install an ESXi instance on baremetal servers. The hosts can be onboarded to vCenter server and managed using OMIVV after successful inventory.

This technical white paper describes how to perform an ESXi deployment and best practices to follow when performing an ESXi deployment.

Introduction

1

The core of the vSphere product suite is the hypervisor (ESXi). A hypervisor is a piece of software that creates and runs virtual machines.

ESXi provides a virtualization layer that abstracts the CPU, storage, memory, and networking resources of the physical host into multiple virtual machines. The applications running in virtual machines can access these resources without direct access to the underlying hardware.

An ESXi deployment is an essential step during any data center setup. The manual process of deploying an ESXi on all servers becomes tedious and time-consuming.

OpenManage Integration for VMware vCenter (OMIVV) reduces the time of an ESXi deployment by automating the process and provides an option to perform deployment on several servers at once without user intervention during the entire process making it as a zero-touch deployment.

On successful deployment of an ESXi on a server, the ESXi host is onboarded to the vCenter and inventoried automatically by OMIVV.

2 Bare-metal discovery

Discovery is the process of adding supported bare-metal server. After a server is discovered, you can use it for system profile and an ISO profile deployment.

Prerequisites:

- The network connectivity from the iDRAC of bare-metal server to the OMIVV virtual machine is required.
- The hosts with existing ESXi instances should not be discovered into OMIVV. Add hosts to the vCenter and host credential profile.
- To deploy ESXi on SD card and to use system profile features in 12G and 13G PowerEdge servers, ensure that iDRAC 2.50.50.50 and later is installed.

OMIVV supports discovering bare-metal servers using auto discovery and manual discovery.

2.1 Auto discovery

Auto discovery is an iDRAC feature that enables newly installed servers to be discovered automatically by OMIVV. Remote management console IP address must be configured.

Prerequisites:

Before attempting to discover the PowerEdge bare-metal servers, ensure that OMIVV is installed. The PowerEdge servers with iDRAC Express or iDRAC Enterprise can be discovered into a pool of bare-metal servers.

For auto discovery to function, the following conditions must be met in your environment:

- Power-ensure that you connect the server to the power outlet.
- Network connectivity—ensure that the iDRAC of the server has network connectivity and communicates with the provisioning server over port 4433. You can obtain the IP address of provisioning server by using a DHCP server or manually specifying it in the iDRAC configuration utility.
- Extra network settings—To resolve DNS names, enable Get DNS server address in DHCP settings.
- Provisioning service location—ensure that iDRAC knows the IP address or hostname of the provisioning service server. OMIVV supports auto discovery with provisioning server functions only.

Note: iDRAC9 auto discovery and iDRAC9 push notifications are not supported.

For more information, see the <u>OMIVV User's Guide</u>.

- Account access disabled—if there are any iDRAC accounts with administrator privileges, first disable them from the iDRAC web console. Once auto discovery completes successfully, the administrative iDRAC account is reenabled with deployment credentials that are entered on the Settings page. For more information about deployment credentials, see the <u>OMIVV User's Guide</u>.
- Auto discovery enabled—ensure that the iDRAC of the server has auto discovery enabled so that the
 auto discovery process can begin. For more information, see the <u>OMIVV User's Guide</u>.

2.2 Manual discovery of bare-metal servers

You can manually add a bare-metal server that is not added using the auto discovery process. Once added, the server is displayed in the list of servers on the **Bare-metal Servers** page of OMIVV. To add the bare-metal servers, on the OMIVV home page, click **Compliance and Deployment** >

Deployment > DISCOVER.

You can create the discovery job to discover range of servers simultaneously. You can configure maximum of 1024 servers in a single discovery job.

Class C IPs are supported and difference in last octet values of start, and end IP are considered to find range of IPs between them. You can configure a maximum of 1024 nodes in a single discovery.

Few example configurations of discovery job are shown in the following sections:

2.2.1 Single node discovery

To discovery a single server in a job:

- 1. Enter only Start IP with all four octets of an IP.
- 2. Enter the credentials manually or select the option **Use Deployment Credentials** to use the settings configured under **Settings>Deployment Credentials**.

iscovery Job Name	SingleNodeDiscovery			
iscovery Job Description	SingleNodeDiscovery			
DO RANGE DATA DELETE			Sear	ch
Start IP ()	End IP 🕼	Exclusion List ()	Use Deployment Credentials	Username 🕕
100.100.100.1	EndOctet	Exclusion List		
			Ranges per page10 _ V	1 - 1 of 1 Range

Figure 1: Single server discovery

2.2.2 Multiple nodes discovery without exclusion

To discover all the servers within a given range:

- 1. Enter all octets of **Start IP**.
- 2. Enter only last octet of End IP.

The following is the sample configuration to discover all servers the IPs from 100.100.100.1 to 100.100.100.50:

	MultipleNodeDiscoveryWith	houtExclusion		
scovery Job Description	MultipleNodeDiscoveryWi	thoutExclusion		
DD RANGE DATA DELETE			Searc	th
Start IP ()	End IP 🕦	Exclusion List ()	Use Deployment Credentials	Username 🕢
100.100.100.1	50	Exclusion List		

Figure 2: Range server discovery

Each IP range in a discovery job can contain a maximum of 256 IPs (Example:192.168.1.0-255).

To discover 1024 IPs in a discovery job, multiple IP ranges must be configured such that the total of all IPs in all the defined ranges does not exceed 1024.

The following screenshot shows the sample configuration for the same with four IP ranges with each range containing 256 IPs.

iscov	ery Job Name	Discovering 1024 IPs				
iscov	ery Job Description	Discovery Job Description				1
DD R	ANGE DATA DELET	E			Search	
	Start IP 🕔	End IP	Exclusion List 🛈	Use Deployment ① Credentials	Username 🛈	Ì
-	152.100.1.0	200		U	1001	-
	192.168.2.0	255	Exclusion List		root	
	192.168.3.0	255	Exclusion List	0	root	
	10010010	000	Provide statistical for the last	-		•
				Ranges per page	10 1-4 of 4 f	Ranges

Figure 3: Discover 1024 IPs.

2.2.3 Multiple nodes discovery with exclusion

The following is the sample configurations to discover all the IPs from 100.100.100.100.1 to 100.100.100.50 excluding IPs from 100.100.100.25 to 100.100.100.30 and also from 100.100.100.40 to 100.100.100.45.

scorery see rearre	Discovery			
iscovery Job Description	Discovering IP Range			
DD RANGE DATA DELETE			Sec	arch
Start IP	End IP	Exclusion List	Use Deployment Credentials	Username 🕥
100.100.100.1	50	25-30,40-45		

Figure 4: Range server discovery with exclusion.

To discover few sets of IPs in a range with a different credential, you can add a separate range for the same and give separate credentials.

The following is the sample configuration to discover IPs from 100.100.100.100.1 to 100.100.100.100.100 except 100.100.100.50 to 100.100.100.70 to be in different credential configuration:

Disco	over Bare-Metal S	erver ()			0
Discov	very Job Name	Discovery			
Discov	very Job Description	Discovering IP Range			
ADD R	RANGE DATA DELETE			4	Search
	Start IP 🕦	End IP 🕔	Exclusion List ()	Use Deployment Credentials	D Username ()
	100.100.100.1	100	50-70		root
	100.100.100.50	70	Exclusion List		root
	nn Now 🕢 🔿 Run Late	· @		Ranges per page	> 1 - 2 of 2 Ranges
 <td>100.100.100.50</td><td>70 7 (1)</td><td>Exclusion List</td><td>Ranges per page. 10</td><td>root</td>	100.100.100.50	70 7 (1)	Exclusion List	Ranges per page. 10	root

Figure 5: Range server discovery with separate credential.

2.3 Discovery jobs

After you submit the discovery job, you can track the status of the job at **OMIVV->Jobs->Discovery Jobs** page. A single entry is available for every server in the range and consolidated status is shown against the job.

To purge jobs older than a given date with the **Successful** or **Failed** or **Canceled** status, click **CLEAR COMPLETED**.

eployment		Discovery Jok	/5				
Niscovery		CLEAR COMPLETED					
irmware Updates	>	Name	Description	Scheduled Time	↓ Status	Collection Size	Progress Summary
ystem Lockdown Mode		MultipleNodeDiscovery_	MultipleNodeDiscovery_	07/28/2020 10:35:34 PM (GMT+05:30)	In Progress	50	Running job for 50 host(s
rift Detection							1-10
rventory	>				07/28/2020 10:35:3	84 PM (GMT+05	:30)
Varranty	>	Discovery Job Details for N	IultipleNodeDiscoveryWitho	utExclusion			
		IDRAC IP	Status	Details Start Date	and Time	[1	End Date and Time
		100.100.100.1	Waiting	07/28/20	20 10:35:35 PM (GMT+05:	30)	
		100.100.100.10	Waiting	07/28/20	20 10:35:35 PM (GMT+05	30)	
		100.100.100.11	Waiting	07/28/20	20 10:35:35 PM (GMT+05:	30)	
		100.100.100.12	Waiting	07/28/20	20 10:35:35 PM (GMT+05:	30)	
		100.100.100.12 100.100.100.13	Waiting In Progress	07/28/20	20 10:35:35 PM (GMT+05: 20 10:35:35 PM (GMT+05:	30) 30)	
		100.100.100.12 100.100.100.13 100.100.100.14	Waiting In Progress Waiting	07/28/20 07/28/20 07/28/20	20 10:35:35 PM (GMT+05: 20 10:35:35 PM (GMT+05: 20 10:35:35 PM (GMT+05:	30) 30) 30)	

Figure 6: Discovery Jobs

2.4 Discovery performance

On a one Gbps link with direct iDRAC network, an IP subnet containing 256 Dell EMC servers take about five to six minutes for the discovery.

3 Create an ISO Profile

An ISO profile is a template in OMIVV that points to a specific ESXi ISO image. It is required to deploy an ESXi installation on a server. An ISO profile requires Dell EMC customized ISO file location on an NFS or CIFS share.

A test connection must be performed in order to save an ISO profile successfully.

Test connection is performed to check the following:

- The CIFS or NFS share is accessible with the provided username and password.
- The ISO image is present at the location provided.

OMIVV supports:

- Server Message Block (SMB) version 1.0 and SMB version 2.0 based CIFS shares
- Windows and Linux-based NFS shares

CIFS share requires username and password for accessing the ISO image. Invalid credentials or missing ISO image renders test connection failed, and ISO profile cannot be saved.

NFS share does not require username and password. It requires the NFS daemon to listen on ports 2049, 4001–4004.

Choose the Reference	e ISO Path and Version (j)
\\100.100.10.237\\mages\ES	X OS images\Esxi6.7 U3-RTM\6.7 U3 Ga\14G\VMware-VMvisc
User Name	sped\devtest
Password	Password
Verify Password	Verify the password entered
ESXi Base Version	ESXi 6.7
	CANCEL BACK FIN

Figure 7: Create an ISO profile

Test Settings		
(i) ISO File Path		
(i) ISO File Path Authentication		
BEGIN TEST		
	CANCEL	BACK

Figure 8: Test connection

3.1 Deploy an ISO profile

To perform an ISO profile deployment (ESXi installation), ensure that you have:

- Discovered bare-metal server
- Created an ISO Profile
- Created Host Credential Profile (the profile used to store the iDRAC credentials and ESXi credentials, which are optional for 6.7 or higher)

OMIVV supports only VMware ESXi Dell EMC customized ISO images installation on target bare-metal servers.

Ensure that bare-metal servers have met the following requirements in your environment:

- Collect System Inventory on Reboot (CSIOR) is enabled.
- Virtualization Technology (VT) is enabled.
- Based on the required installation target, set HDD, SSD, Virtual disk, IDSDM, or BOSS to first boot disk.

3.2 Select installation target

During bare-metal discovery, OMIVV determines the available targets on the server for an ESXi deployment.

The following are the supported targets:

- First boot disk: Hard Disk (HDD), Solid-State Drive (SSD), or Virtual disk created by RAID controllers
- Internal Dual SD Module (IDSDM)
- BOSS module

Notes: VMware supports ESXi installation on SD cards for 6.7 U3 and earlier versions.

Based on the presence of the modules supported, an appropriate target is available for you to select during deployment.

Installation Target Installation to an Internal Dual SD Module is disabled because none of the selected servers have an Internal Dual SD Module. Installation to a BOSS module is disabled because none of the selected servers have a BOSS module. First boot disk Internal Dual SD Module (IDSDM) BOSS

Figure 9: Installation targets

You can select the multiple servers at a time for an ESXi deployment. Installation target selection is a onetime operation for all the servers that are selected for the deployment job.

If one or more servers have IDSDM or BOSS module, applicable targets are available for installation target selection.

In this scenario, if IDSDM or BOSS is selected as installation target, the servers on which the selected target is not present will be skipped from performing deployment. This is notified in the target selection page.

There is also an option to not to skip the servers which do not have selected target present.

You can force deploy the an ESXi on First boot disk and ensure that ESXi is deployed on all the selected servers.

Note: OS deployment is blocked from iDRAC firmware version 4.00.00.00 to 4.32.20.00 when secure boot is enabled.

◯ First boot disk
O Internal Dual SD Module (IDSDM)
O BOSS If any of the selected servers do not support an IDSDM or BOSS module, or if IDSDM or BOSS is not installed in the server(s) during deployment then the deployment operation on those servers is skipped. To deploy hypervisor on the first boot disk of these servers, select this check box.
Deploy the hypervisor to the first boot disk for servers that do not have an available Internal Dual SD Module or Boss.
Note:The first boot disk on the system could be a Hard Disk(HDD), Solid-State Drive (SSD) or Virtual disk created by RAID controllers

Figure 10: Installation targets with options

3.3 Select Host Credential Profile

From OMIVV 5.2 onwards, selection of Host Credential Profile (HCP) and providing root password is mandatory as same is used during setting ESXi password.

The following are applicable for root user during deployment:

- If an ISO profile has ESXi 6.5 and earlier version, the password that is entered in selected host credential profile is used.
- For ESXi 6.7 and later version, the password that is entered in the deployment wizard is used.
- For ESXi 6.5 and earlier version, if password is not entered in host credential profile, the password that is entered in deployment wizard is used. Update the ESXi credentials at host credential profile to ensure that inventory is run successfully after ESXi deployment.

OMIVV provides two options while selecting the host credential profile. Only one host credential profile can be used for all selected bare-metal servers or different host credential profiles can be used for all selected bare-metal servers. Select an appropriate option and enter root password. Entering root password is mandatory.

Note: Confirmation password (Verify Password) is not available, if different host credential profiles are used for all selected bare metal servers. In this case, ensuring valid password is entered is important.

Select Host Cr Do you want to use • Yes O No	edential Profile the same host creder	itial profile for all hosts?	?
Choose a Host Credential	Profile	Select Host Credential Profile	~
Host Credential			
User Name	root		
Password	Password		
Verify Password	Verify Password		
			- 1
			- 1
			_

Select Ho	st Credenti	al Profile		
Do you want	to use the sam	e host credential	profile for all hosts?	
○ Yes ○ No Set individual Ho	st Credential Profi	le for each server 🚯		
Service Tag	Model	IDRAC IP	Host Credential Profil e	Root Passwon
4CT5G2S	PowerEd	100.100.20.119	Select Host Cr€ ~	Password
4				•
	_	_		



3.4 Configure network

The Configure Host Network Settings page allows you to configure:

- OMIVV appliance NIC connected to host which is used for the deployment job
- Connected NIC of the server
- DHCP settings
- Static network configuration requires hostname, DNS, Subnet, Gateway, Host IP, and FQDN
- VLAN





Networking		
Use VLAN Use DHCP		
Preferred DNS Server	Preferred DNS Server	0
Alternate DNS Server	Alternate DNS Server	
IP Address	IP Address	0
Subnet Mask	Subnet Mask	0
Default Gateway	Default Gateway	0

Figure 12: Static network Configuration

When more than one server is selected for deployment, all the servers are listed in network configuration page and individual server can be configured with different settings.

Apply Settings to All Servers allows you to retain same settings across all servers, excluding Fully Qualified Host Name and IP Address.

To disable all network and hostname fields, select the **Use DHCP** check box. Only appropriate NIC for management tasks and OMIVV appliance NIC connected to host must be selected.

Fully Qualified Host Name	
NIC for Management Tasks	QLogic 577xx/578xx 10 Gb Ethernet BCM57810 💙
Appliance NIC Connected to Host Networking	Wired connection 1 - 100.96.50.45 V
🗌 Use VLAN 🗹 Use DHCP	
Preferred DNS Server	
Alternate DNS Server	
IP Address	
Subnet Mask	

Figure 13: DHCP network Configuration

To configure appropriate VLAN, select the **Use VLAN** checkbox.



Figure 14: VLAN Configuration

4 Best practices for OS deployment

Below section describes several best practices to follow for seamless hypervisor installation.

4.1 Customized ISO images

Do not install raw VMware ESXi images on target bare-metal servers. Dell EMC hypervisor engineering team certifies customized ESXi images for individual platform or category of Dell EMC servers. This also includes several drivers or addons to meet specific solution requirement.

You can download ISO images from <u>https://www.dell.com/support/home</u> by providing Service Tag of a server.

Products Solutions Services Support Community	
Product Support Knowledge Base Warranty & Contracts Service Requests & Dispatch Status Orde	r Support Contact Support
PowerEdge	R740
Service Tag: 11BZ9P2 Warranty:	Express Service Code: 2257369814 Log in to add nickname
Product Details: View sys	Citrix XenServer 7.1
< <u>Change product</u>	Red Hat® Enterprise Linux 6 Red Hat® Enterprise Linux 7 Red Hat® Enterprise Linux 8
OVERVIEW DRIVERS & DOWNLOADS DOCUMEN	SUSE Linux ES 12 SuSE Linux ES 15 Ubuntu Server 16.04 LTS Ubuntu © Server 18.04 Ubuntu Server 18.04 LTS
\bigcirc Find a driver for your PowerEdge R740	VMvare ESX 6.0 VMvare ESX 6.5 VMvare ESX 6.7 VMvare ESX 7.0
Keyword	Windows Server 2012 K2 Windows Server 2016 Windows Server 2019 LTSC
Enter a driver name or keyword	VMWare ESXI 7.0 🗸
Category	Format

Figure 15: Download Dell EMC certified ISO image from support.dell.com.

4.2 Lifecycle Controller busy

OMIVV uses WSMAN command to trigger an ESXi deployment. This command is processed by Lifecycle Controller (LC) embedded on iDRAC. If iDRAC is busy in performing other operation, this command fails. Ensure that LC is not busy in executing other operation. Reset iDRAC to proceed with an ESXi deployment job.

To reset in iDRAC9, log in to iDRAC and then go to **More Actions** \rightarrow **Reset iDRAC** or **Maintenance** \rightarrow **Diagnostics** \rightarrow **Reset iDRAC**.

To reset iDRAC7 or 8, log in to iDRAC and then go to **System Property** \rightarrow **Quick Launch Tasks** \rightarrow **Reset iDRAC** or **Overview** \rightarrow **Server** \rightarrow **Troubleshooting** \rightarrow **Diagnostics** \rightarrow **Reset iDRAC**.

Dashboard	System V	🛢 Storage 🗸	\blacksquare Configuration \checkmark	Maintenance	idr. 🍳	AC Settings \smallsetminus
lainten	ance					
Lifecycle Log	Job Queue	System Update	System Event Log	Troubleshooting	Diagnostics	SupportAssist
Command*						

Figure 16: Reset iDRAC

4.3 Disconnected network interfaces

Network traffic for an ESXi deployment is navigated through one of the selected Ethernet adapters on the **Configure Host Network Settings** page.

If the selected NIC is down or not connected to proper gateway (NICs which are reachable to ESXi network and iDRAC network (if they are not present in same network)), ESXi deployment job times out. Ensure to pick properly configured NIC of iDRAC.

Ensure that LC is not busy in executing other operation—such as updates, or any other functions you may be working before deployment. If needed due to a failed attempt, you can reset iDRAC manually to proceed with an ESXi deployment job.

To confirm the NIC connectivity in iDRAC, you can go to iDRAC console and check the NIC status (Up/Down).



Figure 17: Select connected NIC from deployment wizard

4.4 First boot disk selection

First boot disk generally denotes the first boot device that is mentioned in the Boot Sequence (BIOS or UEFI) of BIOS settings.

For example, in the following screenshot, IDSDM is mentioned in boot sequence. IDSDM is not classified as first boot device because only HDD, SSD, and VD are classified as first boot disk.

If you want to install an ESXi on IDSDM, you must select correct target that is IDSDM and not first boot disk.

System BIOS

System BIOS Settings • Boot Settings • UEFI Boot Settings

UEFI Boot Sequence

Internal SD: VMware ESXi

PXE Device 1: Embedded NIC 1 Port 1 Partition 1

AHCI Controller in Slot 3: EFI Fixed Disk Boot Device 2

Boot Option Enable/Disable

- Internal SD: VMware ESXi
- PXE Device 1: Embedded NIC 1 Port 1 Partition 1
- AHCI Controller in Slot 3: EFI Fixed Disk Boot Device 2

Figure 18: Boot Sequence denotes IDSDM as first boot device

ele	ct Deployment Options
Inst	allation Target
() F	First boot disk
0	nternal Dual SD Module (IDSDM)
If a BC on se	BOSS any of the selected servers do not support an IDSDM or BOSS module, or if IDSDM or DSS is not installed in the server(s) during deployment then the deployment operation in those servers is skipped. To deploy hypervisor on the first boot disk of these servers, lect this check box.
	Deploy the hypervisor to the first boot disk for servers that do not have an available Internal Dual SD Module or Boss.
Note or V	e:The first boot disk on the system could be a Hard Disk(HDD), Solid-State Drive (SSD) irtual disk created by RAID controllers

Figure 19: OMIVV does not classify IDSDM as first boot disk

4.5 Correct boot sequence

Ensure that correct boot sequence is selected on the **System BIOS Settings** page. The selection should match the disk selection.

For example, in the following screenshot, Boot sequence for BOSS disk (AHCI) is not appearing first in the list. As a result, after successful installation, BIOS will not load the ESXi from BOSS card and system would behave as ESXi is not installed. This results in the deployment job timing out and failing.



Figure 20: UEFI Boot Sequence



Figure 21: BOSS is selected as installation Target.

4.6 Boot sequence enablement

Ensure that an appropriate Boot Sequence is selected but not cleared from Boot Option of System BIOS Settings else BIOS would not load ESXi after installation.

Boot Option Enable/Disable

- ✓ Integrated Storage Controller 1: VMware ESXi
- Integrated Storage Controller 1: EFI Fixed Disk Boot Device 1
- PXE Device 1: Integrated NIC 1 Port 1 Partition 1
- PXE Device 2: Integrated NIC 1 Port 3 Partition 1
- 🔽 Unavailable: VMware ESXi
- AHCI Controller in Slot 1: EFI Fixed Disk Boot Device 1

Figure 22: Boot Sequence should be enabled.

4.7 Virtual Disk should be created for controller (PERC or BOSS)

To detect local and remote disks of the server, creation of virtual disk for ESXi installation is necessary.

For more information about creation of virtual disk, go to <u>https://www.dell.com/support/article/en-</u> in/sln132533/how-to-initialize-and-create-a-virtual-disk-with-a-dell-poweredge-raid-controller-perc?lang=en

(any existin * Contains a VMFS # Claimed by VMwa	ig VMFS-3 will be partition ire vSAN	automatically u	ipgraded to	VMFS-5)
Storage Device Local: (none) Remote: (none)				Capacity
(Ecc) Cappel	(F1) Details	(F5) Refresh	(Enter)	Continue

Figure 23: When virtual disk is not created

(any existin * Contains a VMFS # Claimed by VMwa	g VMFS-3 will b partition re vSAN	e automatically (upgraded to VMFS-5)
Storage Device			Capacity
Local: DELL PERC Remote: (none)	H730P Mini (na	ia . 644a8420075328(3026d76) 232.38 GiB
(Esc) Cancel	(F1) Details	(F5) Refresh	(Enter) Continue

Figure 24: When virtual disk is created

4.8 In Multi-NIC environment, selection of right OMIVV network selection is important

Host can have either iDRAC and vCenter management NIC in the same network or in the two distinct networks. The ISO image can be saved in any of the networks. The ESXi deployment wizard displays both the OMIVV networks. Ensure that you select the correct vCenter network and OMIVV network applicable to the environment.

Deployment Wizard	Configure Host Network S	settings	?
1 Welcome	✓ BKM7F2S (Missing Identity Informa	APPLY SETTINGS TO ALL SERVERS	
2 Select Server (s)	General Information Service Tag : BKM7F2S	Model : PowerEdge M620	
3 Select Deployment Options	Host Name and NIC		
4 Select Host Credential Profile	Fully Qualified Host Name	Fully Qualified Host Name	
5 Configure Host Network Settings	NIC for Management Tasks	QLogic 577xx/578xx 10 Gb Ethernet BCM57810 $^{\vee}$	
6 Schedule Deployment Job	Appliance NIC Connected to Host Networking Use VLAN Use DHCP	Private network - 172.20.5.28 V Private network - 172.20.5.28 Public network - 100.100.9.90	
	Preferred DNS Server	Preferred DNS Server	
		CANCEL BACK NE	хт
_			

Figure 25: Selection of right OMIVV network during ISO profile deployment

4.9 OMIVV does not support software controller

Onboard SATA controller for Dell EMC PowerEdge servers provides an option to create RAID. The software RAID LUNs are not supported because VMware ESXi does not carry supported drivers. ESXi does not support any software RAID functions. Due to this, OMIVV does not support ISO deployment on software controller.

For more information, see VMware vSphere 6 on Dell EMC PowerEdge Servers Release Notes

4.10 Ensure while providing static network details, valid network details are entered

OMIVV provides an option for user to enter static network details for ESXi. During which a fully qualified domain name for the hostname is mandatory. The use of " localhost " for the FQDN is not supported. The FQDN is used when adding the host to vCenter.

Create a DNS record that resolves the IP address with the FQDN. Configure the DNS server to support reverse lookup requests. The DHCP reservations and DNS host names must be in place and verified before the deployment job is scheduled to run. It is mandatory to enter preferred DNS server, alternate DNS server, IP address, subnet mask, and default gateway.

4.11 Minimum requirements for ESXi installation

Following are the minimum requirements for ESXi installation:

- A host machine with at least two CPU cores
- A minimum of 4 GB of physical RAM. Provide at least 8 GB of RAM to run virtual machines in typical production environments.
- A boot disk of at least 8 GB for USB or SD devices, and 32 GB for other device types such as HDD, SSD, or NVMe. A boot device must not be shared between ESXi hosts.
- Virtualization Technology (VT) flag in BIOS is enabled.
- OMIVV System profiles can be included in deployment profiles to prepare system for OS deployment. Configurations like boot settings and virtual disk configurations along with other settings can be performed using system profiles deployment. For more information about system profile deployment, see <u>OMIVV User's Guide</u>.

Note: The OS deployment is blocked from iDRAC firmware version 4.00.00.00 to 4.32.20.00 when secure boot is enabled.

For more information about installing ESXi, see the following documents:

https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-70-installation-setup-guide.pdf

https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-67-installation-setup-guide.pdf

https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-installation-setup-guide.pdf

4.12 vCenter license for adding host to vCenter after deployment

OMIVV installs ESXi on the required bare-metal server and adds the same to registered vCenter. While performing the addition of host to vCenter, vCenter should have valid license so that host gets added successfully.

4.13 OMIVV does not support installation of ESXi on virtual machine

OMIVV supports ESXi installation only on OMIVV supported servers. For more information about supported servers, see <u>OMIVV 5.2 compatibility Matrix</u>.

4.14 Ensure that OMIVV license for host is available

During deployment, once ESXi installation is successful, host gets added to vCenter and to the previously selected host credential profile. While adding to host credential profile, OMIVV license is consumed. Hence, user must ensure that enough OMIVV license is available.

4.15 ESXi password requirements

By default, you have to include a mix of characters from four-character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash when you create a password. By default, password length is more than 7 and less than 40. Passwords cannot contain a dictionary word or part of a dictionary word.

4.16 Port information for ESXi installation

Minimum port requirements for OMIVV appliance and managed nodes are mentioned in OMIVV compatibility matrix.

4.17 ESXi deployment failure

Whenever ESXi deployment fails, ensure that:

- The ISO location (NFS path) and staging folder paths are accurate.
- The NIC selected during assignment of server identity is accessible by the virtual appliance.
- You select the management NICs based on the network connectivity to the OMIVV.
- The network information provided (including subnet mask and Default Gateway) is accurate if you are using static IP address. Also, ensure that the IP address is not already assigned on the network.
- At least one Virtual Disk, or IDSDM, or BOSS is detected by the system.

4.18 When NPAR is enabled on target node and disabled in System Profile, ESXi deployment fails

An ESXi deployment fails when a system profile with a disabled NIC Partitioning (NPAR) is applied on a target machine. Here, NPAR is enabled on the target node and only one of the partitioned NIC, except partition 1 is selected as the NIC for the management tasks during the deployment process through the deployment wizard.

To overcome this, ensure you are changing the NPAR status using system profile during deployment, ensure that you select only the first partition for management network in the deployment wizard.

4.19 Sometimes MAC address is populated during ESXi deployment

An ESXi deployment fails on PowerEdge Servers when the iDRAC does not populate the MAC address for the selected NIC port.

Update the respective NIC firmware and iDRAC firmware to the latest version and ensure that the MAC address is populated on the NIC port.

4.20 After ESXi deployment, OMIVV fails to add ESXi host to vCenter or failed to add host profile or enter maintenance mode is failed for host

After ESXi deployment, OMIVV queries vCenter to perform the host actions (Add host, Add Host Profile, or Enter Maintenance Mode).

If the query does not receive a response within two minutes, the specific action on vCenter is timed out, and a message is displayed in the task history indicating that the communication failure. However, at times, the vCenter query operations are successful. Hence, manually adding host IP mentioned in VMware task history works.

4.21 After performing ESXi deployment, host is either disconnected or not responding state

ESXi host fails to send heartbeat packets to vCenter because its DNS is not properly configured to lookup FQDN of the vCenter.

Complete the following tasks:

- 1. Remove the ESXi host from the vCenter inventory.
- 2. Add the host using the Add Host wizard in vCenter.
- 3. Create a host credential profile in OMIVV and run the inventory.

4.22 Deployment job times out when network interface card (NIC) of OMIVV is not connected to the ESXi host network

An ESXi deployment has dependency on the selection of NIC. If the correct NIC is not selected, ESXi deployment job times out.

In the Deployment wizard, select an appropriate **Appliance NIC connected to Host** from **Configure Host Settings.** This is required to reach ESXi network during ESXi installation process.

4.23 General failure

OMIVV uses WSMAN command Boot to Network ISO to deploy an ESXi on the target bare-metal servers.

If the WSMAN command fails and gives OSD2 (general failure or an unknown error occurred), reset iDRAC and rerun the command.

For more information, see Event and Error Message Reference Guide.

4.24 Inaccessible network shares (OSD47, OSD17)

iDRAC consumes network share of OMIVV /nfsstage to mount the ISO images. But if nfs daemon is not running with the required ports (2049, 4001–4004) in OMIVV, mount operation may fail. Firewall might be enabled and is preventing access to the share. You must ensure that the firewall is disabled, and nfs daemon is listening on the correct ports.

This issue occurs if the network share (where the ESXi ISO image is present) is corrupted. Retry after creating a new CIFS or NFS share and associate with a new ISO profile.

Error codes (OSD17, OSD47) indicates network errors which prevents iDRAC access to the ISO file.

4.25 Auto discovered systems are displayed without model information in Deployment wizard

This usually indicates that the firmware version that is installed on the system does not meet the recommended minimum requirements. Sometimes, firmware version is not reflected even after updating the iDRAC or any firmware to the minimum requirements. This can be resolved by performing cold booting the system or resetting server or iDRAC.

The newly enabled account on the iDRAC must be disabled and auto discovery should be reinitiated to provide model information and NIC information to OMIVV.

4.26 Server pending reboot

Sometimes, firmware update is scheduled on the server and the update is reflected on the server after reboot. The reboot does not happen immediately. ESXi deployment job may fail if the server is pending for reboot. User can reboot the server and then reschedule or rerun the job.

4.27 Boot order is not guaranteed in UEFI mode

In the UEFI mode, boot sequence option behaves in a different way. The newly created boot label is appended (queued) rather than stacked. Even when an ESXi installation is completed, server boots to first boot label. If any other bootable device is available, it boots to that image rather than newly installed image.

OMIVV supports only bare-metal server where nothing is preinstalled in UEFI mode.

4.28 Host credential profile having AD credentials are not listed in deployment page

OMIVV does not consider AD credentials during an ESXi deployment. OMIVV does not display any host credential profile in case AD credentials are used for iDRAC or ESXi.

4.29 Even though ESXi deployment is successful, inventory fails when selected ISO profile has ESXi 6.5 (or earlier version) image and host credential profile have different or no ESXi password other than which is set in deployment wizard

OMIVV recommends update the ESXi credentials at host credential profile to ensure inventory is run successfully after ESXi deployment, if password is not entered in host credential profile, the password that is entered in deployment wizard is used.

4.30 After performing an ESXi deployment, existing iDRAC jobs are not in seen

OMIVV clears all iDRAC jobs once ESXi deployment is completed on bare-metal servers.

4.31 After performing upgrade to latest version, scheduled ESXi deployment job fails

Scheduled ESXi deployment jobs of older version of OMIVV are not valid for latest version of OMIVV. When user is using latest version of OMIVV, it is recommended to cancel the scheduled job (which was created in older version) and rediscover the bare-metal server followed by ISO profile creation and new deployment job.

4.32 Discovered user used during bare-metal discovery is disabled after performing ESXi deployment

It is recommended to select the host credential profile whose credentials are same as used during bare-metal discovery. Otherwise, the discovered user gets disabled in iDRAC after ESXi deployment as credentials used in host credential profile is used during the same.

4.33 ESXi deployment is blocked when secure boot is enabled

ESXi deployment is blocked from iDRAC 4.00.00.00 to 4.32.20.00 when secure boot is enabled.

4.34 Deployment fails when other OS (RHEL or WINDOWS) is previously installed

OMIVV deploys an OS on bare-metal servers. If any other hypervisor is already installed, deployment might

fail. Remove OS by deleting virtual disk and recreate it.

5 Conclusion

ESXi deployment consists of multiple steps in OMIVV. These steps have internal or external dependencies. Sometimes, you may not aware of these dependencies which results in deployment failure. This technical white paper describes the best practices and dependencies must be followed to use this feature seamlessly. This can improve the responsiveness of an ESXi deployment feature and reduce customer calls for false positive.