



VXRAIL 8.0.XXX IMPLEMENTATION

DOWNLOADABLE CONTENT

Table of Contents

ESCPXD05510 ~ VxRail 8.0.XXX Implementation	7
ESCPXD05510 ~ VxRail 8.0.XXX Implementation Introduction	7
ESCPXD05510 ~ VxRail 8.0.XXX Implementation On-Demand Lab	8
Course Content Key Identifiers	8
Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters	10
Dell Technologies SolVe	10
Generate VxRail Installation Procedures - Common Selections	11
Generate VxRail Installation Procedures - Standard Cluster Configuration Selections	15
Lab 1: Generate a VxRail Installation Procedure	19
Lab 2: Compare VxRail Configuration Procedures	20
Configure VxRail Network Settings	21
Default Management VLAN IDs on VxRail Nodes	21
Modify Default Management Network VLAN IDs on VxRail Nodes	22
Interaction: Modify Default Management Network VLAN ID	23
Network Access to the VxRail Manager VM	23
Connect Service Laptop or Jump Host	24
Configure VxRail Manager VM Network Settings	26
Lab 3: Configure VxRail Manager VM Network Settings	27
Validate the Network Environment for Deployment	28
Manually Validate ToR Switch Configuration	28
ToR Switch - Confirm VLANs Configured for VxRail Networks	29
ToR Switch - Confirm VxRail Node Port Status	30
ToR Switch - Spanning Tree Protocol Considerations	30
ToR Switch - Link Aggregation on VxRail Node Ports	31
Lab 4: Validate ToR Switch Configuration	32
Manually Validate IP Address Availability and Reachability	32
Confirm DNS Readiness	33

Confirm NTP Server Readiness	34
Firewall Port Configuration	35
Lab 5: Validate IP Address Availability, IP Address Reachability, and DNS Readiness	36
Deploy a Standard VxRail Cluster With vSAN OSA	37
Connect to the VxRail Manager VM	37
VxRail Deployment Wizard Landing Page	37
Software License and Maintenance Agreement	38
Selection of the VxRail Cluster Type	39
Selection of Discovered Resources	40
Network Confirmation	41
Configuration Method	42
Global Settings	43
VMware Virtual Distributed Switch (VDS) Settings	44
VMware vCenter Server Settings	45
Host Settings	46
VxRail Manager Settings	47
Virtual Network Settings	48
Validate Configuration	49
Deploy Configuration	50
Deployment Complete	51
Interaction: Deploy a standard VxRail Cluster with VxRail-managed vCenter and predefined VDS	52
Prepare a Customer-Supplied vCenter Server for VxRail Deployment	52
Lab 6: Prepare the Customer-Supplied vCenter Server	55
VxRail with customer-supplied vCenter Server - Deployment Wizard Settings	56
Global Settings	56
VMware vCenter Server Settings	57
New Custom VDS - Deployment Wizard Settings	58
VxRail Deployment with Existing VDS	60
Existing Custom VDS - Deployment Wizard Settings	61
Lab 7: VxRail Deployment with a Customer-Supplied vCenter Server and	

Custom VDS	63
Deploy a Standard VxRail Cluster With vSAN ESA	64
vSan Storage Architecture	64
vSAN ESA Software Requirements	65
vSAN ESA Hardware Requirements	67
vSAN ESA Drive Requirements	69
Verify vSAN ESA Licensing	71
vSAN ESA Encryption Overview	74
vSAN ESA Encryption Key Providers	75
Using Trusted Platform Module (TPM) With a Native Key Provider	77
Configuring Key Providers on a Customer-Supplied vCenter Server	78
Configuring Key Providers on a VxRail-Managed vCenter Server	79
Interaction: Add a Native Key Provider to the vCenter Server	81
Interaction: VxRail with vSAN ESA deployment with a customer-supplied vCenter Server and using a Native Key Provider.	81
Verify VxRail Cluster Deployment	82
VxRail Manager Plugin for vCenter	82
VxRail Dashboard	83
Verify VxRail Version and vCenter Mode	87
VxRail Updates and Compliance Report	88
VxRail Cluster Health Monitoring Status	89
VxRail Cluster - Physical View	90
VxRail Node - Physical View	90
Lab 8: Verify VxRail Deployment Using VxRail Plugin	98
Perform vSAN Health Check	99
Lab 9: Review vSAN Health	100
Manage VMware Licenses	101
Add VMware Licenses	101
Steps To Assign a Perpetual License	105
Configure vSAN Services	111

ESCPXD05510 ~ VxRail 8.0.XXX Implementation

Enable vSAN Performance Service	111
Lab 10: Enable vSAN Performance Service	113
vSAN Services Space Efficiency Options	114
Enable vSAN Space Efficiency Services	115
Verifying Space Savings From Deduplication and Compression	116
Lab 11: Enable vSAN Space Efficiency	118
vSAN Encryption	118
Key Provider Requirement	120
Enable vSAN OSA Encryption	121
Create vSAN Storage Policies	124
Create vSAN storage policy	124
Change vSAN Datastore Default Storage Policy	129
Lab 12: Create Storage Policy	130
Introduction to vSAN ESA Auto-Policy Management	130
Configure Dell Support Account and Remote Support Connectivity	132
Configure Dell Support Account and Remote Support Connectivity	132
Prerequisites for Remote Support Connectivity	135
Enable Remote Support Connectivity	137
Configure VxRail Manager File-Based Backup	141
VxRail Manager File-Based Backup Workflow Overview	141
VxRail Manager Backup and Restore Script	143
Manual Backup Example	145
Schedule Periodic Backup	146
Copy Recovery Bundle to vSAN Datastore	147
VxRail vSAN Datastore - VxRail Backup Folder	148
Lab 13: Configure VxRail Manager File Based Backup	149
Perform VxRail Software Upgrade	150
VxRail Software Upgrade Overview	150
Enabling vLCM	153
Lifecycle Management Options Comparison	157

ESCPXD05510 ~ VxRail 8.0.XXX Implementation

VxRail Software Upgrade Considerations	158
VxRail Software Upgrade High-Level Process	158
VxRail Software Upgrade Using Local Updates	159
Interaction: Perform VxRail Software Upgrade	162
Perform VxRail Cluster Expansion	163
VxRail Cluster Expansion - Add Node to Same Rack	163
Cluster Expansion - Add Node Procedure	163
Using the VxRail Plugin to Add a Node	164
Add VxRail Hosts Wizard	165
Node Added Successfully	171
Lab 14: Add a node to a VxRail cluster	172
Troubleshoot VxRail Implementations	173
VxRail Implementation Troubleshooting Overview	173
VxRail Implementation Process Troubleshooting Example	174
VxRail Log File Locations	176
VxRail Manager Access	178
Log Files Error Example	179
VxRail Knowledge Base (KB) Articles	180
Searching a Knowledge Base (KB)	181
VxRail Log Collection	182
VxRail Plugin Create Log Bundle	182
VxRail Plugin Download Log Bundle	183
VxRail Manager VM - Log Collection CLI	184
VxRail APIs for Gathering Logs	185
vCenter Server, ESXi, and vSAN Support Bundles	187
Lab 15: Perform Log Collection	189
vSAN Troubleshooting	189
VxRail Cluster - All Issues	190
Investigate vSAN Alarms in Skyline Health	190
Investigate VXR Event Codes	191
vSAN Proactive Tests	192
Investigate vSAN Health Using CLI	194

Node Image Management Tool Overview	196
High-Level Steps for Node Image Management Tool	197
You Have Completed This Content	199

Appendix 201

ESCPXD05510 ~ VxRail 8.0.XXX Implementation

ESCPXD05510 ~ VxRail 8.0.XXX Implementation Introduction

This course presents VxRail Implementation procedures. It covers validation of the network environment, system initialization, post-deployment tasks, cluster expansion, and implementation troubleshooting. A hands-on experience with many key installation procedures is available through the virtual lab: VxRail 8.0.XXX Implementation - On Demand Lab. A limited number of additional procedures are presented via interactive simulations and video demonstrations. This course presents tasks which are available to all implementors. Tasks restricted to Dell partners and employees are available separately. VxRail customers who wish to take this course to self-deploy their VxRail system should contact their Dell account manager for more details about the current customer self-installation process requirements (Specifically, the request for product qualification, RPQ).

By the end of this course, you will be able to:

- Generate a VxRail Installation procedure for use during VxRail implementation.
- Configure and validate the network environment for a VxRail deployment.
- Deploy a VxRail cluster with multiple configurations.
- Verify VxRail Plugin functionality after deployment.
- Check vSAN health and perform post-deployment configurations.
- Perform software version upgrade and perform a VxRail cluster expansion.
- Collect logs to troubleshoot a VxRail implementation.



Tip: If available, resources such as job aids, reference guides, and other supplementary materials can be accessed by clicking the Menu button  and navigating to the Resources tab.

ESCPXD05510 ~ VxRail 8.0.XXX Implementation On-Demand Lab

A separate lab is available to practice the implementation tasks that are presented within this course. Key focus areas include configuring network settings, deploying cluster configurations, cluster expansion, and log collection. The lab tasks should be performed when the lab page appears during the course.

The objectives of the lab are to:

- Configure and validate the network environment settings.
- Deploy and verify the VxRail deployment using VxRail Manager Plugin.
- Review and monitor system status, health, and performance.
- Create a storage policy and configure VxRail Manager file based backup.
- Perform a VxRail cluster expansion and log collection.



Lab Activities: To access the lab environment and perform the lab activities, select the following link as applicable:

Partner/Customer

Internal

Course Content Key Identifiers

This course uses the following guidelines:

- All graphics with gold or no callouts can be selected to enlarge.
- Text appearing in the UI element like wizard titles, window titles, and labels appears in **bold** font.
- Command-line commands appear in *command name* style format. For example, review the output of the *ipconfig* command.
- Definitions appear as a [Glossary Term](#).
- Extra details appear as a hot text element.¹

The following terms are used interchangeably between this course and other documentation:

- VxRail Appliance, VxRail system, and VxRail cluster
- VxRail node, VxRail host, and ESXi host
- Internal vCenter server, which is embedded vCenter server, VxRail vCenter server, and VxRail-managed vCenter server
- Management domain, management workload domain, and Mgmt. WLD
- Virtual infrastructure domain, virtual infrastructure workload domain, VI WLD, tenant workload domain, and tenant WLD

¹ Example of a hot text element used in this course.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

Dell Technologies SolVe

Dell Technologies SolVe is an interactive procedure generator that is used to create procedures for servicing Dell products.

SolVe is available as an online or a stand-alone application.

- SolVe Online - Web-based application
 - Can be accessed at - <https://solve.dell.com/solve/home>
 - Automatically updated procedures
- SolVe Desktop - User-installed Windows application
 - Can be downloaded from -
<https://solve.emc.com/desktopbinaries/setup.exe>
 - Offline accessible
 - Manual update

The list of available procedures depends on the access level of the user:
Dell Employee², Partner, or Customer.

² Dell Employees can impersonate all access levels.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

The screenshot shows two side-by-side views of the Dell Technologies SolVe Online interface. Both views have a blue header bar with the text "DELL Technologies SolVe Online" and a red banner below it stating "You are currently impersonating - Customer".

Left View (Customer View): This view is titled "VxRail Appliance". It lists several categories under "VxRail Procedures": "Connectivity", "Install", "Upgrade", "Replacement Procedures", "Miscellaneous", and "Reference Material". Under "Install", there are two sub-links: "Installation Procedures" and "Node Image Management Tool". The "Install" category and its sub-links are highlighted with an orange box.

Right View (Employee View): This view is also titled "VxRail Appliance". It lists similar categories: "Networking Procedures", "VxRail Procedures", "Upgrade", "Replacement Procedures", "Miscellaneous", and "Reference Material". Under "VxRail Procedures", there is a link "Out of Band BIOS Upgrades for 14G". Under "Install", there are three sub-links: "Installation Procedures", "Restricted Procedures", and "Upgrade". The "Install" category and its sub-links are highlighted with an orange box.

SolVe Online - Customer View - VxRail Procedures

SolVe Online - Dell Employee View - VxRail Procedures



Tip: A valid user account is required to access and use SolVe. Customers and Partners must register for a user account. See [KB 000021768](#) for details.

Generate VxRail Installation Procedures - Common Selections

In SolVe Online, the VxRail installation procedures are located under **VxRail Appliance > VxRail Procedures > Install > Installation Procedures**. The **Installation Procedures** link is used to generate the VxRail hardware installation (rack and stack) and the VxRail cluster configuration procedures. The procedure generator prompts the user with a series of input selections in order to generate the required procedure.

To learn about the input selections that are the same for the VxRail hardware installation (rack and stack) and VxRail cluster configuration procedures, select each tab.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

Cluster Verification

Select whether a VxRail VD-4510c or VD-4520c 2-node cluster is getting installed.

The screenshot shows a user interface for generating VxRail installation procedures. On the left, a vertical sidebar displays "VxRail Appliance" and "1 Step 1". The main area is titled "Installation Procedures" and contains a question: "Are you installing a VD-4510c or VD-4520c 2-node cluster?". Below the question are two radio buttons: "Yes" and "No". At the bottom right of the main area are three buttons: "CANCEL", "CLEAR", and "NEXT".

Customer View - Cluster verification

Model

Select the VxRail model. The listing in the Customer view is limited to the models supported for Customer self-deploy.

SolVe highlights relevant knowledge base articles. The informational message must be acknowledged to proceed. The links to the relevant knowledge base articles are also documented in the procedure that is generated.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

Customer View - Select VxRail model

Internal or Partner View - Select VxRail model

Software Version

Select the VxRail software version. The listing in the Customer view is limited to the software versions supported for Customer self-deploy.

VxRail Appliance

Installation Procedures

1 Step 1

2 Step 2

- VxRail ESXi00
- VxRail ESXi005/ESXi005N
- VxRail P10F
- VxRail P10P
- VxRail S470
- VxRail P10F/N
- VxRail P10N
- VxRail P10F/CH/HD-4820c
- VxRail VE-480
- VxRail VP-760

Select the VxRail Software Image on the new Appliance

- v8.0.10
- v8.0.40
- v8.0.100
- v8.0.1000
- v8.0.000
- v7.0.460
- v7.0.45045/452
- v7.0.420
- v7.0.410/411

CANCEL **CLEAR** **BACK** **NEXT**

VxRail Appliance

Installation Procedures

1 Step 1

2 Step 2

- v8.0.10
- v8.0.100
- v8.0.000
- v7.0.460
- v7.0.45045/452
- v7.0.420
- v7.0.410/411
- v7.0.372
- v7.0.370/371
- v7.0.360
- v7.0.350
- v7.0.330
- v7.0.241
- v7.0.240
- v7.0.230
- v7.0.203
- v7.0.202
- v7.0.201
- v7.0.200

CANCEL **CLEAR** **BACK** **NEXT**

Customer View - Select VxRail software version

Internal or Partner View - Select VxRail software version

vSAN Datastore Type

Select the vSAN datastore type. Based on the selected datastore type, SolVe prompts the user for more input.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

VxRail Appliance	Installation Procedures
1 Step 1 2 Step 2 3 Step 3	<p>Select vSAN Datastore Type</p> <p><input checked="" type="radio"/> vSAN OSA (Original Storage Architecture)</p> <p><input type="radio"/> vSAN ESA (Express Storage Architecture)</p> <p>CANCEL CLEAR BACK NEXT</p>

Customer View and Internal or Partner View - Select vSAN datastore type

Cluster Type

Select the cluster and witness type. Customers can only self-deploy a standard cluster.

Acknowledge the informational message to proceed.

VxRail Appliance	Installation Procedures
1 Step 1 2 Step 2 3 Step 3 4 Step 4	<p>What type of cluster is being installed?</p> <p><input checked="" type="radio"/> Normal Cluster (3 or more nodes)</p> <p><input type="radio"/> Customer-supplied</p> <p><input type="radio"/> VMware-supplied</p> <p><input checked="" type="radio"/> N/A</p> <p>CANCEL CLEAR BACK NEXT</p>
VxRail Appliance	Installation Procedures
1 Step 1 2 Step 2 3 Step 3 4 Step 4	<p>What type of cluster is being installed?</p> <p><input checked="" type="radio"/> Normal Cluster (3 or more nodes)</p> <p><input type="radio"/> 2 Node Cluster</p> <p><input type="radio"/> Dynamic Node</p> <p>Select vSAN Witness Type</p> <p><input checked="" type="radio"/> N/A</p> <p>CANCEL CLEAR BACK NEXT</p>

Customer View - Cluster and vSAN Witness type

Internal or Partner View - Cluster and vSAN Witness type

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

Activity

Select the activity. Based on the selected activity, SolVe prompts the user for more input.

VxRail Appliance

Installation Procedures

Choose your activity

Rack and Stack Hardware only

Configure VxRail Appliance only

Perform Both Activities

Procedure for hardware installation

Procedure for VxRail cluster configuration

Step 1

Step 2

Step 3

Step 4

Step 5

Procedure for hardware installation and VxRail cluster configuration

CANCEL CLEAR BACK NEXT

Customer View and Internal or Partner View - Select activity

Generate VxRail Installation Procedures - Standard Cluster Configuration Selections

To learn about the SolVe input selections required to generate the procedure for the deployment of a VxRail standard cluster, select each tab.

SmartFabric Configuration

Select whether a configuration of SmartFabric is required.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

VxRail Appliance	Installation Procedures	X
<ul style="list-style-type: none">1 Step 12 Step 23 Step 34 Step 45 Step 56 Step 6	<p>Is a SmartFabric being configured?</p> <p><input checked="" type="radio"/> No</p>	<p>CANCEL CLEAR BACK NEXT</p>

Internal or Partner View - Select SmartFabric options

vSAN Stretched Cluster

Select whether a vSAN Stretched Cluster is being implemented and whether Witness Traffic Separation is being configured.

VxRail Appliance	Installation Procedures	X
<ul style="list-style-type: none">1 Step 12 Step 23 Step 34 Step 45 Step 56 Step 67 Step 7	<p>Are you installing a vSAN Stretched Cluster</p> <p><input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Are you configuring Witness Traffic Separation?</p> <p><input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A</p>	<p>CANCEL CLEAR BACK NEXT</p>

Internal or Partner View - Select vSAN Stretched Cluster and Witness Traffic Separation options

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

vCenter Server and Networking Options

Select the vCenter Server Option, node discovery method, number of reserved ports for VxRail Networking, number of VMware Virtual Distributed Switch (VDS), and Link Aggregation Type. Some of the networking options depend on this selection.

The screenshot shows the SolVe Online interface for generating VxRail installation procedures. On the left, a vertical navigation bar lists steps 1 through 6. Step 6 is currently selected and highlighted in light blue. The main content area is titled "Installation Procedures". A yellow rectangular box highlights the "Networking Options" section, which contains the following configuration choices:

- Select the vCenter option:
 - Internal VxRail-supplied vCenter with VxRail-supplied virtual distributed switch
 - External Customer-supplied vCenter with VxRail-supplied virtual distributed switch
 - External Customer-supplied vCenter with customer-supplied virtual distributed switch
- Select the node discovery method:
 - Auto
 - Manual
- Select the number of ports reserved for VxRail Networking:
 - Two
 - Four or More
- Select the number of Virtual Distributed Switches for the VxRail Network:
 - One VDS
 - Two VDS
- Select the Link Aggregation Type:
 - Dynamic Link Aggregation
 - None

At the bottom right of the main area are four buttons: CANCEL, CLEAR, BACK, and NEXT (highlighted in dark blue).

Customer View Internal or Partner View - Select vCenter, discovery, and networking options

Connectivity Options

Select the node connectivity options. The options include logging, call-home, and service connectivity. If Top of Rack (ToR) switch configuration content is selected, the configuration steps are documented in the SolVe procedure.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

The screenshots show the 'Step 7' configuration screen for VxRail Appliance. The left one is for 'Customer view' and the right one is for 'Internal or Partner View'. Both screens show sections for 'Select the SysLog Option', 'Service Connectivity Options' (Secure Connect Gateway, Direct, N/A), and 'Include ToR Content' (checkboxes for Dell EMC Networking 0930 SmartFabric and Enterprise VxRail ToR Switch Configuration Guide, Dell EMC Networking 3504P-ON 099 Virtual ToR Switch Configuration, and Do not include ToR Guides). Buttons at the bottom include CANCEL, CLEAR, BACK, and NEXT.

Customer view - Select connectivity options

Internal or Partner View - Select connectivity options

Procedure Usage

The usage information is an optional section. Enter the requested information about the VxRail nodes that this procedure has to be used on.

The screenshot shows the 'Step 8' configuration screen for VxRail Appliance, titled 'Procedure Usage'. It includes fields for 'Serial Number(s)', 'SR Number(s)', and 'Party ID(s)', each with an 'Input Text Here' placeholder. A note says 'Please complete one of the fields below to tell us how this procedure will be used. (Use comma separation for multiple items in a line.)'. Buttons at the bottom include CANCEL, CLEAR, BACK, and NEXT.

Customer and Internal or Partner View - Procedure usage information

Knowledgebase Article Relevancy

This step provides the Dell Knowledge Base articles that are seen in the steps of the SolVe procedure. If any of the articles are not relevant, clear the boxes before proceeding to the next step.

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

The screenshots show the 'Knowledgebase Article Relevancy' step in the wizard. On the left, under 'Customer view', two articles are listed: '541025: VxRail Nodes are not discovered by VxRail manager when customer is using Juniper switches' and '000204006: Dell VxRail: How to gather the recovery keys for TPM security enabled VxRail nodes'. On the right, under 'Internal or Partner View', three articles are listed: '541025: VxRail Nodes are not discovered by VxRail manager when customer is using Juniper switches', '541025: VxRail HBA module', and '000202259: Dell EMC VxRail: Two Node ROBO deployment validation failed at Witness Network Settings'.

Customer view - Knowledgebase Article relevancy verification

Internal or Partner View - Knowledgebase Article relevancy verification

Summary and Generate Procedure

This step shows the selections completed. Review the selections and click **GENERATE**.

The screenshot shows the 'Selections completed' step in the wizard. It lists the completed steps from 1 to 10. The summary section indicates that the user has reached the last step in the wizard and provides a list of completed selections, including the choice of cluster type, software image, storage architecture, witness type, connectivity options, and management IP address.

Customer and Internal or Partner View - Selections summary and generate the procedure

Lab 1: Generate a VxRail Installation Procedure

You are implementing VxRail, and you want to generate the procedure for configuring a new VxRail cluster. VxRail hardware installation and cluster

Use SolVe Online To Generate VxRail Installation Procedures To Configure VxRail Clusters

configuration procedures are generated using SolVe Online or SolVe Desktop.

Lab Tasks

- Log in to SolVe Online.
- Generate the procedure for configuring a standard VxRail 8.0.100 cluster with a customer supplied vCenter and a VxRail VDS.

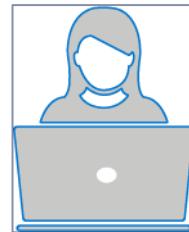


Lab 2: Compare VxRail Configuration Procedures

In this lab exercise, you review and compare the SolVe configuration procedures for VxRail clusters with different vCenter Server and VDS options.

Lab Tasks

- Compare the SolVe configuration procedures to deploy a VxRail cluster with a VxRail-supplied vCenter and a VxRail-supplied VDS.
- Compare the SolVe configuration procedures to deploy a VxRail cluster with a customer-supplied vCenter and a customer-supplied VDS.



Configure VxRail Network Settings

Default Management VLAN IDs on VxRail Nodes

New VxRail nodes are configured with the default port groups and VLAN IDs as shown in the following graphic:

Name	Virtual Switch	Active Clients	VLAN ID
Management Network	vSwitch0	1	0
Private Management Network	vSwitch0	1	3939
Private VM Network	vSwitch0	0	3939
VM Network	vSwitch0	0	0
iDRAC Network	vSwitchiDRACvusb	1	0

New VxRail node - Default port group configuration.

Management Network: The port group that is used for external management is untagged by default and uses the Native VLAN on the ToR switches.

Private Management Network: The port group that is used for automated VxRail node discovery is configured with the default VLAN ID of 3939. The VxRail discovery VLAN ID must be configured on the ToR switches to enable discovery and primary node selection during system initialization.

Private VM Network: The port group that is used for automated VxRail node discovery by the VxRail Manager VM; same VLAN ID as **Private Management Network**.

VM Network: The port group that is used for external management by the VxRail Manager VM; untagged by default like **Management Network**.



Important: If required, the default VLAN assignments can be changed before the VxRail cluster is configured.

Modify Default Management Network VLAN IDs on VxRail Nodes

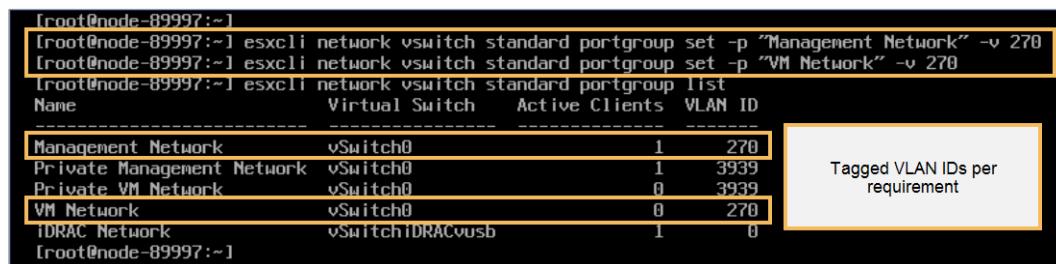
The default port group VLAN IDs can be modified by running the following ESXCLI command from the ESXi Shell of the node:

```
esxcli network vswitch standard portgroup set -p
"<Port Group Name>" -v <VLAN ID>
```

For a tagged external management network, modify the VLAN IDs of the following port groups:

- **Management Network**
- **VM Network**

In the example below a VLAN ID of 270 is set for the external management port groups:



```
[root@node-89997:~] [root@node-89997:~] esxcli network vswitch standard portgroup set -p "Management Network" -v 270
[root@node-89997:~] esxcli network vswitch standard portgroup set -p "VM Network" -v 270
[root@node-89997:~] esxcli network vswitch standard portgroup list
Name          Virtual Switch   Active Clients  VLAN ID
-----
Management Network    vSwitch0        1            270
Private Management Network    vSwitch0        1            3939
Private VM Network    vSwitch0        0            3939
VM Network          vSwitch0        0            270
IDRAC Network       vSwitch1IDRACvusb  1            0
```

Tagged VLAN IDs per requirement

New VxRail node - Modified port group configuration.

For a different VxRail node discovery VLAN ID, modify the VLAN IDs of the following port groups:

- **Private Management Network**
- **Private VM Network**

If the VxRail node discovery VLAN ID is changed, restart the Loudmouth service by running the following CLI command from the ESXi Shell of the node:

```
/etc/init.d/loudmouth restart
```



Important: Make the required VLAN ID modifications for all the VxRail nodes before configuring the VxRail cluster.

Interaction: Modify Default Management Network VLAN ID

The web version of this content contains an interactive activity.

Network Access to the VxRail Manager VM

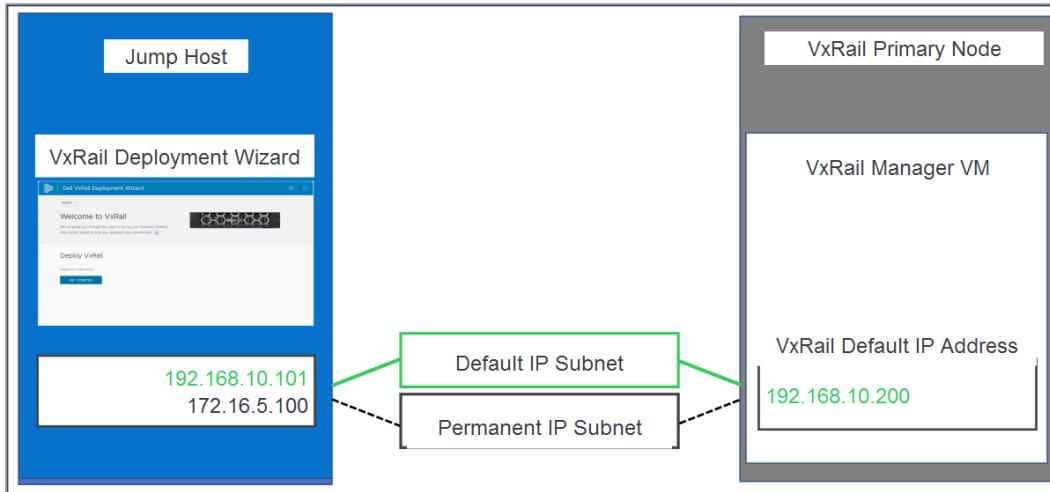
The VxRail Manager VM has a deployment wizard that can be used to deploy a VxRail cluster. The VxRail Deployment Wizard is accessed by connecting to the VxRail manager IP address using a browser. Launch the browser session from a jump host or service laptop which has access to the VxRail management network.

The default IP address of the VxRail Manager for an unconfigured system is 192.168.10.200. The IP address of the VxRail Manager can be changed to the permanent IP address before VxRail is configured.

Before Deployment

Configure the jump host with dual IP addresses. One IP address should be on the 192.168.10.x/24 subnet, and the other on the same subnet as the permanent IP address of the VxRail Manager. The jump host must be able to connect to the VxRail Manager default IP address at the start of the VxRail deployment.

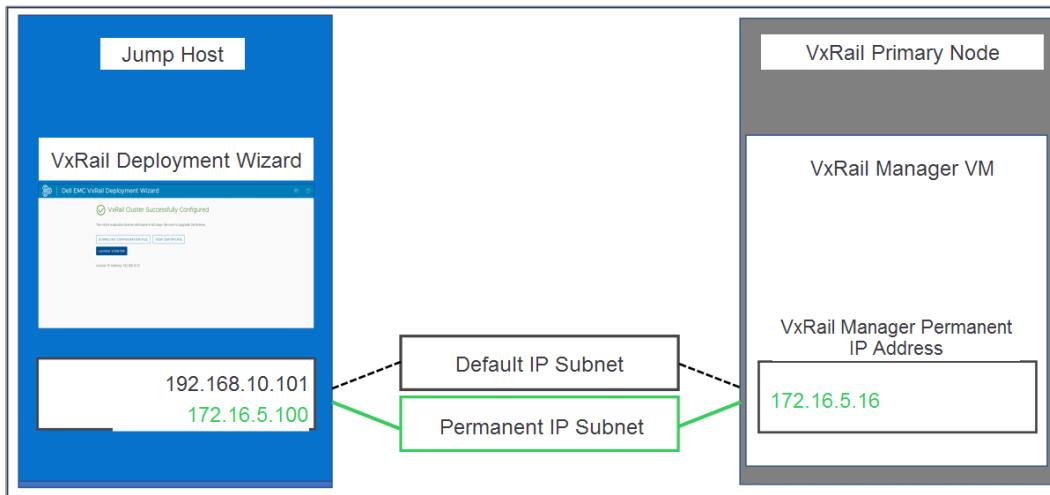
Configure VxRail Network Settings



Start of deployment - Jump host communicates with VxRail Manager with the default IP Address 192.168.10.200

After Deployment

The VxRail deployment process changes the VxRail Manager default IP address to the permanent IP address. Therefore, the jump host must also be able to connect to the permanent IP address.



End of deployment - Jump host communicates with VxRail Manager with the permanent IP Address 172.16.5.16

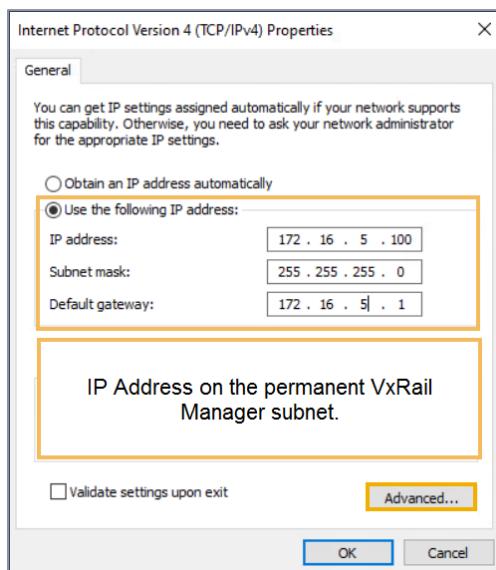
Connect Service Laptop or Jump Host

Configure VxRail Network Settings

The procedure to configure dual IP addresses on the jump host is documented in the SolVe VxRail Installation Procedure. Review Task 1 for details.

High-level steps run from a Windows jump host:

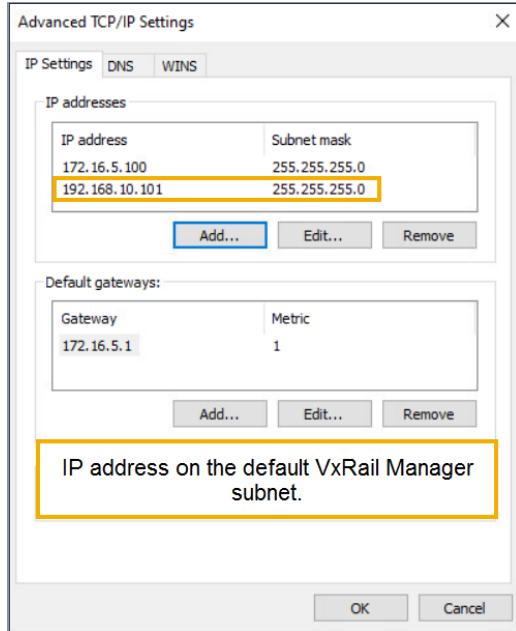
1. Open the TCP/IPv4 properties page for the primary Ethernet adapter.
2. Set an IP address on the same subnet as the permanent address assigned to the VxRail Manager.



Jump host - TCP/IPv4 Properties

3. Use the advanced option to add an IP address on the same subnet as the default VxRail Manager IP address - 192.168.10.x, subnet mask - 255.255.255.0.

Configure VxRail Network Settings



Jump host - Advanced TCP/IP Settings

Configure VxRail Manager VM Network Settings

If deploying VxRail by connecting to the permanent IP address, there is no requirement for dual IP addresses on the jump host. The jump host only has to be able to connect to the permanent IP address, which must be configured before beginning the deployment.

The procedure to assign the VxRail Manager permanent IP address is documented in the SolVe VxRail Installation Procedures. Review Task 25 for details.

To assign the VxRail Manager permanent IP address, run the following command from the ESXi Shell of the designated VxRail primary node:

```
vxrail-primary --config --vxrail-address <IP> --  
vxrail-netmask <netmask> --vxrail-gateway <gateway> --  
vlan <vlanid>
```

In the example below, the VxRail Manager IP address is changed to 172.16.5.16:

Configure VxRail Network Settings

```
[root@node-89515:~] vxrail-primary --config --vxrail-address 172.16.5.16 --vxrail-netmask 255.255.255.0 --vxrail-gateway 172.16.5.1 --vwan 5
PRIMARY: 2023-09-29 20:49:55.364.364Z - INFO Config Manager with IP 172.16.5.16/255.255.255.0 gateway 172.16.5.1
VxRail Manager is already running, no need to power on
PRIMARY: 2023-09-29 20:50:40.615.615Z - INFO Temporary remove the uplinks
PRIMARY: 2023-09-29 20:50:40.659.659Z - INFO Start customizing VxRail Manager address...
PRIMARY: 2023-09-29 20:51:10.916.916Z - INFO Wait until the IP taking effect
PRIMARY: 2023-09-29 20:51:10.929.929Z - INFO Product default IPv4 set to 172.16.5.16 and default IPv6 set to fd39:3939:3939:3939
::200
PRIMARY: 2023-09-29 20:51:10.934.934Z - INFO Restore vSwitch uplinks
PRIMARY: 2023-09-29 20:51:10.979.979Z - INFO Success in completing the setup of Manager network settings
Success in completing the setup of Manager network settings
PRIMARY: 2023-09-29 20:51:11.961.961Z - INFO Success in completing the setup of vwan settings
Success in completing the setup of vwan settings
```

ESXi Shell configuring the VxRail Manager permanent IP address



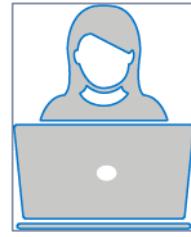
Tip: An alternate method to assign the VxRail Manager permanent IP address is to use the **VxRail Pre-Installation PowerShell Script** available on the [Dell Technologies Support](#) site. You must be logged in to access and download the file.

Lab 3: Configure VxRail Manager VM Network Settings

You have to configure the permanent IP address of the VxRail Manager VM before the VxRail cluster is deployed.

Lab Tasks

- Open a virtual console and log in to the ESXi Shell of an unconfigured VxRail node.
- Configure the VxRail Manager permanent IP address using the ***vxrail-primary*** command.
- Confirm that the Windows Management Host can reach the configured VxRail Manager IP address.



Validate the Network Environment for Deployment

Manually Validate ToR Switch Configuration

Validating the VxRail network environment before configuring the VxRail cluster is recommended for a successful deployment.

The details of the planned VxRail network environment are documented in the VxRail Configuration Report that is available in the VxRail Configuration Portal. See the example of a VxRail Configuration Report.

The VxRail Configuration Portal Pre-deployment Checklist provides guidance for performing a manual network validation.

The network validation must be performed on the subnet that is planned for the VxRail management network.

Pre-deployment Checklist for VxRail-Cluster			
<input type="checkbox"/> Switch Configuration <small>Learn more</small>	<input type="checkbox"/> IP Address Availability <small>Learn more</small>	<input type="checkbox"/> Firewall Port Configuration <small>Learn more</small>	
<ul style="list-style-type: none"> ◦ Verify port speed compatibility between hosts and switches ◦ Verify VLAN configuration <ul style="list-style-type: none"> ▪ Verify all physical switch ports are in trunk mode ▪ Configure pass-through on switch uplinks ◦ Management VLAN <ul style="list-style-type: none"> ▪ Enter VLAN ID “0” if you plan to use native/untagged traffic ▪ Discovery (Internal Management) VLAN <ul style="list-style-type: none"> ▪ Enable IPv6 multicast if using automated host discovery ◦ vSAN VLAN <ul style="list-style-type: none"> ▪ Enable unicast ▪ Verify the VLAN is not uplinked ◦ vSphere VMotion VLAN <ul style="list-style-type: none"> ▪ Configure pass-through on switch uplinks (optional) ◦ VM Guest Network VLAN(s) <ul style="list-style-type: none"> ▪ Configure pass-through on switch uplinks 	<ul style="list-style-type: none"> ◦ Ping the IP addresses and verify there is no response (verify the reserved IP addresses are not being used): <ul style="list-style-type: none"> ▪ VxRail Manager ▪ iDRAC ▪ vSAN ▪ vMotion ▪ ESXi Management Interfaces ▪ Internal vCenter ▪ Secure Remote Services (VxRail provided) 	<ul style="list-style-type: none"> ◦ Verify compliance with the VxRail firewall rules ◦ PUTTY/SSH to the FQDN and Port: <ul style="list-style-type: none"> ▪ VxRail Manager (port 53) ▪ VMware vCenter (port 443) 	
<input type="checkbox"/> IP Address Reachability <small>Learn more</small>		<input type="checkbox"/> Network Time Protocol (NTP) <small>Learn more</small>	
	<ul style="list-style-type: none"> ◦ Ping the IP addresses and verify a response: <ul style="list-style-type: none"> ▪ Gateway on all VxRail virtual networks ▪ Syslog Server ▪ External vCenter ▪ Secure Remote Services (customer provided) 	<ul style="list-style-type: none"> ◦ Verify all cluster hosts have the same date and time 	
<input type="checkbox"/> Domain Name System (DNS) <small>Learn more</small>		<input type="checkbox"/> vCenter Configuration <small>Learn more</small>	
	<ul style="list-style-type: none"> ◦ Verify forward and reverse nslookup for IP address/FQDN: <ul style="list-style-type: none"> ▪ VxRail Manager ▪ VMware vCenter ▪ ESXi Management Interfaces ▪ Secure Remote Services (customer provided) 	<ul style="list-style-type: none"> ◦ If you are using a customer provided VMware vCenter Server, verify the configuration using the UI or PowerCLI: <ul style="list-style-type: none"> ▪ Verify VMware vCenter and VxRail versions are interoperable ▪ Verify that the VMware vCenter administrator and manager accounts work ▪ Verify the VxRail Manager account has no permissions ▪ Verify the datacenter is created without a cluster ▪ Verify that NTP is configured 	
<input type="checkbox"/> Account Passwords <small>Learn more</small>		<input type="checkbox"/> Solve Procedure Documentation <small>Learn more</small>	
		<ul style="list-style-type: none"> ◦ Verify compliance with VxRail password rules 	
<input type="checkbox"/> Solve Procedure Documentation <small>Learn more</small>			
		<ul style="list-style-type: none"> ◦ Generate the VxRail hardware install Solve procedure ◦ Generate the VxRail software install SolVe procedure 	

VxRail Configuration Portal - Pre-deployment Checklist

Perform network validations for:

- Switch configuration
- IP address availability and reachability
- Domain Name System (DNS) server readiness

Validate the Network Environment for Deployment

- Firewall port configuration
- Network Time Protocol (NTP) server readiness

Useful links:

- [VxRail Configuration Portal - Pre-deployment checklist overview](#)
- [VxRail Customer Firewall Configuration spreadsheet](#)

ToR Switch - Confirm VLANs Configured for VxRail Networks

Confirm that all the required VLANs have been created on the ToR switches. Verify all VLANs are active on all the switch ports that are connected to the VxRail nodes. Verify that the External Management VLAN tagging is configured as specified in the VxRail Configuration Report and is active on the uplink port.

```
DTES-VxRail-ToR# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs,
       @ - Attached to Virtual Network
Q: A - Access (Untagged), T - Tagged
  NUM      Status    Description          Q Ports
* 1        Inactive
  10      Active     vMotion             A Eth1/1/17-1/1/18,1/1/20-1/1/32
  20      Active     vSAN               T Eth1/1/1-1/1/16
  1751     Active    External_Mgmt      T Eth1/1/1-1/1/16
  1761     Active    VM_Customer_Netw   A Eth1/1/1-1/1/16,1/1/19
  3939     Active    Internal_Mgmt      T Eth1/1/1-1/1/16
DTES-VxRail-ToR#
```

Dell switch - Configured VLANs

In this example, ToR switch ports 1 through 16 are connected to the VxRail nodes and port 19 is the uplink port. Five VLANs are configured:

- [External_Mgmt](#) VLAN ID 1751 is an access VLAN active on ports 1 through 16 and 19.
- VM Customer Network VLAN ID 1761 is a tagged VLAN, active on ports 1 through 16 and 19.
- [Internal_Mgmt](#) VLAN ID 3939, vMotion VLAN ID 10, and vSAN VLAN ID 20 are all tagged VLANs active on ports 1 through 16.



Important: In a dual ToR configuration, configure the Inter-Switch Links (ISLs) to allow all VxRail VLANs to pass through.

ToR Switch - Confirm VxRail Node Port Status

The switch ports that are connected to the VxRail nodes and the uplink ports must have a status of up. [Trunk mode](#) must be enabled on these ports to support multiple VLANs.

Port	Description	Status	Speed	Duplex	Mode	Vlan	Tagged-Vlans
Eth 1/1/1	Node1_Port1	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/2	Node1_Port2	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/3	Node2_Port1	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/4	Node2_Port2	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/5	Node3_Port1	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/6	Node3_Port2	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/7	Node4_Port1	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/8	Node4_Port2	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/9	Node1_Port3	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/10	Node1_Port4	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/11	Node2_Port3	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/12	Node2_Port4	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/13	Node3_Port3	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/14	Node3_Port4	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/15	Node4_Port3	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/16	Node4_Port4	up	40G	full	T	1751	10,20,1761,3939
Eth 1/1/17		down	0	full	A	1	-
Eth 1/1/18		down	0	full	A	1	-
Eth 1/1/19	Uplink To Ups...	up	40G	full	T	1751	1761
Eth 1/1/20		down	0	full	A	1	-

Dell switch - Interface status

In the example, the VxRail node ports (1-16) and the uplink port (19) are up. The VLAN column shows that 1751 is the access VLAN for ports 1 through 16 while the other VLAN IDs are tagged VLANs.

ToR Switch - Spanning Tree Protocol Considerations

[Spanning Tree Protocol \(STP\)](#) is a protocol to prevent network loops. STP introduces a default 50-second delay before data is allowed to be sent on a port. This delay causes VxRail problems if there is a path failure.

Validate the Network Environment for Deployment

All VxRail node ports should either:

- Be on a switch with STP disabled or,
- Be on a switch with STP enabled, where the ports are configured to rapidly switch to the forwarding state.
 - On Dell switches, set the edge option.
 - On Cisco switches, set the PortFast option.

Consult the switch vendor's documentation for more information

In this example, rapid spanning tree is enabled. The ports are set as [edge ports](#) and have a status of FWD (forwarding). This configuration prevents STP from causing problems with the VxRail system.

Spanning tree enabled protocol rapid-pvst VLAN 1751 Executing IEEE compatible Spanning Tree Protocol							
Interface Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
ethernet1/1/1	128.516	128	500	FWD	0	34519 0c17.e76e.9d00	128.516
ethernet1/1/2	128.520	128	500	FWD	0	34519 0c17.e76e.9d00	128.520
ethernet1/1/3	128.524	128	500	FWD	0	34519 0c17.e76e.9d00	128.524
ethernet1/1/4	128.528	128	500	FWD	0	34519 0c17.e76e.9d00	128.528
ethernet1/1/5	128.532	128	500	FWD	0	34519 0c17.e76e.9d00	128.532
ethernet1/1/6	128.536	128	500	FWD	0	34519 0c17.e76e.9d00	128.536
ethernet1/1/7	128.540	128	500	FWD	0	34519 0c17.e76e.9d00	128.540
ethernet1/1/8	128.544	128	500	FWD	0	34519 0c17.e76e.9d00	128.544
ethernet1/1/9	128.548	128	500	FWD	0	34519 0c17.e76e.9d00	128.548
ethernet1/1/10	128.552	128	500	FWD	0	34519 0c17.e76e.9d00	128.552
ethernet1/1/11	128.556	128	500	FWD	0	34519 0c17.e76e.9d00	128.556
ethernet1/1/12	128.560	128	500	FWD	0	34519 0c17.e76e.9d00	128.560
ethernet1/1/13	128.564	128	500	FWD	0	34519 0c17.e76e.9d00	128.564
ethernet1/1/14	128.568	128	500	FWD	0	34519 0c17.e76e.9d00	128.568
ethernet1/1/15	128.572	128	500	FWD	0	34519 0c17.e76e.9d00	128.572
ethernet1/1/16	128.576	128	500	FWD	0	34519 0c17.e76e.9d00	128.576

Dell switch - Rapid Spanning Tree enabled

ToR Switch - Link Aggregation on VxRail Node Ports

VxRail supports Link Aggregation Group (LAG) with a customer-supplied VDS and VxRail-supplied VDS. NIC teamings in VxRail is the foundation for supporting link aggregation. For link aggregation, ToR switches must support [Link Aggregation Control Protocol \(LACP\)](#).

On a Dell switch, link aggregation is configured using port channels.



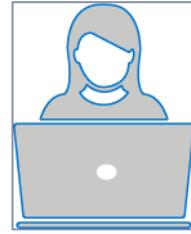
Go to: See the [Dell VxRail Network Planning Guide](#) for more information about link aggregation.

Lab 4: Validate ToR Switch Configuration

You are getting ready to deploy a VxRail cluster by joining an existing vCenter Server. You want to manually validate the network environment before deploying the VxRail cluster.

Lab Tasks

- Validate the ToR switch configuration.



Manually Validate IP Address Availability and Reachability

VxRail components must have unique IP addresses. The required IP addresses depend on the VxRail deployment options and are documented in the VxRail Configuration Report.

The `ping` command, or the PowerShell equivalent `Test-NetConnection`, can be used to confirm that there are no IP address conflicts. The ping test should fail for all the unconfigured components and succeed for all components that exist.

Example 1: VxRail deployed with the VxRail vCenter Server. The IP addresses reserved for the vCenter Server and the ESXi hosts, should fail the ping test. If the VxRail Manager permanent IP address has not been configured, it should also fail.

```
C:\Users\Administrator>ping 192.168.10.16

Pinging 192.168.10.16 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.10.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

Example of an expected failed ping test

Example 2: VxRail deployed by joining an existing vCenter Server with an external Syslog server. The vCenter Server and the Syslog server should be reachable.

```
C:\Users\Administrator>ping 192.168.10.90

Pinging 192.168.10.90 with 32 bytes of data:
Reply from 192.168.10.90: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Example of a successful ping test

Confirm DNS Readiness

When a VxRail is deployed using an external DNS, the DNS must be configured with forward and reverse lookup records for the vCenter Server, ESXi hosts, and the VxRail Manager VM. Depending on the

Validate the Network Environment for Deployment

VxRail deployment options, DNS records for additional components may also be required.

The ***nslookup*** command or the PowerShell equivalent ***Resolve-DnsName*** can be used to confirm the existence of the required records.

```
PS C:\Users\student> nslookup
Default Server: DC.delledu.lab
Address: 192.168.1.2

> server 192.168.1.2
Default Server: DC.delledu.lab
Address: 192.168.1.2                                            DNS Server

> vcluster730-esx01.delledu.lab
Server: DC.delledu.lab
Address: 192.168.1.2                                            Forward lookup for a node (ESXi Host)

Name:   vcluster730-esx01.delledu.lab
Address: 172.16.5.51

> 172.16.5.51
Server: DC.delledu.lab
Address: 192.168.1.2                                            Reverse lookup for a node (ESXi Host)

Name:   vcluster730-esx01.delledu.lab
Address: 172.16.5.51

> vxrail-manager.delledu.lab
Server: DC.delledu.lab
Address: 192.168.1.2                                            Forward lookup for VxRail Manager

Name:   vxrail-manager.delledu.lab
Address: 172.16.5.16

> 172.16.5.16
Server: DC.delledu.lab
Address: 192.168.1.2                                            Reverse lookup for VxRail Manager

Name:   vxrail-manager.delledu.lab
Address: 172.16.5.16
```

DNS lookup example

The FQDN and IP addresses are documented in the VxRail Configuration Report. Check the DNS records for all the required objects. The records should be verified for both:

- FQDN to IP address resolution - Forward DNS check
- IP address to FQDN resolution - Reverse DNS check

Confirm NTP Server Readiness

VxRail implementations use external NTP servers for time synchronization. Confirm that the NTP servers are reachable and functional with the following command from a Windows system:

```
w32tm /stripchart /computer:<NTP Server>
/samples:<Number of samples>
```

```
C:\Users\Administrator>w32tm /stripchart /computer:192.168.10.1 /samples:10
Tracking 192.168.10.1 [192.168.10.1:123].
Collecting 10 samples.
The current time is 2/11/2022 1:47:52 PM.
13:47:52, d:+00.0005321s o:+00.0001595s [ * ]]
13:47:54, d:+00.0004377s o:+00.0001521s [ * ]]
13:47:56, d:+00.0003960s o:+00.0001400s [ * ]]
13:47:58, d:+00.0003337s o:+00.0001227s [ * ]]
13:48:00, d:+00.0003696s o:+00.0001376s [ * ]]
13:48:02, d:+00.0003782s o:+00.0001297s [ * ]]
13:48:04, d:+00.0004431s o:+00.0001613s [ * ]]
13:48:06, d:+00.0004404s o:+00.0001645s [ * ]]
13:48:08, d:+00.0003871s o:+00.0001291s [ * ]]
13:48:10, d:+00.0003763s o:+00.0001446s [ * ]]

C:\Users\Administrator>
```

Example of a reachable and functional NTP server

Firewall Port Configuration

VxRail System components have different port requirements for network traffic. The port information is documented in the VxRail Customer Firewall Configuration spreadsheet, which can be downloaded from the [VxRail Configuration Portal](#). If a firewall exists between the VxRail system and the external components, an administrator must configure the firewall for all the relevant traffic.

The example lists the ports that are used when an existing vCenter Server manages a VxRail cluster. The Firewall Configuration worksheet has been filtered to show the relevant ports.

Validate the Network Environment for Deployment

Function	Secure Remote Services (SRS) - Emb.	Secure Remote Services (SRS) - Exte.	Secure Remote Services (SRS) - Poll...
SmartFabric Services	SNMP	Syslog	Stretched Cluster with WTS
Stretched Cluster without WTS	VMware Cloud Foundation	System Administration	
Top of Rack Switches	vRealize Log Insight	VLAN 2-Node	VMware vSphere - External vCenter
VMware vSphere - LS vMotion			
vSAN Health Check	(blank)		

Function	Source Subnet	Destination Subnet	Name	Port
VMware vSphere - External vCenter	Customer Intranet	External Management	vCenter to Managed Hosts	623, 902 80, 443, 5989, 902
	External Management	Customer Intranet	PSCs - VxRail Mgr	80, 443
			vCenter - VxRail Manager	80, 443
			vCenter to VxRail Manager	80, 443
			VMware vSphere ESXi Dump Collector	8000
			vSphere VASA	8080
			VxRail Mgr - PSCs	5480 80, 443
			ESXi Hosts - vCenter	443 5988 5989 6500 8000 8001 902
			VxRail Mgr - vCenter	5480

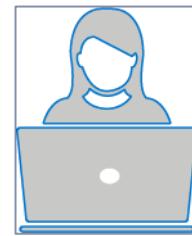
VxRail Firewall Configuration spreadsheet - vCenter Server port usage

Lab 5: Validate IP Address Availability, IP Address Reachability, and DNS Readiness

You are getting ready to deploy a VxRail cluster by joining an existing vCenter Server. The VxRail Manager permanent IP address has already been configured. You want to manually validate the network environment before deploying the VxRail cluster.

Lab Tasks

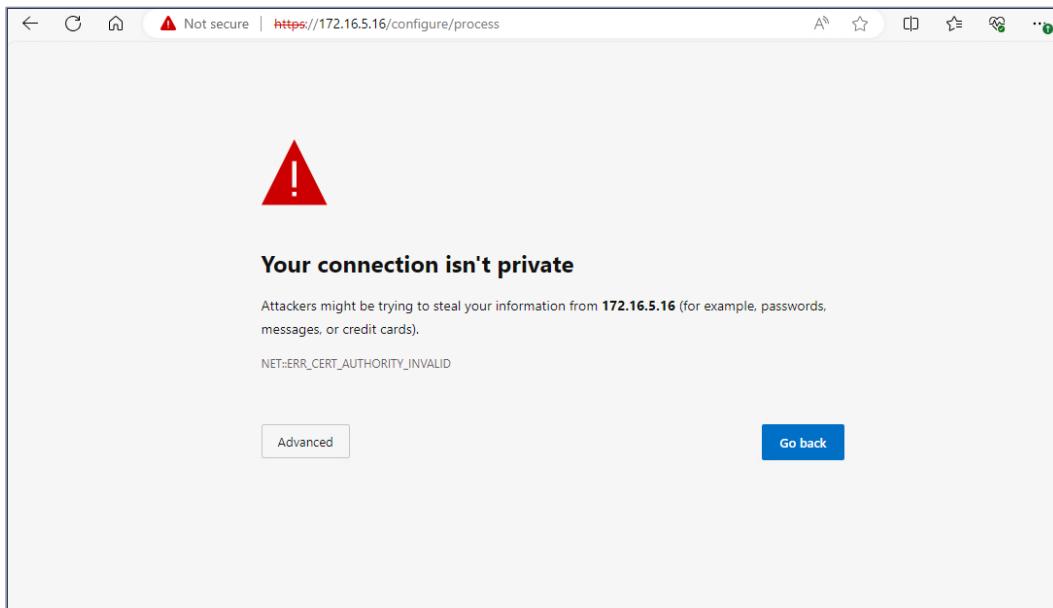
- Validate IP address availability, IP address reachability, and DNS readiness.



Deploy a Standard VxRail Cluster With vSAN OSA

Connect to the VxRail Manager VM

To launch the VxRail Deployment Wizard, open a browser session to the VxRail Manager - <**VxRail Manager IP Address**>. If configured, connect to the permanent IP address, else connect to the default IP address 192.168.10.200. A safety warning page appears since the self-signed certificate is untrusted by the browser.



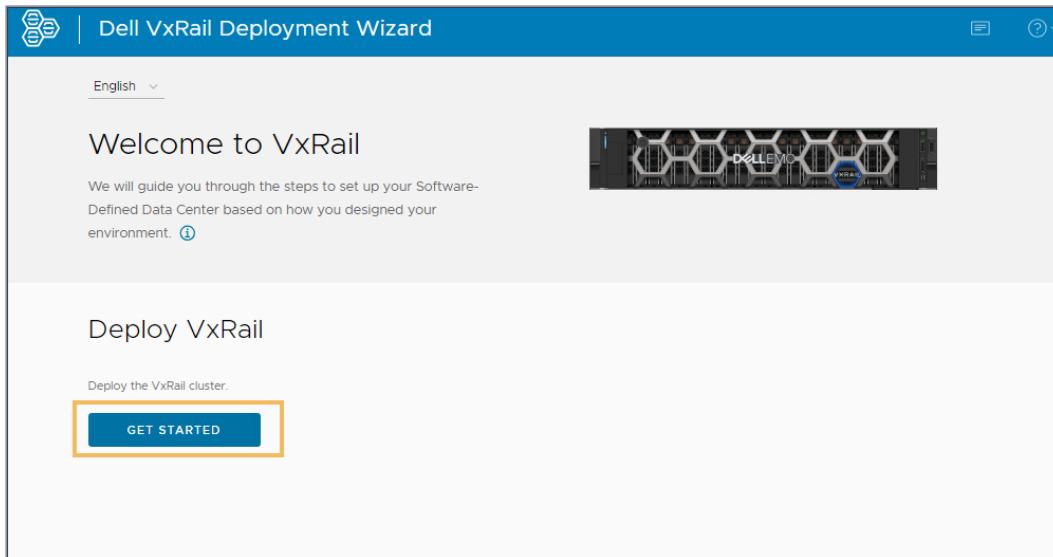
Browser Safety Warning - Chrome

VxRail Deployment Wizard Landing Page

This wizard is a step-by-step guide to configure a VxRail cluster.

To start the VxRail configuration, click **GET STARTED**.

Deploy a Standard VxRail Cluster With vSAN OSA

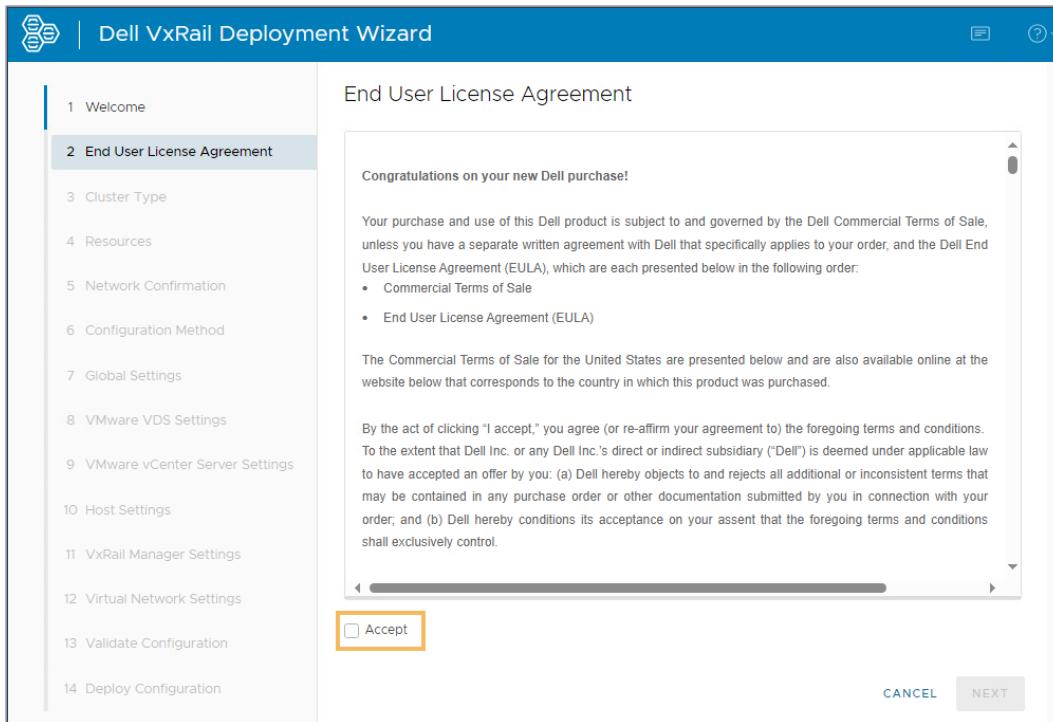


Deployment Wizard Landing Page

Software License and Maintenance Agreement

The **End User License Agreement** page of the wizard includes the Commercial Terms of Sale and the End User License Agreement (EULA). The EULA must be accepted to continue the configuration.

Deploy a Standard VxRail Cluster With vSAN OSA

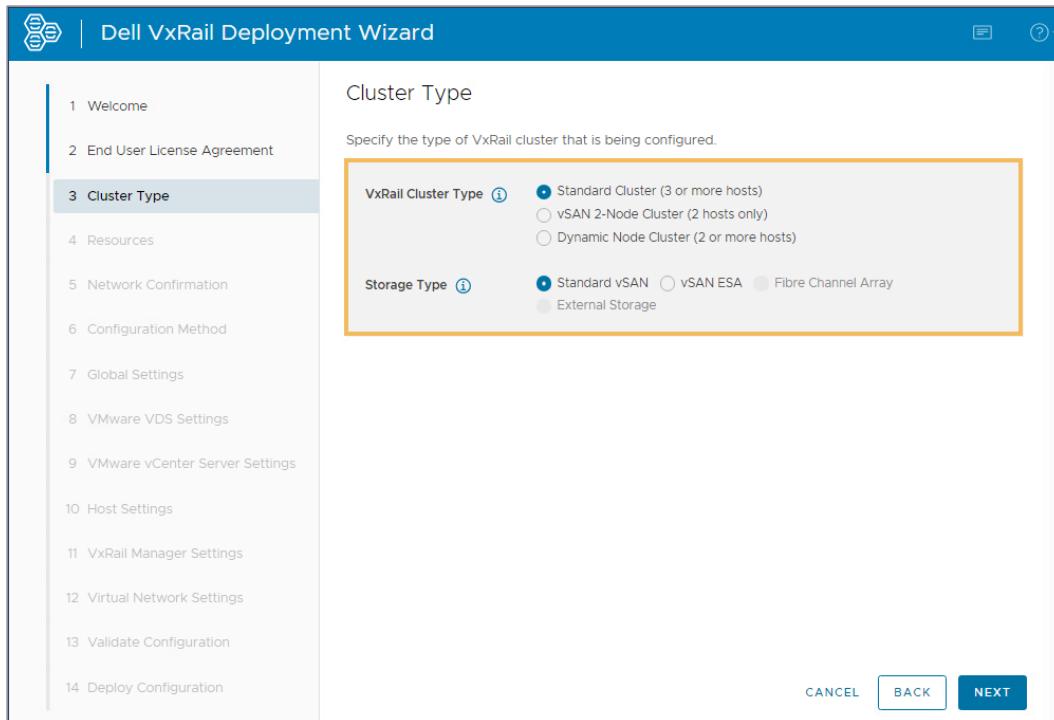


End User License Agreement

Selection of the VxRail Cluster Type

The **Cluster Type** page of the wizard has the **VxRail Cluster Type** and **Storage Type** options that must be chosen for the deployment. A VxRail standard cluster or vSAN 2-Node cluster must use standard vSAN storage or vSAN ESA. A dynamic node cluster can use Fibre Channel attached storage or External storage.

Deploy a Standard VxRail Cluster With vSAN OSA



Cluster Type - Selections for a standard cluster

Selection of Discovered Resources

The **Resources** page of the wizard shows the discovered hosts for a cluster configuration. For a standard VxRail cluster, select three to six hosts for the deployment. Additional hosts can be added later as part of Day 2 activities.

The **Drive Configuration** can be selected based on the drives that are configured on the nodes.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the 'Resources' step of the Dell VxRail Deployment Wizard. On the left, a navigation pane lists steps from 1 to 14. Step 4, 'Resources', is selected. The main area displays 'Cluster Hosts' with four hosts listed:

Service Tag	PSNT	Model	iDRAC IP Address
V073001	V07300100000000	VxRail E660N	20.12.145.41
V073002	V07300200000000	VxRail E660N	20.12.145.42
V073003	V07300300000000	VxRail E660N	20.12.145.43
V073004	V07300400000000	VxRail E660N	20.12.145.44

Below the hosts, it says '3 hosts selected' and '4 hosts discovered'. Under 'Drives', there is a dropdown menu set to 'Up to 2 Disk Groups (up to 4 capacity drives and 1 cache drive per group)'. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Discovered Resources

Network Confirmation

The **Network Confirmation** page of the wizard has two prerequisites.

Select the checkboxes to acknowledge each statement.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The title bar reads "Dell VxRail Deployment Wizard". The left sidebar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation (highlighted in blue), 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings, 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings, 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration. The main panel is titled "Network Confirmation" and displays the message: "The VxRail ToR switch and management VLAN must be set-up and be configured according to best practices before configuring the VxRail Cluster." It includes a link "LEARN MORE". Below this, two items are checked in a yellow-bordered box: "The VxRail ToR switches are set-up and configured according to best practices." and "The VxRail management VLAN is configured on the TOR switches and ESXi hosts according to best practices." At the bottom right are buttons for "CANCEL", "BACK", and "NEXT".

Network Confirmation

Configuration Method

The **Configuration Method** page shows two options to input configuration settings, **Step-by-step user input** or **Upload a configuration file**.

If the **Step-by-step user input** is selected, all the fields in the wizard are blank and require user input.

If the **Upload a Configuration File** method is selected, the JSON file that was previously created using the VxRail Configuration Portal is uploaded.

Deploy a Standard VxRail Cluster With vSAN OSA

Dell VxRail Deployment Wizard

VxRail Cluster Type: Standard (3 hosts)

Configuration Method

A configuration file can be uploaded to provide the wizard with VxRail cluster configuration settings.

Method

Step-by-step user input (i)

Upload a configuration file (i)

1 Welcome
2 End User License Agreement
3 Cluster Type
4 Resources
5 Network Confirmation
6 Configuration Method
7 Global Settings
8 VMware VDS Settings
9 VMware vCenter Server Settings
10 Host Settings
11 VxRail Manager Settings
12 Virtual Network Settings
13 Validate Configuration
14 Deploy Configuration

CANCEL BACK NEXT

Configuration Method



Tip: The Deployment Wizard allows changes after the configuration file has been uploaded.

Global Settings

The **Global Settings** page of the wizard is where the following settings are entered:

- Top-level DNS Domain
- Chosen vCenter Implementation
- DNS Server type and IP Addresses
- vSphere HA Isolation Address
- Optional NTP and Syslog Servers information

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the 'Dell VxRail Deployment Wizard' interface. The left sidebar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings (which is selected), 8. VMware VDS Settings, 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings, 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration. The main panel is titled 'Global Settings' and shows 'VxRail Cluster Type: Standard (3 hosts)'. It includes fields for 'Top Level Domain' (delledu.lab), 'vCenter Server' (radio buttons for 'VxRail-managed VMware vCenter Server' and 'Customer-managed VMware vCenter Server'), 'DNS Server' (radio buttons for 'Internal (VxRail Manager Service)' and 'External'), 'DNS Server IPv4 Address(es)', 'vSphere HA Isolation Address' (radio buttons for 'No Isolation Address' and 'Isolation Address'), 'NTP Server' (radio buttons for 'No NTP Server' and 'NTP Server'), and 'NTP Server IPv4 address(es) or FQDN(s)'. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Global Settings



Tip: A comma-separated list of IP addresses (DNS, NTP, Syslog) or Hostnames (NTP and Syslog) can be used when entering multiple IP addresses.

VMware Virtual Distributed Switch (VDS) Settings

The **VMware VDS Settings** page is where the VDS and NIC information is configured.

There are two types of configurations for a VDS:

1. The **Predefined** VDS Configuration provides a default configuration that is based on the number of NICs selected.
2. The **Custom** VDS Configuration allows flexibility in the virtual network configuration.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The title bar reads "Dell VxRail Deployment Wizard". On the left, a vertical navigation menu lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings (which is highlighted in blue), 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings, 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration. The main content area is titled "VMware VDS Settings" and displays the "General" configuration. It shows the "vCenter Server" as "VxRail-managed VMware vCenter Server". Under "VDS Configuration", it is set to "Predefined". Under "NIC configuration", it is set to "4x10GbE or Higher". At the bottom right of the content area are three buttons: "CANCEL", "BACK", and "NEXT". Above the content area, a note says "VxRail Cluster Type: Standard (3 hosts)".

VDS Settings

VMware vCenter Server Settings

The **VMware vCenter Server Settings** page is where the vCenter Server FQDN, vCenter login credentials, and vCenter Management credentials are entered.

Deploy a Standard VxRail Cluster With vSAN OSA

VMware vCenter Server Settings
VxRail Cluster Type: Standard (3 hosts)

Provide the VMware vCenter Server configuration settings for the VxRail cluster.

VMware vCenter Server

VMware vCenter Server ⓘ VxRail vCenter Server
Automatically accept the VMware vCenter Server trusted root CA certificates ⓘ *

Yes No

VMware vCenter Server Hostname * vxrail-vcenter

Preview vxrail-vcenter.delledu.lab

VMware vCenter Server IPv4 Address * 172.16.5.13

Join an existing VMware SSO domain
Yes No

Same Password For All Accounts
Yes No

CANCEL BACK NEXT

vCenter Server Settings



Important: If the configuration file is uploaded, the file will not have the passwords and would require manual entry.

Host Settings

The **Host Settings** page is where the rack and host information is entered.

There are two Host Configuration Methods:

1. The **Autofill** method enables hostnames to be generated based on a pattern and assigns IP addresses sequentially from a starting IP address.
2. The **Advanced** method allows flexibility in the specification of the host configuration details, for example unique names or nonconsecutive IP addresses.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The left sidebar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings, 9. VMware vCenter Server Settings, 10. Host Settings (which is selected and highlighted in blue), 11. VxRail Manager Settings, 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration.

The main panel is titled "Host Settings" and displays the configuration for a "Standard (3 hosts)" cluster. It includes sections for "ESXi Hosts", "Hosts", and "Preview".

- Host Configuration Method:** Advanced (selected)
- Same Rack For All Hosts:** No (selected)
- Same Credentials For All Hosts:** No (selected)
- Hosts:**
 - Service Tag: V073001
 - PSNT: V07300100000000
 - ESXi Hostname: vcluster730-esx01
 - Preview: vcluster730-esx01.delledu.lab
 - ESXi IPv4 Address: 172.16.5.51
- Buttons at the bottom:** CANCEL, BACK, and NEXT (highlighted in blue)

Host Settings

VxRail Manager Settings

The **VxRail Manager Settings** page is where the hostname, IP address, and account passwords for the VxRail Manager are entered.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. On the left, a vertical navigation bar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings, 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings (which is selected and highlighted in blue), 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration. The main panel is titled "VxRail Manager Settings" and displays the configuration for a "Standard (3 hosts)" cluster. It includes fields for "VxRail Manager Hostname" (vxrail-manager), "VxRail Manager IPv4 Address" (172.16.5.16), "VxRail Manager Root Username" (root), "VxRail Manager Root Password" (redacted), "Re-enter VxRail Manager Root Password" (redacted), "VxRail Manager Service Account Username" (mystic), and "VxRail Manager Service Account Password" (redacted). At the bottom are "CANCEL", "BACK", and "NEXT" buttons.

VxRail Manager Settings

Important: Dell Support uses the **VxRail Manager Service Account** (mystic) to access the VxRail Manager VM. The root account does not allow SSH login access, Dell Support logs in as mystic first. The root and mystic user account passwords must be different.

Virtual Network Settings

On the **Virtual Network Settings** page, the VxRail Management Network, vSAN, and vMotion network information are entered. If a Guest Network is to be used, that network information is entered as well.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The left sidebar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings, 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings, 12. Virtual Network Settings (highlighted in blue), 13. Validate Configuration, and 14. Deploy Configuration. The main panel is titled "Virtual Network Settings" and displays "VxRail Cluster Type: Standard (3 hosts)". It provides configuration settings for the "VxRail Management Network" and "vSAN". Under "VxRail Management Network", the Management Subnet Mask is set to 255.255.255.0, the Management Gateway IPv4 Address is 172.16.5.1, and the Management VLAN ID is 5. The Port Binding option is set to "Ephemeral Binding". Under "vSAN", the VSAN Configuration Method is set to "Advanced", the ESXi Hostname is vcluster730-esx01, and the VSAN IPv4 Address is 172.16.10.51. At the bottom right are "CANCEL", "BACK", and "NEXT" buttons.

Virtual Network Settings

Validate Configuration

The **Validate Configuration** page is where VxRail Manager verifies that the entered configuration matches the physical environment.

The validation process may require several minutes depending on the cluster size and type.

Deploy a Standard VxRail Cluster With vSAN OSA

Dell VxRail Deployment Wizard

VxRail Cluster Type: Standard (3 hosts)

1 Welcome
2 End User License Agreement
3 Cluster Type
4 Resources
5 Network Confirmation
6 Configuration Method
7 Global Settings
8 VMware VDS Settings
9 VMware vCenter Server Settings
10 Host Settings
11 VxRail Manager Settings
12 Virtual Network Settings
13 Validate Configuration
14 Deploy Configuration

VALIDATE CONFIGURATION

CANCEL BACK NEXT

Validation Configuration



Important: If any errors are reported, they are summarized in red text on the screen. Select **View Log** for more details.

Deploy Configuration

When the configuration is successfully verified, the deployment process is ready to begin.

Deploy a Standard VxRail Cluster With vSAN OSA

Dell VxRail Deployment Wizard

Deploy Configuration VxRail Cluster Type: Standard (3 hosts)

1 Welcome
2 End User License Agreement
3 Cluster Type
4 Resources
5 Network Confirmation
6 Configuration Method
7 Global Settings
8 VMware VDS Settings
9 VMware vCenter Server Settings
10 Host Settings
11 VxRail Manager Settings
12 Virtual Network Settings
13 Validate Configuration
14 Deploy Configuration

CANCEL BACK DEPLOY CONFIGURATION

Deploy Configuration



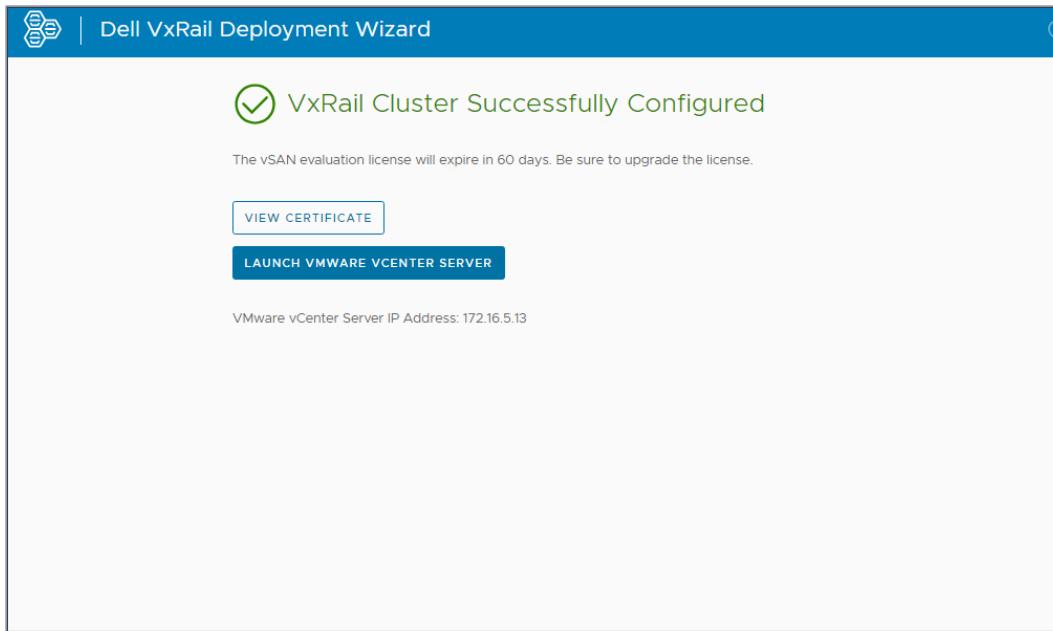
Tip: If using the default IP to start configuration, when notified, redirect to the new VxRail Manager IP to complete the deployment.

Deployment Complete

This page shows a successful deployment. The final configuration file and certificate can be downloaded for use later.

To verify that the cluster was properly deployed and configured, launch vCenter to begin the post-deployment verification process.

Deploy a Standard VxRail Cluster With vSAN OSA



Deployment Complete

Interaction: Deploy a standard VxRail Cluster with VxRail-managed vCenter and predefined VDS

The web version of this content contains an interactive activity.

Prepare a Customer-Supplied vCenter Server for VxRail Deployment

The details of the customer-supplied vCenter Server are documented in the VxRail Configuration Report that is available in the VxRail Configuration Portal. [Example of a VxRail Configuration Report](#).

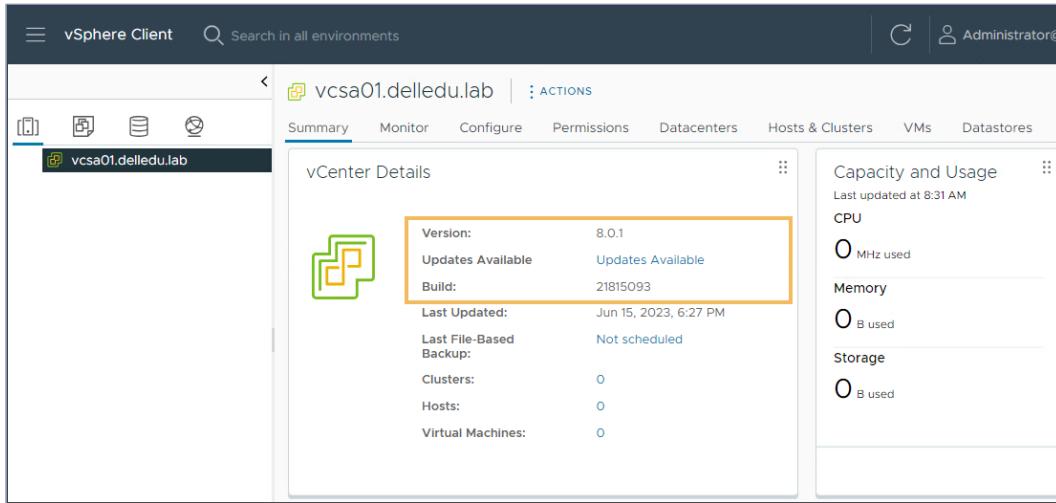
Before beginning the deployment, log in to the vSphere Client, review the vCenter Server version, and verify the required data center and vCenter Server accounts. To learn more about these tasks, select each tab.

vCenter Server Version

Confirm that the vCenter Server version is at the supported version as documented in the [VxRail and external vCenter interoperability matrix](#). For

Deploy a Standard VxRail Cluster With vSAN OSA

example, the recommended vCenter Server version for VxRail 8.0.100 is 8.0 U1a (8.0.1.00100) or later¹.



The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The user is signed in as "Administrator@...". The main pane displays "vCenter Details" for the host "vcsa01.delledu.lab". The "Version" field is highlighted with an orange box and contains "8.0.1". Other details shown include "Updates Available" and "Build: 21815093". To the right, there's a "Capacity and Usage" section showing 0 MHz used for CPU, 0 B used for Memory, and 0 B used for Storage. The navigation bar at the top includes tabs for Summary, Monitor, Configure, Permissions, Datacenters, Hosts & Clusters, VMs, and Datastores.

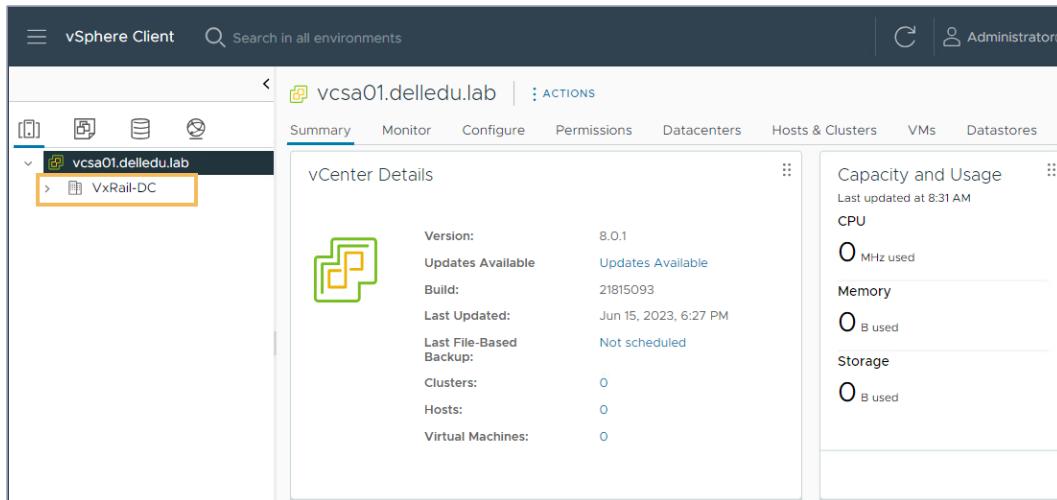
vCenter Server Version

¹ The interoperability matrix does not list the build number that is displayed in the vSphere Client. View [VMware KB 2143838](#) for the correlation between vCenter Server versions and build numbers. For example, vCenter Server 8.0 U1a (8.0.1.00100) correlates to build 21815093.

Data Center

Confirm that the required data center exists in vCenter and that there is not a cluster with the proposed name within the data center. If the data center does not exist, create the data center in vCenter.

Deploy a Standard VxRail Cluster With vSAN OSA



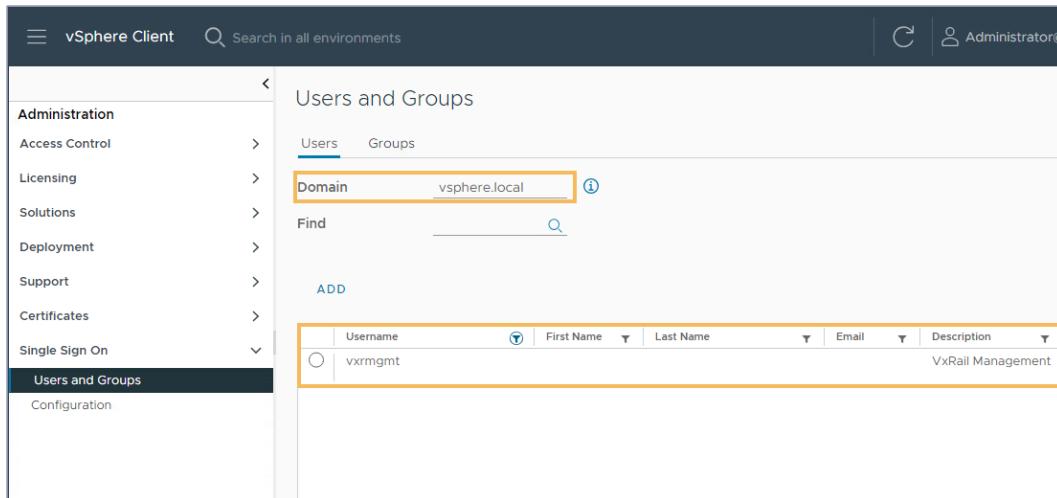
vCenter Server - Data Center created

User account for VxRail Management

Confirm that the VxRail Management user account exists and is assigned either the **VMware HCIA Management** role or no role. VMware HCIA Management role would exist if another VxRail cluster was already attached to the same vCenter. The VxRail Management user must be part of the tenant SSO domain.

If the VxRail Management user does not exist, create the user account with no role assignments. The VxRail deployment process assigns the **VMware HCIA Management** role. Review Task 24 of the example SolVe procedure.

Deploy a Standard VxRail Cluster With vSAN OSA



The screenshot shows the 'Users and Groups' section of the vSphere Client. The left sidebar has 'Administration' selected. In the main area, 'Users' is selected under 'Users and Groups'. The 'Domain' dropdown is set to 'vsphere.local'. A table lists users, with one entry for 'vxrmgmt' highlighted by an orange box. The table columns are: Username, First Name, Last Name, Email, and Description. The description for 'vxrmgmt' is 'VxRail Management'.

Username	First Name	Last Name	Email	Description
vxrmgmt				VxRail Management

VxRail Management User

User account for VxRail Configuration

Confirm that the vCenter Server user account that is used for the VxRail configuration exists. While the existing vCenter Server administrator account can be used, if security is a concern, create a VxRail configuration user account for the deployment.

The VxRail configuration user account requires roles with specific privileges. Review Task 25 of the example SolVe procedure.

Create and assign the following roles to the new VxRail configuration user:

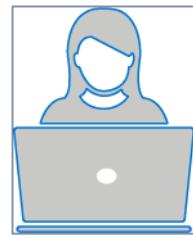
- VxRail Initial Global
- VxRail Datacenter Global

Lab 6: Prepare the Customer-Supplied vCenter Server

You are getting ready to deploy a VxRail cluster by joining a customer-supplied vCenter Server. You want to prepare the customer-supplied vCenter Server for the VxRail deployment.

Lab Tasks

- Log in to the customer-supplied vCenter Server.
- Check the vCenter Server version.
- Create the VxRail Management user.
- Create the data center.



VxRail with customer-supplied vCenter Server - Deployment Wizard Settings

The Deployment Wizard settings that are specific to a VxRail cluster with a customer-supplied vCenter Server are in the following pages:

- Global Settings
- vCenter Server Settings
- VDS Settings

Global Settings

For a customer-supplied vCenter Server, select **Customer-managed VMware vCenter Server**. The **DNS Server** is automatically set to **External**.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The left sidebar lists 14 steps, with step 7 'Global Settings' highlighted. The main panel displays 'Global Settings' for a 'Standard (3 hosts)' cluster. Key configurations shown include:

- General:** Top Level Domain is set to `delledu.lab`.
- vCenter Server:** The 'Customer-managed VMware vCenter Server' option is selected.
- DNS Server:** Set to `External`.
- NTP Server:** The 'NTP Server' radio button is selected.
- Logging:** Set to `No Logging`.

At the bottom right are buttons for `CANCEL`, `BACK`, and `NEXT`.

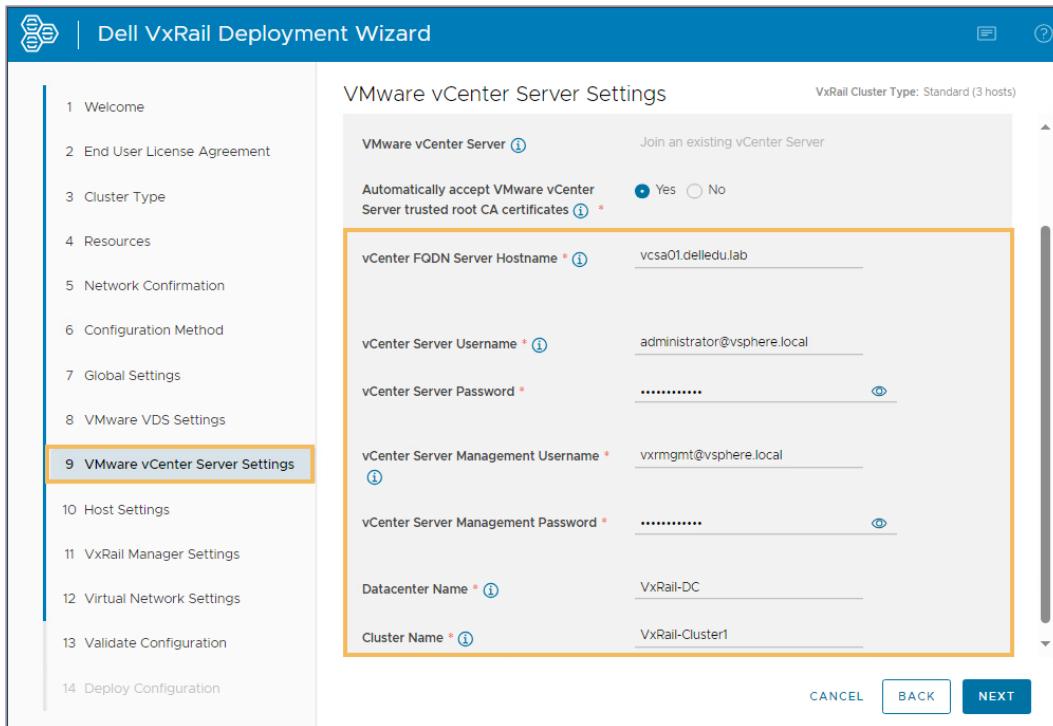
Global Settings for a customer-supplied vCenter Server

VMware vCenter Server Settings

Settings for a customer-supplied vCenter Server:

- vCenter FQDN Server Hostname** - Fully qualified name of the customer-supplied vCenter Server
- vCenter Server Username** - User account with sufficient privileges for VxRail configuration
- vCenter Server Management Username** - VxRail Management user account
- Datacenter Name** - Existing data center
- Cluster Name** - Unique name for new VxRail cluster

Deploy a Standard VxRail Cluster With vSAN OSA



Customer-supplied vCenter Server Settings

New Custom VDS - Deployment Wizard Settings

For customized VDS configurations, the **VDS Settings** page has a **General** section and sections for each **VDS**.

To learn how to set the VDS Settings for a customized VxRail deployed VDS, select each tab.

VDS Settings - General

For a customized VxRail deployed VDS, in the **General** section, set the **VDS Configuration** to **Custom**, **VDS Type** to **New**, and specify the **Number of VDS**.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the Dell VxRail Deployment Wizard interface. The left sidebar lists 14 steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, 6. Configuration Method, 7. Global Settings, 8. VMware VDS Settings (highlighted with a yellow box), 9. VMware vCenter Server Settings, 10. Host Settings, 11. VxRail Manager Settings, 12. Virtual Network Settings, 13. Validate Configuration, and 14. Deploy Configuration.

The main panel title is "VMware VDS Settings" and the sub-section title is "General". It displays the following configuration:

- vCenter Server: Customer-managed VMware vCenter Server
- VDS Configuration: Custom (radio button selected)
- VDS Type: New (radio button selected)
- Number of VDS: 1 (radio button selected)

Below this, the "VDS" section contains:

- MTU: 5000
- Host NICs: 2 (radio button selected)
- VDS LAG: Yes (radio button selected)

At the bottom right are "CANCEL", "BACK", and "NEXT" buttons.

VMware Custom New VDS Settings - General

VDS Settings - VDS

In the VDS section, set the **MTU**, the number of **Host NICs**, **NIC configuration**, and **VDS Port Group Teaming and Failover** policies.

In the example, the MTU is set and two NICs are mapped to uplinks. All the port groups are configured as active/active.

Deploy a Standard VxRail Cluster With vSAN OSA

The screenshot shows the 'VDS' configuration page. It includes fields for MTU (set to 5000), Host NICs (selected as 2), and VDS LAG (set to No). Under 'NIC configuration', two uplinks are defined: 'Uplink1' (vmnic2) and 'Uplink2' (vmnic3). The 'VMware VDS Port Group Teaming and Failover' section lists traffic types and their teaming policies:

Network Traffic Type	Active	Active/Standby	Teaming Policy	Load Balancing	VMkernel MTU
Discovery *	uplink1	uplink2	active/active	Route based on physical NIC load	1500
Management *	uplink2	uplink1	active/active	Route based on physical NIC load	1500
vCenter Server *	uplink1	uplink2	active/active	Route based on physical NIC load	
vSAN *	uplink2	uplink1	active/active	Route based on physical NIC load	5000
vMotion *	uplink1	uplink2	active/active	Route based on physical NIC load	5000
Guest VM (optional)	uplink1	uplink2	active/active	Route based on physical NIC load	

VMware Custom New VDS Settings

VxRail Deployment with Existing VDS

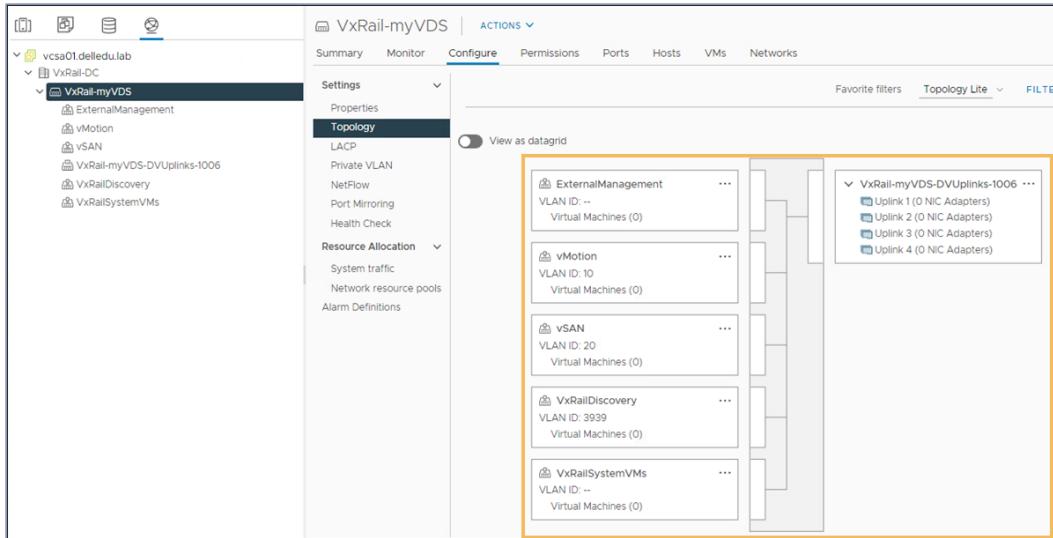
The details of the existing VDS are documented in the VxRail Configuration report and in the VxRail Configuration JSON file. [Excerpt of JSON with VDS details.](#)

Before deploying the VxRail cluster, log in to the vCenter Server and verify the VDS settings. The existing VDS settings must match the details in the VxRail Configuration report. The values are case-sensitive. Excerpt of SolVe procedure to verify VDS settings.

Key settings to verify:

- Names of VDS, uplinks, and port groups
- Number of uplinks
- Details of each port group

Deploy a Standard VxRail Cluster With vSAN OSA



Existing VDS - Four uplinks, port groups for external management, VxRail discovery, vSAN, vMotion, and VxRail system VMs

Existing Custom VDS - Deployment Wizard Settings

The **VDS Settings** page of the Deployment Wizard has settings that are specific for a VxRail cluster that is deployed with an existing VDS.

To learn how to set the VDS Settings, select each tab.

[VDS Settings - General](#)

For an existing VDS, in the **General** section, set the **VDS Configuration** to **Custom**, **VDS Type** to **Existing**, and specify the **Number of VDS**.

Deploy a Standard VxRail Cluster With vSAN OSA

VMware VDS Settings

VxRail Cluster Type: Standard (3 hosts)

Provide the VMware VDS configuration settings that will be applied to the hosts in the VxRail cluster.

General

vCenter Server <small> ⓘ </small>	Customer-managed VMware vCenter Server
VDS Configuration <small> * ⓘ </small>	<input type="radio"/> Predefined <input checked="" type="radio"/> Custom
VDS Type <small> * ⓘ </small>	<input type="radio"/> New <input checked="" type="radio"/> Existing
Number of VDS <small> * ⓘ </small>	<input checked="" type="radio"/> 1 <input type="radio"/> 2

VMware Custom Existing VDS Settings - General

VDS Settings - VDS

In the top part of the VDS section, specify the **VDS Name**, set the number of **Host NICs**, and if applicable **VDS LAG**.

Under **NIC configuration**, specify the uplink names and select NICs.

Under **VDS Port Group Teaming and Failover**, specify the port group names and the **VMkernel MTU**. The MTU value cannot exceed the MTU configured on the VDS.

Deploy a Standard VxRail Cluster With vSAN OSA

VDS

VDS Name * i	VxRail-myVDS	
Host NICs	<input type="radio"/> 2 <input checked="" type="radio"/> 4 <input type="radio"/> 6 <input type="radio"/> 8	
VDS LAG i	<input type="radio"/> Yes <input checked="" type="radio"/> No	
NIC configuration		
Uplink	Uplink Name	NIC
Uplink1 *	Uplink 1	vminic0 - Intel(R) Ethernet 10G 4P X550 rNDC INTEGRATED: 1, Port: 1
Uplink2 *	Uplink 2	vminic1 - Intel(R) Ethernet 10G 4P X550 rNDC INTEGRATED: 1, Port: 2
Uplink3 *	Uplink 3	vminic2 - Intel(R) Ethernet 10G 4P X550 rNDC INTEGRATED: 1, Port: 3
Uplink4 *	Uplink 4	vminic3 - Intel(R) Ethernet 10G 4P X550 rNDC INTEGRATED: 1, Port: 4
VMware VDS Port Group Teaming and Failover		
Network Traffic Type	Port Group Name	VMkernel MTU i
Discovery *	VxrailDiscovery	1500
Management *	ExternalManagement	1500
vCenter Server *	VxRailSystemVMs	
vSAN *	vSAN	5000
vmotion *	vmotion	5000

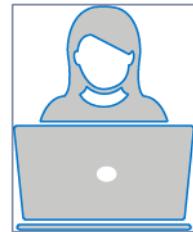
VMware Custom Existing VDS Settings - Four NICs, no LAG

Lab 7: VxRail Deployment with a Customer-Supplied vCenter Server and Custom VDS

You are ready to deploy a VxRail cluster with an customer-supplied vCenter Server and a customized VxRail deployed VDS.

Lab Tasks

- Launch the VxRail Deployment Wizard.
- Upload the VxRail configuration file.
- Validate the VxRail configuration.
- Deploy the VxRail cluster.



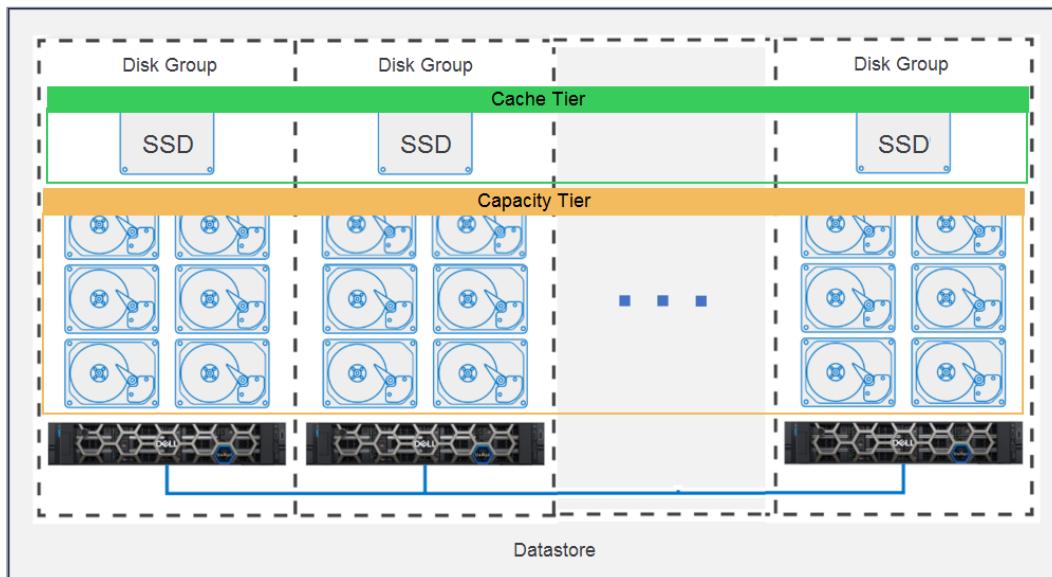
Deploy a Standard VxRail Cluster With vSAN ESA

vSan Storage Architecture

vSAN offers two storage architectures. The Original Storage Architecture (OSA) and Express Storage Architecture (ESA). To learn more about the two architectures, select each tab.

OSA

OSA is based on disk groups that contain a single cache drive that is partnered with multiple capacity drives. Performance and capacity are balanced based on number and size of disk groups. VM I/O passes through the cache tier before interacting with the capacity tier. OSA supports flash for cache while capacity drives can either be flash or hard disk drives.



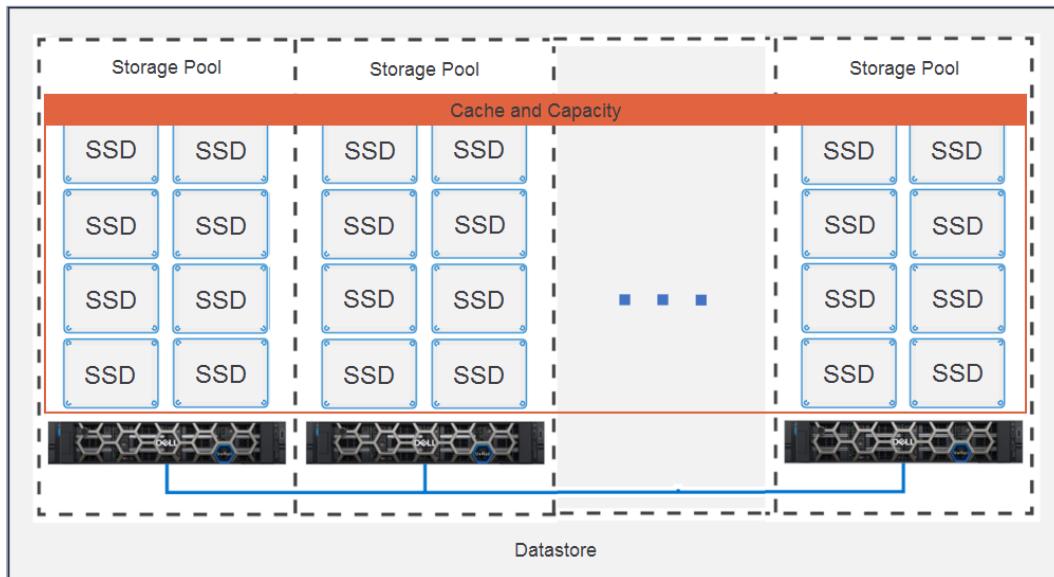
OSA Architecture

ESA

ESA is based on storage pools where all disks contribute cache and capacity resources. It is a single-tier architecture that is optimized for high-performance NVMe based flash devices. Performance and capacity are

Deploy a Standard VxRail Cluster With vSAN ESA

balanced across the entire datastore. ESA provides simplified management, smaller failure domains, and supports NVMe drives only.



ESA Architecture



Deep Dive: For more information, go to [An Introduction to the vSAN Express Storage Architecture](#) and [Comparing the Original Storage Architecture to the vSAN eight Express Storage Architecture](#).

vSAN ESA Software Requirements

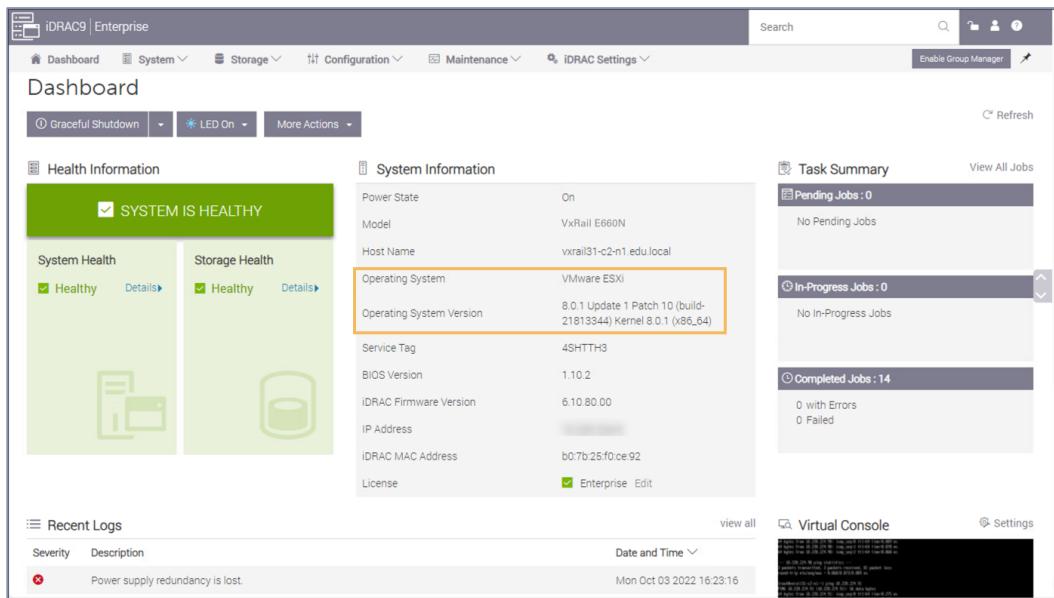
vSAN ESA requires vSphere ESXi 8.0 on each node in the cluster, and a vSphere vCenter 8.0. A Customer-supplied vCenter must be upgraded to version 8.0 before beginning the deployment.

To learn more about how to verify the vSphere software versions, select each tab.

Deploy a Standard VxRail Cluster With vSAN ESA

vSphere ESXi

The current ESXi version on each node can be verified in the **System Information** section on the iDRAC Dashboard.



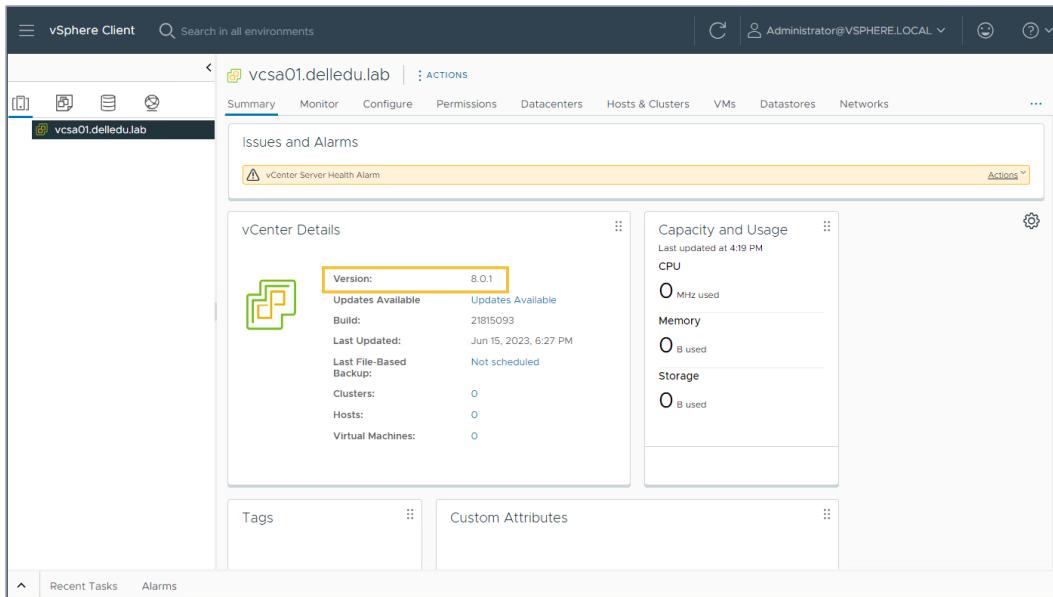
The screenshot shows the iDRAC9 Enterprise dashboard. In the center, under 'System Information', the 'Operating System Version' is highlighted and shows '8.0.1 Update 1 Patch 10 (build-21813344) Kernel 8.0.1 (x86_64)'. To the right, the 'Task Summary' section shows 'Pending Jobs : 0', 'In-Progress Jobs : 0', and 'Completed Jobs : 14'. At the bottom left, the 'Recent Logs' section shows a single log entry: 'Power supply redundancy is lost.' with a timestamp of 'Mon Oct 03 2022 16:23:16'.

iDRAC Dashboard with the ESXi 8.0 version identified

vSphere vCenter

The current vCenter version can be verified in the **Summary** tab of the vCenter appliance in the vSphere Client.

Deploy a Standard VxRail Cluster With vSAN ESA



vCenter appliance Summary tab with the vCenter 8.0 version identified

vSAN ESA Hardware Requirements

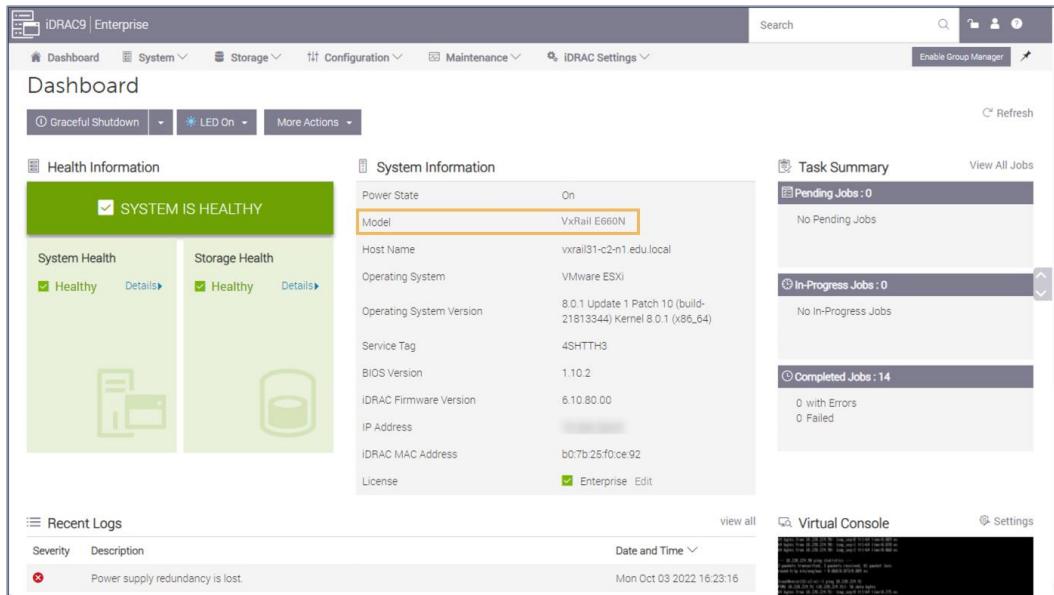
vSAN ESA is supported on P670N and E660N models only. Depending on the VxRail model, each node must have a minimum of 16-32 CPU cores and a minimum of 128-512 GB memory capacity. All nodes in the cluster must be the same model and configuration to deploy successfully.

To learn more about verifying the hardware requirements, select each tab.

Model

The VxRail model can be verified in the **System Information** section on the **iDRAC Dashboard**.

Deploy a Standard VxRail Cluster With vSAN ESA

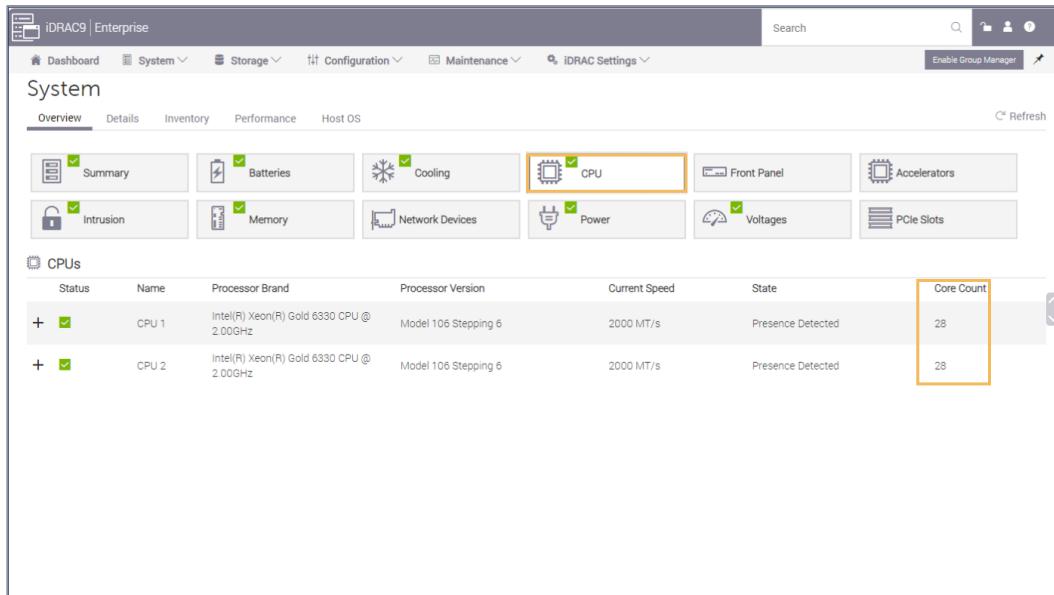


The screenshot shows the iDRAC9 Enterprise Dashboard. In the 'System Information' section, the 'Model' field is highlighted with an orange box, showing 'VxRail E660N'. Other details include Power State (On), Host Name (vxrail31-c2-n1.edu.local), Operating System (VMware ESXi), and Service Tag (4SH7TH3). The 'Task Summary' section shows 0 pending, 0 in-progress, and 14 completed jobs. The 'Recent Logs' section shows a single entry: 'Power supply redundancy is lost' on Mon Oct 03 2022 16:23:16.

iDRAC Dashboard with the VxRail model identified

CPU

The number of CPU cores can be verified on the iDRAC **System > CPU** page. The image below shows a total of 56 cores in the node.



The screenshot shows the iDRAC9 Enterprise System > CPU page. The 'CPU' icon is highlighted with an orange box. The table lists two CPUs: CPU 1 (Intel Xeon Gold 6330 @ 2.00GHz, Model 106 Stepping 6) and CPU 2 (Intel Xeon Gold 6330 @ 2.00GHz, Model 106 Stepping 6). Both have a current speed of 2000 MT/s and a state of 'Presence Detected'. The 'Core Count' column for both is highlighted with an orange box and shows the value 28.

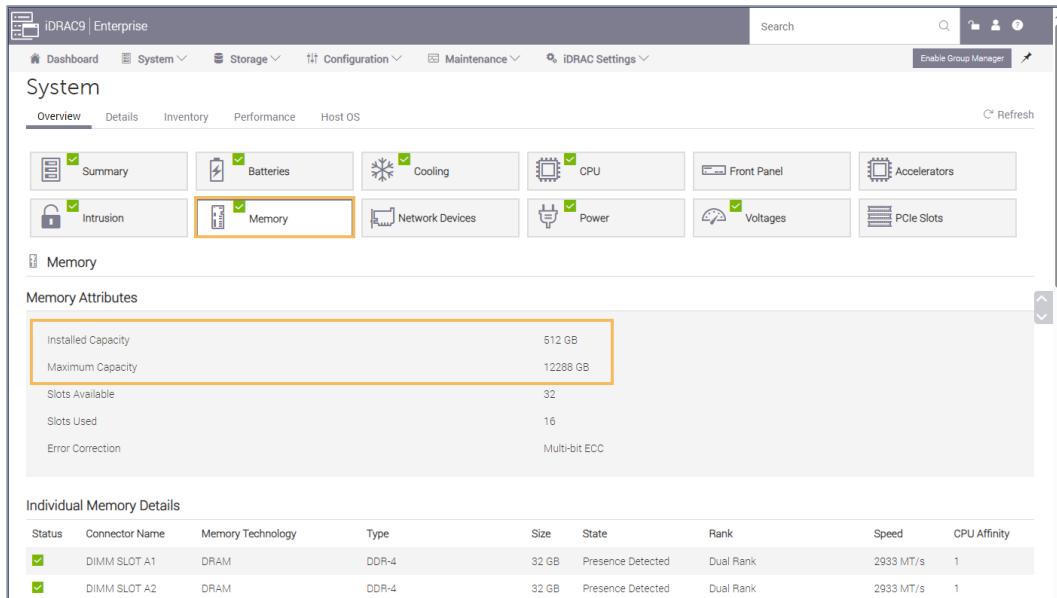
Status	Name	Processor Brand	Processor Version	Current Speed	State	Core Count
+ <input checked="" type="checkbox"/>	CPU 1	Intel(R) Xeon(R) Gold 6330 CPU @ 2.00GHz	Model 106 Stepping 6	2000 MT/s	Presence Detected	28
+ <input checked="" type="checkbox"/>	CPU 2	Intel(R) Xeon(R) Gold 6330 CPU @ 2.00GHz	Model 106 Stepping 6	2000 MT/s	Presence Detected	28

iDRAC System > CPU page with the number of CPU cores identified

Deploy a Standard VxRail Cluster With vSAN ESA

Memory

The memory capacity of each node can be verified on the **iDRAC System > Memory** page.



The screenshot shows the iDRAC9 Enterprise interface with the 'System' tab selected. Under 'System', the 'Memory' tab is highlighted with an orange border. In the 'Memory Attributes' section, the 'Installed Capacity' and 'Maximum Capacity' are both listed as 512 GB. Below this, 'Slots Available' is 32 and 'Slots Used' is 16. The 'Error Correction' is listed as Multi-bit ECC. At the bottom, there is a table titled 'Individual Memory Details' showing two entries: DIMM SLOT A1 and DIMM SLOT A2, both of which are DRAM DDR-4 type, 32 GB size, and show 'Presence Detected' status.

Status	Connector Name	Memory Technology	Type	Size	State	Rank	Speed	CPU Affinity
✓	DIMM SLOT A1	DRAM	DDR-4	32 GB	Presence Detected	Dual Rank	2933 MT/s	1
✓	DIMM SLOT A2	DRAM	DDR-4	32 GB	Presence Detected	Dual Rank	2933 MT/s	1

iDRAC System > Memory page with the memory capacity identified

vSAN ESA Drive Requirements

vSAN ESA is supported only with qualified NVMe drives. Depending on the VxRail model, ESA requires a minimum of four to six NVMe drives per VxRail node. Disk drives must populate the disk slots sequentially starting in slot 0. Bus protocol is PCIe for supported NVMe drives.

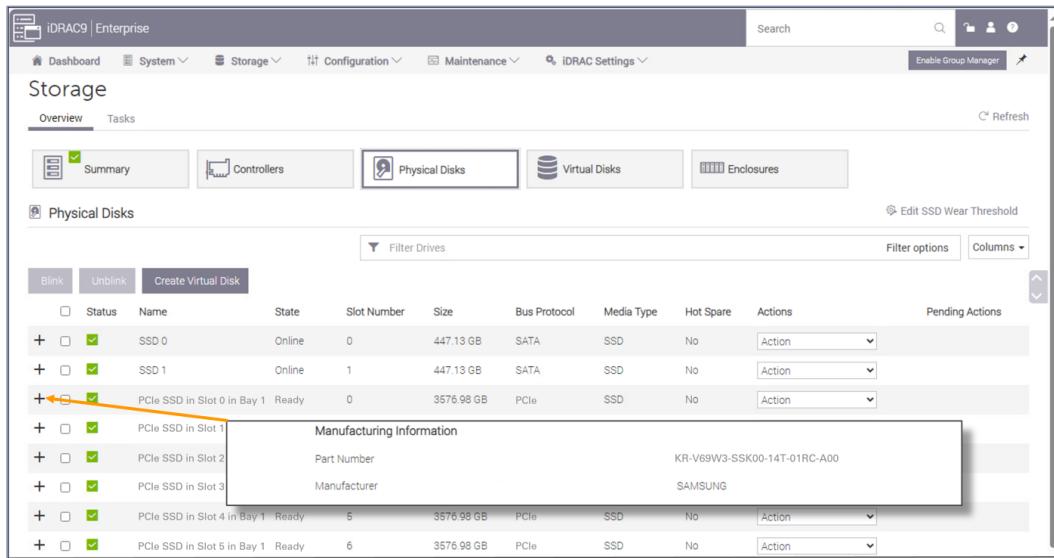
To learn more about verifying the NVMe drive requirements, select each tab.

Vendor

The **Manufacturer** and **Part Number** can be verified on the **iDRAC Storage > Physical Disks** page. Select the **Plus (+)** sign next to the drive and scroll down to **Manufacturing Information**.

Deploy a Standard VxRail Cluster With vSAN ESA

See the [VxRail 8.X Support Matrix pg 57](#) for the complete list of supported NVMe manufacturers and models.



The screenshot shows the iDRAC9 Enterprise interface with the 'Storage' tab selected. Under 'Physical Disks', a list of drives is displayed. A context menu is open over the first drive, labeled 'PCIe SSD in Slot 1'. The menu displays 'Manufacturing Information' with the part number 'KR-V69W3-SSK00-14T-01RC-A00' and the manufacturer 'SAMSUNG'.

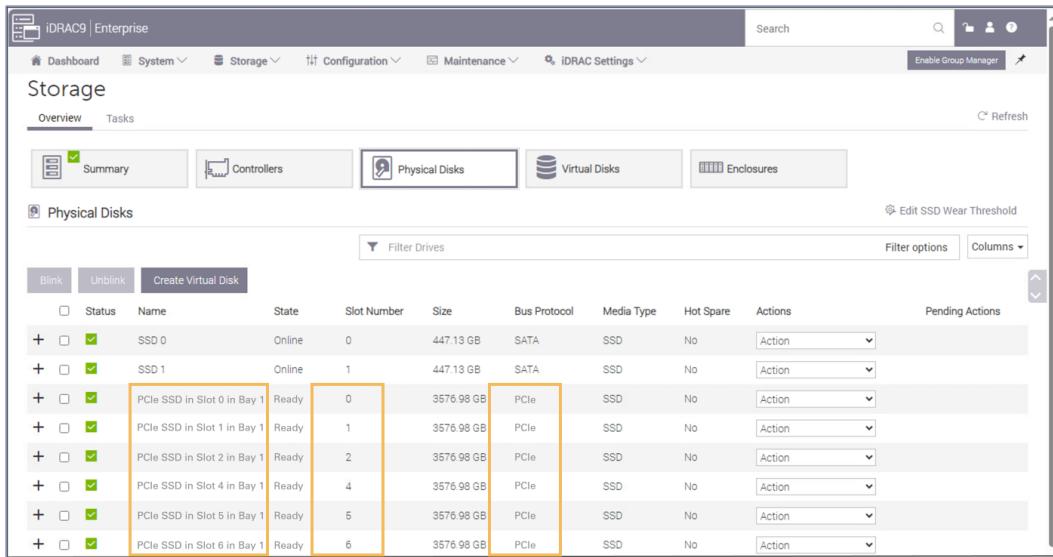
Slot Number	Size	Bus Protocol	Media Type	Hot Spare	Action
0	447.13 GB	SATA	SSD	No	Action
1	447.13 GB	SATA	SSD	No	Action
Ready	3576.98 GB	PCIe	SSD	No	Action
Ready	3576.98 GB	PCIe	SSD	No	Action
Ready	3576.98 GB	PCIe	SSD	No	Action
Ready	3576.98 GB	PCIe	SSD	No	Action

iDRAC Storage > Physical Disks page with the Part Number and Manufacturer identified

Disk Placement

The number of drives and their placement can be verified on the iDRAC **Storage > Physical Disks** page. See the [VxRail 8.X Support Matrix](#) for more information on Disk slots for a given VxRail Model.

Deploy a Standard VxRail Cluster With vSAN ESA



The screenshot shows the iDRAC Storage interface with the 'Physical Disks' tab selected. A table lists physical disks with columns for Status, Name, State, Slot Number, Size, Bus Protocol, Media Type, Hot Spare, Actions, and Pending Actions. Six NVMe drives are highlighted with orange boxes around their Slot Number, Size, and Bus Protocol columns. The drives are labeled: PCIe SSD in Slot 0 in Bay 1, PCIe SSD in Slot 1 in Bay 1, PCIe SSD in Slot 2 in Bay 1, PCIe SSD in Slot 4 in Bay 1, PCIe SSD in Slot 5 in Bay 1, and PCIe SSD in Slot 6 in Bay 1. All are listed as Ready, 3576.98 GB, PCIe, SSD, No, and Action.

Status	Name	State	Slot Number	Size	Bus Protocol	Media Type	Hot Spare	Actions	Pending Actions
+	SSD 0	Online	0	447.13 GB	SATA	SSD	No	Action	
+	SSD 1	Online	1	447.13 GB	SATA	SSD	No	Action	
+	PCIe SSD in Slot 0 in Bay 1	Ready	0	3576.98 GB	PCIe	SSD	No	Action	
+	PCIe SSD in Slot 1 in Bay 1	Ready	1	3576.98 GB	PCIe	SSD	No	Action	
+	PCIe SSD in Slot 2 in Bay 1	Ready	2	3576.98 GB	PCIe	SSD	No	Action	
+	PCIe SSD in Slot 4 in Bay 1	Ready	4	3576.98 GB	PCIe	SSD	No	Action	
+	PCIe SSD in Slot 5 in Bay 1	Ready	5	3576.98 GB	PCIe	SSD	No	Action	
+	PCIe SSD in Slot 6 in Bay 1	Ready	6	3576.98 GB	PCIe	SSD	No	Action	

iDRAC Storage > Physical Disks page with the Name, Slot Number, and Bus Protocol of the NVMe drives identified

Verify vSAN ESA Licensing

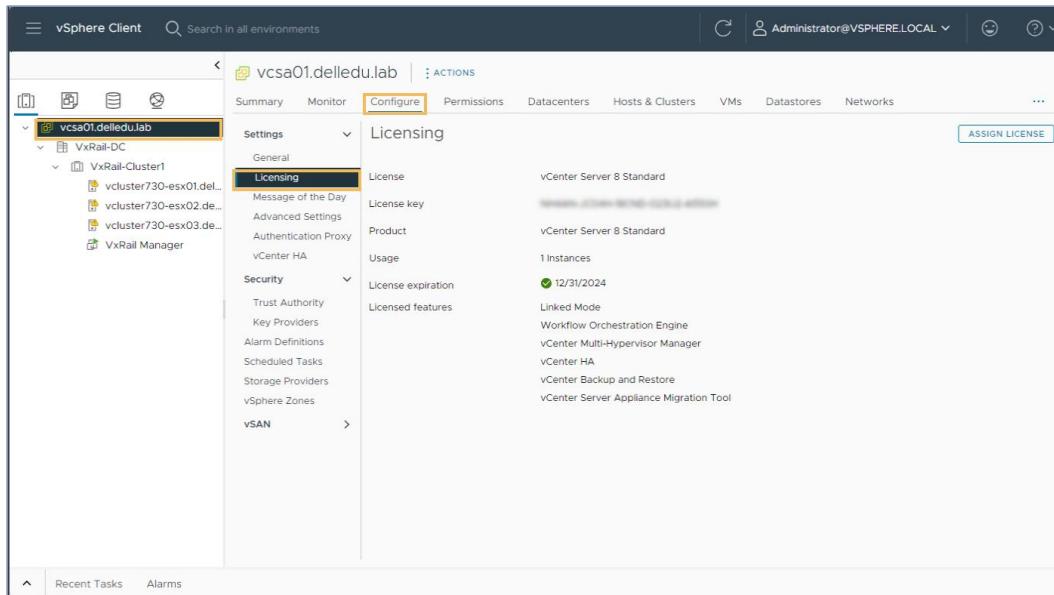
To learn more about how to verify the vSphere software licenses, select each tab.

vCenter License

A vCenter version 8 license is required for vCenter instances supporting a VxRail cluster running ESA.

To verify the vCenter license, select the vCenter appliance and go to **Configure > Settings > Licensing**.

Deploy a Standard VxRail Cluster With vSAN ESA



The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The top navigation bar includes "vcsa01.delledu.lab", "Actions", "Administrator@VSPHERE.LOCAL", and a help icon. Below the title bar, the left sidebar shows a tree structure: "vcsa01.delledu.lab" expanded to show "VxRail-DC" which contains "VxRail-Cluster1" (with three sub-items: "vccluster730-esx01.dell...", "vccluster730-esx02.dell...", "vccluster730-esx03.dell...") and "VxRail Manager". The main content area has tabs: "Configure" (highlighted), "Monitor", "Permissions", "Datacenters", "Hosts & Clusters", "VMs", "Datastores", and "Networks". Under "Configure", the "Licensing" tab is selected. The "General" section shows "License" as "vCenter Server 8 Standard". The "Product" section shows "vCenter Server 8 Standard". The "Usage" section shows "1 Instances" with a green checkmark next to "12/31/2024". The "Licensed features" section lists "Linked Mode", "Workflow Orchestration Engine", "vCenter Multi-Hypervisor Manager", "vCenter HA", "vCenter Backup and Restore", and "vCenter Server Appliance Migration Tool". A blue button "ASSIGN LICENSE" is located at the top right of the "Licensing" section.

vCenter Server Configure Licensing page showing the vCenter license

vSAN License

ESA requires either a vSAN Advanced, Enterprise, or Enterprise Plus license.

To verify the vSAN license, select the VxRail cluster and go to **Configure > Licensing > vSAN Cluster**.

Deploy a Standard VxRail Cluster With vSAN ESA

The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The top navigation bar includes "Actions", "Administrator@VSPHERE.LOCAL", and help icons. The left sidebar shows a hierarchy: "vcsa01.delledu.lab" > "VxRail-DC" > "VxRail-Cluster1". The main content area has tabs: "Summary", "Monitor", "Configure" (which is selected and highlighted in orange), "Permissions", "Hosts", "VMs", "Datastores", "Networks", and "Updates". Under "Configure", there are sections for "Services", "vSphere DRS", "vSphere Availability", "Configuration" (with sub-options like "Quickstart", "General", "Key Provider", "VMware EVC", "VM/Host Groups", "VM/Host Rules", "VM Overrides", "I/O Filters", "Host Options", "Host Profile", "Licensing", and "vSphere Cluster Services"), and "Datastores". The "Licensing" section is expanded, and "vSAN Cluster" is selected. The right panel displays "vSAN Cluster Licensing" details:

License	vSAN 8 Enterprise
License key	[REDACTED]
Product	vSAN Enterprise
Usage	3 CPUs (up to 32 cores)
License expiration	Never
Licensed features	ISCSI All Flash Stretched Cluster RAIDS/RAID6 Support Storage Savings by Dedupe and Compression vSAN Encryption vSAN File Services HCI Mesh Data-in-Transit Encryption vSAN Shared Nothing Storage

A blue button "ASSIGN LICENSE" is located in the top right corner of the licensing panel.

Cluster Configure vSAN Cluster page showing the vSAN license

vSphere License

vSphere ESXi version 8 licenses are required for each VxRail node in the cluster.

To verify the vSphere license, select each node and go to **Configure > System > Licensing**.

Deploy a Standard VxRail Cluster With vSAN ESA

The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The top navigation bar includes "Actions", "Administrator@VSPHERE.LOCAL", and a help icon. The left sidebar shows a tree structure with "vcsa01.delledu.lab" expanded, revealing "VxRail-DC" and "VxRail-Cluster1". "Vxcluster730-esx01.delledu.lab" is selected and highlighted with a yellow box. The main content area has tabs: "Summary", "Monitor", "Configure" (which is selected and highlighted with a yellow box), "Permissions", "VMs", "Datastores", "Networks", and "Updates". The "Configure" tab is further divided into sections: "Storage", "Networking", "Virtual Machines", and "System". The "Licensing" section is currently active, showing the following details:

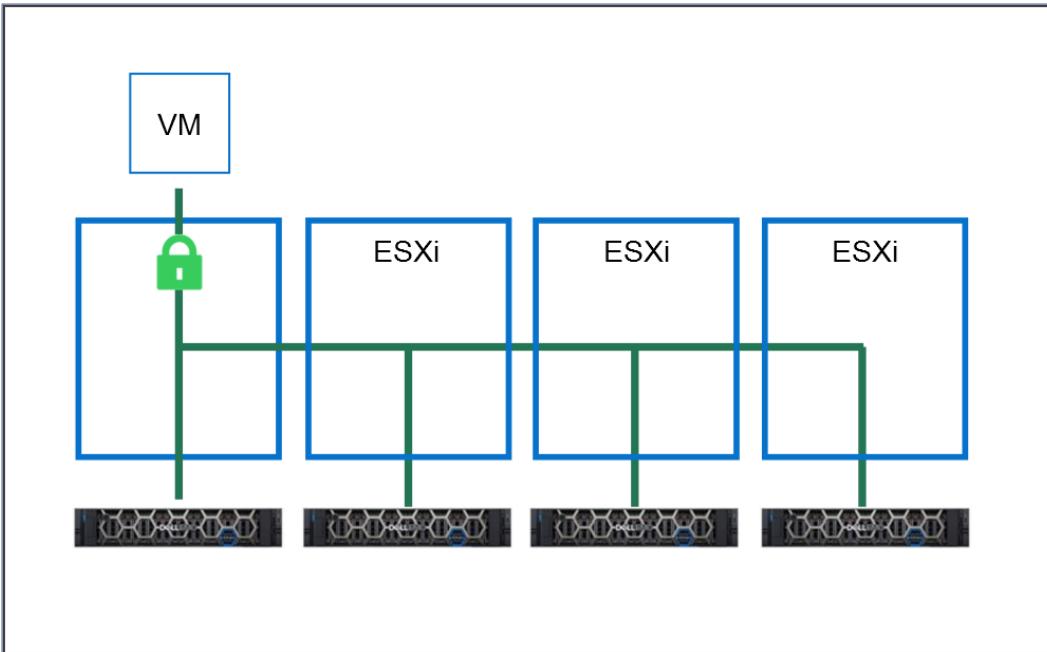
License	vSphere 8 Enterprise Plus
License key	XXXXXXXX-XXXX-XXXX-XXXX-XXXX
Product	vSphere 8 Enterprise Plus
Usage	1 CPUs (up to 32 cores)
License expiration	12/31/2024
Licensed features	Unlimited virtual SMP H.264 for Remote Console Connections vCenter agent for VMware host vSphere API Content Library Storage APIs vSphere vMotion X-Switch vMotion vSphere HA vSphere Data Protection vShield Endpoint vSphere Replication vShield Zones Hot-Pluggable virtual HW

At the bottom right of the main content area is a button labeled "ASSIGN LICENSE". The footer of the vSphere Client includes "Recent Tasks" and "Alarms".

Node 1 Configure Licensing page showing the vSphere license for the node

vSAN ESA Encryption Overview

When a vSAN ESA cluster is encrypted, the VM data is encrypted when written to the datastore. This encryption step only occurs once, and all vSAN traffic that is transmitted across hosts remains encrypted. This process results in improved security and reduced overhead.



vSAN ESA encrypted datastore



Important: Encryption can only be enabled on an ESA datastore during the initial build. Encryption cannot be disabled once the datastore is encrypted.

vSAN ESA Encryption Key Providers

Encryption of a vSAN ESA datastore supports both the Native Key Provider and a Standard Key Provider.

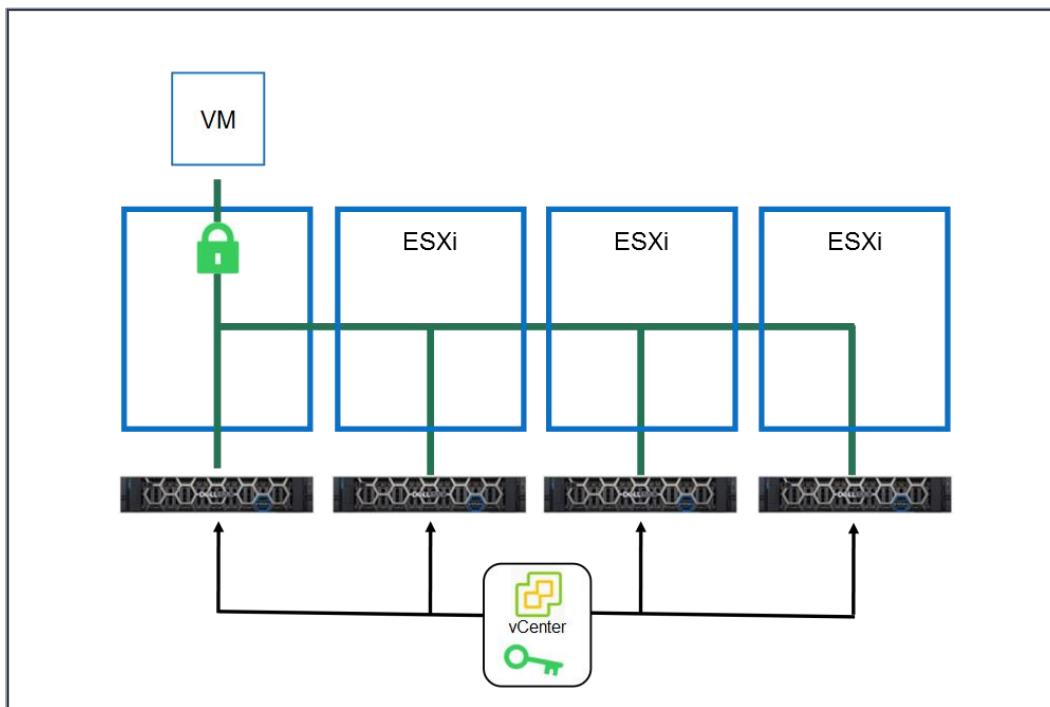
To learn more about the key providers, select each tab.

Native Key Provider

With a Native Key Provider, vCenter Server generates a primary key and pushes the key to all hosts in the cluster. The primary key is stored in vCenter, and on each host. The ESXi hosts use the primary key to generate data encryption keys. The Native Key Provider method requires

Deploy a Standard VxRail Cluster With vSAN ESA

a vSAN Enterprise Plus license. Access to a backup of the primary key is required for data recovery, if vCenter is inaccessible.

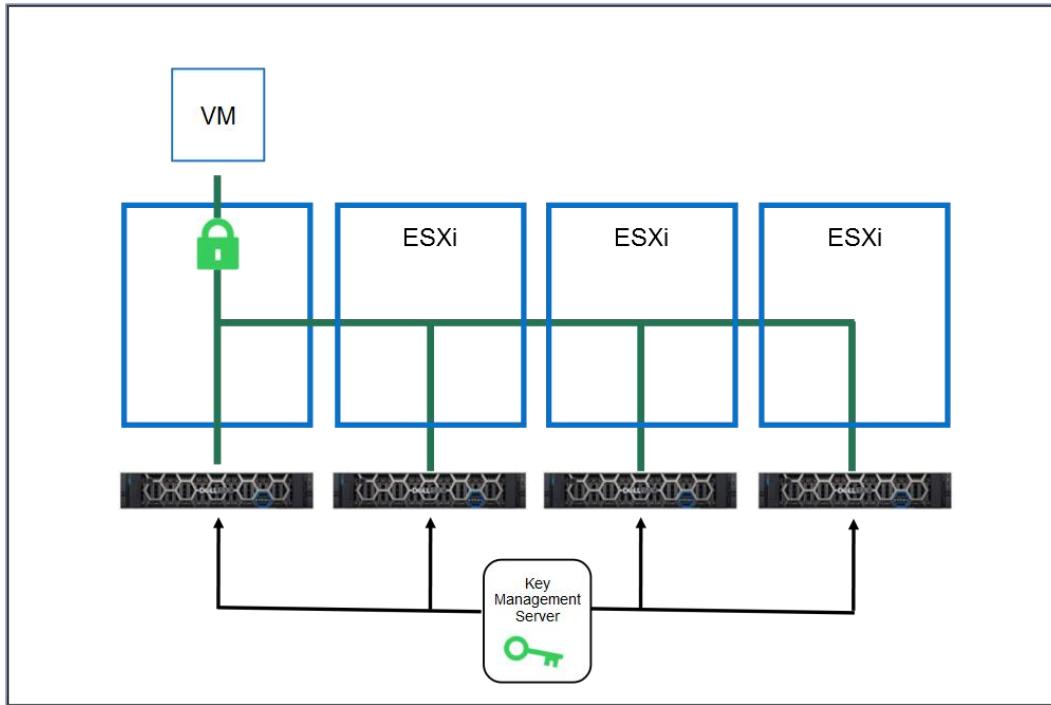


vSAN ESA Native Key Provider

Standard Key Provider

With a Standard Key Provider, the primary key is stored on a compatible Key Management Server (KMS). ESXi hosts use the primary key to generate data encryption keys. Use this method in environments where an external KMS is required. Connectivity to the KMS is required for initialization and recovery.

Deploy a Standard VxRail Cluster With vSAN ESA



vSAN ESA Standard Key Provider

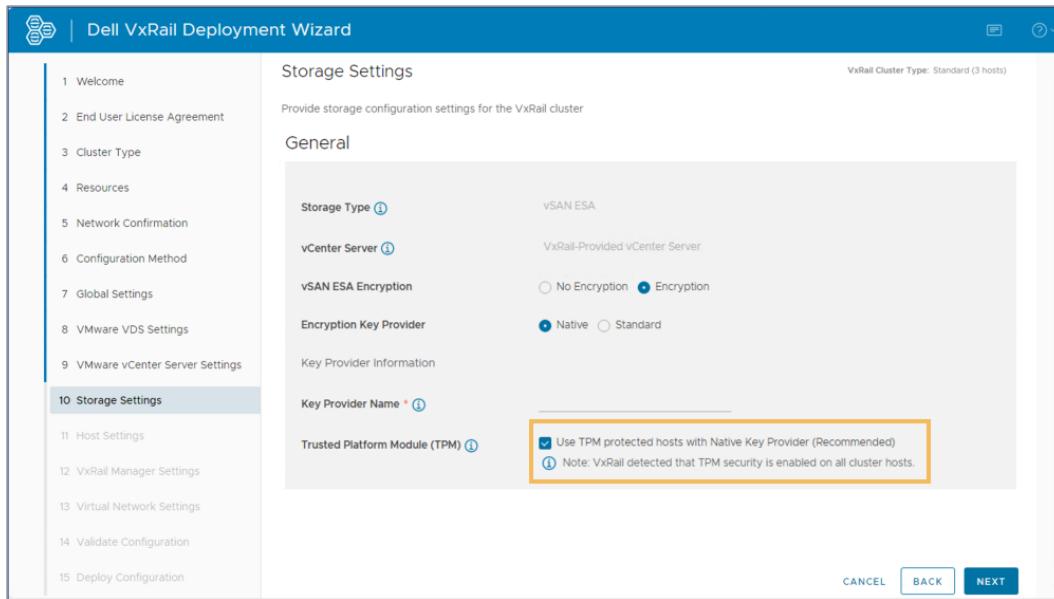


Deep Dive: For more information about vSAN encryption, go to [vSAN Encryption Services](#).

Using Trusted Platform Module (TPM) With a Native Key Provider

When the primary key is generated, it is stored in the local configuration on each host. When TPM is enabled, the primary key is protected by the TPM. If the host reboots the primary key can be read from the configuration if the key provider is offline or inaccessible. TPM must be enabled on each host before the start of the VxRail initial build.

Deploy a Standard VxRail Cluster With vSAN ESA



VxRail Deployment Wizard with the option to use TPM protected host selected

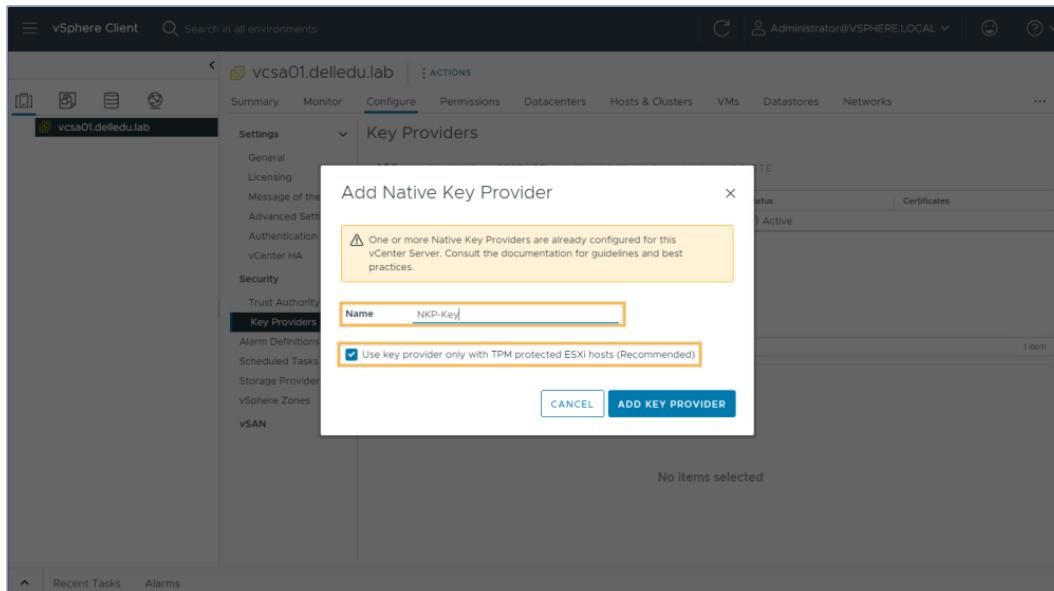


Tip: Enabling TPM 2.0 on the VxRail hosts to support encryption is recommended as a best practice, but not required.

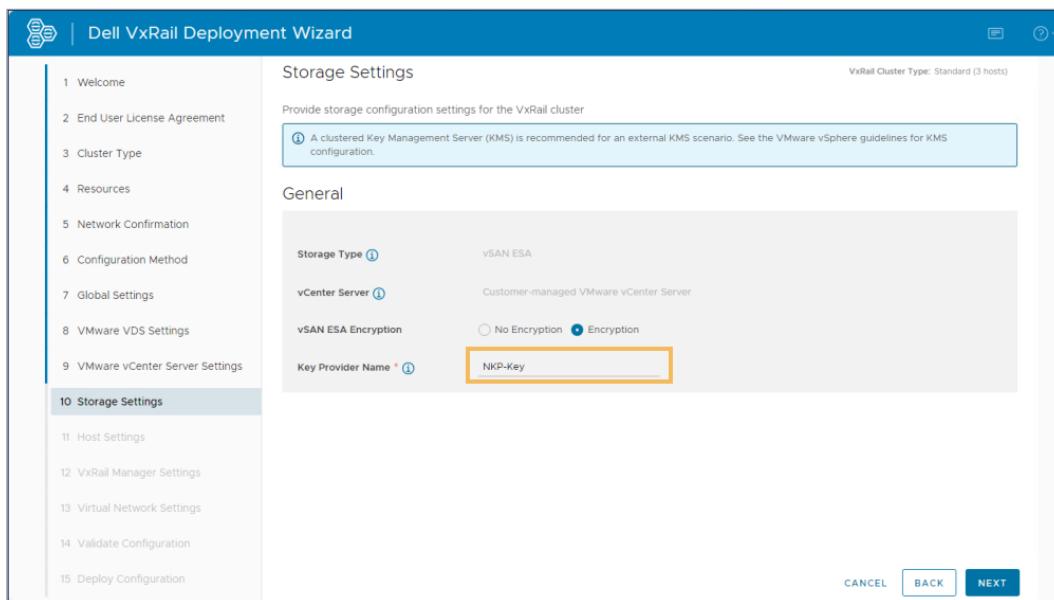
Configuring Key Providers on a Customer-Supplied vCenter Server

For a customer-supplied vCenter, only a Native Key Provider is supported for vSAN ESA encryption. The Native Key Provider must be configured in vCenter before the VxRail initial build. The option to use TPM with encryption is set when the Key Provider is added in vCenter. The Key Provider name that is entered in the **VxRail Deployment Wizard** must be an exact match to the Key Provider name in vCenter.

Deploy a Standard VxRail Cluster With vSAN ESA



vCenter Add Native Key Provider Wizard showing the Key Provider Name



VxRail Deployment Wizard showing the Key Provider Name

Configuring Key Providers on a VxRail-Managed vCenter Server

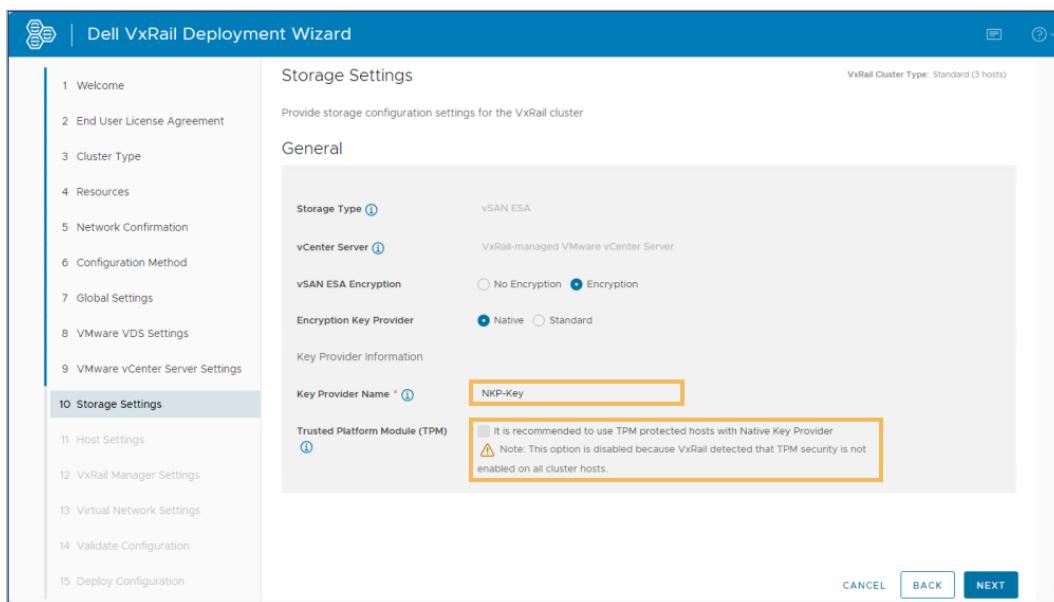
For a VxRail-managed vCenter Server, Native and Standard Key Providers are supported for vSAN ESA encryption.

Deploy a Standard VxRail Cluster With vSAN ESA

To learn more about the key providers, select each tab.

Native Key Provider

When a VxRail-managed vCenter Server is deployed, the Native Key Provider is configured on vCenter during the initial build. A name for the key provider is entered into the **VxRail Deployment Wizard**. If TPM is not enabled on all the hosts before the start of VxRail initial build, the **Trusted Platform Module (TPM)** option is disabled.

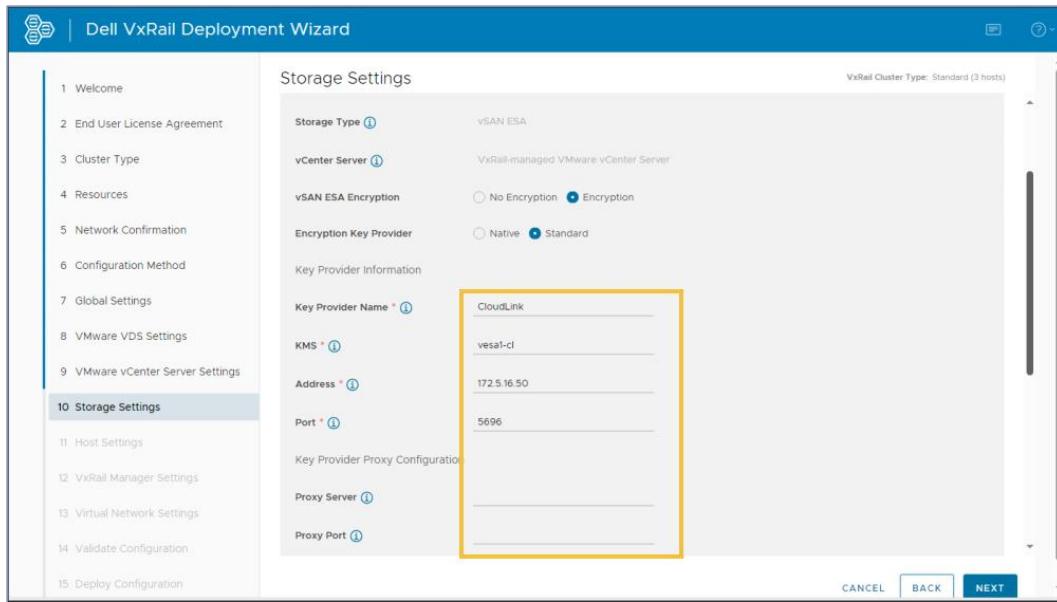


VxRail Deployment Wizard showing the TPM option disabled

Standard Key Provider

For a Standard Key Provider, the KMS settings are entered into the **VxRail Deployment Wizard**. A compatible KMS must be deployed in the data center before the VxRail initial build. See the [VMware Compatibility Guide](#) to identify Key Management Servers that are supported for vSAN ESA encryption.

Deploy a Standard VxRail Cluster With vSAN ESA



VxRail Deployment Wizard showing KMS settings

Interaction: Add a Native Key Provider to the vCenter Server

The web version of this content contains an interactive activity.

Interaction: VxRail with vSAN ESA deployment with a customer-supplied vCenter Server and using a Native Key Provider.

The web version of this content contains an interactive activity.

Verify VxRail Cluster Deployment

VxRail Manager Plugin for vCenter

Name	Type	Status	VMware Certified	Vendor
VMware Cloud Provider Services Plugin	Remote	Deployed	No	VMware, Inc.
VMware vCenter Server Lifecycle Manager	Remote	Deployed	Yes	VMware, Inc.
VMware vSphere Lifecycle Manager Client	Remote	Deployed	Yes	VMware, Inc.
VMware vSphere Lifecycle Manager	Local	Deployed	Yes	VMware, Inc.
VxRail HTML5 Client Plugin	Local	Deployed	No	DellEMC

vSphere Client Plugins

VxRail Manager functionality in the vSphere Client is provided by the VxRail Manager Plugin. The VxRail Manager Plugin for vCenter is automatically installed during the VxRail deployment process.

After a successful VxRail deployment, log in to the vSphere Client:

- Confirm that the VxRail Plugin is deployed.
- Use the VxRail Plugin to validate:
 - Overall system health with the VxRail Dashboard.
 - VxRail installed versions at a system and component level.
 - VxRail component information at a physical view of the cluster and node level



Tip: There are KB articles to help troubleshoot issues that are related to the VxRail Plugin, for example [KB 193869](#).

VxRail Dashboard

The **VxRail Dashboard** provides a centralized location to view information about VxRail. The VxRail Dashboard is found in the vSphere Client under the **Menu > VxRail**.

The **Support**, **VxRail Community**, and **Knowledge Base** panes are only populated and available when the VxRail Manager system has Internet connectivity. To learn more about the **VxRail Dashboard**, select the five red hotspot.

VxRail Dashboard

The screenshot shows the vSphere Client interface with the 'VxRail' menu selected. The main area displays the 'VxRail Dashboard' for the cluster 'VxRail-Cluster1'. The dashboard features four main sections: 'System Health' (status: Healthy), 'Support' (status: Dell Technologies connectivity is inactive or not configured), 'VxRail Community' (warning: cluster cannot connect to the support website), and 'Knowledge Base'. Each section is highlighted with a red box and a number (1, 2, 4, 5) in a corner. At the bottom, there is a 'Recent Tasks' and 'Alarms' navigation bar.

1: System Health provides a quick reference for overall system health status. The health status aggregates health metrics from iDRAC, vCenter, and VxRail Manager.

Clicking the health status link takes you to the Issues and Alarms view of the VxRail Cluster in the vSphere Client.

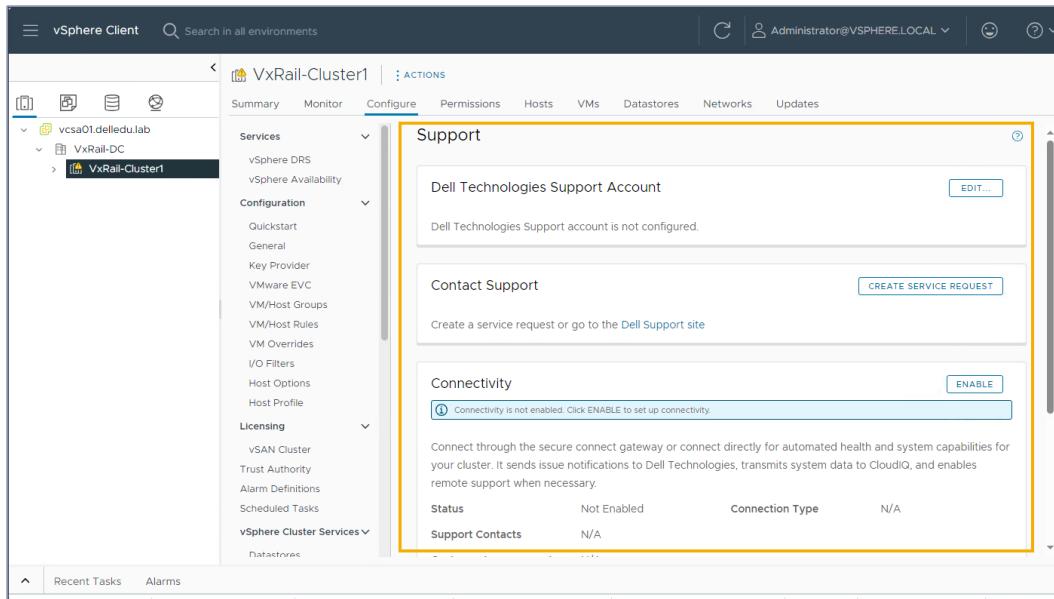
The health status can be shown as:

- Healthy - System normal, no major problems to address.
- Error - System has an error that should be addressed when possible.
- Warning - System needs attention. For example, a disk space limit has been reached, or an online support heartbeat cannot be sent.
- Critical - Immediate action is required. Events that could cause downtime or data loss unless they are addressed immediately.

2: The **Support** section of the dashboard is useful for checking the status of the VxRail or configuring the Dell Technologies Support Account on the VxRail system. It is also useful for engaging Dell Support resources through opening a Service Request (SR) or chat. You can also download useful resources that are associated with VxRail.

A valid Dell Support account that is associated with the VxRail system is required to engage Support resources. Clicking the **Configure Connectivity** link brings you to the VxRail Support page shown below. Use this page to configure the Dell Technologies Support Account and Secure Connect Gateway.

Verify VxRail Cluster Deployment



The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The top navigation bar includes "Actions", "Administrator@VSPHERE.LOCAL", and a help icon. The left sidebar shows a tree structure with "vcsa01.delledu.lab" expanded, showing "VxRail-DC" and "VxRail-Cluster1". The main content area has tabs "Summary", "Monitor", "Configure" (which is selected), "Permissions", "Hosts", "VMs", "Datastores", "Networks", and "Updates". The "Configure" tab is expanded, showing sections for "Services", "vSphere DRS", "vSphere Availability", "Configuration" (with sub-options like Quickstart, General, Key Provider, VMware EVC, VM/Host Groups, VM/Host Rules, VM Overrides, I/O Filters, Host Options, Host Profile), "Licensing" (with sub-options like vSAN Cluster, Trust Authority, Alarm Definitions, Scheduled Tasks), and "vSphere Cluster Services" (with sub-options like Datastores). A yellow box highlights the "Support" section, which contains three panels: "Dell Technologies Support Account" (status: not configured, "EDIT..." button), "Contact Support" (status: not configured, "CREATE SERVICE REQUEST" button), and "Connectivity" (status: not enabled, "ENABLE" button). Below the connectivity panel, there is a table:

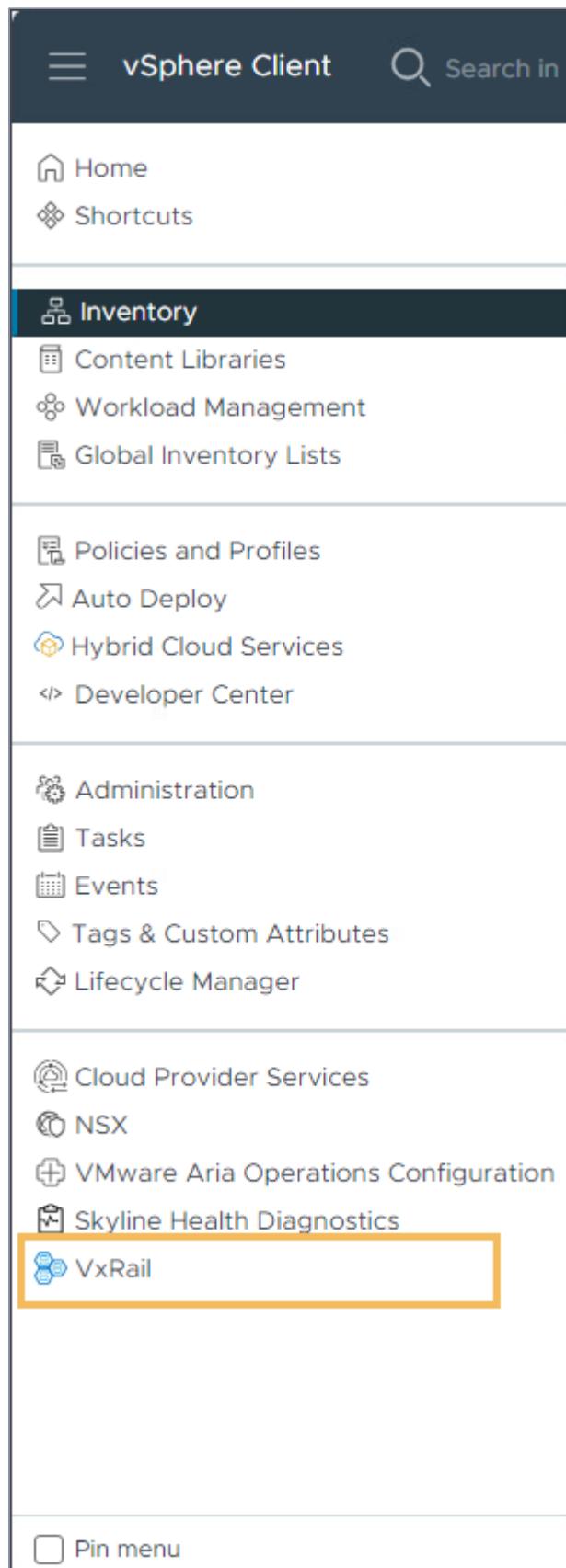
Status	Not Enabled	Connection Type	N/A
Support Contacts	N/A		

Configure > VxRail > Support

3: The VxRail Dashboard displays the overall system health, support resources, VxRail community information, and Knowledge Base articles.

To access the VxRail Dashboard, click **Menu > VxRail**.

Verify VxRail Cluster Deployment



Verify VxRail Cluster Deployment

Menu > VxRail

4: The **VxRail Community** section of the dashboard provides web links to articles within the VxRail community space. The VxRail online community is a collection of insights and community discussions from VxRail users and VxRail experts. It can be a useful resource in managing the VxRail. This section is only populated if the VxRail has internet connectivity.

VxRail Community page - <https://www.dell.com/community/VxRail/bd-p/vxrail>

5: The Dell Knowledge Base is another resource for information regarding VxRail systems. The **Knowledge Base** section lists web links to popular or useful KB articles for quick reference. To access the KB articles, the VxRail Manager VM must be able to access the Dell Support site with a valid Dell Support account.

Verify VxRail Version and vCenter Mode

The screenshot shows the vSphere Client interface with the title bar "vSphere Client". In the top navigation bar, there is a search bar "Search in all environments" and a user dropdown "Administrator@VSPHERE.LOCAL". Below the search bar, the cluster name "VxRail-Cluster1" is displayed. The main content area is titled "System" and contains the following sections:

- VxRail**: Displays the version "Version: 8.0.100-28049150" and the date "Installed On Oct 16, 2023, 4:44:13 PM".
- Helpful Information**: Links to "Product Documentation", "Privacy Statement", and "Update".
- About VxRail**: A brief description of the VxRail integration for VMware vCenter Server.
- Copyright**: Copyright notice: "Copyright (c) 2023 Dell Inc. or its subsidiaries. All Rights Reserved."

On the left side, the navigation tree shows the cluster structure: "vcsa01.delledu.lab" > "VxRail-DC" > "VxRail-Cluster1". The "VxRail" section under "Desired State" is selected. At the bottom, there is a table for "Recent Tasks" and a "More Tasks" button.

VxRail System Information page

The VxRail code version is displayed on the **VxRail > System** page in the vSphere Client.

Verify VxRail Cluster Deployment

The **Helpful Information** section provides a link to product documentation and a link to the VxRail updates page.

Important: For VxRail Clusters deployed with the VxRail-managed vCenter Server, the page also displays the **Convert vCenter Mode** section. The vCenter Mode can be converted from VxRail-managed to a Customer-supplied vCenter Server. After the conversion, the vCenter Server Appliance continues to reside in the VxRail vSAN datastore. However, VxRail Manager does not manage the LCM of the vCenter Server.

VxRail Updates and Compliance Report

The screenshot shows the vSphere Client interface with the following details:

- Left Sidebar:** Shows the environment tree with "vcsa01.delledu.lab" and "VxRail-DC".
- Top Bar:** Shows "vSphere Client", a search bar, and the user "Administrator@VSPHERE.LOCAL".
- Central Area:**
 - VxRail-Cluster1** is selected in the navigation pane.
 - Configure Tab:** Selected in the top navigation bar.
 - Updates Sub-tab:** Selected in the Configure tab navigation.
 - Compliance Tab:** Selected in the Updates sub-tab navigation.
 - Compliance Status:** The cluster is compliant (green checkmark).
 - Recommended Action:** The compliance drift report is generated.
 - Compliance Report:** A link to view the report.
 - Next Scheduled Report:** 10/18/2023 12:00:00 AM.
 - Installed Components and Versions:** Lists the installed components and their versions:
 - VxRail System: 8.0.100-28049150 (Installed On Oct 16, 2023, 4:44:13 PM)
 - VxRail Manager: 8.0.100-28049149
 - VMware vCenter Server Appliance: 8.0.1-21560480
- Bottom Task List:** Shows a task named "Stop service" completed.

VxRail Updates page - Compliance tab

The installed components and versions are displayed on the **Compliance** tab of the **VxRail > Updates** page.

The compliance report includes information about each component and subcomponent compliance state. By clicking the **Create New Report**

Verify VxRail Cluster Deployment

button, an administrator can create a report verifying the compliance of the cluster components.

The compliance report runs automatically every 24 hours.

VxRail Cluster Health Monitoring Status

The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". The left sidebar shows a tree structure with "vcsa01.delledu.lab" expanded, revealing "VxRail-DC" and "VxRail-Cluster1". The main content area has a breadcrumb path "Cluster > Configure > VxRail > Health Monitoring". The "Health Monitoring" section is highlighted with an orange border. It contains a sub-section titled "VxRail Cluster Health Monitoring" which states: "When health monitoring is disabled, the VxRail cluster health status is ignored. This is useful if cluster is disabled during node replacement." Below this, there is a "Health Monitoring Status" field set to "Enabled" with a green toggle switch. At the bottom of the main content area, there is a table titled "Recent Tasks" with one entry: "Refresh service information" for target "vcluster730-esxi03..." completed by initiator "VSPHERE.LOCAL\vxrmgmt" at 10/17/2023, 12:09:43... with a duration of 3 ms.

Health Monitoring Status

The **VxRail Cluster Health Monitoring** is enabled by default, and should remain enabled under normal circumstances. The setting can be disabled during cluster maintenance operations to prevent false alarms. For example, health monitoring is automatically disabled during VxRail upgrade operations or when adding a VxRail node to the existing cluster.

Verify VxRail Cluster Deployment

VxRail Cluster - Physical View

The screenshot shows the vSphere Client interface with the 'VxRail-Cluster1' selected in the inventory. The 'Physical View' tab is active. Key information displayed includes:

- Cluster ID: 52b0d0f1-e306-5b5e-940b-e45cad3158bf
- Last Timestamp: Oct 16, 2023 4:49:02 PM
- Number of Chassis: 3
- Connected: Yes
- Cluster Health: Healthy
- Operational State: OK

A specific node is selected, showing its details:

- Hostname: vcluster730-esx01.delledu.lab
- VxRail Service Tag: V073001
- Rack Name: Virtual Rack
- Rack Position: 1
- Model: VxRail E660N
- ESXi IP v4: 172.16.3.31
- IDRAC IPv4 address: 20.12.145.41

VxRail Cluster Physical View

Verifying that the physical view of the cluster is functioning correctly and displaying the expected information is an important step in validating the deployment. The **Physical View** of the Cluster is accessed by **Cluster > Monitor > VxRail > Physical View**. This view shows the physical view of all the VxRail chassis and the nodes that it contains.

In the example shown, the cluster has three VxRail E660N nodes.

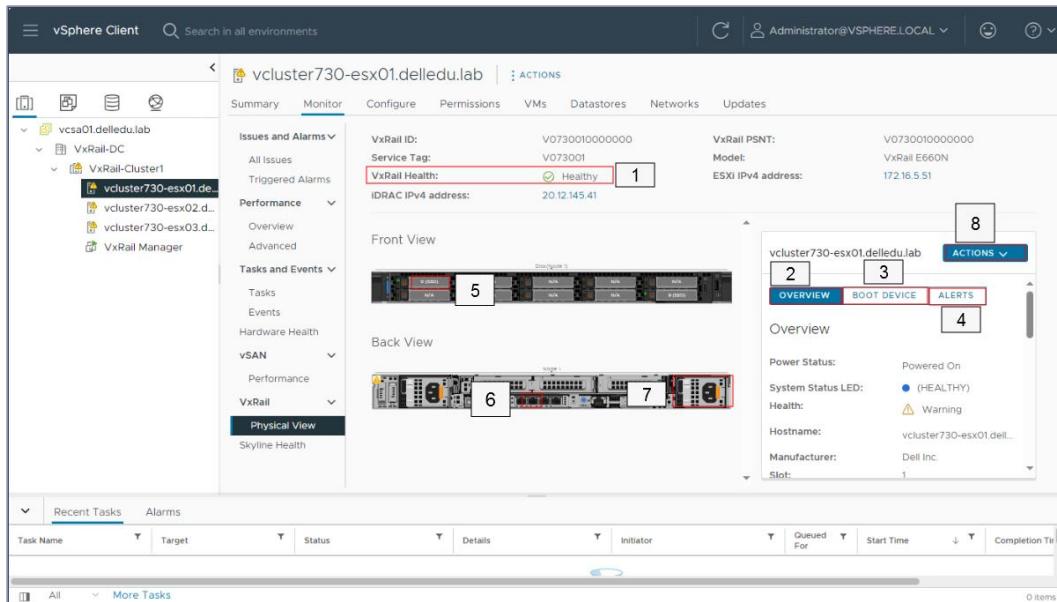
VxRail Node - Physical View

Validate the physical view of an individual node by selecting it from the inventory list. Then select the **Monitor > VxRail > Physical View**.

The graphic shows the details of a VxRail E660N node. To learn about the physical view of an individual node, select the seven red hotspots.

VxRail Node Physical View

Verify VxRail Cluster Deployment



1: The top of the display shows specific node identification information. This information is where an indication of an unhealthy state would be seen. If the node is in an unhealthy state, look under **Alerts** to identify the issue discovered.

2: OVERVIEW

The **OVERVIEW** tab displays the power status, system LED status, health, hostname, node PSNT, serial number, location data, firmware versions, and component versions.

Verify VxRail Cluster Deployment

The screenshot shows the 'OVERVIEW' tab selected in the navigation bar. A yellow box highlights the 'Power Status' section, which shows 'Powered On'. Other visible details include the system being healthy (blue LED), with a warning icon for health.

Overview	
Power Status:	Powered On
System Status LED:	● (HEALTHY)
Health:	⚠ Warning
Hostname:	vcluster730-esx01.delle...
Manufacturer:	Dell Inc.
Slot:	1
Serial Number:	V073001
Drive Configuration:	Up to 2 Disk Groups (u...
Location	
Rack Name:	Virtual Rack
Rack Position:	1
Firmware Versions	
BIOS:	1.8.2
BMC:	6.00.30.00
Non-Expander Back Pl...	3.72
BOSS:	2.5.13.4008
CPLD Firmware:	1.0.3
Component Versions	
VMware ESXi:	8.0.1-21495797
VxRail VIB:	8.0.100-21666983
NIC Driver Icen:	1.9.8.0-1OEM.702.0.0.1...
Security	
Encryption Mode:	None
Security Status:	Disabled
TPM:	Not Installed
TPM Status:	Disabled
TPM Version:	--

Node 1 Overview

3: BOOT DEVICE

The **BOOT DEVICE** tab displays details about the boot device. The example that is shown is an E560F node.

Verify VxRail Cluster Deployment

The screenshot shows a web-based management interface for a VxRail cluster. At the top, the cluster name "vcluster730-esx01.delledu.lab" is displayed next to an "ACTIONS" dropdown menu. Below the header, there are three tabs: "OVERVIEW" (selected), "BOOT DEVICE" (highlighted in blue), and "ALERTS". The main content area is titled "Boot Device 1 - M.2 Riser" and displays the following device specifications:

Serial Number:	BTYH10360LT4480K
Slot:	0
Device Model:	SSDSCKKB480G8R
Device Type:	SSD
Protocol:	SATA
Health:	100%
Capacity:	447.13GB
Power Cycle Count:	--
Power On Hours:	--
Block Size:	512 bytes
Firmware Version:	XC31DL6R

Below this, another section titled "Boot Device 2 - M.2 Riser" is shown, which contains identical or very similar device specifications, indicating two M.2 SSDs in the system.

Node 1 Boot Device

4: ALERTS

The **ALERTS** tab lists the triggered VxRail alerts specific to the node. All VxRail alerts start with VXR.

The screenshot shows the 'esx-269-vxrail4.vsb.edu' node details page. The 'ALERTS' tab is selected, indicated by a red border and a red badge with the number '3'. Below the tab, there are filters: 'All' (3), 'Critical' (2), and 'Error' (1). Three alerts are listed:

- VXR01000C new** (Host processor status) - Oct 16, 2020, 9:11:18 AM. Action: Follow suggested actions in [KB198383](#).
- VXR010012 new** (Host hardware system board status) - Oct 16, 2020, 9:11:18 AM. Action: Follow suggested actions in [KB198293](#).
- VXR014013 new** (Host battery status) - Oct 16, 2020, 9:11:18 AM. Action: Follow suggested actions in [KB198304](#).

Example - A G560 node with three active alerts.

5: Disk Information

By clicking any of the active disks, you can find information about the disk health and monitoring. The **Actions** menu in this section would be used to replace an unhealthy drive.

Disk Information

ACTIONS X

INFORMATION ALERTS

Status LED:	(HEALTHY)
Health:	Healthy
Serial Number:	V073001DVSN00
Manufacturer:	SAMSUNG
Slot:	0
Model:	MZILS1T9HEJH0D3
Protocol:	SAS
Disk Type:	SSD
GUID:	6000c2968d7c124dae149f74704 e20de
Capacity:	400.0GB
Remaining Write Endurance:	100%
Firmware Revision:	DSL7

Disk information example - A E660N node with a healthy status

6: NIC Details

The MAC address of the NIC, link speed, and the link status is displayed in the **INFORMATION** section. The **DRIVER VERSION** section shows the NIC driver versions.

Verify VxRail Cluster Deployment

The screenshot shows a window titled "Network Interface Controller Informa..." with two tabs: "INFORMATION" (selected) and "DRIVER VERSION". The "INFORMATION" tab displays the following details:

MAC Address:	00:50:56:84:5e:4f
Link Status:	Up
Link Speed:	10 Gbps
Port:	1
Firmware Family Version:	19.5.12

Node 1 NIC Information

The screenshot shows a window titled "Network Interface Controller Informa..." with two tabs: "INFORMATION" (selected) and "DRIVER VERSION". The "INFORMATION" tab displays the following driver versions:

NIC Driver ixgben:	1.8.9.0-1OEM.700.1.0.15525992
NIC Driver bnxtnet:	216.0.72.0-1OEM.700.1.0.15525992
NIC Driver bnxtroce:	216.0.65.0-1OEM.700.1.0.15525992

Node 1 NIC Driver Version

7: Power Supply Information

The power supply details are displayed. The **ALERTS** section displays any power supply-related alerts.

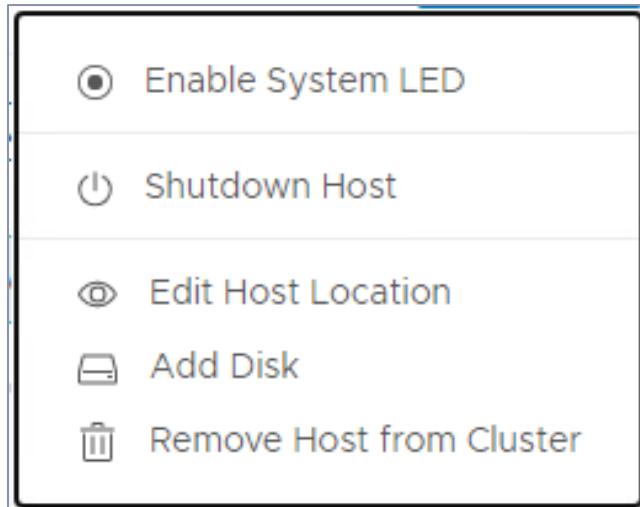
Verify VxRail Cluster Deployment

The screenshot shows a 'Power Supply Information' card. At the top left is a power icon, followed by the title 'Power Supply Information'. On the right is a close button ('X'). Below the title are two tabs: 'INFORMATION' (which is selected) and 'ALERTS'. The main content area contains the following data:

Serial Number:	V073001PSUSN000
Slot:	1
Health:	 ⓘ Healthy
Part Number:	OCMPGMA01
Revision Number:	00.23.32
Name:	Power Supply 1
Manufacturer:	DELL

Node 1 Power Supply Information

8: The **ACTIONS** menu is used to initiate maintenance tasks:



Node 1 Actions

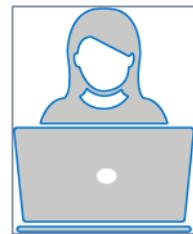
Lab 8: Verify VxRail Deployment Using VxRail Plugin

You want to verify a cluster deployment using the VxRail Plugin.

Verify VxRail Cluster Deployment

Lab Tasks

- Confirm that the VxRail Plugin has been deployed.
- Use the VxRail Plugin to validate:
 - Overall system health.
 - VxRail installed versions at a system and component level.
 - VxRail component information using the physical view for the cluster and node.



Perform vSAN Health Check

Dell recommends checking the health of the vSAN Cluster after a VxRail deployment. Use **Skyline Health** to monitor the status of cluster components and troubleshoot problems. Access **Skyline Health** by selecting the VxRail cluster in the **Hosts and Clusters** view and then select **vSAN > Skyline Health** on the **Monitor** tab.

Skyline Health findings are divided into several categories. To learn more about **Skyline Health**, select the six red hotspots.

Skyline Health dashboard of VxRail-Cluster1

A screenshot of the vSphere Client interface. The left sidebar shows a tree view of the environment, including 'vcsa01.delledu.lab' and 'VxRail-DC'. Under 'VxRail-DC', there is a 'VxRail-Cluster1' entry which is expanded to show 'vccluster730-esx01.d...', 'vccluster730-esx02.d...', 'vccluster730-esx03.d...', and 'VxRail Manager'. The main pane displays the 'Skyline Health' dashboard for 'VxRail-Cluster1'. At the top, it says 'Last checked: Oct 27, 2023, 1:06:03 PM' with a 'RETEST' button. Below this is a 'Cluster health score' gauge showing 98/100, labeled 'Attention' on the left and 'Healthy' on the right. To the right is a 'Health score trend' graph showing a recent dip from 99 to 98. Further down, there are sections for 'Health findings' and 'Performance service status'. The 'Health findings' section shows four categories: 'UNHEALTHY (1)', 'HEALTHY (48)', 'INFO (3)', and 'SILENCED (1)'. The 'Performance service status' section shows a yellow warning icon. The bottom of the dashboard has buttons for 'VIEW DETAILS', 'Sort by', and 'Score impact'. The overall interface is light-colored with blue and green highlights for different components.

1: The vSAN Skyline Health check runs every 60 minutes by default. The date and time of the last check is displayed here.

2: Skyline Health can be run on demand by clicking the **RETEST** button. The purpose of the **RETEST** option is to ensure that recent changes made to the cluster did not have a negative impact.

3: The **Unhealthy** tab shows system warnings. A warning status for **Performance service** is not unusual soon after the VxRail deployment because **Performance service** is disabled by default.

4: The **Healthy** tab shows the compliant or healthy components of the VxRail cluster or vSAN component.

5: The **Info** tab shows Health findings which may not impact the cluster running state but are important for awareness.

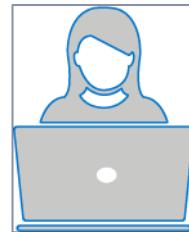
6: The **Silenced** tab shows any alert that the Administrator acknowledged and silenced. The alert can be restored as needed.

Lab 9: Review vSAN Health

You have completed the deployment of the VxRail cluster and must check the vSAN cluster health using **Skyline Health**.

Lab Tasks

- Log in to the existing vCenter Server.
- Review the **Custom Attributes** of the cluster.
- Review the **vSAN Overview** dashboard.
- Complete a health check of the vSAN cluster using **Skyline health**.



Manage VMware Licenses

Add VMware Licenses

The VxRail-managed vCenter Server comes with a vCenter Server Standard license.

The VxRail system is shipped with 60-day evaluation licenses for vSphere and vSAN. The vSphere evaluation period starts when the VxRail nodes are first powered on. New licenses must be applied before the end of the evaluation period to avoid impact.

VMware is now offering a licensing subscription model. You can either continue to use vSAN license keys or purchase a subscription. You can convert your vCenter server instances to the subscription before the current license expires. Review the [Purchase Subscriptions](#) article to learn more about the VMware license subscription program.

Examples of impact due to license expiration include:

- ESXi host license expires: The host is disconnected from the vCenter Server. All powered on virtual machines continue to work, but cannot be powered back on.
- vSAN license expires: The storage capacity of the host cannot be modified.



Important: Licenses that are purchased through Dell are provided through Partner Activation Codes. The license must be activated through the VMware Customer Connect account.

Licenses are viewed and added through the vSphere Client. To learn more about how to navigate licensing through the vSphere Client, select the four (4) red hotspots.

vSphere License Management

Manage VMware Licenses

The screenshot shows the vSphere Client interface with the 'Licenses' page open. The left sidebar shows various administrative categories like 'Access Control', 'Licensing', 'Solutions', and 'Deployment'. The main area has three tabs: 'Licenses' (selected), 'Products' (highlighted with a red box), and 'Assets'. Below the tabs is a table with columns: License, License Key, Product, Usage, and Capacity. The first row is an evaluation license for vCenter Server 8 Standard. The second row is a vSphere 8 Enterprise Plus license. At the bottom of the table is an 'EXPORT' button.

1: New vSphere and vSAN licenses can be obtained through an existing Enterprise License Agreement (ELA) or by purchasing them through Dell, VMware, or an authorized Dell partner.

2: The **Products** tab displays the available product licenses.

This screenshot shows the same vSphere Client interface as above, but the 'Products' tab is selected. The table now lists two products: 'vCenter Server 8 Standard' and 'vSphere 8 Enterprise Plus'. Both rows are highlighted with a yellow background. The rest of the interface is identical to the previous screenshot.

Example that displays the Products tab with available licenses

3: The **Assets** tab displays the license status of various assets like **vCenter Server Systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, and **Solutions**. The **Asset** page is also used to assign available licenses

Manage VMware Licenses

to the various assets. To assign an available license, select the asset and click **Assign License**.

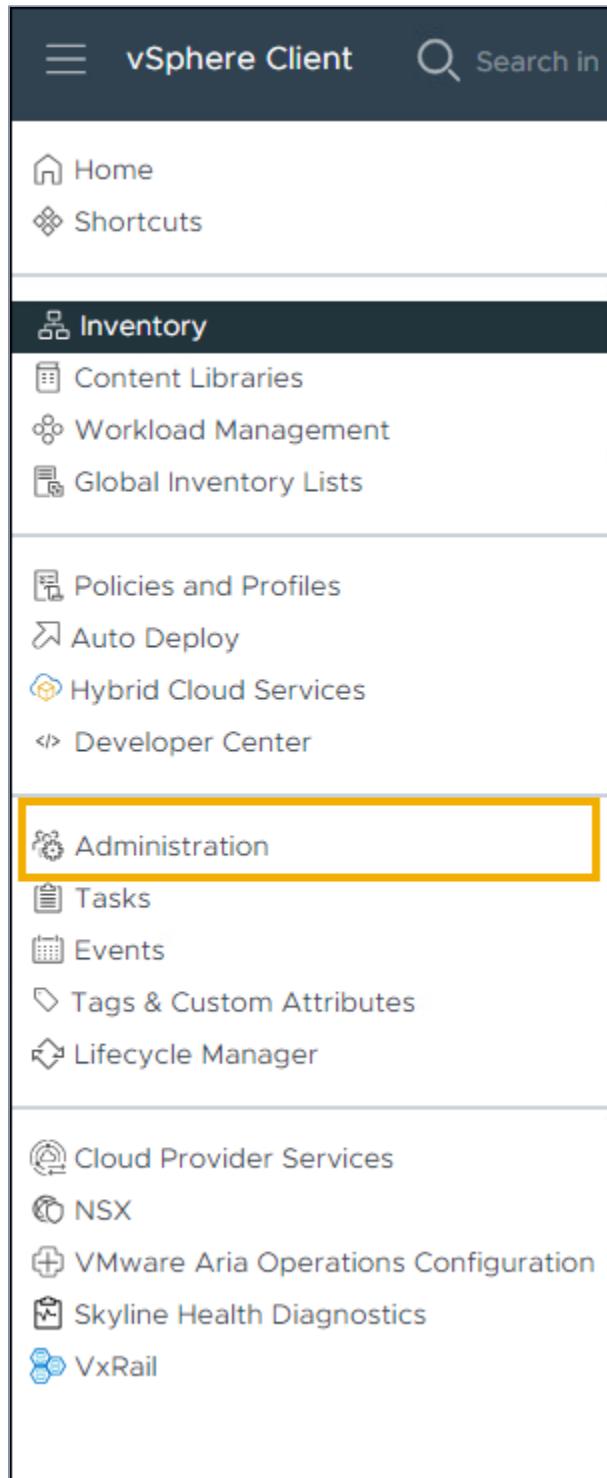
The screenshot shows the vSphere Client interface under the 'Administration' menu, specifically the 'Licensing' section. The 'HOSTS' tab is selected in the top navigation bar. A table lists three hosts: 'vcluster730-esx01.delledu.lab', 'vcluster730-esx02.delledu.lab', and 'vcluster730-esx03.delledu.lab'. Each host entry includes columns for Asset, Usage, Product, License, and License Expiration. The 'ASSIGN LICENSE' button is highlighted with an orange box. The 'LICENSES' tab is also highlighted in the sidebar.

Asset	Usage	Product	License	License Expiration
vcluster730-esx01.delledu.lab	2 CPUs (up to 32 core...)	vSphere 8 Enterprise Pl...	vSphere 8 Enterprise Pl...	12/31/2024
vcluster730-esx02.delledu.lab	2 CPUs (up to 32 core...)	vSphere 8 Enterprise Pl...	vSphere 8 Enterprise Pl...	12/31/2024
vcluster730-esx03.delledu.lab	2 CPUs (up to 32 core...)	vSphere 8 Enterprise Pl...	vSphere 8 Enterprise Pl...	12/31/2024

Example presenting the Assets > HOSTS tab

4: From the **Menu** drop down, select **Administration**. From the Administration page, expand **Licensing** to view the licensing options.

Manage VMware Licenses



Example presenting the Menu dropdown options available in the vSphere Client

Additional information:

- [Software Licensing Options for VxRail](#)

Manage VMware Licenses

- [VMware vSphere and vSAN Editions Feature Comparison](#)
- [About ESXi Evaluation and Licensed Modes](#)
- [How to activate Partner Activation Codes \(PAC\) for vSphere License](#)

Steps To Assign a Perpetual License

The vSphere Client is used to add and assign a vSAN license to a VxRail cluster. Licenses have to be added to vCenter and then assigned to the respective component. To learn more about the step-by-step process, select each tab.

View Expiring License

When a license is about to expire, a notification is displayed at the top of the vSphere Client page. Clicking the **MANAGE YOUR LICENSES** button launches the **Licenses** page, which can also be accessed by going to **Administration > Licensing**.

The screenshot shows the vSphere Client interface with the 'Licenses' page open. The 'VSAN CLUSTERS' tab is selected under the 'Assets' category. A table lists a single item: 'VxRail-Cluster1' with '6 CPUs (up to 32 cores)' usage and 'Evaluation Mode'. The 'License' column shows 'Evaluation License' and 'License Expiration' as '12/30/2023'. A callout box highlights this row with the text: 'In this example the vSAN license for the VxRail cluster is about to expire.' The left sidebar shows the 'Administration' menu with 'Licensing' selected.

Manage Licenses

Add License

There are multiple ways to add a license. One of the ways is to go to the **Licenses** tab and click **ADD**. The **ADD** button allows multiple licenses for ESXi hosts, clusters, and solutions to be added. Clicking **ADD** launches the **New Licenses** wizard.

The screenshot shows the vSphere Client interface with the 'Licenses' tab selected. The 'ADD' button is highlighted with a yellow box. A callout box points to a note stating: 'The Licenses tab lists all the available licenses. A vSAN license to replace the evaluation license has not been added yet.'

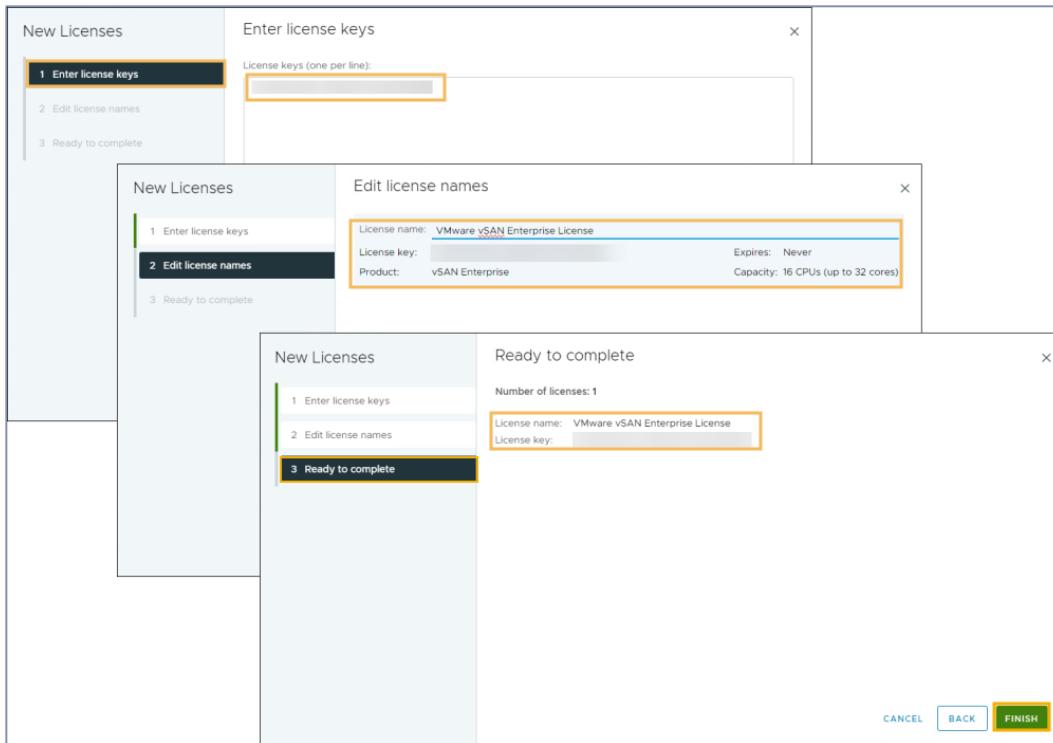
License	License Key	Product	Usage	Capacity
Evaluation License		vCenter Server 8 ...	1 Instances	2 Instances
vSphere 8 Enter...		vSphere 8 Enterprise Plus	6 CPUs (up to 32 core...)	16 CPUs (up to 32 core...)

View and add Licenses

New License Wizard

Follow the wizard to enter the license keys on the **Administration > Licenses** page.

Manage VMware Licenses



New Licenses wizard

[View Newly Added License](#)

The newly added license can be viewed from the **Licenses** tab.

Manage VMware Licenses

The screenshot shows the 'Licenses' tab in the vSphere Client. The left sidebar has 'Administration' expanded, with 'Licensing' selected. The main area displays a table of licenses:

	License	License Key	Product	Usage	Capacity
<input type="checkbox"/>	Evaluation License	--	--	--	--
<input type="checkbox"/>	vCenter Server 8...	[Redacted]	vCenter Server 8 Standard	1 Instances	2 Instances
<input type="checkbox"/>	VMware vSAN	[Redacted]	vSAN Enterprise	0 CPUs (up to 32 core-)	16 CPUs (up to 32 core-)
<input type="checkbox"/>	vSphere 8 Enterp...	[Redacted]	vSphere 8 Enterprise Plus	6 CPUs (up to 32 core-)	16 CPUs (up to 32 core-)

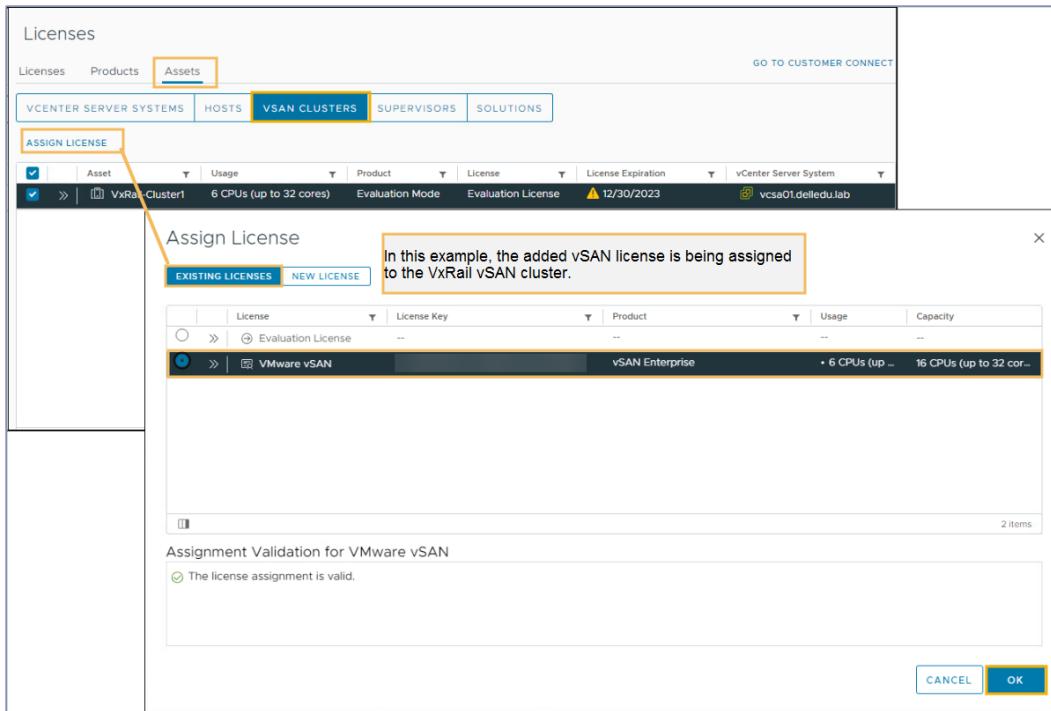
A callout box points to the 'VMware vSAN' row with the text: 'The License tab displays the details of the newly added VMware vSAN Enterprise license details.'

View newly added License

Assign License

After the license keys are added, go to the **Assets** tab. Select **VSAN CLUSTERS** and then **VxRail-vSAN cluster1**. Clicking **ASSIGN LICENSE** launches the **Assign License** wizard. Assign the newly added vSAN license key to the VxRail vSAN cluster.

Manage VMware Licenses

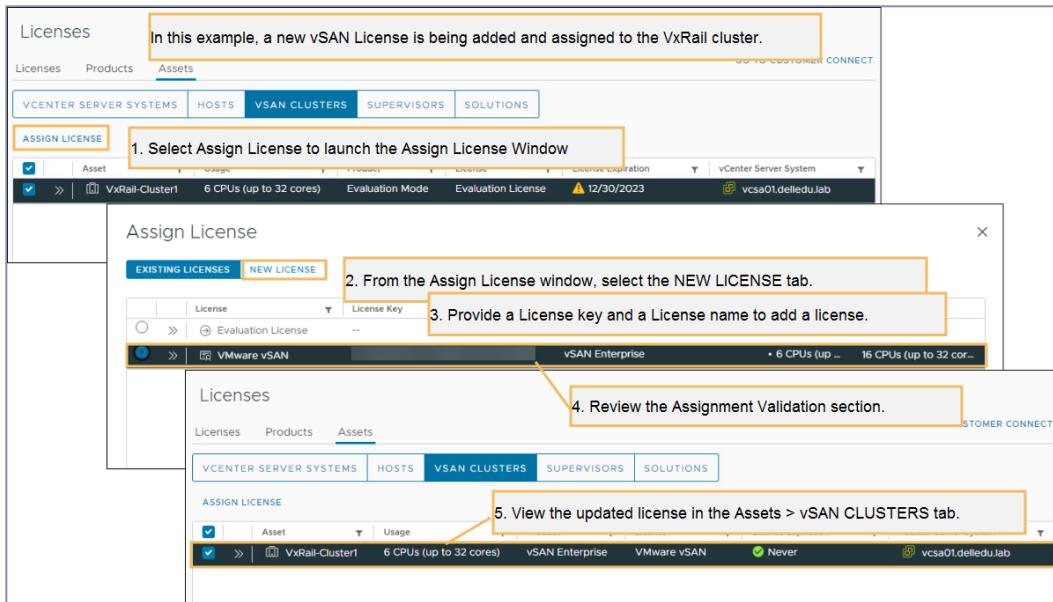


Assign License

Alternate Way To Add and Assign License

Alternatively, licenses can also be added from the **Assets** tab. Select one or more assets and click **ASSIGN LICENSE**. From the **Assign License** window, go to the **NEW LICENSE** tab to add the asset license key and provide a name for the license.

Manage VMware Licenses



An alternate way to add and assign License in vSphere

Configure vSAN Services

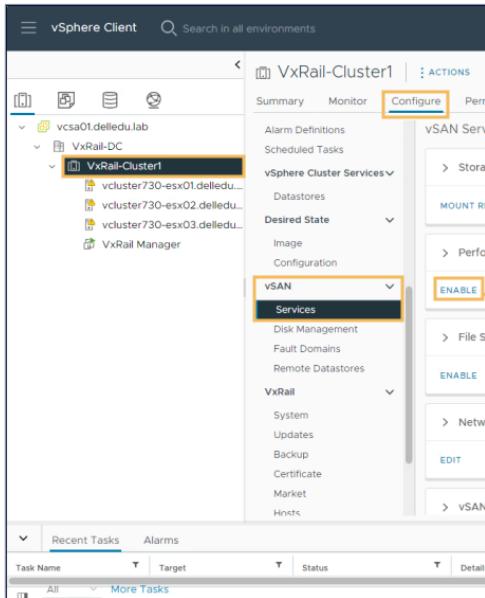
Enable vSAN Performance Service

The vSAN performance data is used for troubleshooting and performance analysis. Once enabled, performance data is stored in a database on the vSAN datastore.

The vSAN Performance service is disabled by default. For VxRail deployments performed by Dell or Dell partners, the vSAN Performance service is manually enabled during the deployment process as required in the [Test Plan](#). The Dell or Dell partner implementation teams must complete the document after a VxRail deployment. The Test Plan is handed off to the customer at the conclusion of the implementation.

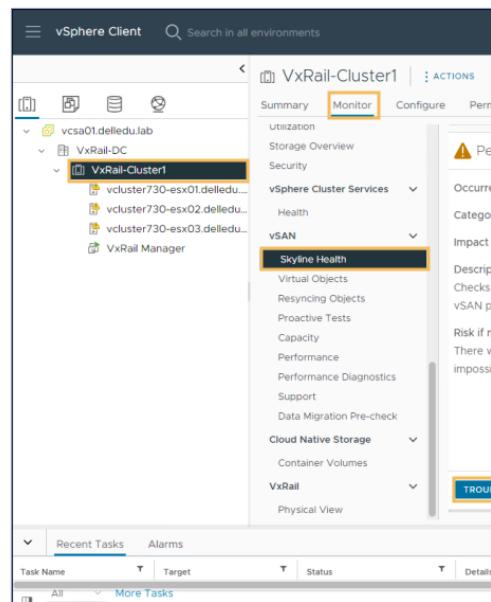
Configure vSAN Services

To manage the vSAN Performance service, select the VxRail cluster, and go to **Configure > vSAN > Services**. The Performance service is disabled by default as shown in the graphic.



Enable vSAN Performance service through **Configure > vSAN > Services**

- The vSAN Performance service
- can also be enabled from the VxRail cluster. Browse to **Monitor > vSAN > Skyline Health** as shown in the graphic. To enable, click **TROUBLESHOOT**.



Enable vSAN Performance service through **Monitor > vSAN > Skyline Health > Troubleshoot**

Selecting **TROUBLESHOOT** brings up the **vSAN Performance Service Settings**. In the settings, enable the vSAN performance service and then select the storage policy. The vSAN default storage is adequate for the vSAN performance history database. The **vSAN Performance Service Settings** dialog is shown in the graphic.

Configure vSAN Services

vSAN Performance Service Settings | VxRail-Cluster

Enable vSAN Performance service

Storage policy: vSAN Default Storage Policy

The vSAN performance history database is stored as a vSAN object. The policy controls the availability, space consumption, and performance of that object. If the object becomes unavailable, the performance history for the cluster is also unavailable.

CANCEL APPLY

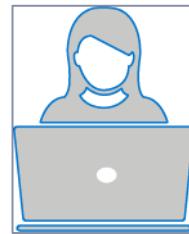
Select the default storage policy for vSAN Performance Service

Lab 10: Enable vSAN Performance Service

You have completed the deployment of the VxRail cluster and must enable the **vSAN Performance service**. The **vSAN Performance service** can be enabled through **Skyline Health**.

Lab Tasks

- Enable the vSAN Performance service.
- Run the Skyline Health Check.
- Confirm that the vSAN Performance service is collecting data.



vSAN Services Space Efficiency Options

vSAN supports two space efficiency options on OSA all-flash systems:

- Compression only
- Deduplication and compression

While both options reduce redundant data that is stored on the hard drives, space efficiency features are only supported for all-flash disk groups.

Enabling space efficiency options at initial setup is recommended to avoid the overhead and potential performance impact of the reformatting operations.



Important: Deduplication is not available with vSAN ESA. vSAN ESA enables better performing compression capabilities as a storage policy.

	Compression only	Deduplication and compression
Failure domain	Disk - If a capacity disk fails, only the disk is affected.	Disk Group - If a capacity disk fails the entire disk group is affected.
Capacity disk addition to disk group	Disk group reformatting is not required.	Disk group reformatting is not required, but recommended for maximum space savings.

Capacity savings potential ³	Moderate	High
Resource overhead	Minimal	High

Differences between vSAN OSA Compression only and Deduplication and compression



Go to: For more information about the vSAN Space Efficiency options, browse to: [Using Deduplication and compression](#)

Enable vSAN Space Efficiency Services

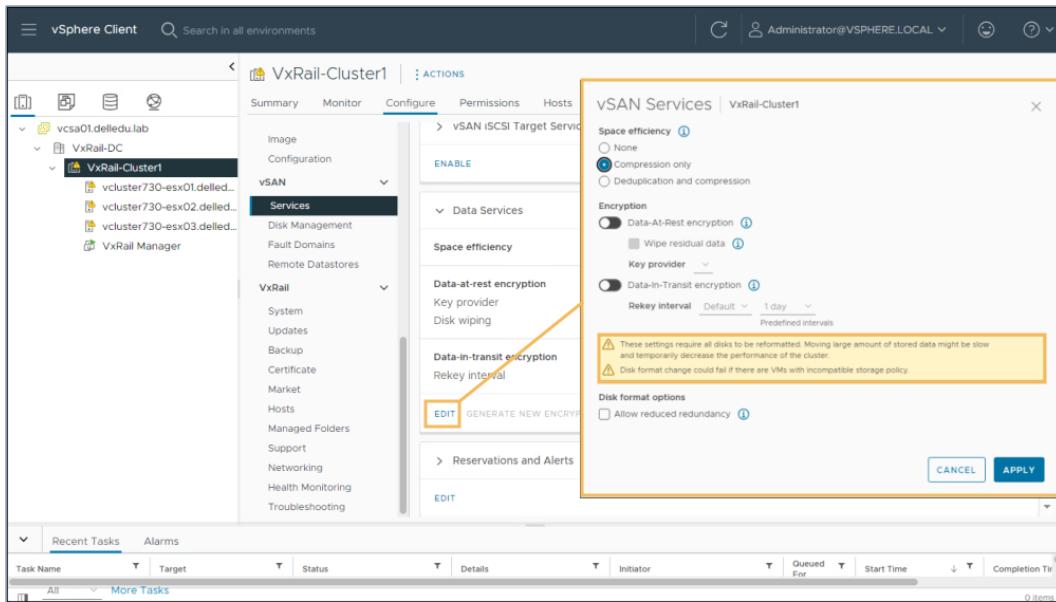
vSAN **Space efficiency** options are disabled by default. The options are enabled at the vSAN cluster level from the **vSAN Services** page.



Important: For vSAN ESA, compression is enabled by default on the cluster at the policy level. If compression on some of the virtual machine workloads is not required, a customized storage policy can be created and applied to the virtual machines. Also, compression for ESA is only for new data, old data is left uncompressed even after compression is turned on for an object.

³ Capacity savings are workload-dependent and not guaranteed.

Configure vSAN Services



vSAN Services page with vSAN Services dialog



Important: vSAN OSA performs a rolling reformat of all the disk groups on every host when space efficiency options are enabled or disabled. vSAN evacuates the disk group, removes the disk group, and then re-creates the disk group with a new format.

Verifying Space Savings From Deduplication and Compression

The storage savings depend on different factors such as the datatype and the number of duplicate blocks. Space efficiency and capacity savings are monitored from the **vSAN Capacity** page in the **CAPACITY USAGE** section.

To learn about capacity usage, select each tab.

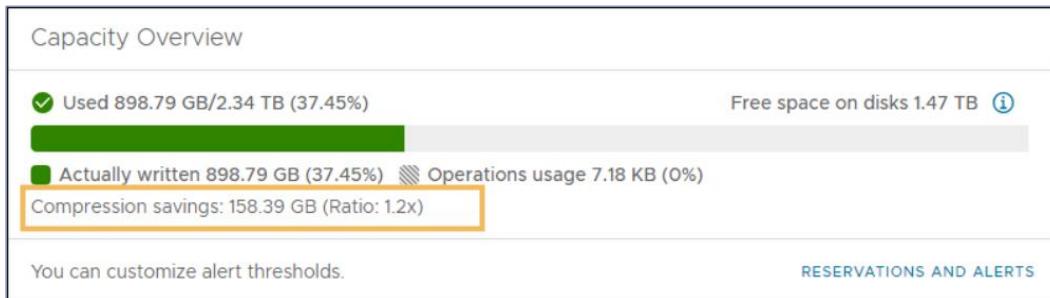
Capacity Overview

The **Capacity Overview** section displays the space savings. The ratio is based on the required logical capacity before applying **Deduplication and**

compression, compared to the physical capacity required after applying **Deduplication and compression**. It might take several minutes for capacity updates to be reflected in the capacity usage window as the disk is reclaimed and reallocated.

The **Compression savings** ratio is calculated as follows: **(Actually written + Compression savings) / Actually written** = Rounded-off Ratio.

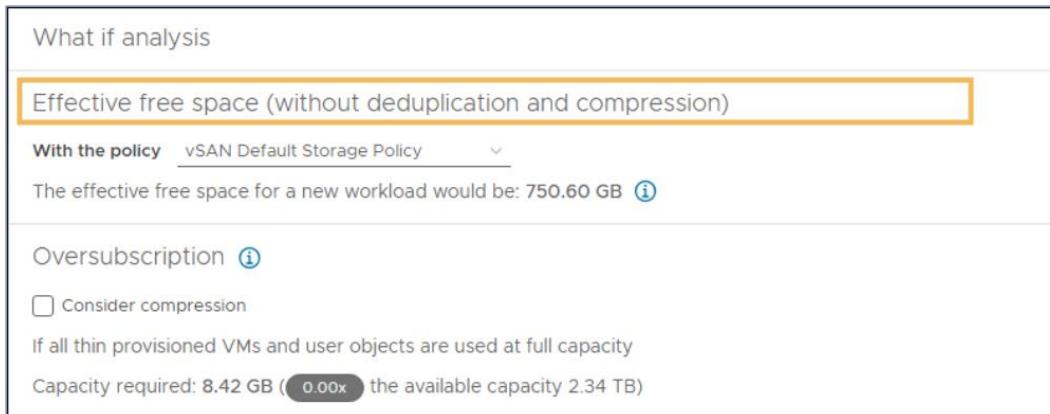
Example based on screenshot: $(898.79+158.39)/898.79=1.1762$ which rounds to 1.2.



vSAN Capacity Overview

What if analysis

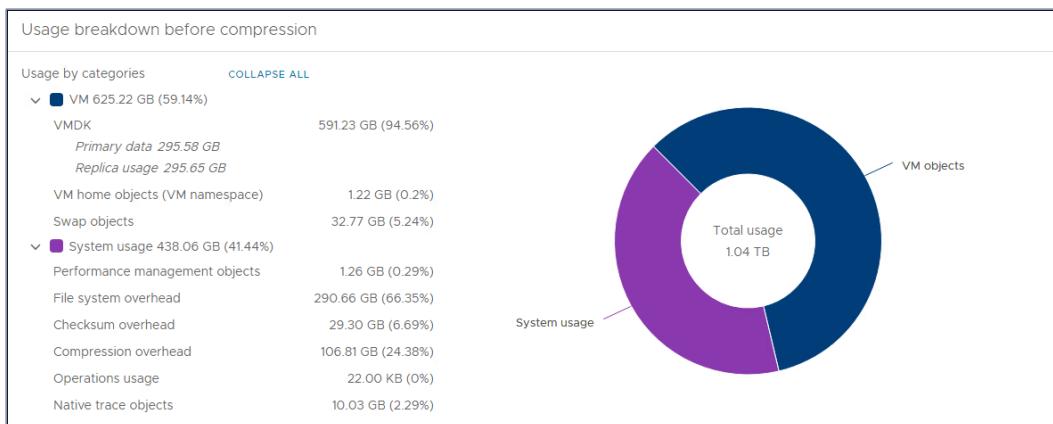
The **What if analysis** displays what would be the effective free space for a new workload without deduplication and compression, with the selected storage policy.



vSAN What if analysis

Usage breakdown

The **Usage breakdown before compression** section displays the logical space that is required before deduplication and compression are applied. You can further expand each usage category.



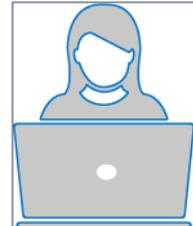
vSAN Usage breakdown

Lab 11: Enable vSAN Space Efficiency

You have completed the deployment of the VxRail cluster and must enable compression to improve vSAN Space Efficiency.

Lab Tasks

- Review vSAN capacity usage.
- Enable Compression only.
- Review space savings.



vSAN Encryption

vSAN supports Data-in-Transit and Data-at-Rest encryption. The two encryption options are unrelated and can be enabled or disabled independently at the cluster level. vSAN encryption is supported in hybrid, All-flash, stretched, and 2-Node cluster configurations.

To learn about some of the differences between vSAN Data-in-Transit and Data-At-Rest encryption, see the table.

vSAN Data-in-Transit Encryption	vSAN Data-At-Rest Encryption (D@RE)
Data and metadata is encrypted as it moves between data hosts and witness host ⁴ .	Data that is written to the vSAN datastore is encrypted.
A key provider is not required. vSAN uses symmetric keys that are generated dynamically and shared between hosts. Hosts generate an encryption key when they establish a connection and they use the key to encrypt all traffic between the hosts.	A key provider is required. vSAN uses asymmetric (public) keys. The vCenter Server requests encryption keys from an external Key Management Server (KMS). The KMS generates and stores the keys, and the vCenter Server obtains the key IDs from the KMS and distributes them to the ESXi Hosts.
Data and metadata is encrypted using AES 256-bit encryption.	Data is encrypted using XTS AES 256 cipher, in both the cache and capacity tiers of the vSAN datastore.
File service data traffic is encrypted between the vSAN Virtual Distributed File System (VDFS) proxy and server.	Data is encrypted after all other processing, such as deduplication and compression, is complete.

Additional information:

- [Using Encryption in a vSAN Cluster](#)

⁴ A Witness host applies only to vSAN 2-node and vSAN stretched cluster architectures.

Key Provider Requirement

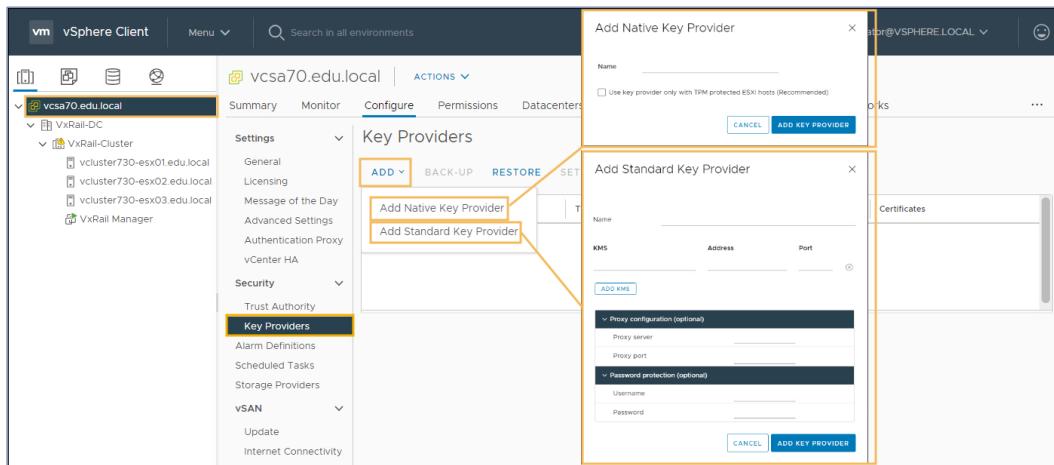
Data-At-Rest Encryption requires a key provider be added to the vCenter Server. Once a key provider is added, a trust must be established between the vCenter Server and the KMS before the encryption service is enabled.

Add Key Provider

To add a key provider, in the left navigation pane, select the vCenter Server. Then select the **Configure** tab. In the middle pane, scroll down to **Security**, select **Key Providers**, and click **ADD**.

There are two options for setting up a key provider:

- A vSphere Native Key Provider (NKP) is an internal key provider.
- A Standard Key Provider is an external key provider.



Add Encryption Key Providers

Establish Trust

A trust must be established between the KMS and the vCenter Server after adding a key provider. Use the appropriate product documentation for setting up the KMS.

Configure vSAN Services

The screenshot shows the vSphere Client interface with the title 'Configure vSAN Services'. The left sidebar shows a tree view with 'vcsa70.edu.local' selected, under which 'VxRail-DC' is expanded to show 'vxcluster730-esx01.edu.local', 'vxcluster730-esx02.edu.local', and 'vxcluster730-esx03.edu.local'. The 'Key Providers' section is selected in the center pane. A context menu is open over a row for 'KMS-1' (IP 192.168.10.12, Port 5696), with options like 'KMS trust vCenter', 'Make KMS trust vCenter', and 'Upload Signed CSR Certificate'. Below the table, there are buttons for 'Add KMS Servers', 'Make vCenter Trust KMS', 'Make KMS Trust vCenter', and 'TRUST KMS'.

Configure Key Provider

Additional information:

- [Set up the Standard Key Provider](#)
- [Set up a Native Key Provider](#)
- [VMware Certified Key Management Servers list](#)

Enable vSAN OSA Encryption

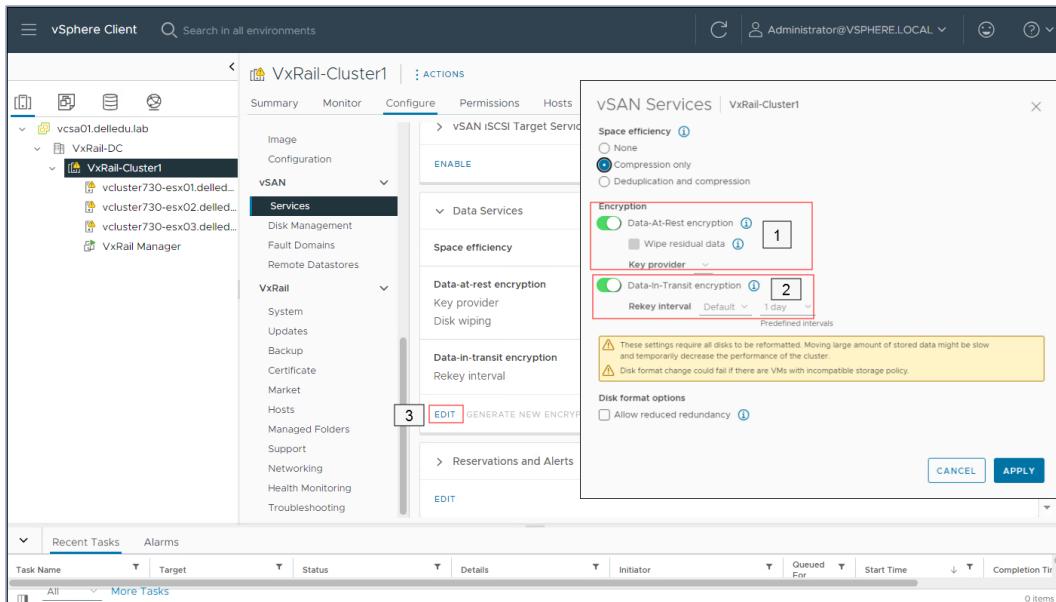
vSAN OSA encryption can be enabled during initial configuration or later. The best practice is to enable the **Data-At-Rest encryption** service right after the initial build.

vSAN OSA encryption is enabled from the **vSAN Services** page. In the example, both **Data-at-Rest encryption** and **Data-in-Transit encryption** are enabled.

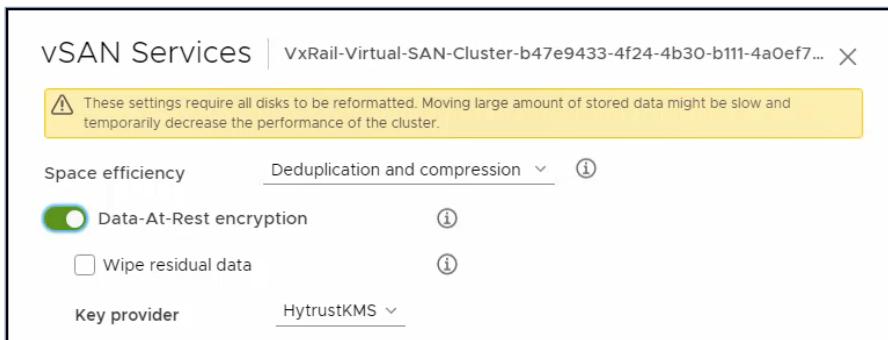
To learn more about enabling vSAN OSA encryption, select the three (3) red hotspots.

vSAN Services page with the vSAN Services dialog

Configure vSAN Services



1: Data-at-Rest encryption initiates a rolling disk reformat. Review the warning at the top of the page.



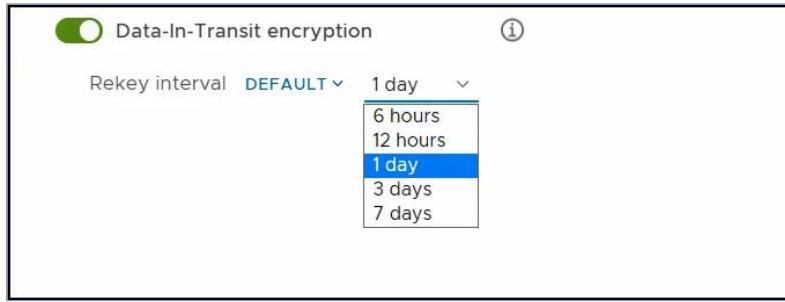
vSAN Services dialog with warning.

The **Wipe residual data** check box erases residual data from devices before enabling encryption. Keep this box cleared unless you want to wipe existing data from the storage devices when encrypting a cluster containing VM data.

The **Key provider** defaults to the key provider that has been added to the vCenter Server.

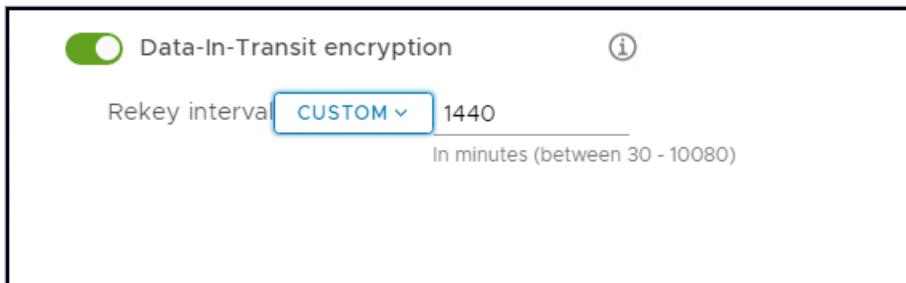
2: vSAN initiates the rekey process to generate new keys at the scheduled intervals. The default rekey interval is set to one day. The **Rekey interval** can be changed to match corporate compliance requirements.

Configure vSAN Services



Default Rekey interval options

You can also set a **CUSTOM** Rekey interval by manually entering the values between 30 to 10080 minutes.



Custom Rekey interval

3: Clicking **EDIT** launches the **vSAN Services** dialog.

Create vSAN Storage Policies

Create vSAN storage policy

VM Storage Policies has vSAN specific attributes. A VM Storage Policy can be assigned to a vSAN datastore as the default policy.

VM Storage Policies are created from the **VM Storage Policies** page of the vSphere client.

To learn more about creating a VM Storage Policy using the **Create VM Storage Policy** wizard, select each tab. This example shows how to create a RAID-5 **VM Storage Policy**.

Name and description

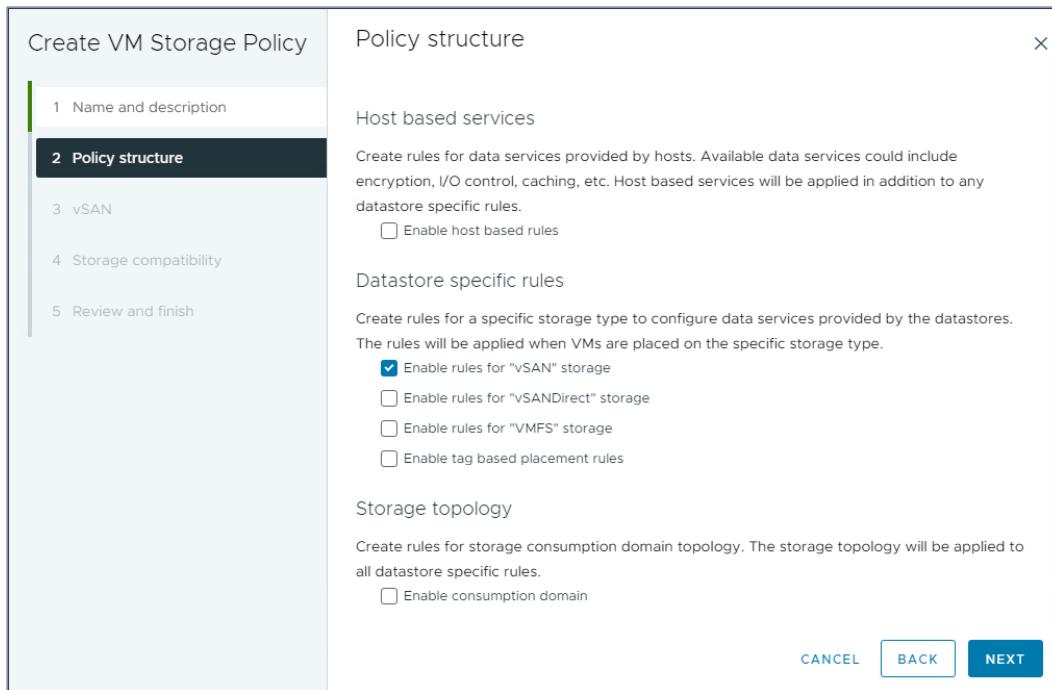
On the **Name and description** page, create a unique name and a description for the new policy.

The screenshot shows the 'Create VM Storage Policy' wizard on the 'Name and description' step. The left sidebar lists four steps: 1. Name and description (selected), 2. Policy structure, 3. Storage compatibility, and 4. Review and finish. The main panel shows the configuration for the 'Name and description' step. It includes a 'vCenter Server:' dropdown set to 'VCSA01.DELLEDU.LAB', a 'Name:' field containing 'RAID- 5', and a 'Description:' text area with the text 'RAID-5 Storage Policy allowing 1 FTT with Erasure Coding.' At the bottom right are 'CANCEL' and 'NEXT' buttons.

Create VM Storage Policy wizard-Name and description

Policy structure

In the **Policy structure** page, check **Enable rules for "vSAN" storage**. A **vSAN** page is added to the wizard after enabling the rules for vSAN storage.

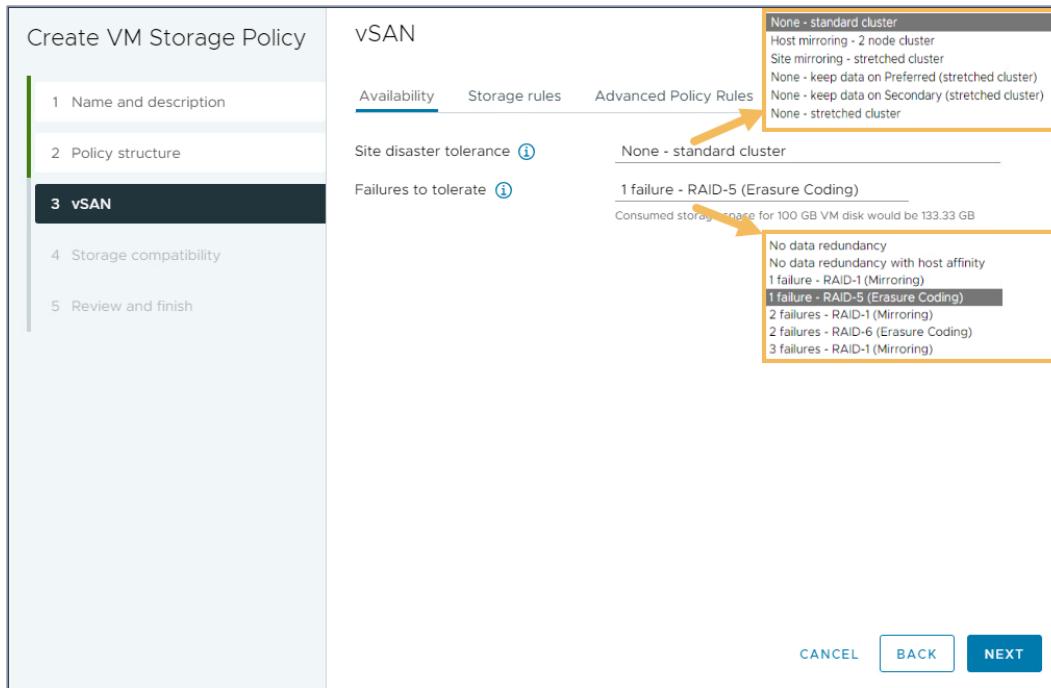


Create VM Storage Policy wizard-Policy structure

vSAN Availability

Specify the required **Site disaster tolerance** and **Failures to tolerate** in the **vSAN Availability** page.

Create vSAN Storage Policies



Create VM Storage Policy wizard-vSAN Availability

Site disaster tolerance provides options for standard and stretched clusters.

Failures to tolerate provides options for **No data redundancy**, **Mirroring**, and **Erasure Coding**.

Mirroring supports one, two, or three Fault Domain failures. For N failures tolerated, N+1 copies of the object are created.

Erasure coding supports one Fault Domain failure with RAID-5 or two Fault Domain failures with RAID-6. Erasure coding is supported on All-flash systems only.

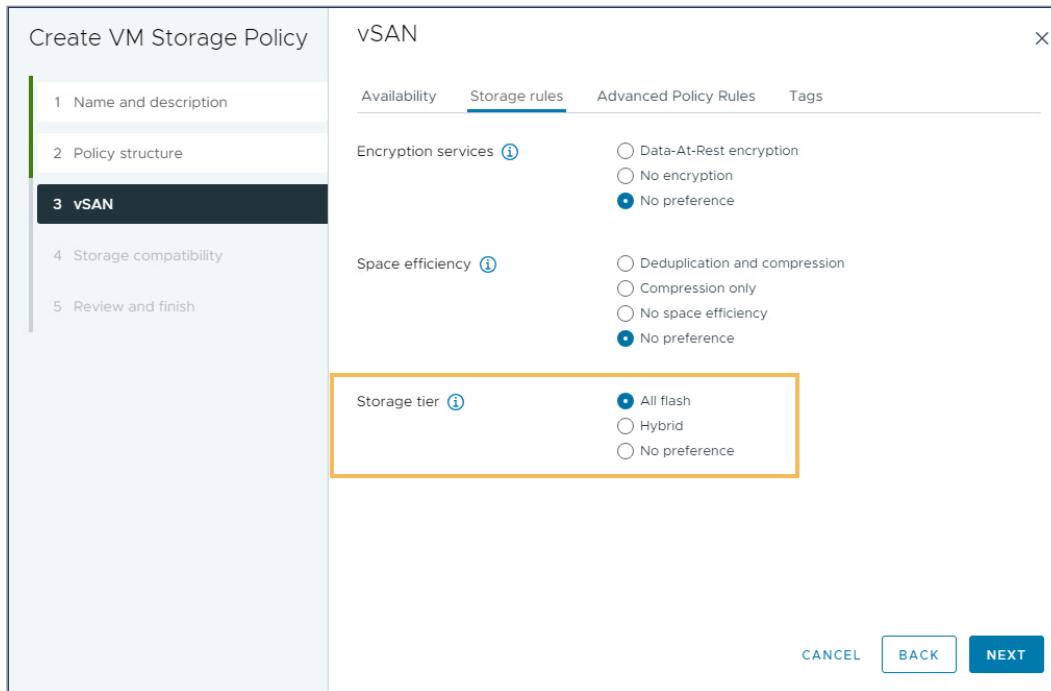
The [required minimum number of fault domains](#) depends on the **Failures to tolerate** setting.

vSAN Storage rules

An All-flash configuration is required when using RAID-5/6 (Erasure Coding).

Create vSAN Storage Policies

In the example below, the datastore must be on an **All flash** Storage tier and **No preference** for encryption services or space efficiency.

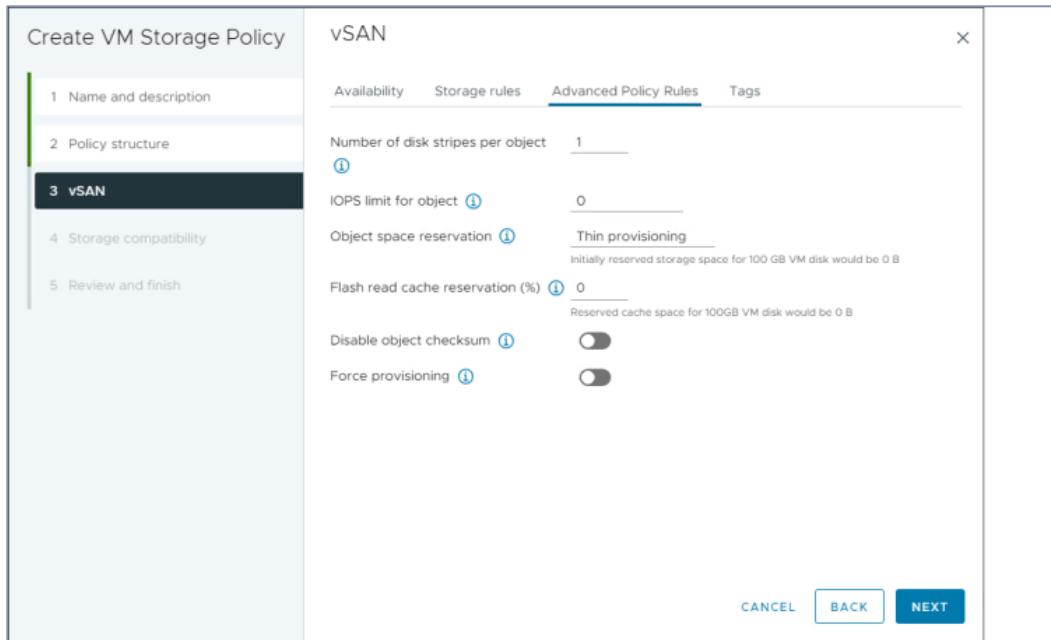


Create VM Storage Policy wizard-Storage rules highlighting vSAN RAID-5/6 must be All-flash

vSAN Advanced Policy Rules

Under the **Advanced Policy Rules**, additional rules can be configured. For additional vSAN policy rules, see the [vSAN Advanced Policy Rules](#). In this example, the default values have been selected.

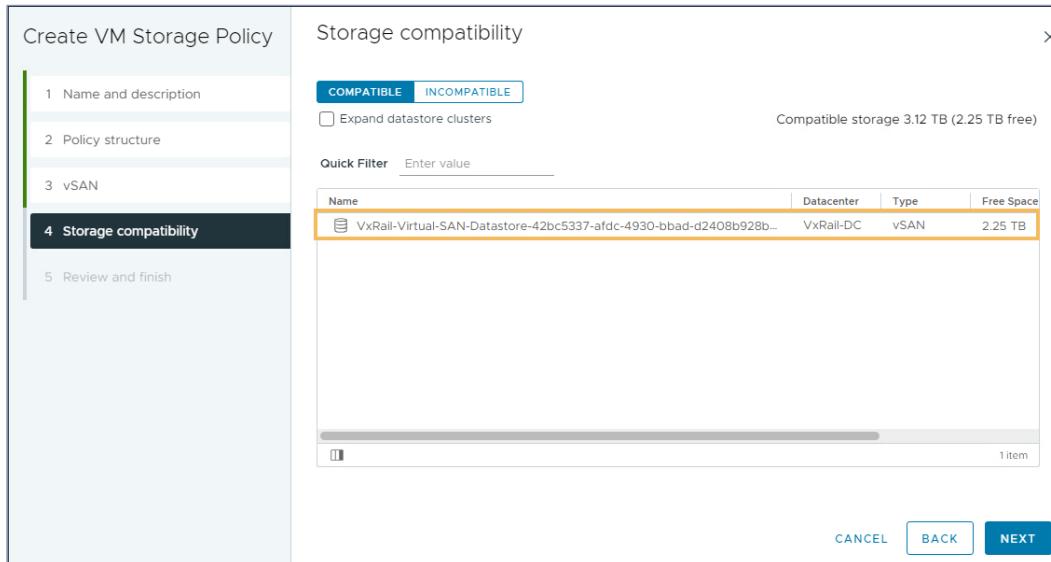
Create vSAN Storage Policies



Create VM Storage Policy wizard-vSAN Advanced Policy Rules

Storage compatibility

The **Storage compatibility** page lists the datastores compatible with the policy settings. In this example, there is only one vSAN datastore that meets the requirements of the configured storage policy.

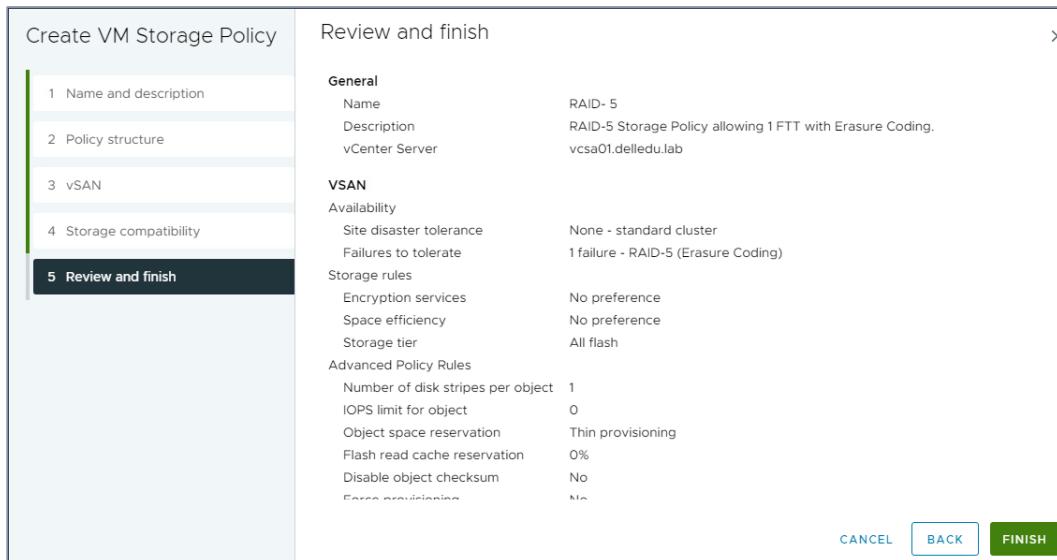


Create VM Storage Policy wizard-Storage compatibility

Incompatible datastores can be located by selecting **INCOMPATIBLE**.

Review and finish

Review the defined policy. Clicking **FINISH** creates the policy.



Create VM Storage Policy wizard-Review and finish

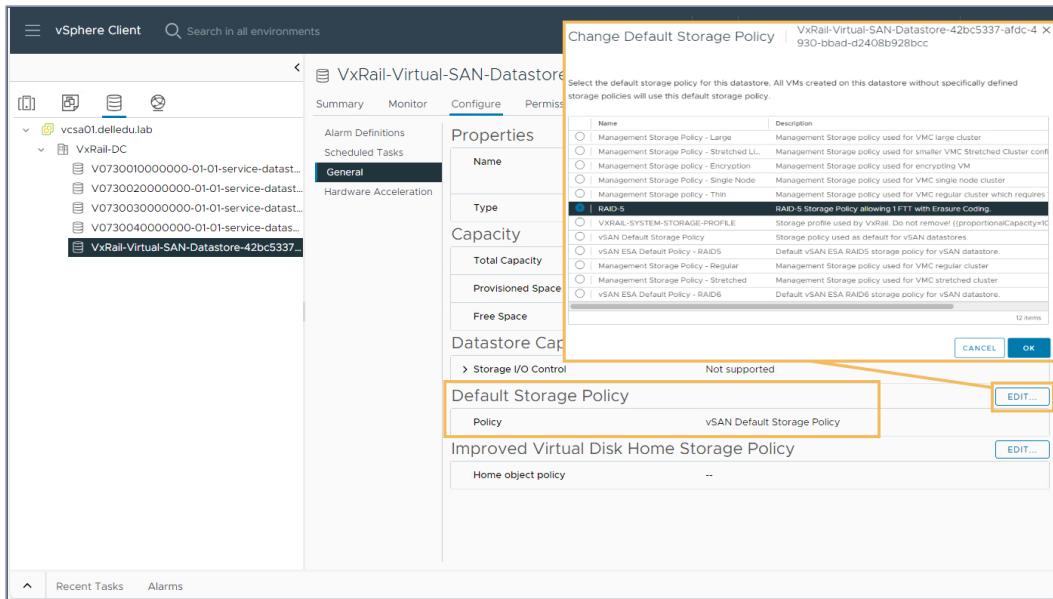
Change vSAN Datastore Default Storage Policy

If a storage policy is not specified while creating a VM, the system uses a default storage policy that is associated with the datastore. The default storage policy for a vSAN datastore is the **vSAN Default Storage Policy**.

However, the default storage policy for the vSAN datastore can be changed. For space efficiency, administrators with All-flash VxRail systems may choose to implement a storage policy with RAID-5 erasure coding as the default policy. In the example, a storage policy that is named **RAID-5** was created. This policy was assigned as the new default storage policy for the vSAN datastore.

Changing the vSAN datastore default storage policy has no impact on currently assigned storage policies.

Create vSAN Storage Policies



VxRail vSAN Datastore - Configure tab showing the Change Default Storage Policy wizard

Lab 12: Create Storage Policy

You want to create a RAID 5 vSAN Storage Policy and make the new policy the default for the vSAN datastore.

Lab Tasks

- Create a RAID 5 vSAN Storage Policy.



Introduction to vSAN ESA Auto-Policy Management

Auto-Policy Management is a cluster-specific default storage policy that helps administrators run workloads on an ESA cluster using the optimal level of resilience and efficiency. When enabled, vSAN recommends storage policies to optimize capacity utilization based on the cluster size and type.

To learn more about Auto-Policy Management, watch the video.

Movie:

The web version of this content contains a movie.

vSAN ESA Auto-Policy Management



Deep Dive: For more information about Auto-Policy Management, go to [Auto-Policy Management Capabilities with the ESA in vSAN 8 U1](#).

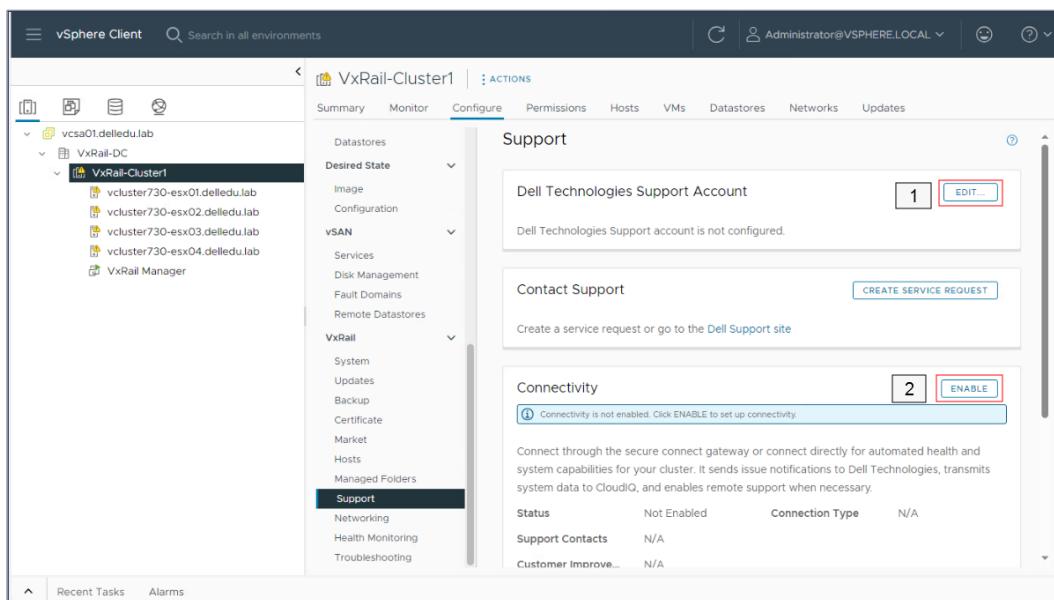
Configure Dell Support Account and Remote Support Connectivity

Configure Dell Support Account and Remote Support Connectivity

An active Dell Support Account is required for configuring remote support connectivity. The support account and connectivity are configured from the VxRail **Support** page.

To access the **Support** page from the vSphere Client, select the **Configure** tab for the **VxRail-Cluster1**, then scroll down to **VxRail > Support**. To learn more about the configuration of support account and connectivity, select the two red hotspots.

VxRail Support page



1:

Enter the support account credentials on this screen to link the account with the VxRail system and allow access to support services. Before installation, obtain a support account from <https://www.dell.com/myaccount/>. The support account is used to:

Configure Dell Support Account and Remote Support Connectivity

Edit Dell Technologies Support Account

Login with your Dell Technologies Support account credentials.

Username * example@onlinesupport.com

Password * 

Don't have an account? [Create an Account](#)

[CANCEL](#) [OK](#)

Edit Dell Technologies Support Account

- Register the VxRail system.
- Obtain product license files.
- Update system software.
- Download VxRail documents.
- Access the VxRail Marketplace.
- Browse VxRail community and support resource.

2: The Status of Connectivity is Not Enabled.

Configure Dell Support Account and Remote Support Connectivity

Connectivity

ENABLE

Info Connectivity is not enabled. Click ENABLE to set up connectivity.

Connect through the secure connect gateway or connect directly for automated health and system capabilities for your cluster. It sends issue notifications to Dell Technologies, transmits system data to CloudIQ, and enables remote support when necessary.

Status	Not Enabled	Connection Type	N/A
Support Contacts	N/A		
Customer Improve...	N/A		

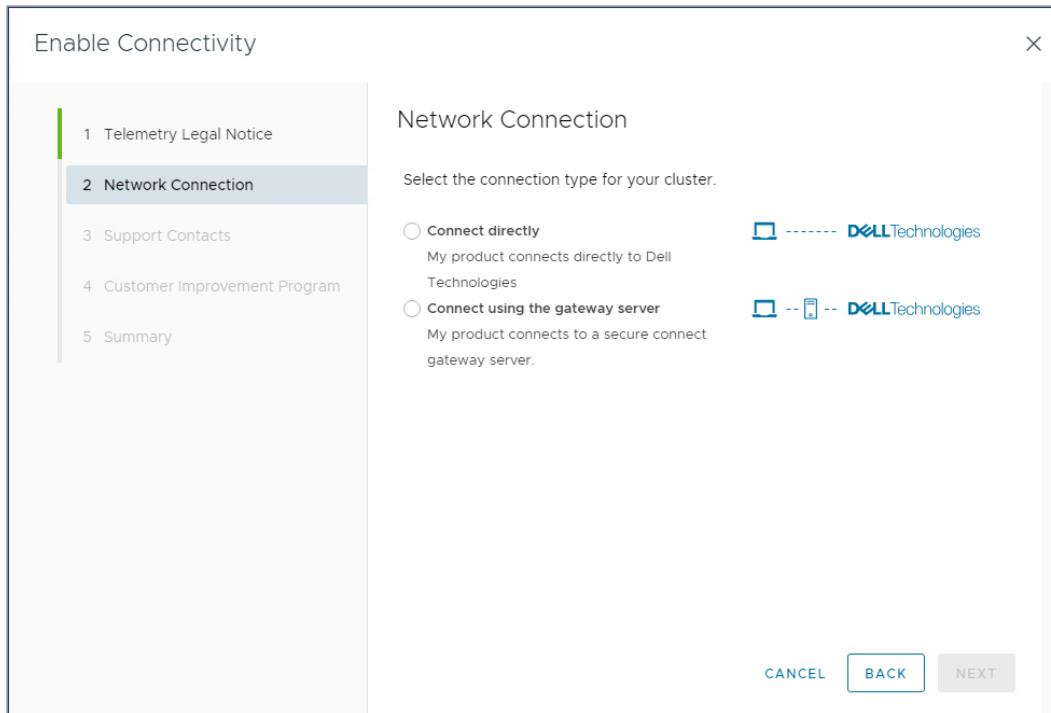
Connectivity Status window

Clicking **ENABLE** launches the **Enable Connectivity** wizard. Use this wizard to connect directly to Dell Technologies or using the gateway server.

The **Connect directly** configuration connects the VxRail system directly to the Dell Technologies.

The **Connect using the gateway server** configuration deploys a new SCG instance.

Configure Dell Support Account and Remote Support Connectivity



Enable Connectivity wizard

Prerequisites for Remote Support Connectivity

Remote Support Connectivity provides secure, automated access between Dell Support and a VxRail system. It allows the system to send configuration data to Dell Support, transmits system data to CloudIQ, and enables Remote Support to connect with the system.

There are two connectivity options available with VxRail:

- **Connect Directly:** The VxRail system connects directly to Dell Technologies using a connectivity agent running on the VxRail Manager. This solution is designed for customers with a single VxRail cluster or customers who want to dedicate connectivity for individual VxRail systems. The other VxRail clusters or devices cannot share the direct connection.
- **Connect using the Gateway Server:** The VxRail system connects to an existing customer-managed Secure Connect Gateway to communicate with Dell Technologies. Multiple VxRail clusters or other

Configure Dell Support Account and Remote Support Connectivity

Dell Technologies products that support Secure Connect Gateway 5.0 connectivity can use a single Secure Connect Gateway.

To learn about the prerequisites for each connectivity option, select each tab.

Prerequisites for connecting directly

- The VxRail system status is set to 'installed' in the Dell Install Base (IB) database.
- The VxRail cluster must have the network connectivity to the Dell Customer Support Systems.
- The VxRail cluster could resolve the DNS names of the Dell Customer Support systems.
- The VxRail cluster must be configured to use NTP servers.
- The active Dell Support account credential is obtained before configuration.

Prerequisites for connecting using the secure connect gateway

- The VxRail system status is set to 'installed' in the Dell Install Base (IB) database.
- The active Secure Connect Gateway is deployed.¹
- The VxRail cluster must have the network connectivity to the Secure Connect Gateway.
- The VxRail cluster must be configured to use NTP servers.
- The active Dell Support account credential is obtained before configuration.

¹For supported Secure Connect Gateway versions, see the [VxRail 8.X Support Matrix](#). If Secure Connect Gateway is not installed, go to the [Dell support page](#) to download the installation files. The Secure Connect Gateway can be installed on the VxRail cluster or any other non-VxRail vSphere node.

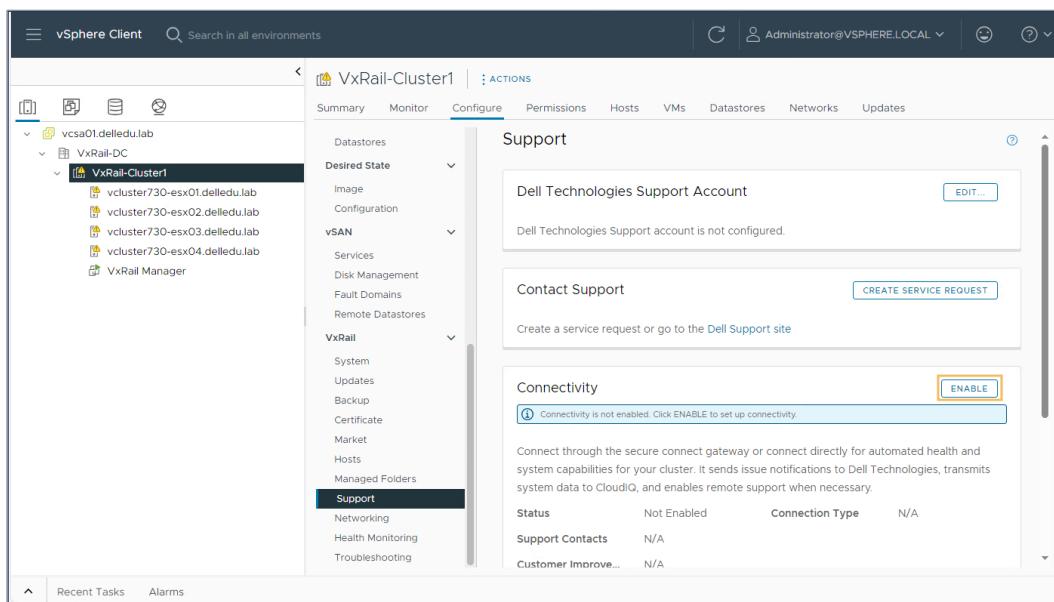
Configure Dell Support Account and Remote Support Connectivity

Enable Remote Support Connectivity

To learn about enabling Remote Support Connectivity, select each tab.

Launch Enable Connectivity Wizard

In the **Connectivity** section of the **VxRail > Support** page, select **ENABLE** to open the **Enable Connectivity** wizard. The Internet connection for VxRail Manager must be enabled on the **VxRail > Networking** page in order to enable Remote Connectivity here.

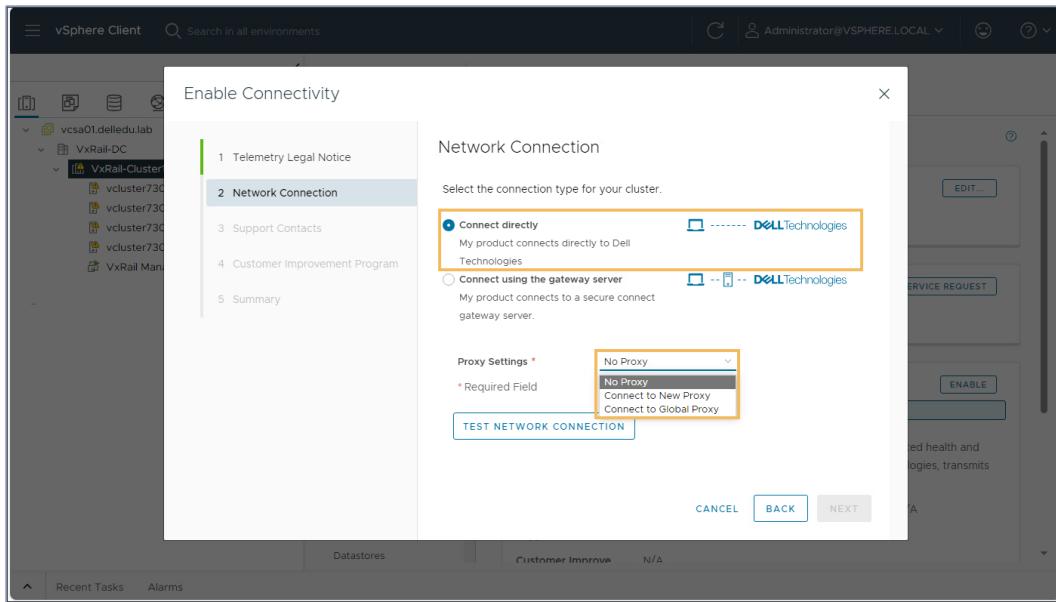


VxRail Plugin Support page with the Connectivity Enable button identified

Network Connection - Connect Directly

In the **Network Connection** step of the wizard, select **Connect directly**, if the VxRail system connects directly to Dell support. Administrators can choose **No Proxy**, **Connect to Global Proxy** that has been configured in the **VxRail > Networking** page or **Connect to New Proxy**.

Configure Dell Support Account and Remote Support Connectivity

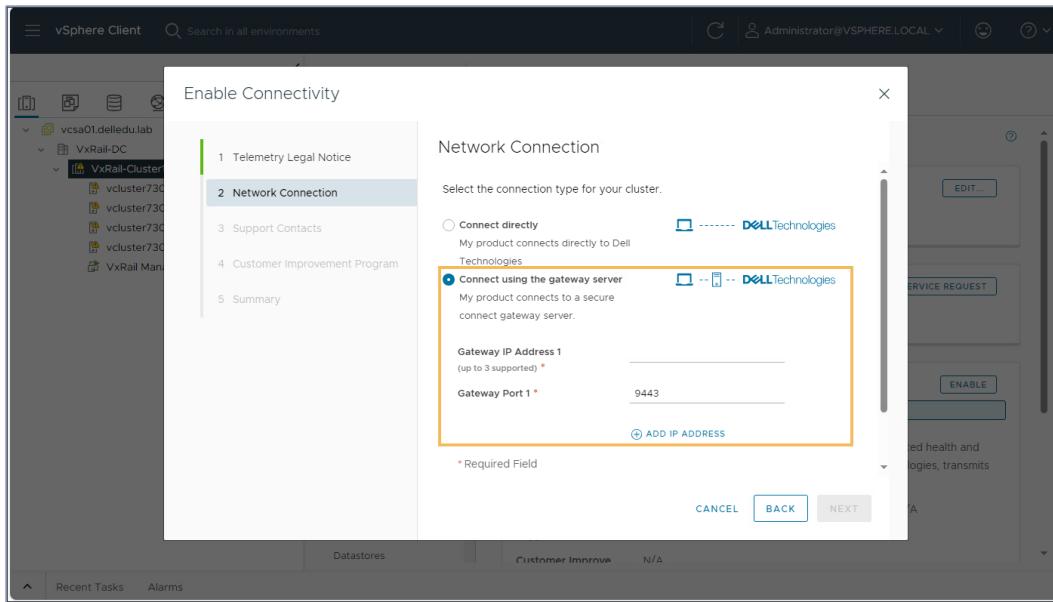


Enable Connectivity wizard - Network Connection step with the Connect directly configuration options identified

Network Connection - Connect using Gateway

In the **Network Connection** step of the wizard, select **Connect using the gateway server**, if the VxRail system connects to an SCG. Enter the IP address and port for the gateway.

Configure Dell Support Account and Remote Support Connectivity

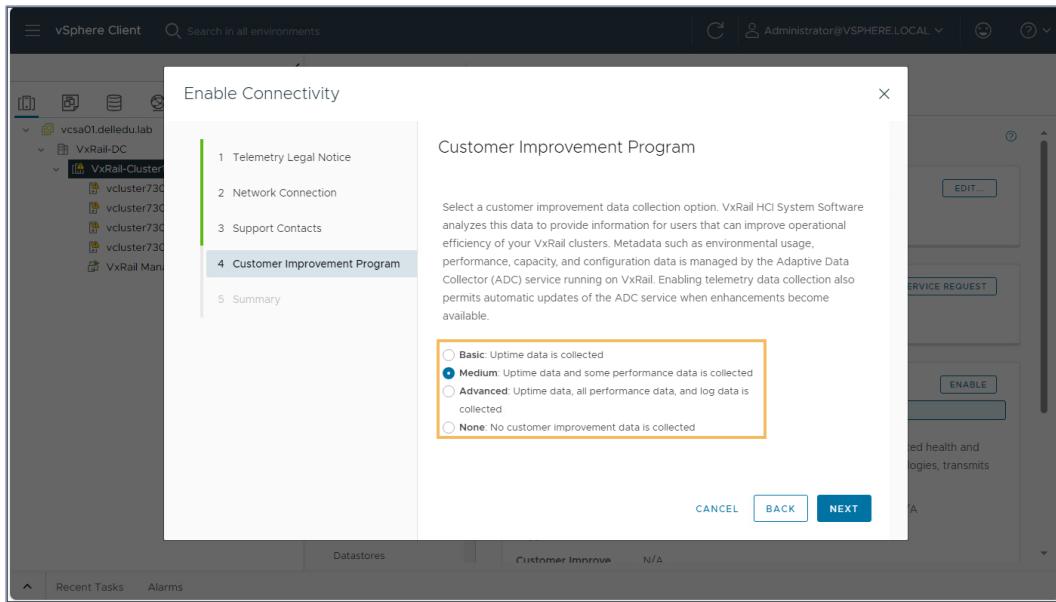


Enable Connectivity wizard - Network Connection step with the Connect using Gateway Server configuration options identified

Customer Improvement Program

The **Customer Improvement Program** collects usage, performance, capacity, and configuration information of the VxRail system. Dell Technologies uses this information to improve VxRail and the customer experience. Participation in the program is optional, and administrators can choose the level of data that is collected. However, for the APEX Private Cloud, select **Medium** or **Advanced**. This participation is required for telemetry data to be sent to CloudIQ.

Configure Dell Support Account and Remote Support Connectivity



Enable Connectivity wizard - Customer Improvement Program step with the data collection options identified

Review and follow the SolVe procedure to enable connectivity.



Important: Once remote connectivity is configured, none of the parameters can be changed. Remote Connectivity has to be disabled and configured again.

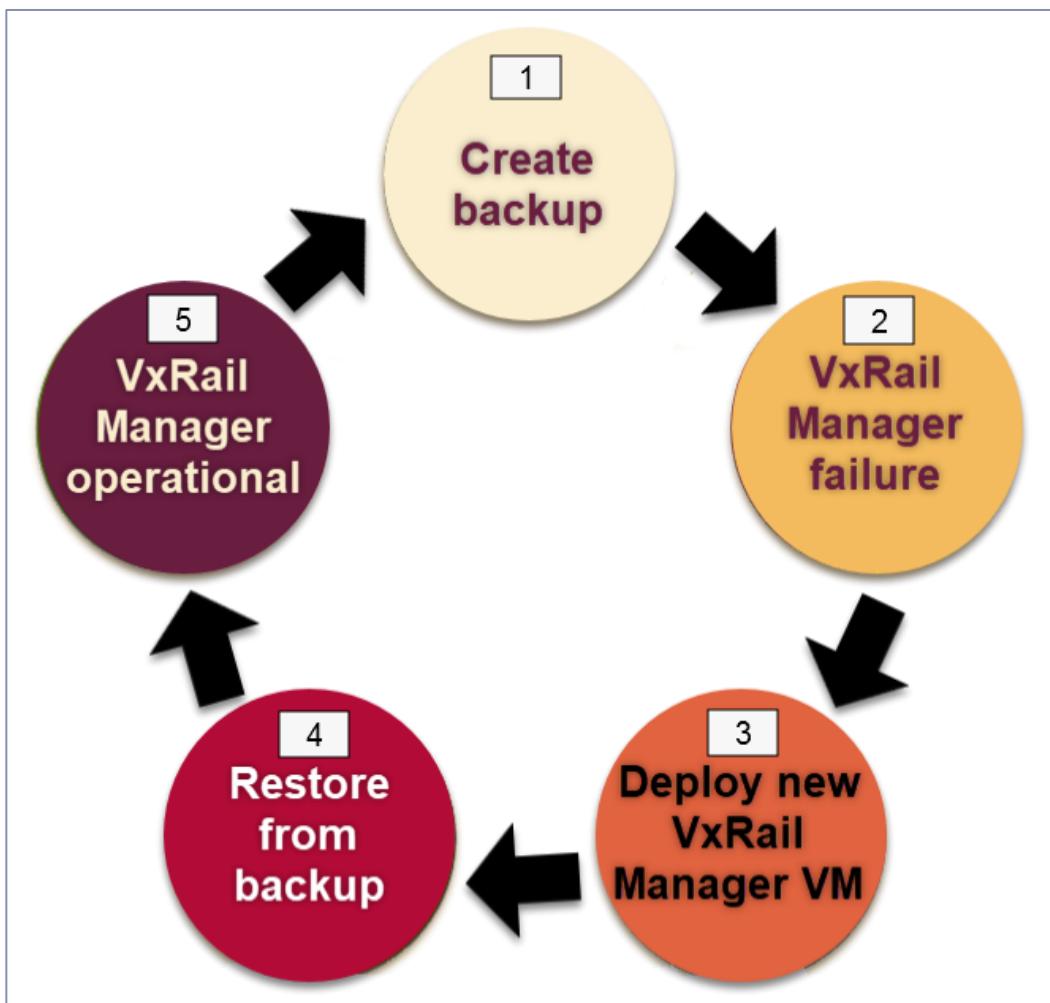
Configure VxRail Manager File-Based Backup

VxRail Manager File-Based Backup Workflow Overview

The VxRail Manager file-based backup and restore mechanism is designed to help recover from a catastrophic failure of the VxRail Manager VM. The benefit is that there is no requirement for any data protection product.

To learn about the VxRail Manager file-based backup and recovery process, select each colored circle:

VxRail Manager file-based backup and recovery process



Configure VxRail Manager File-Based Backup

1: The VxRail Manager backup and restore script is a Python script available on the VxRail Manager VM. The backup script archives VxRail Manager configuration files, database tables, and optionally the log files.

For a standard VxRail cluster, the backup archives are stored in a folder on the VxRail vSAN datastore. The script can be run manually or set up for automatic backups on a scheduled basis.

To setup the automated backup, follow the 'How To' Perform VxRail Manager File-Based Backup SolVe procedure.

2: The restoration of the VxRail Manager VM may become necessary under certain circumstances. For example, the accidental deletion of the VxRail Manager VM or an unrecoverable failure of the VxRail Manager VM.

Customers must engage Dell Support for assistance with the restore process.

3: The restore process starts with the deployment of a new VxRail Manager VM that matches the version of the current VxRail Manager.

4: During the restore, the backed-up configuration is applied to the newly deployed VxRail Manager VM.

The VMware vCenter Server and the vSAN cluster must be healthy for a successful restore.

5: The VxRail Manager VM and the VxRail cluster must be operational and healthy in order to setup VxRail Manager file-based backup.

The backup can be configured after the initial deployment of a VxRail system, or after the VxRail Manager VM has been restored from a file-based backup.

SolVe procedure - 'How To' Perform VxRail Manager File-Based Backup



Important: Customers must engage Dell Support for assistance with the VxRail Manager file-based restore process.

VxRail Manager Backup and Restore Script

To run a backup, select one of the backup scripts that are provided on the VxRail Manager VM. These scripts archive the VxRail Manager configuration files, database tables, and optionally the logs. The created backups are stored in a folder on the VxRail primary datastore.

To locate the scripts, find the `/mystic/vxm_backup_restore` folder on the VxRail Manager VM. To run the script, open a console or a secure shell (SSH) session to the VxRail Manager VM and run the script as the root user.

Configure VxRail Manager File-Based Backup

```
vxrail-manager:/mystic/vxm_backup_restore # python vxm_backup_restore.py -h_
Current user is root. We can do current job.
usage: vxm_backup_restore.py [-h] [-b] [-c] [-6] [--period PERIOD]
                             [--hour HOUR] [--minute MINUTE]
                             [--weekday WEEKDAY] [--monthday MONTHDAY]
                             [--rotation ROTATION] [--keeplog] [-r]
                             [-vcenter VCENTER] [-username USERNAME]
                             [-password PASSWORD] [-l] [-v] [-d] [-n]
                             [--ipv4_address IPV4_ADDRESS] [--gateway GATEWAY]
                             [--netmask NETMASK] [--ipv6_address IPV6_ADDRESS]
                             [--gateway_v6 GATEWAY_V6]
                             [--prefixlength PREFIXLENGTH]

backup/restore

optional arguments:
  -h, --help            show this help message and exit
  -b, --backup          Backup Management Console
  -c, --config          Management Console backup schedule configuration
  -6, --ipv6            ipv6 support
  --period PERIOD      config period value [manual daily weekly monthly]
  --hour HOUR           config backup time value[hour]
  --minute MINUTE       config backup time value[minute]
  --weekday WEEKDAY     config weekday for weekly backup, [0-6] to present
                        [Sun to Sat]
  --monthday MONTHDAY  config monday for monthly backup, value [1-28]
  --rotation ROTATION   config rotation files limit, value [7-24]
  --keeplog             Keep Management Console marvin and mystic log with
                        backup or config.
  -r, --restore          Restore Management Console
  --vcenter VCENTER     vCenter server FQDN or IP
  --username USERNAME    vCenter server username
  --password PASSWORD    vCenter server password
  -l, --list              List current backup files.
  -v, --verbose          verbose output.
  -d, --listdockerservice List K8s Service Version
  -n, --confignetwork    Config Network
  --ipv4_address IPV4_ADDRESS
                        network ipv4 address
  --gateway GATEWAY      network gateway
  --netmask NETMASK       network netmask
  --ipv6_address IPV6_ADDRESS
                        network ipv6 address
  --gateway_v6 GATEWAY_V6
                        network gateway ipv6
  --prefixlength PREFIXLENGTH
                        prefixlength

vxrail-manager:/mystic/vxm_backup_restore #
```

VxRail Manager backup and restore script - Syntax

Tip: There are two versions of the script -



`vxm_backup_restore.py` and
`vxm_backup_restore_limited_bandwidth.py`.

The limited bandwidth script is designed for use cases such as a VxRail 2-Node Cluster in remote offices with Internet bandwidth limitations. The two scripts are identical from a procedural point of view.

Manual Backup Example

To learn about the options used, and the steps the script performs, select the four red hotspots.

Example of running the backup script manually

```

vxrail-manager:/mystic/vxm_backup_restore # python vxm_backup_restore.py -b --keeplog
Current user is root. We can do current job.
Starting to acquire lock.
Acquire lock successfully
Starting to get authentication info.
Connecting to vCenter [vcса01.delledu.lab]
Download vxmbbackup.json from datastore.
datacenter path is /VxRail-DC
download file http_url: https://vcса01.delledu.lab/folder/VxRail_backup_folder/vxmbbackup.json?dsName
=VxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f0&dcPath=%2FUxRail-DC
Start to backup Management Console.
lock box pre copy .....
Dumping database.....
Dumping database succeeded.
Dumping private key.....
Dumping private key succeeded
Archiving system files.....
stop K8s services.....
Start backup to archived_file [/tmp/UxRailBackup/UxRailArchive_20231201174854_28049149.tgz]
Starting K8s services.....
Wait 30 seconds retry[1/50]
Wait 30 seconds retry[2/50]
Archiving system files succeeded: /tmp/UxRailBackup/UxRailArchive_20231201174854_28049149.tgz
Removing temp private key.....
Creating backup path: /UxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f01/UxRail_bac
kup_folder on datastore.....
'vim.Datacenter:datadatacenter-1001'
Creating backup path succeeded
Uploading archived file to datastore 'vim.Datastore:datadatastore-2019'
datacenter path is /VxRail-DC
download file http_url: https://vcса01.delledu.lab/folder/VxRail_backup_folder/UxRailArchive_2023120
1174854_28049149.tgz?dsName=VxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f0&dcPath
=%2FUxRail-DC
-----update json-----
-----pop json-----
add backup record
{"rotation": [{"id": 0, "filename": "UxRailArchive_20231201174434_28049149.tgz", "version": "8.0.100-28049
149"}, {"id": 1, "filename": "UxRailArchive_20231201174854_28049149.tgz", "version": "8.0.
100-28049149"}], "node_number": 3}, {"id": 1, "filename": "UxRailArchive_20231201174854_28049149.tgz", "version": "8.0.
100-28049149"}, {"node_number": 3}], "backup_policy": {"rotation_type": "Manual", "week_day": "0", "month_day": "1", "backup_time_hour": "0", "backup_time_minute": "0", "backup_file_limit": "7", "keep_log": "0"}}
datacenter path is /VxRail-DC
download file http_url: https://vcса01.delledu.lab/folder/VxRail_backup_folder/vxmbbackup.json?dsName
=VxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f0&dcPath=%2FUxRail-DC
Uploading archived file to datastore succeeded.
remove local temporary archive file /tmp/UxRailBackup/UxRailArchive_20231201174854_28049149.tgz.
Management Console backup finished.
Starting to release lock.
Release lock successfully
Removing temp private key.....
vxrail-manager:/mystic/vxm_backup_restore #

```

1: The **-b** option is used to backup the VxRail Manager. The **--keeplog** option is used to include the VxRail Manager logs in the backup archive.

2: The script maintains a catalog of all the backups in the **vxmbbackup.json** file on the VxRail vSAN datastore. The catalog file is created when the backup script is run for the first time. Then, each time the script runs, the catalog file is downloaded from the vSAN datastore

Configure VxRail Manager File-Based Backup

and updated with the latest information. The updated catalog file is uploaded back to the datastore after the backup operation is complete.

3: The script creates the backup archive locally on the VxRail Manager VM and then uploads the archive to the VxRail vSAN datastore.

4: Once the backup archive has been successfully uploaded to the VxRail vSAN datastore, the local archive on the VxRail Manager VM is deleted.

Schedule Periodic Backup

The scheduled backup frequency can be daily, weekly, or monthly. The backup schedule uses the operating system time zone that is set on the VxRail Manager VM. To learn about determining the time zone setting, the options for scheduling a backup, and the steps the script performs, select the three red hotspots.

Example of scheduling a periodic backup

```
vxrail-manager:/mystic/vxm_backup_restore # date
Fri 01 Dec 2023 06:14:38 PM UTC
1
vxrail-manager:/mystic/vxm_backup_restore # python vxm_backup_restore.py -c --period daily --hour
--minute 0 --rotation 7 --keeplog
Current user is root. We can do current job.
Download vxmbackup.json from datastore.
Starting to get authentication info.
Connecting to vCenter [vcsa01.delledu.lab]
datacenter_path is /UxRail-DC
download file http_url: https://vcsa01.delledu.lab/folder/UxRail_backup_folder/vxmbackup.json?dsName
=UxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f0&dcPath=/ZFUxRail-DC
Auto backup time is 0:0
2
Current auto backup will not keep logs
Current stored backup files limitation is [?]
-----update crontab-----
3
0 1 * * * root /usr/bin/logger 'UxM rotation backup start.' && python /mystic/vxm_backup_restore/vxm
_backup_restore.py -b --keeplog

cronjob is updated.
datacenter path is /UxRail-DC
download file http_url: https://vcsa01.delledu.lab/folder/UxRail_backup_folder/vxmbackup.json?dsName
=UxRail-Virtual-SAN-Datastore-f0b0f897-504b-4310-a74d-791c66fcf0f0&dcPath=/ZFUxRail-DC
schedule config is updated and uploaded to datastore
{"rotation": [{"id": 0, "filename": "UxRailArchive_20231201174434_28049149.tgz", "version": "8.0.100-28049
149", "node_number": 3}, {"id": 1, "filename": "UxRailArchive_20231201174854_28049149.tgz", "version": "8.0.
100-28049149", "node_number": 3}], "backup_policy": {"rotation_type": "daily", "week_day": "0", "month_day": "1", "backup_time_hour": "1", "backup_time_minute": "0", "backup_file_limit": "7", "keep_log": "1"}}

current backup rotation type is daily
Auto backup time is 1:0
Current auto backup will keep logs
Current stored backup files limitation is [?]
[Schedule config job END]

vxrail-manager:/mystic/vxm_backup_restore #
```

1: Determine the VxRail Manager operating system time zone with the **date** command. In this system, the time zone is UTC.

Configure VxRail Manager File-Based Backup

2: In this example, the VxRail Manager backup schedule is set to daily at 01:00 UTC. The time is specified in the 24-hour format. The rotation is set to 7 (retain up to seven backup files), and the VxRail Manager logs are included.

3: The script updates the Cron job on the VxRail Manager VM with the requested schedule. The schedule information is updated in the `vxmbbackup.json` file. The updated `vxmbbackup.json` file is uploaded to the VxRail vSAN datastore.



Best Practice: In addition to the periodic backups, Dell Technologies recommends doing a manual backup immediately after a service procedure such as a node addition, removal, or replacement.

Copy Recovery Bundle to vSAN Datastore

VxRail systems include a Recovery Bundle on the VxRail Manager VM. The Recovery Bundle contains code that is used during the VxRail node add process. If the node is at a lower version, the Recovery Bundle is used to upgrade the node to the version of the cluster.

The Recovery Bundle must be backed up to the vSAN datastore for a successful VxRail Manager file-based restore. The Recovery Bundle is in the `/data/store2/recovery` folder.

Use the `scp` command to copy the bundle from the VxRail Manager VM to the vSAN datastore.

```
mystic@vxrail-manager:~> scp /data/store2/recovery/recoveryBundle-8.0.100.zip root@vcluster730-esx01.delledu.lab:/vmfs/volumes/vsan:5258a44e4b33d609-14d04006d7ae3477/VxRail_backup_folder
The authenticity of host 'vcluster730-esx01.delledu.lab (172.16.5.51)' can't be established.
ECDSA key fingerprint is SHA256:H1ts4OT0ge0HALWR+Mq+KzzzXndxK0CV55TBcca+NuA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'vcluster730-esx01.delledu.lab,172.16.5.51' (ECDSA) to the list of known hosts.
Password:
recoveryBundle-8.0.100.zip
mystic@vxrail-manager:~>
```

Example of copying the Recovery Bundle to the VxRail vSAN datastore

Configure VxRail Manager File-Based Backup

Before running the `scp` command, enable SSH on the VxRail node that is used for the copy process. In the example shown, the VxRail node in question is `vcluster730-esx01.delledu.lab`. The `scp` command challenges for the root password of the specific VxRail node.



Important: A VxRail software upgrade creates a version-specific Recovery Bundle. The new bundle should be backed up to the vSAN datastore after the software upgrade.

VxRail vSAN Datastore - VxRail Backup Folder

The backup archives, the backup catalog, and the Recovery Bundle are all stored in the VxRail vSAN datastore in a folder named

VxRail_backup_folder. The example shows the Recovery Bundle, the `vxmbbackup.json` file, and two backup archives.

The screenshot shows the VxRail vSAN Datastore interface. The left sidebar shows a tree view of the datastore structure, with the `VxRail_backup_folder` highlighted. The main pane displays a list of files and folders within this folder. The list includes:

Name	Type	Path
sdid.sdf	Folder	[VxRail-Virtual-SAN-Datastore-f0b0f8]
recoveryBundle-8.0.100.zip	File	[VxRail-Virtual-SAN-Datastore-f0b0f8]
vxmbbackup.json	File	[VxRail-Virtual-SAN-Datastore-f0b0f8]
VxRailArchive_20231201174434_28049149.tgz	File	[VxRail-Virtual-SAN-Datastore-f0b0f8]
VxRailArchive_20231201174854_28049149.tgz	File	[VxRail-Virtual-SAN-Datastore-f0b0f8]

Below the list, there is a table for Recent Tasks and Alarms, showing a completed task to delete a file.

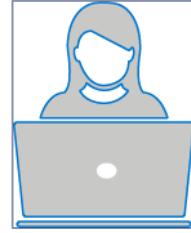
VxRail vSAN datastore - VxRail backup folder

Lab 13: Configure VxRail Manager File Based Backup

You have completed the deployment of the VxRail cluster and must configure VxRail Manager file-based backup.

Lab Tasks

- Log in to the vSphere Client and browse the contents of the VxRail vSAN datastore.
- Log in to the VxRail Manager VM and:
 - Review the syntax of the VxRail Manager backup and restore script.
 - Run the backup script manually.
 - Retrieve the list of backup archives.
 - Configure a periodic backup schedule.
- Browse the contents of the VxRail vSAN datastore and confirm the existence of the new backup folder and archives.



Perform VxRail Software Upgrade

VxRail Software Upgrade Overview

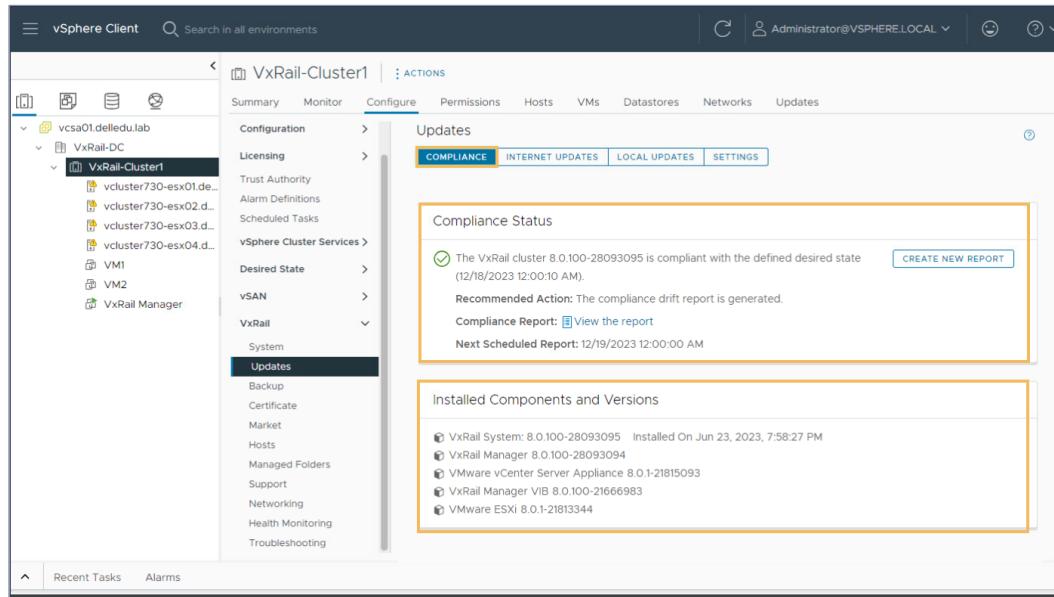
The VxRail software update is initiated from the VxRail Plugin. To initiate a software update, select the **Configure** tab for a cluster. In the middle pane, select **VxRail > Updates**.

To learn more about VxRail updates, select each tab.

COMPLIANCE

The **COMPLIANCE** tab displays the **Compliance Status** of the cluster. The **Compliance Report** runs daily, or administrators can manually generate a report.

This tab also displays the components that are installed on the cluster and their versions.



VxRail Plugin Updates COMPLIANCE tab

INTERNET UPDATES

The **INTERNET UPDATES** tab allows administrators to directly access and download the required update bundle. Advisory reports can also be generated from this tab using the **ACTIONS** menu.

To use the Internet updates option, VxRail Manager must have Internet connectivity and be configured with a Dell support account.

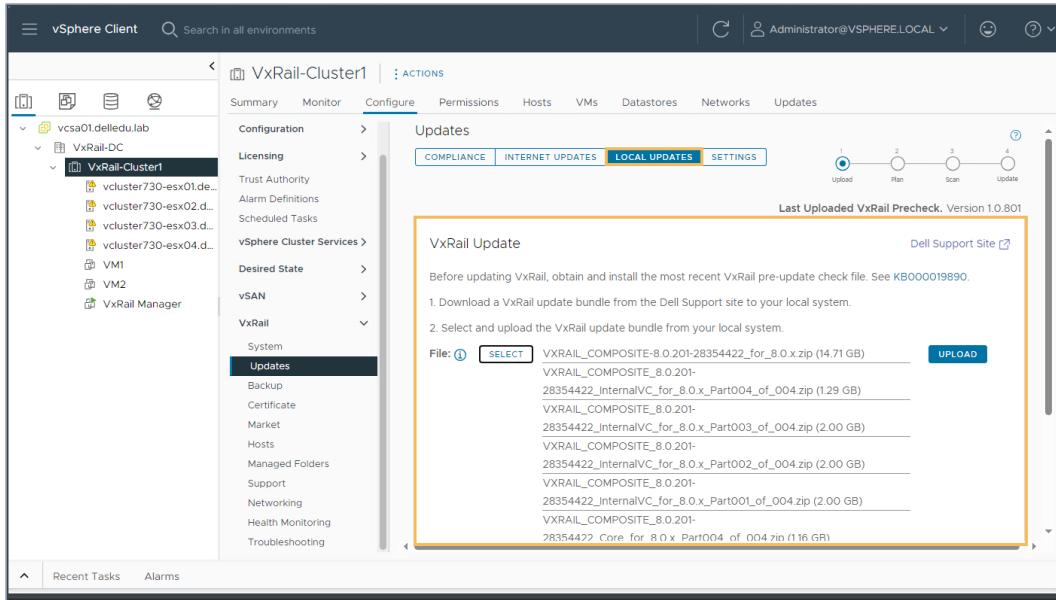
VxRail Plugin **INTERNET UPDATES** tab

LOCAL UPDATES

The **LOCAL UPDATES** tab allows administrators to upgrade a VxRail system that is not connected to the Internet. To perform a local update, download the upgrade bundle from the Dell Support Site and upload the bundle into VxRail.

Administrators can download a single bundle that contains all the required files, or if there are bandwidth limitations, download the bundle in multiple parts. The multiple files can be uploaded into VxRail to perform the upgrade.

Perform VxRail Software Upgrade



VxRail Plugin LOCAL UPDATES tab showing multiple files that are uploaded to VxRail

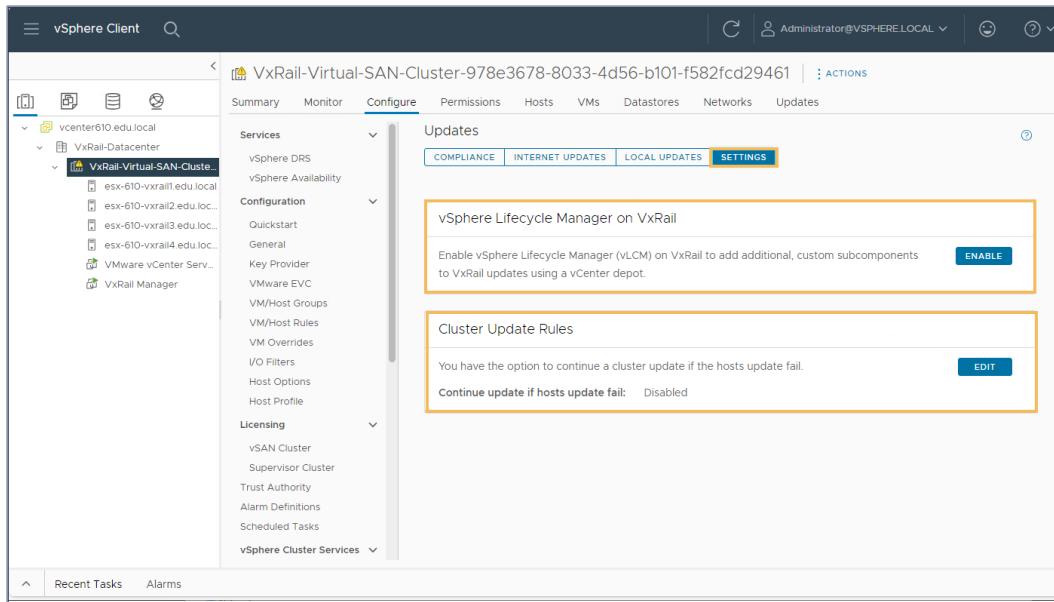
SETTINGS

The **SETTINGS** tab allows administrators to enable vSphere Lifecycle Manager (vLCM) on VxRail. vLCM is an enhanced version of vSphere Update Manager (VUM). VxRail Administrators can continue to use VxRail LCM, or enable vLCM on VxRail.

Whether VxRail LCM or vLCM on VxRail is used, upgrades must be done through the VxRail Plugin Update page. Upgrading through the vSphere Lifecycle Manager UI is not supported and can cause the cluster to become noncompliant and unstable.

Administrators can also enable **Cluster Update Rules** from this tab. When **Cluster Update Rules** is enabled, the cluster update will continue to the next host if the update of the current host fails. The LCM will retry the update on the host that failed after all the other hosts are updated.

Perform VxRail Software Upgrade



VxRail Plugin Updates SETTINGS tab

Enabling vLCM

To learn about enabling vLCM on VxRail, select each tab.

Disable VMware Download Sources

When vLCM on VxRail is enabled, the vSphere Lifecycle Manager points to folders in VxRail Manager as the download source instead of VMware folders.

You must disable all default VMware-based **Download Sources**, before enabling vLCM on VxRail. Disabling the VMware folders causes the system to point to the VxRail folders. Failure to disable these settings results in failure messages during vLCM enablement for VxRail.

To disable the **Download Sources**, go to **vSphere Menu > Lifecycle Manager > Settings > Patch Setup**.

Perform VxRail Software Upgrade

The screenshot shows the 'Lifecycle Manager' interface in the 'Updates' section. On the left, there's a sidebar with 'Administration' (Patch Downloads, Patch Setup), 'Host Remediation' (Images, Baselines, VMs), and 'Image Depot'. The main area displays a table of patches from the internet, with one row highlighted: 'https://172.17.46.37/vlcm/depot/hsm/depot...' (Status: Yes, Connectivity: Connected, Source: Custom, Component: Host, Description: VxRail Manager Online Depot). A 'CHANGE DOWNLOAD SOURCE' button is visible at the top right of the table.

vSphere Client Lifecycle Manager Patch Setup page showing VxRail Manager as the source depot

Enable vLCM on VxRail

vLCM on VxRail is enabled by selecting the **ENABLE** button on the **VxRail > Updates > Settings** page. To enable vLCM on VxRail, the VxRail system must be in a compliant state.

The screenshot shows the 'vSphere Client' interface for a 'VxRail-Virtual-SAN-Cluster'. The left navigation pane shows 'vcenter610.edu.local' and 'VxRail-Datacenter'. The main panel is on the 'Configure' tab, specifically the 'Updates' sub-tab under 'Settings'. It shows a section for 'vSphere Lifecycle Manager on VxRail' with a note: 'Enable vSphere Lifecycle Manager (vLCM) on VxRail to add additional, custom subcomponents to VxRail updates using a vCenter depot.' A blue-bordered 'ENABLE' button is highlighted. Below it is a 'Cluster Update Rules' section with a note: 'You have the option to continue a cluster update if the hosts update fail.' and a 'Continue update if hosts update fail:' dropdown set to 'Disabled'.

VxRail Plugin Updates SETTINGS tab with the vLCM on VxRail ENABLE button highlighted

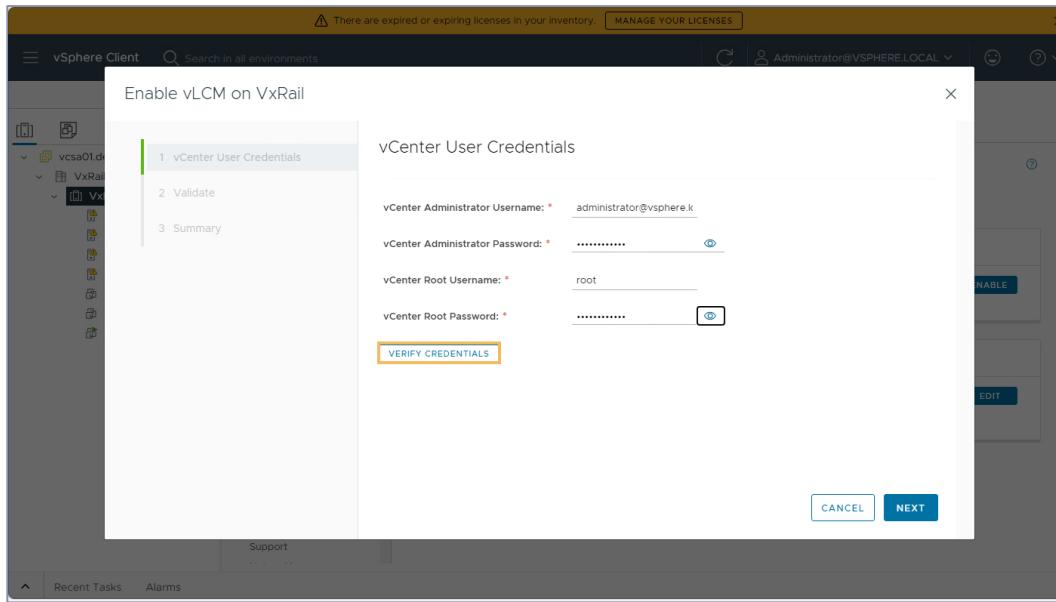
Enter Credentials

Selecting the **ENABLE** button launches the **Enable vLCM on VxRail Wizard**. On the **vCenter User Credentials** page of the wizard, enter the

Perform VxRail Software Upgrade

credentials for the vCenter managing the cluster and select the **VERIFY CREDENTIALS** button.

After the **VERIFY CREDENTIALS** button is selected, the system will [request confirmation that a self-signed certificate can be added to the SSL Certificate folder on the vCenter Server](#).

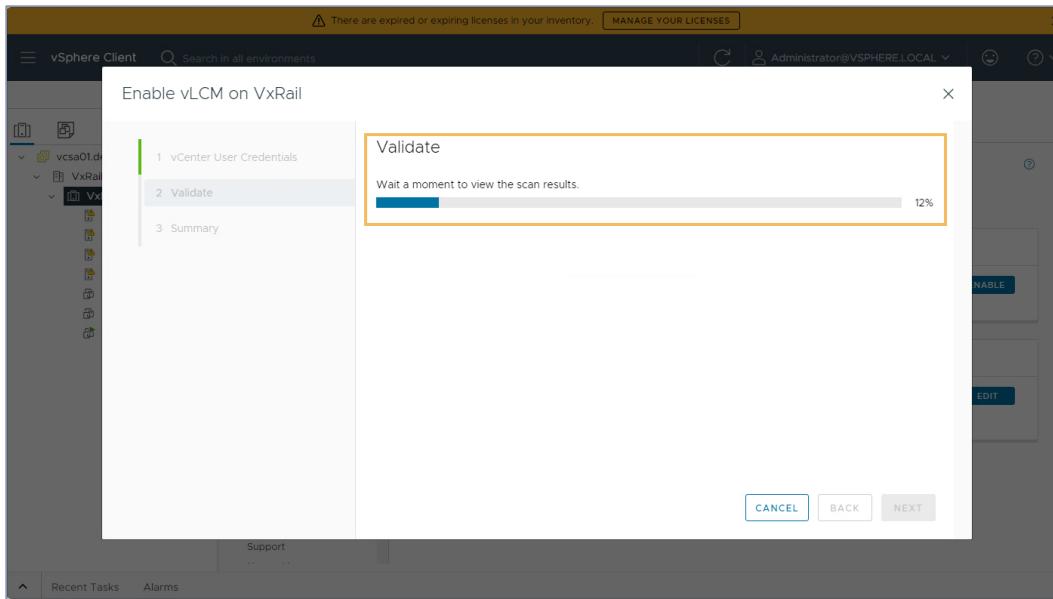


Enable vLCM on VxRail Wizard vCenter User Credentials page

Validate

Once the credentials have been validated, the system will validate that the cluster is ready to enable vLCM on VxRail.

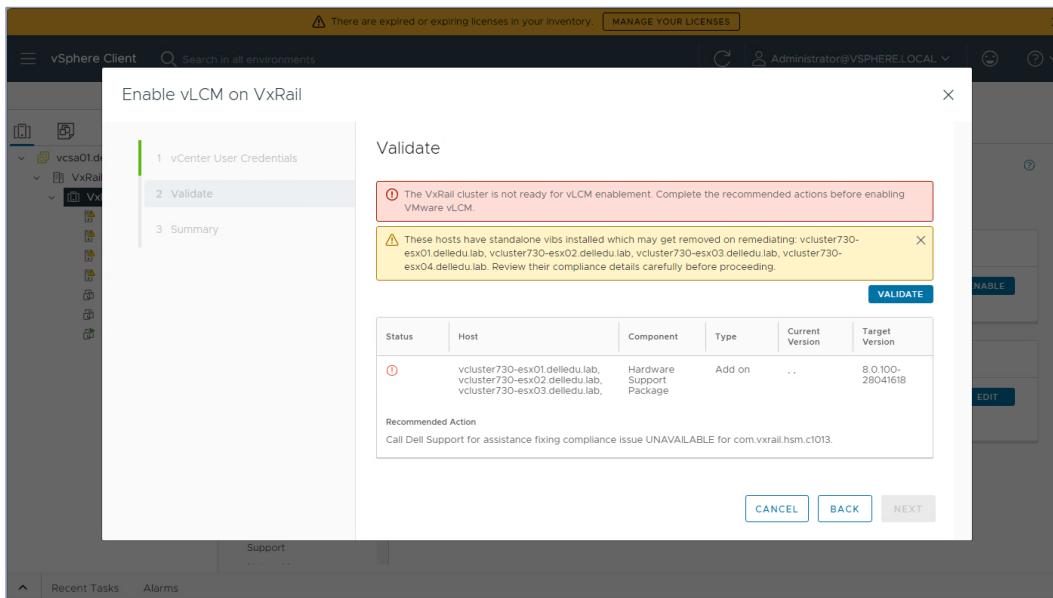
Perform VxRail Software Upgrade



Enable vLCM on VxRail Wizard Validate page

Remediate issues

After the validation, the wizard will display any issues that need to be remediated before enabling vLCM on VxRail.



Enable vLCM on VxRail Wizard Validation page showing remediation issues

Lifecycle Management Options Comparison

VxRail offers two options for lifecycle management: vSphere Lifecycle Manager on VxRail and VxRail LCM.

- vSphere Lifecycle Manager on VxRail is beneficial in environments that have installed custom components and software on their VxRail install base and want a unified upgrade experience. vLCM on VxRail facilitates the upgrades of the custom components.
- VxRail LCM is beneficial in environments that do not have a requirement for a customized LCM process. The components and software that are deployed on the VxRail installed base are within the supported scope of VxRail LCM.

vLCM on VxRail	VxRail LCM
Customized environment - Custom components and software can be installed on the VxRail.	Engineered ecosystem - Fully integrated, preconfigured, and tested VxRail environment.
Desired state – Administrators define, maintain, and validate a desired state.	Validated State - Software, drivers and firmware are defined, tested, and validated by Dell.
Homogenous hosts – Nodes must have identical configurations within a cluster.	Heterogenous hosts – Supports mixed node configurations within a cluster.
Requires support from multiple vendors.	Requires support from a single vendor.



Caution: Once vLCM is enabled for VxRail a cluster, you cannot revert to VxRail LCM.

Review the [How does vSphere LCM compare with VxRail LCM? Blog](#) for more information about vLCM.

VxRail Software Upgrade Considerations

Certain VxRail versions allow the direct upgrade to VxRail version 8.0.xxx. See the [VxRail version 8.0.x Release Notes](#) for the exact version information.

The release notes also provide details of the fixes and features in each release compared to previous releases. These details help drive the decision to upgrade.

Consider the following before performing a VxRail Software upgrade to version 8.0.xxx:

- The external vCenter Server should be at the supported version level before upgrade. See the [VxRail and External vCenter interoperability Matrix](#) for more information.
- VMware Horizon and other integrated VMware solution software should be at the supported version. Check the specific solution release notes before upgrading.

VxRail Software Upgrade High-Level Process

Perform the following high-level steps to upgrade VxRail software:

- Download the appropriate SolVe procedure.
- Ensure that the following passwords are available:
 - VxRail Manager root
 - vCenter Administrator
 - vCenter Server Appliance (VCSA) root
- Ensure the appropriate licenses are available.

Perform VxRail Software Upgrade

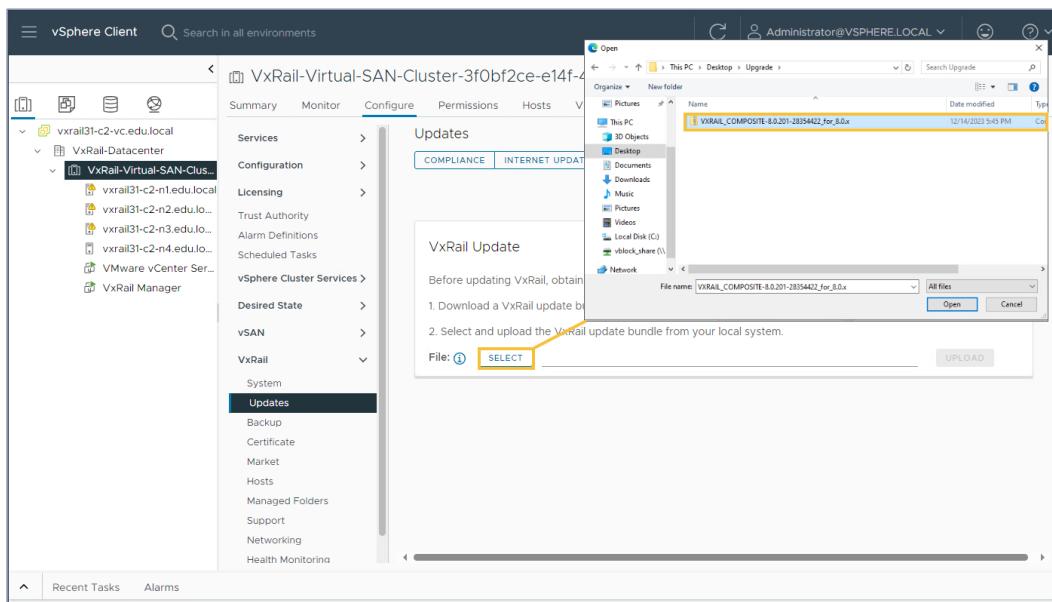
- Run [VxVerify](#) to check update readiness of the VxRail system.
- Ensure the cluster and vSAN are healthy.
- Take a snapshot of each service VM.
- Perform the upgrade.

VxRail Software Upgrade Using Local Updates

To learn more about updating VxRail Software using local updates, select each tab.

Select File

In the open file dialog, select the update file(s) that were previously downloaded and saved locally. If multipart files are used, ensure that all multipart files are uploaded at the same time and do not rename any of the files.

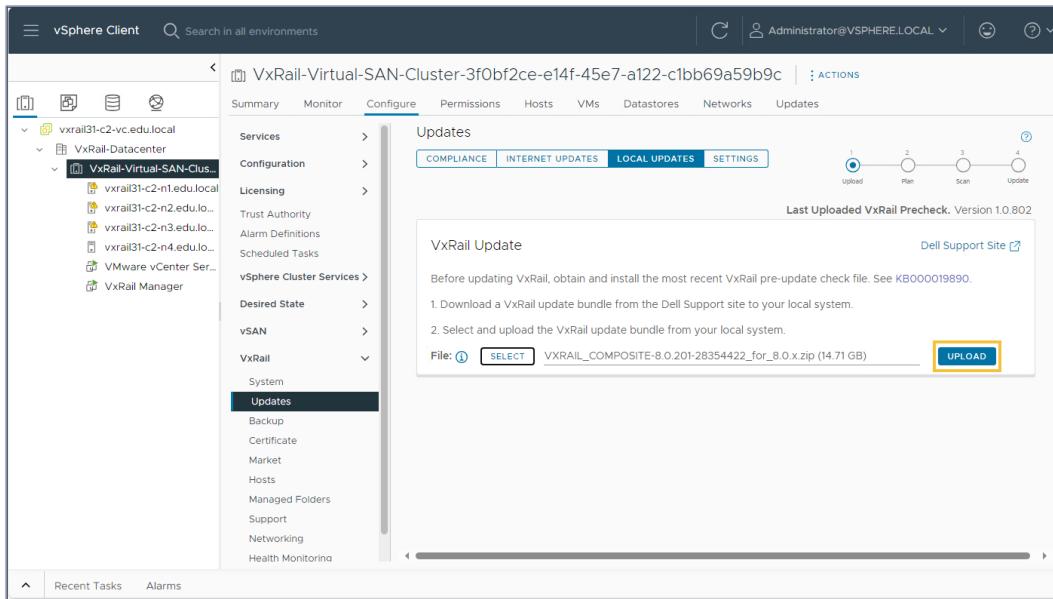


VxRail Local Updates page showing a VxRail Composite bundle selected

Upload File

Upload the update bundle. Once the files are uploaded, the system will automatically begin the extraction and prechecking.

Perform VxRail Software Upgrade



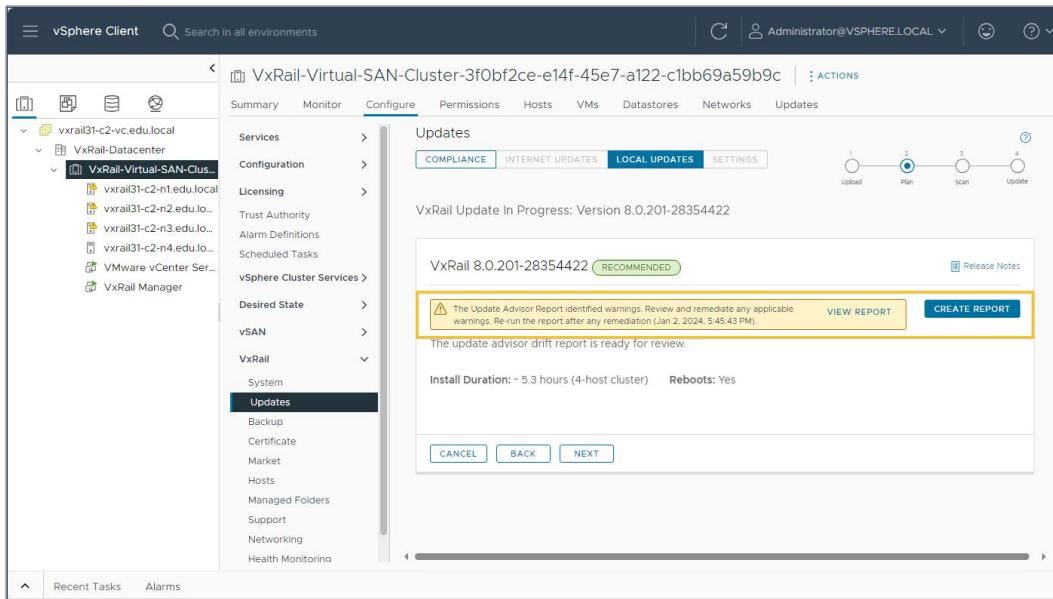
VxRail Local Updates page with the UPLOAD button highlighted

Create Advisory Report

Create an Advisory Report to view the impact of an update on all components in a VxRail system. The report provides guidance on what the final cluster configuration will be once the update process completes. If the Advisory Report identifies any issues, they must be remediated before beginning the update.

View a sample [Advisory Report](#).

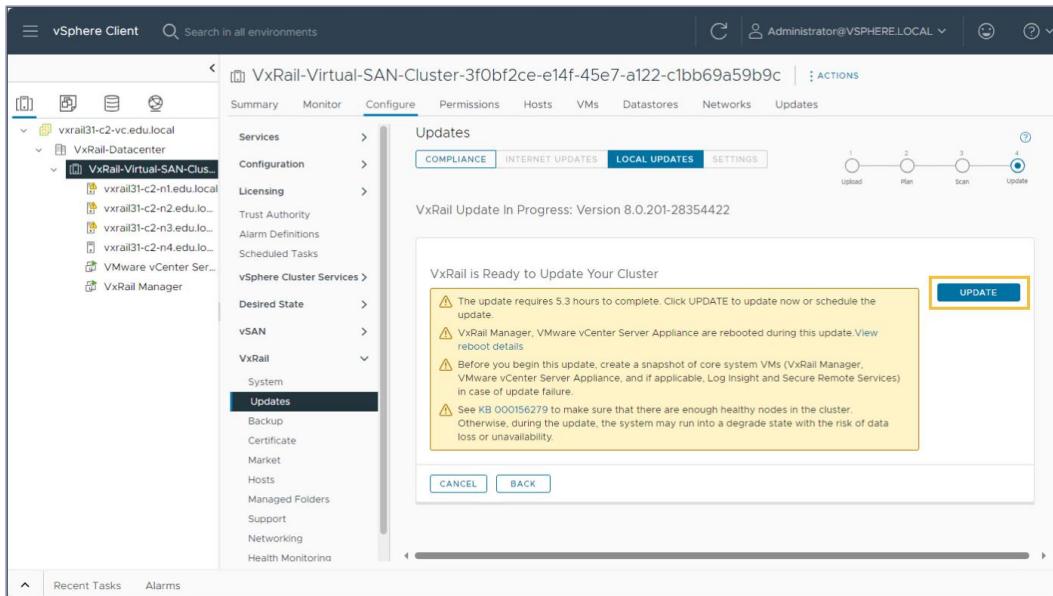
Perform VxRail Software Upgrade



VxRail Local Updates page with the CREATE REPORT button highlighted

Update Cluster

Begin the update. During the update, vCenter may be disconnected and require a login. Monitor the update until it completes successfully.



VxRail Local Updates page with the UPDATE button highlighted

Interaction: Perform VxRail Software Upgrade

The web version of this content contains an interactive activity.

Perform VxRail Cluster Expansion

VxRail Cluster Expansion - Add Node to Same Rack

The initial deployment of a VxRail cluster is limited to six nodes. Nodes can be added to the cluster in one to six node increments. For VxRail deployments with more than six nodes, build the VxRail cluster with six nodes, and then add the rest of the nodes.

While a VxRail cluster can be expanded beyond a single physical rack, the typical use case is for cluster expansion within the same rack. When adding nodes within the same Layer 2 segment, the IP addresses must be on the same subnets as the existing cluster.

The add node process confirms that the new node hardware, firmware, and software are compatible with the cluster. Compatible nodes at an older version are automatically upgraded to the cluster version during the node add process.

Contact Dell support for assistance with incompatible nodes.

Planning Considerations for Scalability

Cluster Expansion - Add Node Procedure

A standard VxRail cluster with E660N nodes has been deployed. The automatic node discovery method was used during initial configuration.

To add a E660N node to the cluster in the same rack, use [SolVe](#) to generate the Compute Node and Dynamic Node Expansion procedure.

Topic
VxRail Hardware Upgrade Procedures
Selections
Select a procedure: Compute Node and Dynamic Node Expansion What VxRail Software Version is the Cluster running?: v8.0.000/100/101/110/111/200 Select vSAN Datastore Type: vSAN OSA (Original Storage Architecture) Select Encryption Option: No encryption Select Security Option: None Select the node discovery method: Auto using node discovery network Is the VxRail cluster configured with only PCIe-based Ethernet ports?: No Is this a dynamic node cluster?: No Is the system a vSAN Stretched Cluster?: No Is the node discovery VLAN set to the default of 3939: Yes SmartFabric Services Network Options: No SmartFabric Services Configured on Network Select a procedure: Layer 2 - Add New Node(s) Select the VxRail Appliance to be Added to the Existing Cluster: VxRail E660N

SolVe procedure selections for adding a node.

Follow the procedure to complete the node add process. High-level steps:

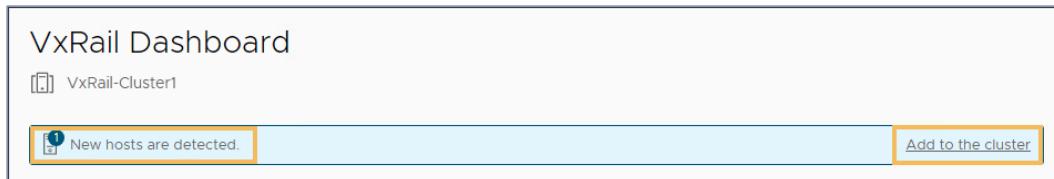
- Mount the node in the rack.
- Connect the node to AC power.
- Connect the node to the ToR switches.
- Power on the node.
- Configure iDRAC for the node.
- Verify the date and time settings on the node.
- Adjust the VLAN IDs of the port groups on the node if necessary.
- Add the node to the VxRail cluster.

Example:Compute Node and Dynamic Node Expansion Procedure.

Using the VxRail Plugin to Add a Node

For VxRail clusters configured with automatic node discovery, the **VxRail Dashboard** displays a notification when new nodes are discovered.

Perform VxRail Cluster Expansion



VxRail Dashboard - New hosts detected

Selecting **Add to the cluster** redirects to the **Hosts** page of the VxRail cluster. Alternatively, select the cluster and go to **Configure>VxRail>Hosts**.

To initiate the node add process, select **ADD**.

A screenshot of the vSphere Client interface. The left sidebar shows a tree structure with 'vcsa01.delledu.lab' expanded, showing 'VxRail-DC' and 'VxRail-Cluster1'. 'VxRail-Cluster1' is selected. The main pane is titled 'VxRail-Cluster1' and has tabs for 'Summary', 'Monitor', 'Configure' (which is highlighted), 'Permissions', 'Hosts', 'VMs', 'Datastores', 'Networks', and 'Updates'. Under 'Configure', there's a section for 'Cluster Hosts' with tabs for 'HOSTS' (which is selected) and 'NETWORK SEGMENTS'. Below this, it says 'Manage the VxRail cluster hosts. Add network segments before adding hosts to a L3 network.' There's a table with columns: Service Tag, PSNT, Model, Operation Status, ESXi Host Management IPv4, and Hostname. Three hosts are listed: V073001, V073002, and V073003. An 'ADD' button is visible above the table. The table shows the following data:

Service Tag	PSNT	Model	Operation Status	ESXi Host Management IPv4	Hostname
V073001	V0730010000000	VxRail E660N	Available	172.16.5.51	vcluster730-esx0
V073002	V0730020000000	VxRail E660N	Available	172.16.5.52	vcluster730-esx0
V073003	V0730030000000	VxRail E660N	Available	172.16.5.53	vcluster730-esx0

VxRail Cluster Hosts page

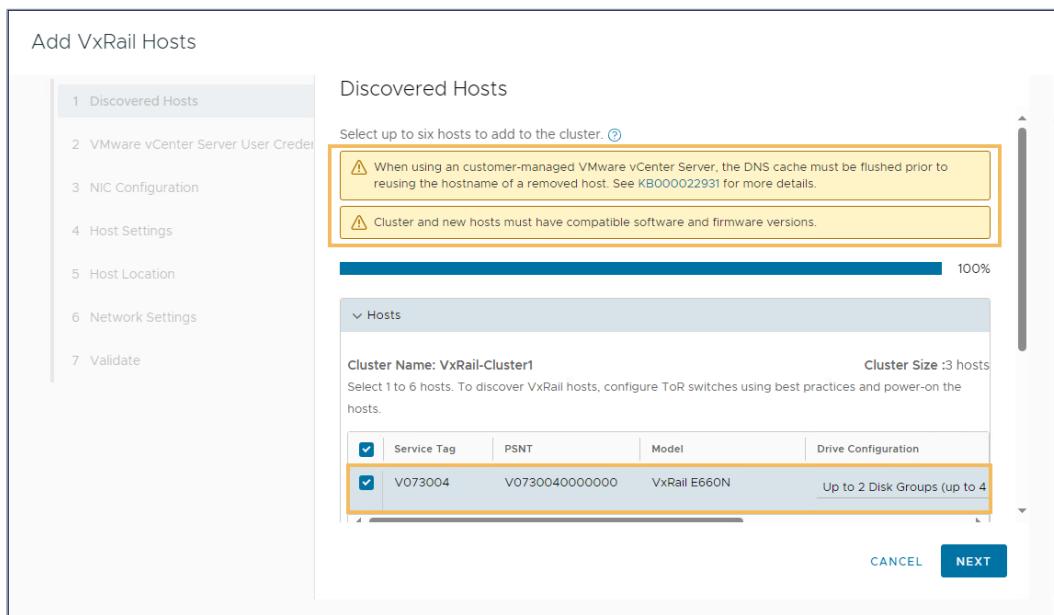
Add VxRail Hosts Wizard

Selecting **ADD** on the VxRail **Hosts** page launches the **Add VxRail Hosts** wizard. To learn how to use the **Add VxRail Hosts** wizard, select each tab:

Discovered Hosts

For VxRail clusters configured with automatic node discovery, the discovered nodes and compatibility status are listed. Relevant warnings are also shown. For VxRail clusters configured with manual node discovery, the hosts must be manually discovered.

Select the nodes that should be added to the cluster. In the example, one compatible node has been discovered. Click **NEXT**.



Add VxRail Hosts wizard-Discovered Hosts

VMware vCenter Server User Credentials

Provide the VMware vCenter user credentials. Click **NEXT**.

Perform VxRail Cluster Expansion

The screenshot shows the 'Add VxRail Hosts' wizard with the second step selected: 'VMware vCenter Server User Credentials'. A sidebar on the left lists steps 1 through 7. The main area contains fields for 'Username' (administrator@vsphere.local) and 'Password', both highlighted with an orange border. Buttons at the bottom include 'CANCEL', 'BACK', and 'NEXT'.

Add VxRail Hosts wizard-VMware vCenter Server User Credentials

NIC Configuration

Map the physical NICs to the uplinks on the VDS. The NIC to uplink mapping defaults to that of the first node in the VxRail cluster. Click **NEXT**.

The screenshot shows the 'Add VxRail Hosts' wizard with the third step selected: 'NIC Configuration'. The sidebar shows steps 1-7. The main area displays two tables. The top table, 'NIC Configuration', shows a single host entry with service tag V073004, model VxRail E660N, and 4 NDC. The bottom table, 'Select NICs and VMNICs', shows the same host details and lists two NIC entries. The second NIC entry, 'NDC Slot 1 Port 4 Intel(R) Ethernet 10G 4P X550 rNDC', is highlighted with an orange border. Buttons at the bottom include 'CANCEL', 'BACK', and 'NEXT'.

Add VxRail Hosts wizard-NIC Configuration

Perform VxRail Cluster Expansion

Host Settings

Provide the hostname, IP address, management username, management password, and root password. For VxRail implementations with an external DNS server, ensure that the forward and reverse Type A records have been added. Click **NEXT**.

The screenshot shows the 'Add VxRail Hosts' wizard with the 'Host Settings' step selected. On the left, a vertical navigation bar lists steps 1 through 7. Step 4, 'Host Settings', is highlighted with a green bar. The main panel displays host configuration settings:

- Host**
 - Service Tag: V073004
 - PSNT: V073004000000
 - ESXi Hostname *: vcluster730-esx04
 - Preview: vcluster730-esx04.delledu.lab
 - ESXi IPv4 address *: 172.16.5.54
 - ESXi Management Username *: esxmgmt
- Buttons**: CANCEL, BACK, NEXT

A callout box highlights the note: "Verify that new hostnames and IP addresses have been added to the DNS lookup records."

Add VxRail Hosts wizard-Host Settings

Host Location

Optionally provide the rack name and position. Click **NEXT**.

Perform VxRail Cluster Expansion

Add VxRail Hosts

Host Location

You have the option to provide host rack information.

Service Tag	PSNT	ESXi Hostname	ESXi IP Address	Rack Name	Rack Position
V073004	V0730040000000	vcluster730-esx04	172.16.5.54	Virtual Rac	4

CANCEL BACK NEXT

Add VxRail Hosts wizard-Host Location

Network Settings

Provide the vSAN and vMotion network information. Click **NEXT**.

Add VxRail Hosts

Network Settings

vSAN

ESXi Hostname	vcluster730-esx04
IPv4 address *	172.16.10.54
Gateway IPv4 address	
Subnet Mask	255.255.255.0
VLAN ID	10

vSphere vMotion

ESXi Hostname	vcluster730-esx04
IPv4 address *	172.16.20.54

CANCEL BACK NEXT

Add VxRail Hosts wizard Network Settings - vSAN and vMotion

Validate

Validate the input settings before adding the node to the cluster. The validation process is similar to the validation performed by the VxRail Deployment Wizard during the initial configuration. The validation process could be used to determine the readiness of the environment for node addition without adding the nodes.

To start the validation process, click **VALIDATE**.

The screenshot shows the 'Add VxRail Hosts' wizard in progress, specifically the 'Validate' step. On the left, a vertical sidebar lists steps from 1 to 7: 'Discovered Hosts', 'VMware vCenter Server User Credentials', 'NIC Configuration', 'Host Settings', 'Host Location', 'Network Settings', and 'Validate'. Step 7 is highlighted with a green bar. The main panel is titled 'Validate' and contains instructions: 'Review the information below and click VALIDATE to validate the host and network configuration.' Below this, a section titled 'Hosts' shows '1 hosts will be added.' A table provides detailed information for one host:

Service Tag	PSNT	Model	Hostname	ESXi IPv4 address	vSphere vMotion IPv4	vSAN IPv4
V073004	V073004000000	VxRail E660N	vcluster730-esx04.delledu.lab	172.16.5.54	172.16.20.54	172.16.10.54

At the bottom right of the main panel are three buttons: 'CANCEL', 'BACK', and a prominent blue 'VALIDATE' button.

Add VxRail Hosts wizard-Validate

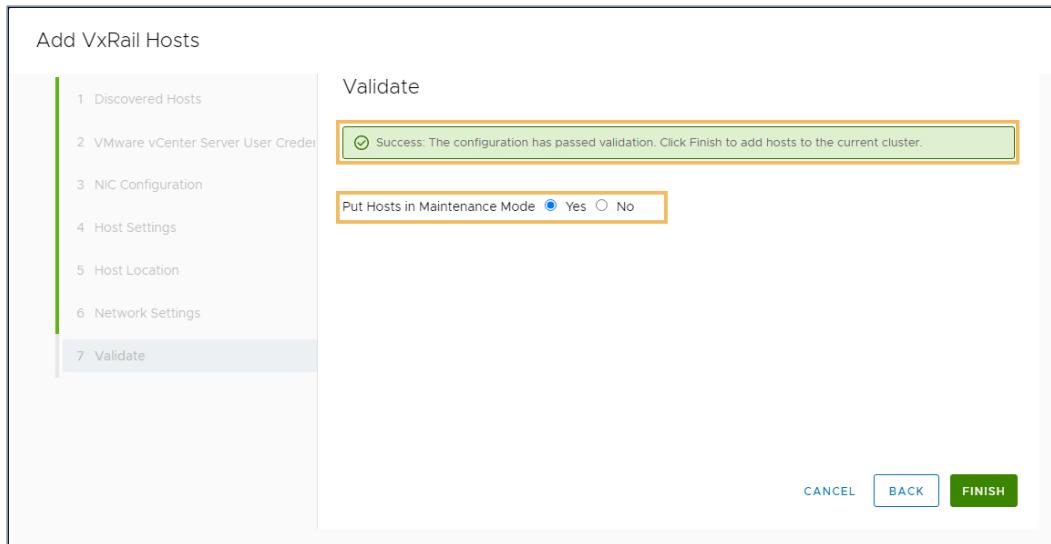
Finish

After a successful validation, add the node to the cluster.

The host can be left in Maintenance Mode after the node add process completes. The default setting is **Yes**.

To start the node add process, click **FINISH**.

Perform VxRail Cluster Expansion



Successful validation

Node Added Successfully

A node has been successfully added to the VxRail cluster. In this example, the node was left in maintenance mode.

The node resources are available to the cluster when the node is taken out of maintenance mode. Taking the node out of maintenance mode could lead to DRS or vSAN disk rebalance activities. Hence, take the node out of maintenance mode when the cluster activity is low.

Perform VxRail Cluster Expansion

The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and "Search in all environments". The top navigation bar includes "Actions", "Administrator@VSPHERE.LOCAL", and a help icon. The left sidebar shows a tree structure with "vcsa01.delledu.lab", "VxRail-DC", and "VxRail-Cluster1" selected. Under "VxRail-Cluster1", there are sub-items: "Datastores", "Desired State", "Image", "Configuration", "vSAN", "Services", "Disk Management", "Fault Domains", "Remote Datastores", "VxRail", "System", "Updates", "Backup", "Certificate", "Market", and "Hosts" (which is currently selected). The main content area is titled "Cluster Hosts" and shows a table of hosts. A message box at the top says "Added 1 host(s). Health monitoring is disabled during this task." It lists one host: "Hostname: vcluster730-esx04.delledu.lab, PSNT: V0730040000000, Status: Available, Actions: DISMISS". Below this is a warning message: "Hosts are in maintenance mode. Exit maintenance mode for each added host." A table below shows two hosts: "V073004" and "V073001". The "V073004" row has columns: Service Tag (V073004), PSNT (V0730040000000), Model (VxRail E660N), Operation Status (Available), ESXi Host Management (172.16.5.54), and Hostname (vcluster730-esx04.delledu.lab).

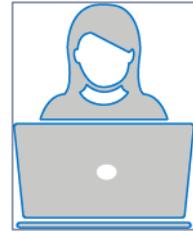
Node added successfully to the VxRail cluster

Lab 14: Add a node to a VxRail cluster

You are ready to add a VxRail node to a previously deployed VxRail cluster.

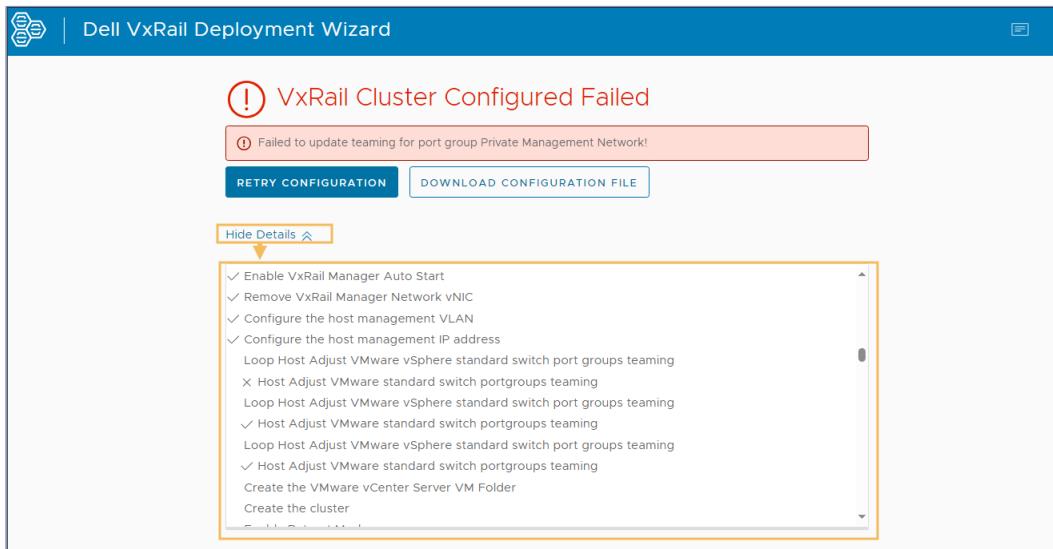
Lab Tasks

- Review the VxRail Compute Node Expansion procedure.
- Check the management VLAN ID and the Loudmouth service status on the new VxRail node.
- Add the new VxRail node to the VxRail Cluster.
- Confirm that the VxRail vSAN datastore is compatible with a RAID 5 vSAN storage policy.
- Set the RAID 5 vSAN storage policy as the default storage policy for the vSAN datastore.



Troubleshoot VxRail Implementations

VxRail Implementation Troubleshooting Overview



VxRail Deployment Wizard Configuration Failure

The VxRail Deployment Wizard displays the status, warnings, and errors for configuration tasks that are part of the implementation process.

Troubleshooting hints:

- Retry the installation to resolve issues that may be the result of a timeout during execution.
- Verify that the configuration wizard has the expected values after uploading a JSON file.
- Use the vSphere Client if vCenter is available, to determine the root cause and resolve issues.
- Use the VMware Host Client and iDRAC to determine the root cause and resolve issues.
- Reimage nodes if necessary with assistance from Dell Support.
 - Determine the root cause of the failure before reimaging.
 - Collect logs before reimaging.

VxRail Implementation Process Troubleshooting Example

This following scenario describes an example of troubleshooting a validation error during deployment. To learn more about this scenario, select each tab.

Review the Error

Review the error in the validation step of the VxRail Deployment Wizard.

The screenshot shows the Dell VxRail Deployment Wizard interface. The left sidebar lists 13 steps: Welcome, End User License Agreement, Cluster Type, Resources, Network Confirmation, Configuration Method, Global Settings (highlighted in red), VMware VDS Settings, VMware vCenter Server Settings, Host Settings, VxRail Manager Settings, Virtual Network Settings, and Validate Configuration. The main panel is titled 'Validate Configuration' and displays a 'Field Error' message: 'Unable to access the NTP service on the specified NTP server(s): 192.168.10.253.' Below the message are two buttons: 'DOWNLOAD CONFIGURATION FILE' and 'VALIDATE CONFIGURATION'.

VxRail Deployment Wizard Validation Error

Locate the Configuration Details

Notice that the **Global Settings** tab shows a red exclamation and that once clicked also shows which field has an issue. The image shows an NTP server access error.

Troubleshoot VxRail Implementations

The screenshot shows the 'Global Settings' page of the Dell VxRail Deployment Wizard. The left sidebar lists steps from 1 to 13, with '7 Global Settings' highlighted. The main area shows 'General' settings. Under 'DNS Server', 'External' is selected. Under 'NTP Server', '192.168.10.253' is entered, which is highlighted with a red box and has a tooltip: 'Unable to access the NTP service on the specified NTP server(s): 192.168.10.253.' Other fields include 'vCenter Server' (VxRail-managed VMware vCenter Server selected), 'vSphere HA Isolation Address' (No Isolation Address selected), and 'Logging' (No Logging selected). The top right corner indicates 'VxRail Cluster Type: Standard (3 hosts)'.

VxRail Deployment Wizard Global Settings Error

Perform Troubleshooting Steps

For the NTP server access error, perform the following troubleshooting steps:

- Review the **NTP Server(s)** field and confirm that the IP address originally entered is the correct IP.
- If the IP address is correct, ping the NTP Server to check availability.
- If the ping is successful, validate the NTP service is running on the machine.

Update the VxRail Deployment Wizard

- If a field in the Deployment Wizard needs an update, go to the appropriate page and manually correct the field that contains the incorrect value. Once the value is corrected, validate the cluster again.

Troubleshoot VxRail Implementations

Dell VxRail Deployment Wizard

Global Settings

VxRail Cluster Type: Standard (3 hosts)

General

Top Level Domain *

vCenter Server * VxRail-managed VMware vCenter Server Customer-managed VMware vCenter Server

DNS Server

DNS Server IPv4 Address(es) *

vSphere HA Isolation Address No Isolation Address Isolation Address

NTP Server No NTP Server NTP Server

NTP Server IPv4 address(es) or FQDN(s) Changed from 192.168.10.253

Logging No Logging Syslog Server

1 Welcome
2 End User License Agreement
3 Cluster Type
4 Resources
5 Network Confirmation
6 Configuration Method
7 Global Settings
8 VMware VDS Settings
9 VMware vCenter Server Settings
10 Host Settings
11 VxRail Manager Settings
12 Virtual Network Settings
13 Validate Configuration

VxRail Deployment Wizard Global Setting Corrected

- If required, save the changes to a new VxRail cluster configuration file.

```
{  
  "global": {  
    "cluster_type": "STANDARD",  
    "cluster_management_netmask": "255.255.255.0",  
    "cluster_management_gateway": "172.16.5.1",  
    "cluster_vsan_netmask": "255.255.255.0",  
    "cluster_vmotion_netmask": "255.255.255.0",  
    "ntp_servers": [  
      "192.168.1.253"  
    ],  
    "is_internal_dns": false,  
    "dns_servers": [  
      "192.168.1.2"  
    ],  
    "syslog_servers": [],  
    "top_level_domain": "delledu.lab",  
    "ha_isolation_addresses": []  
  },  
  "version": "8.0.100",  
  "storage": {  
    "disk_group_type": "1002"  
  },  
  "hosts": [  
    {  
      "hostname": "vcluster730-esx01",  
      "accounts": {  
        "root": {  
          "username": "root",  
          "password": "VxRail@R0cks"  
        }  
      }  
    }  
  ]  
}
```

Cluster Configuration File Setting Corrected

VxRail Log File Locations

For VxRail, operations are broken into categories. Day 1 operations are cluster initialization tasks. Day 2 operations are tasks that are performed after initialization, like expansion and upgrades.

Troubleshoot VxRail Implementations

The table lists VxRail Manager VM log files that are useful when troubleshooting both categories.

Log Files	Description	Location on the VxRail Manager VM
dayone.log	Consolidated first run (Day 1) configuration messages and information	/var/log/microservice_log
firstboot.log subboot.log	Native service not started, microservice not run correctly (Day 1)	/var/log
short.term.log long.term.log	Micro service information (Day 1 and 2)	/var/log/microservice_log
lcm-web.log lcm-migration.log lcm-do.log	VxRail upgrades information (Day 2)	/var/log/mystic
loudmouth.log	Node discovery information (Day 1 and 2)	/var/log/vmware/loudmouth

localhost_access_log.txt	HTTP request information (Day 1 and 2)	/var/log/vmware/marvin/tomcat/logs
marvin.log	Scale out and node replacement (Day 2) messages and information	/var/log/vmware/marvin/tomcat/logs



Tip: For more information about VxRail log file locations, see the [Dell EMC VxRail: List of useful commands and log files](#)

VxRail Manager Access

One method to view log files on the VxRail Manager VM, is to use an SSH client. When logging in, use the mystic account since root access is disabled for SSH. The IP address and password combination that is used during an SSH client session depends on the stage of the VxRail cluster installation:

- IP Address:
 - Unconfigured VxRail Manager VM = default (192.168.10.200)
 - Configured VxRail Manager VM = IP address defined during first run
- mystic Password:
 - Unconfigured VxRail Manager VM = default (VxRailManager@201602!)

Troubleshoot VxRail Implementations

- Configured VxRail Manager VM = mystic password defined during first run

If unable to use the SSH client, connect to VxRail Manager console. If the VxRail Manager VM was added to vCenter, use the vSphere client, otherwise use the VMware Host client on the primary VxRail node. Log in to the console for the VxRail Manager VM to view log files.

Log Files Error Example

The screenshot shows the 'Dell VxRail Deployment Wizard' interface. On the left, a vertical navigation bar lists steps: 1. Welcome, 2. End User License Agreement, 3. Cluster Type, 4. Resources, 5. Network Confirmation, and 6. Configuration Method. Step 3 is currently selected. To the right, under 'Validate Configuration', it says 'Validation may require several minutes or longer depending upon the size and type of cluster'. Below this, a 'Field Error' section is highlighted in pink, containing three error messages:

- ! Error while setting up the VLAN for validation.
- ! Network adapters ['vmnic1'] on host 1 cannot communicate with other hosts on VLAN 0.
- ! The PNIC vmnic1 is down in host V073001.

At the bottom, there are two buttons: 'DOWNLOAD CONFIGURATION FILE' and 'VALIDATE CONFIGURATION'.

VxRail Deployment Wizard Validation Error

In this example, the VxRail validation failed with a "vmnic1 is down" error. The error information that is shown is also in the VxRail Manager logs. Since the issue is with first run, start by examining dayone.log.

Example search commands:

- `cat /var/log/microservice_log/dayone.log | grep ERROR`

Using this general search criteria displays all errors, which can make it hard to find the correct error message in the [output](#).

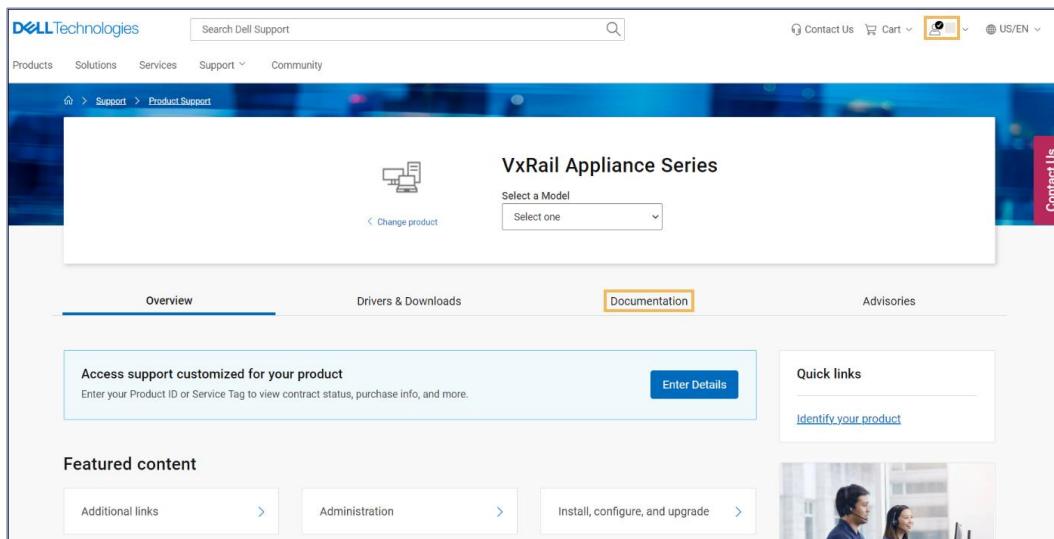
- `cat /var/log/microservice_log/dayone.log | grep "vmnic1 is down"`

Using more exact search criteria displays a more helpful [output](#).

VxRail Knowledge Base (KB) Articles

Links to KB articles that supplement the VxRail ecosystem can be found in SolVe procedures, VxRail Manager, and the Dell Support site. The **Documentation** tab on the VxRail Support page displays KB articles that are related to VxRail Manager.

To access VxRail related KB articles from the Dell Support site, go to the [VxRail Support page](#). After a successful login, the VxRail Support page appears.



VxRail Support page

Select **Documentation** on the VxRail Support page. Select **KNOWLEDGE BASE ARTICLES** from the left panel, or scroll down the page to view the **Knowledgebase Articles** section and select **See All**.

Troubleshoot VxRail Implementations

The screenshot shows a section titled "Knowledgebase Articles" under the "KNOWLEDGE BASE ARTICLES" category. A sub-section header "TOP SOLUTIONS" is visible above the main content area. The main content area displays a list of articles related to VxRail troubleshooting:

- VxRail: Node health-check fails for test 'gpuhw' [View Page](#)
- VxRail: VxRM health-check fails for test 'vc_pw_char' [View Page](#)
- VCF on VxRail: VxRM health-check fails for test 'sd_tinyvc' [View Page](#)
- RPS (Remote Proactive Services) Average Activity Lengths & Lead Times [View Page](#)
- Security Configuration Guides: How to deploy and use Dell EMC products securely [View Page](#)
- VxRail: Information on VMSA-2022-0004 and VxRail environments [View Page](#)
- Dell EMC VxRail: VxRM health-check fails for test 'snoop_dvs' [View Page](#)
- Dell VxRail: Security Technical Implementation Guide on VxRail [View Page](#)

A "See All" button is located in the top right corner of the article list.

Knowledge Base Article list

Searching a Knowledge Base (KB)

To access a KB from the Dell Support site, use the search box at the top of the page or select the **Documentation** tab to get a search box. In the search box, type the error message or the Article ID and press enter, and then select the KB.

Example: VxRail cluster deployment fails with the message "failed to add host into cluster."

Troubleshoot VxRail Implementations

The screenshot shows the Dell Technologies Support website interface. At the top, there's a navigation bar with links for Products, Solutions, Services, and Support. A search bar at the top right contains the query "VxRail failed to add hosts into cluster". Below the search bar, a secondary search bar also displays the same query. To the left, there's a sidebar titled "Resources" with categories like Downloads & Drivers, Forums, Knowledgebase, Manuals & Documents, Dell Support by Topic, and Support Videos. Another sidebar titled "Product Category Selector" lists categories such as Converged Infrastructure, Data Center Infrastructure, Data Protection, Desktops & All-in-Ones, and Electronics & Accessories. The main content area shows search filters (Language: English) and results. The first result is a knowledge base article titled "Dell EMC VxRail: VxRail cluster deployment fails with message 'failed to add host into cluster'". The article includes steps for generating a CSR and replacing existing certificates, along with a link to the full article.

Knowledge Base Article search

VxRail Log Collection

On a VxRail system, logging is enabled on multiple layers of the Dell and VMware software stack. The VxRail Plugin provides a simple process to collect and download all the required log bundles. CLI scripts for log collection are available on the VxRail Manager. The VxRail API provides ways to automate and schedule the process of generating and downloading the log bundles.

The [Dell VxRail 8.0.x Administration Guide](#) details the log bundle collection steps with the VxRail Plugin and with the VxRail Manager VM CLI scripts.

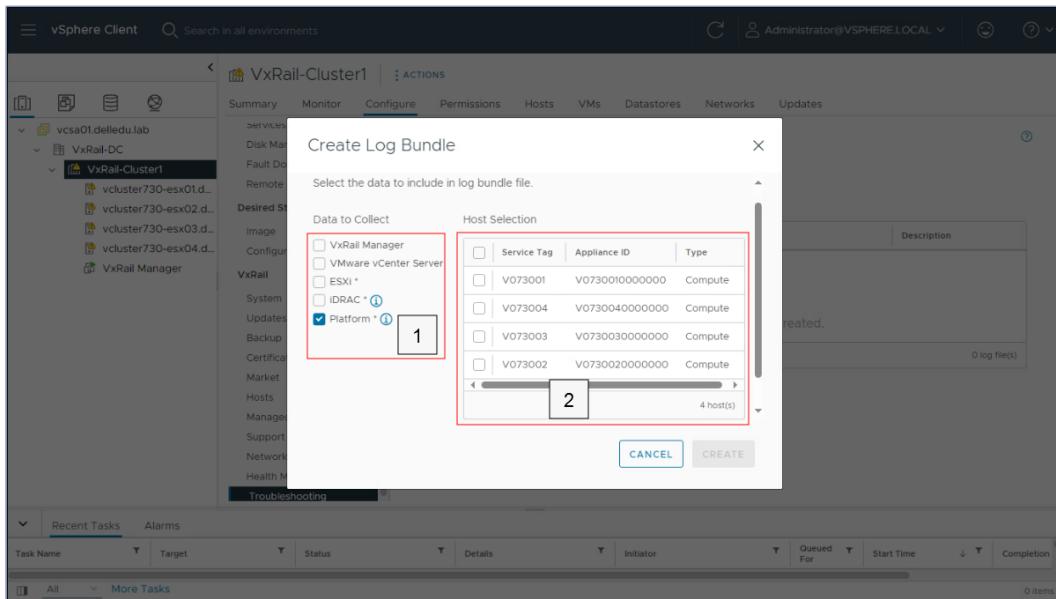
VxRail Plugin Create Log Bundle

To access the **Log Collection** page in the vSphere client, select the VxRail cluster **Configure** tab, and then select **VxRail > Troubleshooting**. Selecting **CREATE** opens the **Create Log Bundle** dialog box as shown in the graphic.

Troubleshoot VxRail Implementations

To learn more about creating a log bundle, select the two red hotspots.

Create a Platform Log Bundle for a host using the vSphere Client



1: The Data to Collect section is used to select the required log bundles: VxRail Manager, vCenter, ESXi, iDRAC, and Platform.

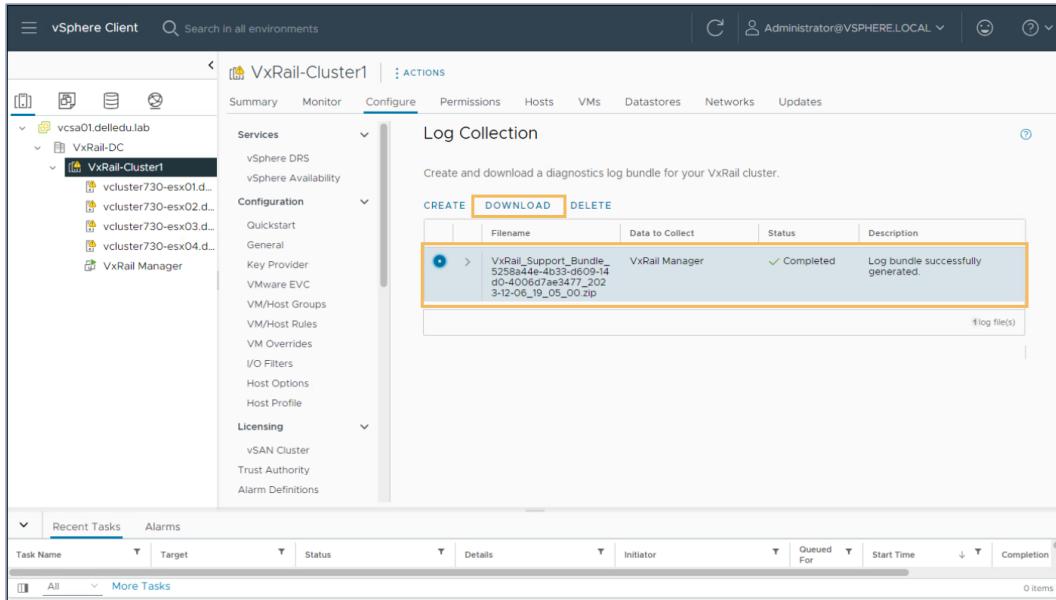
For 2-Node VxRail clusters, the Witness log bundle can also be collected.

2: The Host Selection section becomes visible and required when ESXi, iDRAC, or Platform are selected.

VxRail Plugin Download Log Bundle

When the log bundle generation process is complete, the log bundle is available to download. To download the log bundle, select the bundle and click **DOWNLOAD**. The log bundle can be sent to the Dell support team for troubleshooting and diagnosis.

Troubleshoot VxRail Implementations



The screenshot shows the vSphere Client interface with the navigation bar at the top. The main pane displays the 'Log Collection' section for 'VxRail-Cluster1'. A table lists a single log bundle entry:

Filename	Data to Collect	Status	Description
VxRail Support Bundle 5258a44e-4b33-d609-14 d0-4006d7ae3477_202 3-12-06_19_05_00.zip	VxRail Manager	Completed	Log bundle successfully generated.

Below the table, there is a note: 'Create and download a diagnostics log bundle for your VxRail cluster.' The 'DOWNLOAD' button is highlighted in orange. At the bottom of the screen, a task bar shows 'Recent Tasks' and 'Alarms'.

Log bundle generated successfully and available for download

VxRail Manager VM - Log Collection CLI

If the vCenter UI is unavailable, logs can also be collected using the command line. VxRail provides scripts on the VxRail Manager VM for log collection. To run the log collection scripts, open a console or a secure shell (SSH) session to the VxRail Manager VM and login with `mystic` and `root` password. The scripts can be found in the `/mystic` folder.

The `generateLogBundle.py` script is used to collect the log bundles for specific components by using the following options:

- VxRail Manager: `-v, --vxm`
- vCenter Server: `-c, --vcenter`
- Node-specific bundles - use the `--nodes` option to pick specific nodes
 - ESXi: `-e, --esxi`
 - iDRAC: `-i, --idrac`
 - Platform: `-p --platform`

Troubleshoot VxRail Implementations

```
mystic@vxrail-manager:/mystic> [python generateLogBundle.py] -h
usage: generateLogBundle.py [-h] [-r REQUEST_ID] [-t TYPES]
                            [-n NODES] [-v] [-c] [-e] [-i] [-p] [-w]

Collect log bundles via VxRailManager.

optional arguments:
  -h, --help            show this help message and exit
  -r REQUEST_ID, --request-id REQUEST_ID
                        use request id to resume a request looping if the
                        script is interrupted.
  --types TYPES         types of generated log bundle.
  --nodes NODES         nodes of generated log bundle.
  -v, --vnxm             generate vnx log bundle.
  -c, --vcenter          generate vcenter log bundle.
  -e, --esxi              generate esxi log bundle.
  -i, --idrac              generate idrac log bundle.
  -p, --platform           generate platform log bundle.
  -w, --witness            generate witness host log bundle.

mystic@vxrail-manager:/mystic> _
```

Script for collecting VxRail logs - Syntax.

The **generateFullBundle** script collects log bundles for all components on all nodes; it does not collect the witness log bundle. See the 8.0.XXX Admin guide to collect the witness log bundle.

The generated log bundles are located under `/tmp/mystic/dc`.

VxRail APIs for Gathering Logs

The scripts would use the API or make API calls to generate and download the required logs. Custom scripts and applications can be automated with the VxRail API to automatically generate and download the required logs. The VxRail API base URL is: <https://<VxRail Manager IP Address or FQDN>/rest/vxm/>.

The table lists the relevant VxRail APIs for gathering and downloading logs.

Task	Example Endpoint Path	Body	Method	Successful Response
------	-----------------------	------	--------	---------------------

Troubleshoot VxRail Implementations

Request to generate a new log bundle	/v1/support/logs	Types - <code>vxm</code> , <code>vcenter</code> , <code>esxi</code> , <code>iDrac</code> Nodes - List of serial numbers Autoclean - true/false	POST	202 Accepted with Request ID
Monitor request	/v1/requests/<Request ID>		GET	State of request – Monitor until complete. Completed state returns Log ID, name, and location of log bundle.
Detailed information about log bundle	/v1/support/logs/<Log ID>		GET	Detail log bundle information - Log ID, location, name, size....
Download log bundle	/v1/support/logs/<Log ID>/download		GET	Binary stream of log bundle

Troubleshoot VxRail Implementations

VxRail PowerShell cmdlets make the VxRail API accessible using a scripting interface that is familiar to PowerCLI users. The VxRail API PowerShell Modules complement VMware PowerCLI.

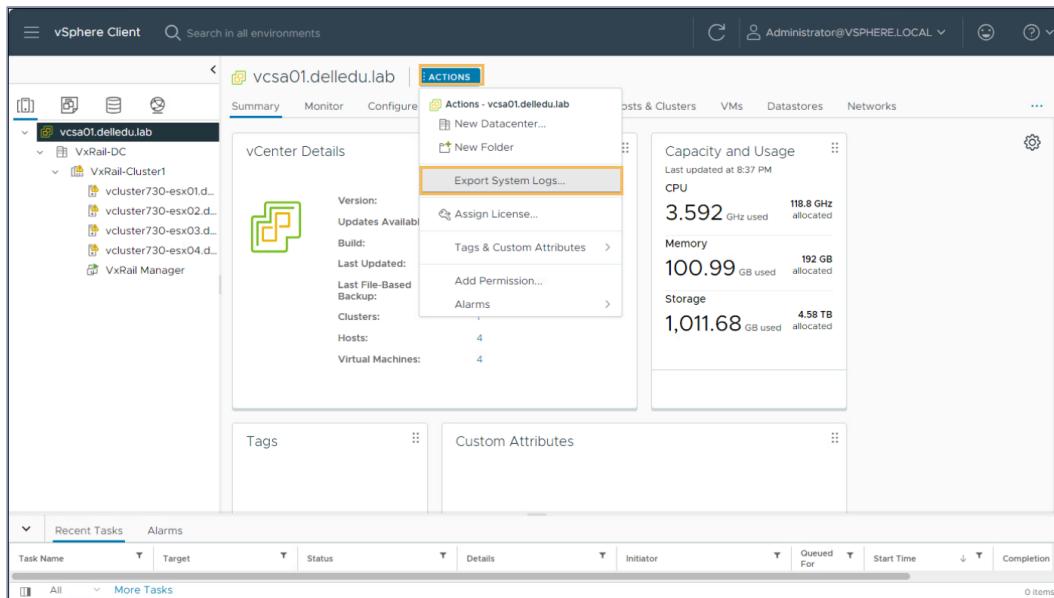
vCenter Server, ESXi, and vSAN Support Bundles

Dell Support or VMware Support may request diagnostic information that is related to the vCenter Server or the ESXi nodes. The vSphere Client can be used to export the system logs for the ESXi hosts, vCenter Server, and vSphere Client. Performance data from the ESXi nodes can be optionally included.

The vSAN support logs are contained in a normal ESXi support bundle in the form of vSAN traces. As vSAN is distributed across multiple ESXi hosts, it is best practice to gather the ESXi support logs for all hosts that are configured for vSAN.

vCenter Server Support Bundle

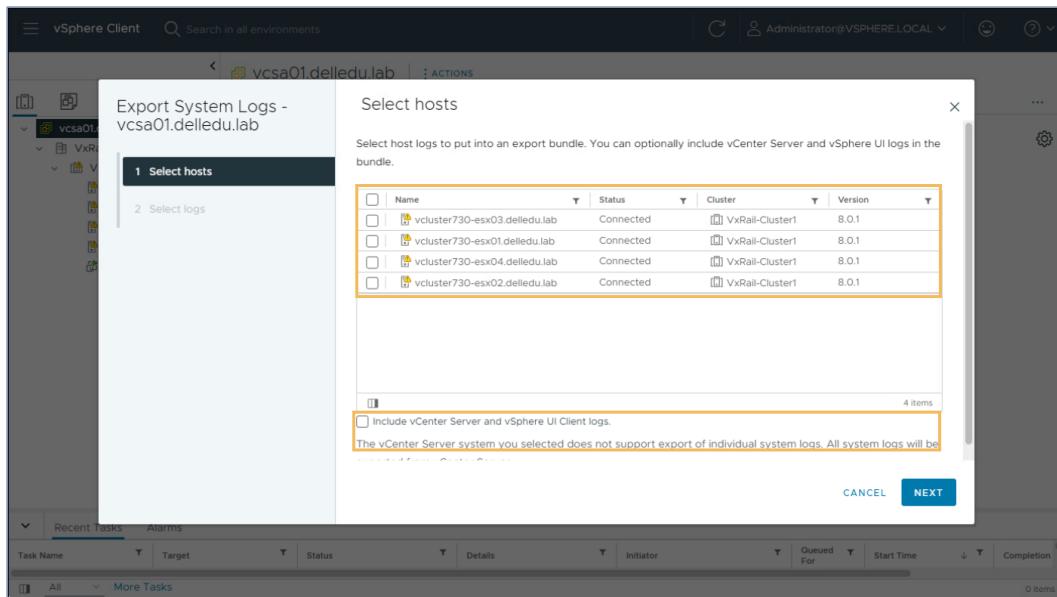
To export system logs from the vSphere Client, click the **ACTIONS** button and then select **Export System Logs**.



Export vCenter logs using the actions menu in the vSphere client

vSphere Client Export System Logs

In the **Export System Logs** dialog, select the relevant ESXi hosts. Optionally, select the **Include vCenter Server and vSphere UI Client logs**.

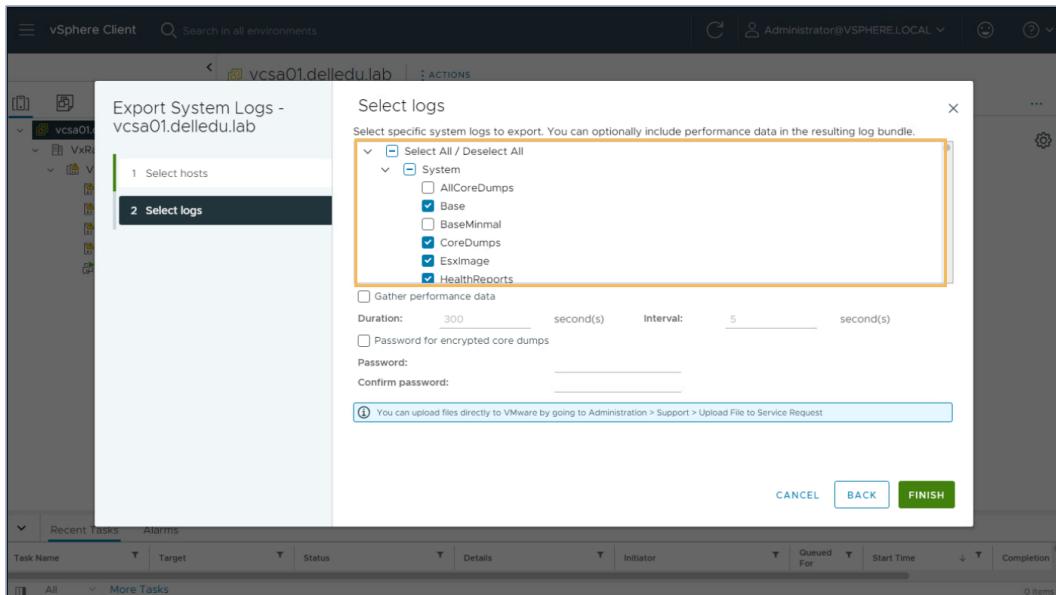


Export System logs Wizard using the actions menu in the vSphere client - Select hosts

vSphere Client Select System Logs

In the **Select logs** page, select the specific system logs and optionally include performance data in the log bundle. Typically, the support representative specifies the logs that are required.

Troubleshoot VxRail Implementations



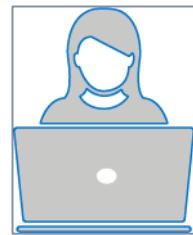
Export System Logs Wizard using the actions menu in the vSphere client - Select logs

Lab 15: Perform Log Collection

You have completed the deployment of the VxRail cluster and must collect logs for troubleshooting the VxRail Manager.

Lab Tasks

- Collect logs with the VxRail Plugin.
- Collect logs with the vSphere Client.



vSAN Troubleshooting

vSAN troubleshooting is typically performed using one or more of the following resources:

- vSphere Client
 - All Issues View
 - vSAN Skyline Health
 - vSAN Proactive Tests
- **`esxcli vsan`** commands

Troubleshoot VxRail Implementations

- Documentation
 - vSAN Monitoring and Troubleshooting
 - Dell VxRail Event Code Reference
- Dell and VMware knowledge base
 - Dell Support - VxRail Knowledge Base
 - VMware Knowledge Base

VxRail Cluster - All Issues

The **All Issues** view shows all triggered alarms relevant to the cluster. vSAN alarms start with vSAN, and VxRail related alarms have VXR in the event code.

The screenshot shows the 'All Issues' view in the VxRail interface. The left sidebar has sections for 'Issues and Alarms' (with 'All Issues' selected), 'Triggered Alarms' (Performance, Overview, Advanced), 'Tasks and Events' (Tasks, Events), and 'Namespaces' (Overview, Kubernetes events). The main area displays a table of issues:

Issue	Type	Trigger Time	Status
esx-269-vxrail4.vsb.edu: Host connection and po...	Triggered Alarm	06/13/2022, 01:07 PM	Alert
vSAN network alarm 'Hosts disconnected from V...	Triggered Alarm	06/13/2022, 01:07 PM	Alert
vSAN data alarm 'vSAN object'	Triggered Alarm	06/13/2022, 01:07 PM	Alert
esx-269-vxrail4.vsb.edu: Network uplink redund...	Triggered Alarm	06/13/2022, 01:05 PM	Alert
vSAN performance service alarm 'Stats DB object'	Triggered Alarm	06/13/2022, 01:07 PM	Alert
vSphere HA failover in progress	Triggered Alarm	06/13/2022, 01:06 PM	Warning
esx-269-vxrail4.vsb.edu: vsphere HA host status	Triggered Alarm	06/13/2022, 01:05 PM	Alert
vSphere HA failover operation in progress in clu...	Configuration Issue	06/13/2022, 01:07 PM	Alert

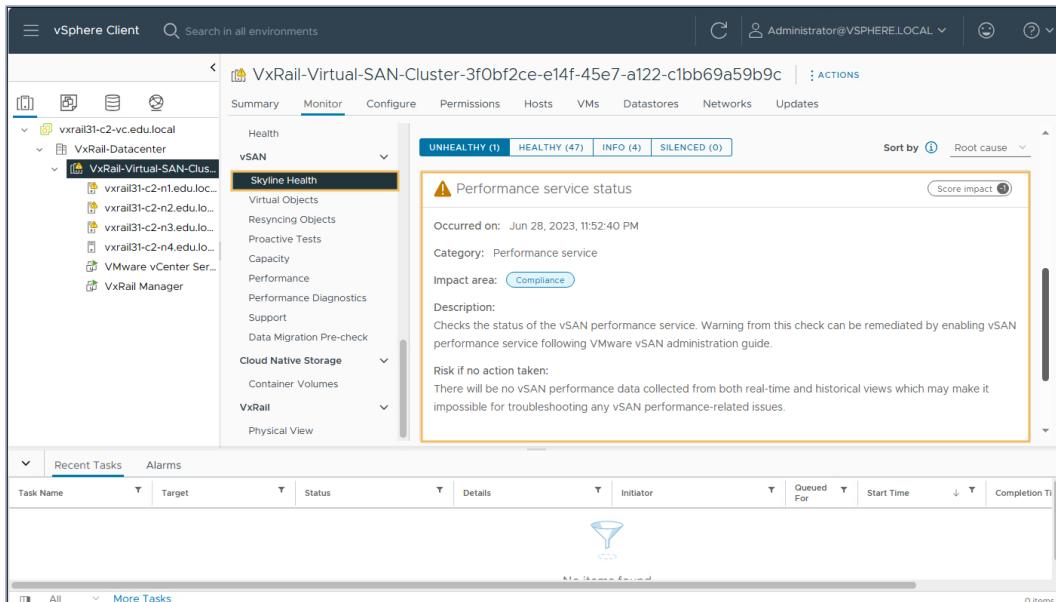
A callout box points to the first three items in the list, with the text: 'vSAN health alarms described in detail in the vSAN Skyline Health view'.

Triggered alarms example shown in All Issues

Investigate vSAN Alarms in Skyline Health

Skyline Health can be used to monitor the health of the system. You can run health checks and send the data to Dell Technologies and VMware for advanced analysis.

Troubleshoot VxRail Implementations



The screenshot shows the vSphere Client interface with the 'vSphere Client' header and a search bar. The left sidebar shows a tree view of environments, including 'vxrail31-c2-vc.edu.local' and 'VxRail-Datcenter'. The main pane is titled 'VxRail-Virtual-SAN-Cluster-3f0bf2ce-e14f-45e7-a122-c1bb69a59b9c'. The 'Health' section is selected, and the 'vSAN' sub-section is expanded. The 'Skyline Health' tab is active, displaying an 'UNHEALTHY (1)' status. A single alarm is listed: 'Performance service status' (Category: Performance service, Impact area: Compliance). The description states: 'Checks the status of the vSAN performance service. Warning from this check can be remediated by enabling vSAN performance service following VMware vSAN administration guide.' The 'Recent Tasks' tab is also visible at the bottom.

Performance service status error reported in Skyline Health

Investigate VXR Event Codes

VXR event codes are documented in the VxRail Event Code Reference and in the **Alarm Definitions** within vCenter Server.

To learn about VXR event codes and alarm definitions select each tab.

VxRail Event Code Reference Example

The VxRail Event Code Reference lists all the VXR alarms, severity level, message, added in version, and a link to the applicable Dell KB article.

This example from the [VxRail Event Code Reference](#) shows the information for the VXR014020 event. A Dell Support account is required to access the VxRail Event Code Reference document.

VXR014020 MYSTIC014020	Error	Network uplink redundancy lost: Failure of the network cable, disconnect of cable, failure of the physical network card, failure of network switch/port/etc. Lost uplink redundancy on DVPort(s). Physical NIC is down. Lost uplink redundancy on a virtual switch. Physical NIC is down.	4.5.000 4.7.000 7.0.000	198269
---------------------------	-------	---	-------------------------------	--------

VxRail event code and reference example

VXR Alarm Definition in vCenter Server Example

VXR Alarm Definitions are shown on the **Alarm Definitions** page for all triggered VXR Alarms. To view VXR alarm definitions, filter the Alarm Name column by VXR or vxr as the filter is case insensitive.

The example shows the information for the VXR508NIC100 alarm.

Alarm Name	Object type	Defined In	Enabled
VXR508NIC100 ALARM NIC port down	Host	vxrail31-c2-vc.local	Enabled

Filtered VXR Alarm Definitions example

vSAN Proactive Tests

vSAN includes two proactive tests to validate the cluster: the **VM Creation Test** and the **Network Performance Test**. The vSAN proactive tests are available under the **Monitor** tab of the VxRail cluster. To learn about vSAN Proactive Tests select each tab.

VM Creation Test

The **VM Creation Test** creates a VM on every host and then deletes it. If the creation and deletion tasks succeed, it can be concluded that many aspects of vSAN are operational. This active test only takes a few seconds to run. The test can find issues that cannot be found with passive

Troubleshoot VxRail Implementations

tests such as node isolation, cluster segmentation, and other configuration issues.

Go to the **Monitor** tab of the VxRail cluster. Select **Proactive Tests**. Select **VM Creation Test**. Click **RUN TEST**.

The screenshot shows the vSphere Client interface with the 'Monitor' tab selected for a VxRail cluster named 'VxRail-Virtual-SAN-Cluster-3f0bf2ce-e14f-45e7-a122-c1bb69a59b9c'. In the 'Proactive Tests' section, 'VM Creation Test' is selected. A large blue button labeled 'RUN TEST' is prominent. Below the test section, a table titled 'Recent Tasks' displays several completed tasks related to vSAN configuration. At the bottom of the screen, a footer bar includes links for 'ESCPXD05510 ~ VxRail 8.0.XXX Implementation-SSP', 'Copyright 2024 Dell Inc', and 'Page 193'.

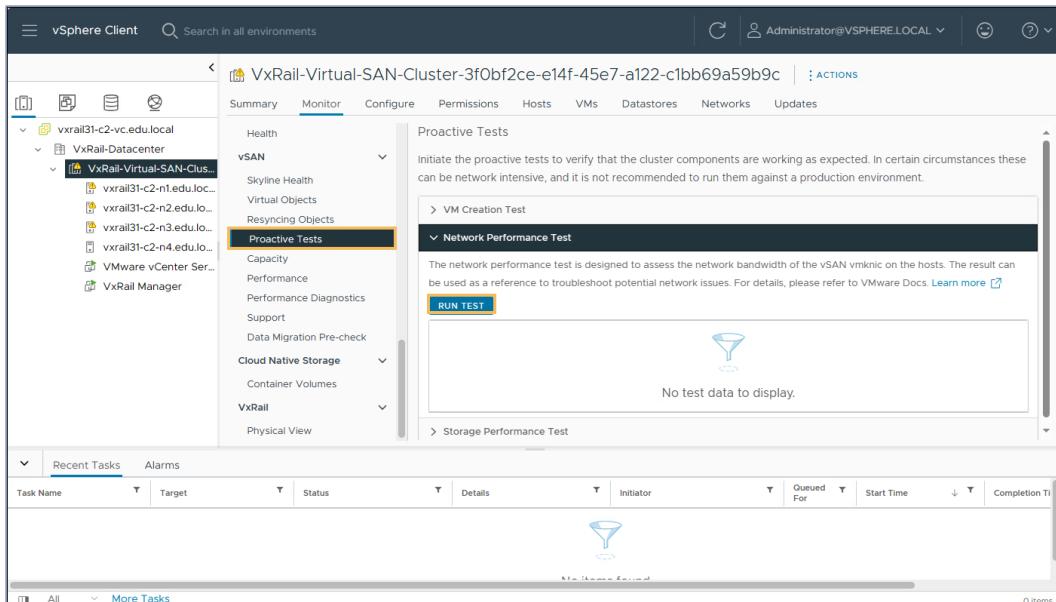
Virtual machine creation test example

Network Performance Test

The **Network Performance Test** is designed to assess the network connectivity and bandwidth of the hosts. The test is performed in a ring structure; every host sends packets to its next host while receiving from the previous host. The test examines the network bandwidth that can be achieved between hosts and reports warnings if the bandwidth is less than 850 Mbps. Low network bandwidth can negatively impact vSAN performance.

Go to the **Monitor** tab of the VxRail cluster. Select **Proactive Tests**. Select **Network Performance Test**.

Troubleshoot VxRail Implementations



The screenshot shows the vSphere Client interface with the 'Monitor' tab selected. On the left, the navigation tree shows a VxRail cluster named 'VxRail-Virtual-SAN-Cluster-3f0bf2ce-e14f-45e7-a122-c1bb69a59b9c'. Under the 'Health' category, the 'Proactive Tests' option is highlighted. Within 'Proactive Tests', the 'Network Performance Test' is selected, and a 'RUN TEST' button is visible. Below the test section, a message states 'No test data to display.'

Network performance test example

Investigate vSAN Health Using CLI

ESXCLI commands can be used to troubleshoot vSAN issues. The commands are documented in the VMware [vSAN Monitoring and Troubleshooting](#) guide.

To learn more about investigating vSAN health using the CLI select each tab.

Overall vSAN Health

Example - the ESXi shell has been enabled and the following command has been issued: **`esxcli vsan health cluster list`**

Troubleshoot VxRail Implementations

```
Most tools can prompt for secrets or accept them from standard input.  
VMware offers powerful and supported automation tools. Please  
see https://developer.vmware.com for details.  
  
The ESXi Shell can be disabled by an administrative user. See the  
vSphere Security documentation for more information.  
[root@vxrail31-c2-n1:~] esxcli vsan health cluster list  
Health Test Name          Status  
  
Overall health findings    yellow (vSAN performance service issue)  
Performance service        yellow  
  Performance service status yellow  
  
Network  
  Hosts with connectivity issues green  
  vSAN cluster partition      green  
  All hosts have a vSAN vmknic configured green  
  vSAN: Basic (unicast) connectivity check green  
  vSAN: MTU check (ping with large packet size) green  
  vMotion: Basic (unicast) connectivity check green  
  vMotion: MTU check (ping with large packet size) green  
  Network latency check     green  
  
Physical disk  
  Operation health          green  
    Congestion               green  
    Component limit health   green  
    Component metadata health green  
    Memory pools (heaps)     green  
    Memory pools (slabs)     green  
    Disk capacity             green
```

Overall vSAN Health - status yellow

Cluster Partition Health

Example - Status of cluster partition health test - **esxcli vsan health cluster get -t clusterpartition**

```
[root@vxrail31-c2-n1:~] esxcli vsan health cluster get -t clusterpartition  
vSAN cluster partition      green  
  
Checks if the vSAN cluster is partitioned due to a network issue.  
Ask VMware: http://www.vmware.com/esx/support/askvmware/index.php?eventtype=com.vmware.vsan.health.test.clusterpartition  
  
Partition list  
Host      Partition      Host UUID  
172.16.40.84    1            64513e12-0d54-18d3-ae89-e43d1ad99790  
172.16.40.83    1            6451430a-ad45-dc3b-421c-e43d1ad9d3e0  
172.16.40.81    1            64518378-7da2-402f-70ab-e43d1ad9ae30  
172.16.40.82    1            64518379-7f0f-e58b-7ced-e43d1ad9ac00  
  
[root@vxrail31-c2-n1:~]
```

Cluster partition health - status green

vSAN Object Health

Example - Status of the health of vSAN objects - **esxcli vsan debug object health summary get**

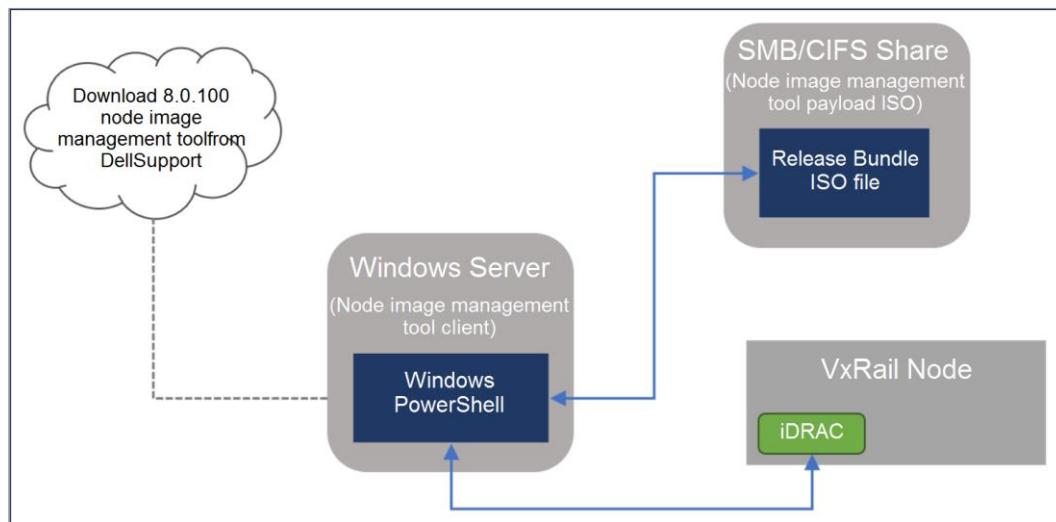
Troubleshoot VxRail Implementations

```
[root@vxrail31-c2-n1:~] esxcli vsan debug object health summary get
Health Status          Number Of Objects
-----
remoteAccessible          0
inaccessible              0
reduced-availability-with-no-rebuild 0
reduced-availability-with-no-rebuild-delay-timer 0
reducedAvailabilityWithPolicyPending 0
reducedAvailabilityWithPolicyPendingFailed 0
reduced-availability-with-active-rebuild 0
reducedAvailabilityWithPausedRebuild 0
data-move                 0
nonavailability-related-reconfig 0
nonavailabilityRelatedInComplianceWithPolicyPending 0
nonavailabilityRelatedInComplianceWithPolicyPendingFailed 0
nonavailability-related-incompliance 0
nonavailabilityRelatedInComplianceWithPausedRebuild 0
healthy                  32
[root@vxrail31-c2-n1:~]
```

vSAN Object Health - Healthy

Node Image Management Tool Overview

The VxRail node image management tool provides a convenient way to facilitate the node imaging process. The tool includes the deployment of firmware, drivers, operating systems, and appliance software.



Node Image Management Tool Workflow

The node image management tool consists of two parts:

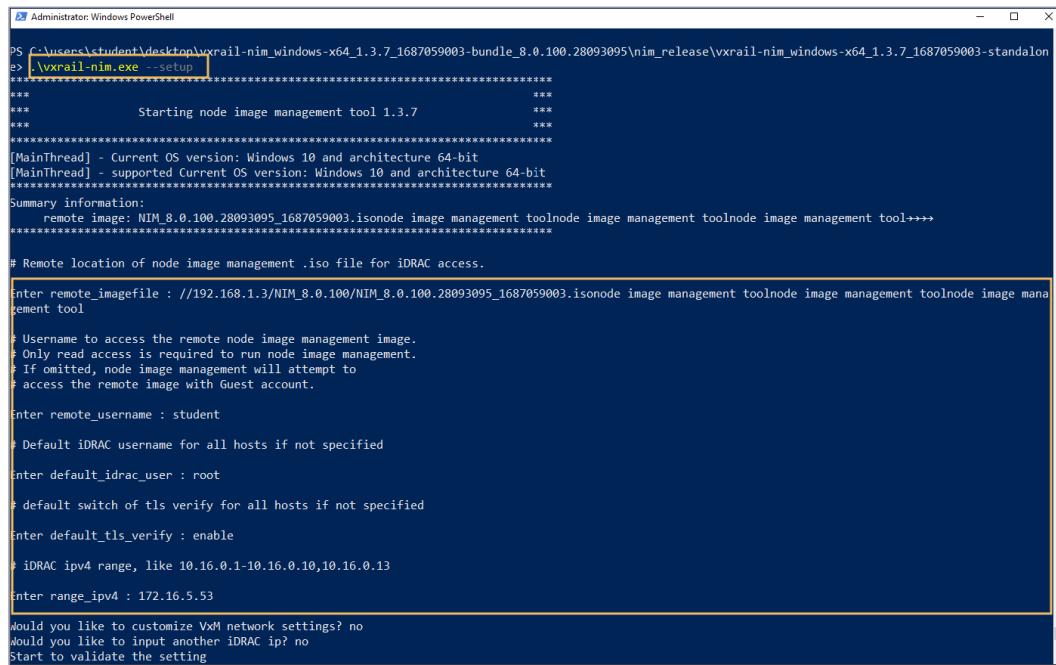
Node image management tool client: An executable CLI tool to enable the user to image VxRail nodes. The tool, with a few parameters, builds connections to the iDRAC on the target VxRail nodes, and consumes the node image management tool payload ISO.

Node image management tool payload ISO: A bootable image that consists of all the necessary payload. The node Image management tool client and iDRAC access the ISO image using the SMB or CIFS file sharing service.

High-Level Steps for Node Image Management Tool

Download the Solve Procedure for the node image management tool. See an example of a Solve Procedure for a VxRail P670F.

The following high-level steps are performed on the Windows operating system.



```
Administrator: Windows PowerShell
PS C:\users\student\Desktop\vxrail-nim_windows-x64_1.3.7_1687059003-bundle_8.0.100.28093095\nim_release\vxrail-nim_windows-x64_1.3.7_1687059003-standalone> [vxrail-nim.exe --setup]
*****
*** Starting node image management tool 1.3.7 ***
*****
[MainThread] - Current OS version: Windows 10 and architecture 64-bit
[MainThread] - supported Current OS version: Windows 10 and architecture 64-bit
*****
***** Summary information: *****

remote Image: NIM 8.0.100.28093095_1687059003.iso node image management tool node image management tool node image management tool +++
***** # Remote location of node image management .iso file for iDRAC access.

Enter remote_imagefile : //192.168.1.3/NIM_8.0.100/NIM_8.0.100.28093095_1687059003.iso node image management tool node image management tool node image management tool

# Username to access the remote node image management image.
# Only read access is required to run node image management.
# If omitted, node image management will attempt to
# access the remote image with Guest account.

Enter remote_username : student

# Default iDRAC username for all hosts if not specified

Enter default_idrac_user : root

# default switch of tls verify for all hosts if not specified

Enter default_tls_verify : enable

# iDRAC ipv4 range, like 10.16.0.1-10.16.0.10,10.16.0.13

Enter range_ipv4 : 172.16.5.53

Would you like to customize VxM network settings? no
Would you like to input another iDRAC ip? no
Start to validate the setting
```

Performing a reimaging of a node with the node image management tool

- Log in to Dell support and download the node image management tool.
- Extract the downloaded file.
- Start a PowerShell session with administrator privileges.
- In PowerShell, browse to the extracted file and run the file by typing the command **vxrail-nim.exe --setup**.
- Enter the credential for accessing the node image ISO file.

Troubleshoot VxRail Implementations

- Enter the VxRail network details.
- To begin the reimage process, type the following command: ***vxrail-nim.exe --all***.

You Have Completed This Content

Click the **Save Progress & Exit** button in the course menu or below to record this content as complete.

Go to the next learning or assessment, if applicable.

Appendix

Port Type Set to Edge

This example shows an excerpt of the ***show running-configuration spanning-tree*** command from a Dell switch. The VxRail node ports are set to edge.

```
DTE5-VxRail-ToR# show running-configuration spanning-tree
!
!
interface ethernet1/1/1
  spanning-tree port type edge
!
interface ethernet1/1/2
  spanning-tree port type edge
!
interface ethernet1/1/3
  spanning-tree port type edge
!
interface ethernet1/1/4
  spanning-tree port type edge
!
interface ethernet1/1/5
  spanning-tree port type edge
!
interface ethernet1/1/6
  spanning-tree port type edge
!
interface ethernet1/1/7
  spanning-tree port type edge
!
interface ethernet1/1/8
  spanning-tree port type edge
!
```

Dell switch - VxRail node ports set to edge

VxRail Configuration Report

Appendix

Example of a VxRail Configuration Report

VxRail Configuration JSON - Existing VDS Details

```

"network": {
    "nic_profile": "ADVANCED_CUSTOMER_SUPPLIED_VDS",
    "vds": [
        {
            "name": "VxRail-myVDS", VDS name
            "nic_mappings": [
                {
                    "uplinks": [ Uplink names and physical NICs
                        {
                            "name": "Uplink 1",
                            "physical_nic": "vmnic0"
                        },
                        {
                            "name": "Uplink 2",
                            "physical_nic": "vmnic1"
                        },
                        {
                            "name": "Uplink 3",
                            "physical_nic": "vmnic2"
                        },
                        {
                            "name": "Uplink 4",
                            "physical_nic": "vmnic3"
                        }
                    ]
                }
            ],
            "portgroups": [ Port group names, types, VLAN IDs, and MTU
                {
                    "name": "VxRailDiscovery",
                    "type": "VXRAILDISCOVERY",
                    "vlan_id": 3939,
                    "vmk_mtu": 1500
                },
                {
                    "name": "VxRailSystemVMs",
                    "type": "VXRAILSYSTEMVM",
                    "vlan_id": 0
                },
                {
                    "name": "ExternalManagement",
                    "type": "MANAGEMENT",
                    "vlan_id": 0,
                    "vmk_mtu": 1500
                },
                {
                    "name": "vSAN",
                    "type": "VSAN",
                    "vlan_id": 20,
                    "vmk_mtu": 1500
                },
                {
                    "name": "vMotion",
                    "type": "VMOTION",
                    "vlan_id": 10,
                    "vmk_mtu": 1500
                }
            ]
        }
    ]
}

```

Software Licensing Options for VxRail

The purchase of the VxRail hardware includes the following software licenses:

- VMware vCenter Server - for clusters with the VxRail-managed vCenter Server⁵
- VMware vSphere and VMware vSAN - 60-day evaluation licenses
- RecoverPoint for Virtual Machines - five licenses per node
- CloudIQ SaaS multicluster management Tier 1⁶

The following VMware licenses are required:

- VMware vCenter Server - for clusters with customer-supplied vCenter Server
- VMware vSphere - Standard, Enterprise Plus, or Remote Office Branch Office (ROBO)
- VMware vSAN⁷ - Standard, Advanced, Enterprise, or Enterprise Plus

VxRail supports VMware perpetual or subscription-based licenses. Perpetual licenses can be purchased from Dell, VMware channel partners, or directly from VMware. Subscription-based licenses must be purchased directly from VMware.

⁵ This vCenter Server license is not transferable to a customer-supplied vCenter Server.

⁶ The Tier 1 license provides monitoring and reporting using the CloudIQ web portal. A fee-based license is required for active cluster management.

⁷ vSAN license is not required for VxRail dynamic node clusters or for VxRail satellite nodes.

VMware vSphere and vSAN Editions Feature Comparision

Feature	vSAN Standard	vSAN Advanced	vSAN Enterprise	vSAN Enterprise Plus
Deduplication and Compression		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RAID 5/6 Erasure Coding		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data-at-rest and Data-in-transit Encryption			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Stretched Cluster			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Services			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VMware HCI Mesh			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
vSAN Express Storage Architecture		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

vSAN Editions - Feature comparison

Minimum Number of Fault Domains

The tables show the minimum number of fault domains that are required to support various **Failures to tolerate** settings.

Number of failures to tolerate	Mirror copies	Minimum number of fault domains
1	2	3
2	3	5
3	4	7

Number of Failures to Tolerate	Erasure Coding	Minimum Number of Fault Domains
1	RAID 5	4
2	RAID 6	6

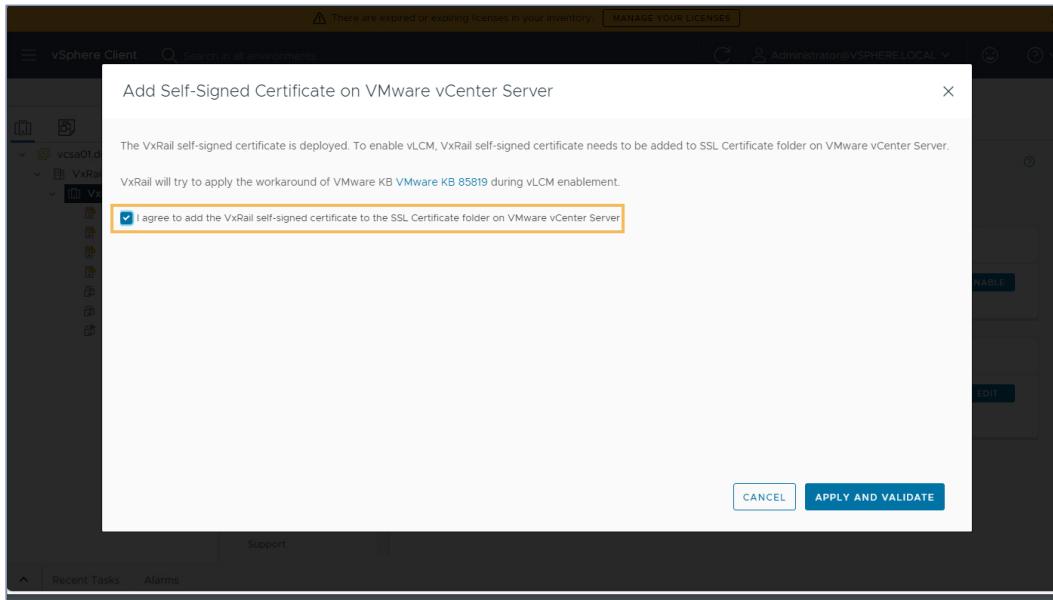
vSAN Advanced Policy Rules

The table shows the **vSAN Advanced Policy Rules**.

Number of disk stripes per object	Minimum number of capacity drives across which each replica of a virtual machine object is striped. Default is one (recommended). Maximum value is 12.
IOPs limit for object	IOPs is calculated as the number of I/O operations using a weighted size. If the system uses the default base size of 32 KB, a 64 KB I/O represents two I/O operations.

Object space reservation	The percentage of the logical size of the virtual machine object that must be reserved when deploying a virtual machine. Default is Thin Provisioning. The Thick provision option fully reserves storage for the VM (100% space reservation). Space reservation can also be set at the percentage values of 25%, 50%, or 75%. If deduplication or compression is enabled, the space reservation must be set to either 0 or 100. If set to 100, no data reduction is attempted.
Flash read cache reservation (%)	Flash capacity reserved as read cache for the virtual machine object. The value is specified as a percentage of the logical size of the virtual machine disk object. Other objects cannot use the reserved flash capacity. Unreserved flash is shared among all objects. Flash read cache reservation (%) is only applicable for hybrid configurations and should only be changed with input from support
Disable object checksum	The setting is disabled by default; the object calculates checksum information to ensure the integrity of its data. If enabled, the object does not calculate checksum information.
Force Provisioning	The setting is disabled by default. If enabled, the object is provisioned even if the datastore is incompatible with the storage policy.

Add Self-Signed Certificate on VMware vCenter Server



Add Self-Signed Certificate on VMware vCenter Server confirmation

VxVerify

VxVerify is a tool for checking the health of the nodes and the service VMs. It is designed to detect issues that could cause complications or failures during VxRail LCM upgrades. VxVerify is run from the VxRail Manager. It automatically uploads and runs scripts against each ESXi node and system VM and then analyzes the collected data. Since the tool is updated regularly, ensure you have the latest version before using it. Acquire the latest version of the tool before using it. Follow [KB 21527](#) for instructions on how to run VxVerify.

In the below example, VxVerify is copied over to the VxRail Manager virtual machine. An Administrator with root credentials runs the python script. Any issues that the script identifies must be resolved before performing an LCM upgrade.

```
#=====#
| VxVerify Menu Driven launcher |
#=====#
1) Upgrade healthcheck      5) Unused5
2) Core upgrade healthcheck 6) Unused6
3) General healthcheck     7) Unused7
4) Core post-upgrade check 8) Quit
Please enter your choice: 1
Upgrade healthcheck selected.
Enter target version: 8.0.201
Enter VC SSO credentials? (Y/N)Y
VC SSO user [default: administrator@vsphere.local]: administrator@vsphere.local
Enter VC SSO password:
Run recommended option with VC root credentials? (Y/N)Y
VC root user [default: root]: root
Enter VC root password:
VC SSO user AND VC root user present.
VxVerify triggered via shell script in test profile 2
Running VxVerify 3.31.215, pre-upgrade healthcheck on VxRail 8.0.100.
In case of program errors consult article www.dell.com/support/kbdoc/000066460.
Step 1 of 10: VxVerify: Sending Minions to each host. The Minions then run ESXi and VM tests.
Step 2: Start minion program on node: vcluster730-esx01.delledu.lab
Step 2: Start minion program on node: vcluster730-esx02.delledu.lab
Step 2: Start minion program on node: vcluster730-esx03.delledu.lab
Step 3: 26 tests complete with ESXi minion in progress on ['vcluster730-esx01', 'vcluster730-esx02', 'vcluster730-esx03']
Step 2: Start vxdiag log analysis on VxRM
Step 4: Tests completed on: vcluster730-esx01
Step 4: Tests completed on: vcluster730-esx02
Step 4: Tests completed on: vcluster730-esx03
Step 4: Test results received from host: vcluster730-esx01.delledu.lab
Step 4: Test results received from host: vcluster730-esx02.delledu.lab
Step 4: Test results received from host: vcluster730-esx03.delledu.lab
Step 5: Running VxRM and VC API tests
Step 6: Analyzing LCM upgrade history.
Step 6: No LCM history to include in a table.
Step 7: VC tests with root user.
Step 8: SSO administrator user/pw supplied, VCSA admin tests running.
```

Output of VxVerify python script

Sample Advisory Report

Appendix

VxRail Update Advisor Report for Cluster VxRail-Virtual-SAN-Cluster-f3234d1c-dfc3-4495-8402-f134356836d7

[EXPORT REPORT](#)

1. VxRail Update Advisor Report Summary

Update Readiness Status: ⚠ Review and remediate any applicable warnings identified below before installing the VxRail 8.0.201-28354422 update.

Timestamp: 01/08/2024 05:34:11 PM

Cluster Name: VxRail-Virtual-SAN-Cluster-f3234d1c-dfc3-4495-8402-f134356836d7

Current State: VxRail 8.0.100-28093095

Desired State: VxRail 8.0.201-28354422

Install Duration: Approximately 4.6 hours

Last VxRail Integrated Backup: Go to the [VxRail Backup Page](#) to complete a VxRail integrated backup before updating the cluster.

Release Notes: [Dell VxRail 8.0.201](#)

2. VxRail Components

Component Status: 🟢 No components require remediation before installing the VxRail 8.0.201-28354422 update.

[Hide Details](#)

Total Components: 6 🟢 Ready for update: 6 Group by component

	Status	Summary	Component Type	Component	Current Version	Expected Version	Target Version	Host Quick Boot	Service Tag
>	🟢	Ready for cluster update	ESXI_HOST	esx-611-vxrail3.edu.local	--	--	--	Quickboot compatible	7NK6BZ2
>	🟢	Ready for cluster update	ESXI_HOST	esx-611-vxrail1.edu.local	--	--	--	Quickboot compatible	7NK4BZ2
>	🟢	Ready for cluster update	ESXI_HOST	esx-611-vxrail4.edu.local	--	--	--	Quickboot compatible	7NK7BZ2
>	🟢	Ready for cluster update	ESXI_HOST	esx-611-vxrail2.edu.local	--	--	--	Quickboot compatible	7NK5BZ2
	🟢	Ready for cluster update	SOFTWARE	VMware vCenter Server Appliance	8.0.1	8.0.1	8.0.2	--	--
	🟢	Ready for cluster update	SOFTWARE	VxRail Manager	8.0.100	8.0.100	8.0.201	--	--

3. VxRail Precheck Version 1.0.802

Precheck Status: ⚠ Review and remediate any applicable warnings identified below before installing the VxRail 8.0.201-28354422 update.

[Hide Details](#)

Total Prechecks: 309 ⚠ Warning: 1 🟢 Success: 308 Group by component

	Status	Summary	Component Type	Component
>	🟢	Ready for cluster update	Esxi host	esx-611-vxrail1
>	🟢	Ready for cluster update	Esxi host	esx-611-vxrail2
>	🟢	Ready for cluster update	Esxi host	esx-611-vxrail3
>	🟢	Ready for cluster update	Esxi host	esx-611-vxrail4
>	🟢	Ready for cluster update	vCenter Server	vCenter Server
>	🟢	Ready for cluster update	VxRail Manager	VxRail Manager
>	🟢	Ready for cluster update	Storage	Storage
>	⚠	Review the warnings	Cluster	Cluster

4. VxRail Custom Components (User-Managed Components)

[Hide Details](#)

Total Custom Components: 1

Summary	Component	Current Version
Current version detected.	OLogic Fibre Channel HBA Driver	5.4.80.0-IOEM.800.1.0.20143090

ESCPXD05510 ~ VxRail 8.0.XXX Implementation-SSP

Sample Advisory Report

Planning Considerations for Scalability

The balance and flexibility of a VxRail protects the initial investment. Start with what is needed and then expand by adding nodes and or drives to increase performance and capacity as needed.

- All systems in a cluster must be running the same version of VxRail software.
- All-flash, all-NVMe, and Hybrid nodes cannot be mixed in the same cluster. However, mixing of all-flash and all-NVMe nodes in a cluster is allowed.
- All G Series nodes in a chassis must be identical. A G series chassis can be partially populated.
- All systems in the cluster must run the same base network speed (100 GbE, 25 GbE, 10 GbE, or 1 GbE).
- A cluster can have a varied number of drives, CPU, memory, and model types.
- A cluster can have between 2-64 nodes.
 - If 1 GbE base networking speed is used, there is a limit of a maximum of eight nodes in the cluster.
 - 1 GbE base networking speed is only supported with hybrid single processor nodes.
- AMD-based nodes and Intel-based nodes cannot be mixed in the same cluster.
- Use the [VxRail Node Addition Matrix](#) to verify that the new node versions are compatible.
- Node discovery method
 - If existing cluster used manual discovery, continue to use manual discovery.
 - If existing cluster used automatic discovery, use either automatic or manual discovery.

Search Results for All Errors in Dayone.log

Appendix

```
2021-11-06-20:09:20 microservice.nano-service "2021-11-06 20:09:20,051 [ERROR] <Thread-1:140005743164232> lock_service.py acquire() (4  
1): HTTPConnectionPool(host='api-gateway', port=8080): Max retries exceeded with url: /rest/vxm/internal/lockservice/v1/lock/acquire (4  
Caused by NewConnectionError('urllib3.connection.HTTPConnection object at 0x7f55a01fae80>; Failed to establish a new connection: [Err  
no -3] Temporary failure in name resolution'))"  
2021-11-06-20:09:20 microservice.nano-service "2021-11-06 20:09:20,051 [ERROR] <Thread-1:140005743164232> general_lock_service.py is_l  
ock_acquired() (49): Exception during communicate with lock service"  
2021-11-06-20:09:20 microservice.nano-service "2021-11-06 20:09:20,071 [ERROR] <Thread-1:140005743164232> lock_service.py release() (6  
4): HTTPConnectionPool(host='api-gateway', port=8080): Max retries exceeded with url: /rest/vxm/internal/lockservice/v1/lock/release (6  
Caused by NewConnectionError('urllib3.connection.HTTPConnection object at 0x7f55a0209908>; Failed to establish a new connection: [Err  
no -3] Temporary failure in name resolution'))"  
2021-11-06-20:09:20 microservice.nano-service "2021-11-06 20:09:20,071 [ERROR] <Thread-1:140005743164232> general_lock_service.py _re  
lease() (40): Exception during communicate with lock service"  
2022-05-31-18:23:54 microservice.nano-service "2022-05-31 18:23:54,058 [ERROR] <Thread-1:140388928400200> lock_service.py acquire() (4  
2): HTTPConnectionPool(host='api-gateway', port=8080): Max retries exceeded with url: /rest/vxm/internal/lockservice/v1/lock/acquire (4  
Caused by NewConnectionError('urllib3.connection.HTTPConnection object at 0x7faed3b2e828>; Failed to establish a new connection: [Err  
no -3] Temporary failure in name resolution'))"  
2022-05-31-18:23:54 microservice.nano-service "2022-05-31 18:23:54,058 [ERROR] <Thread-1:140388928400200> general_lock_service.py is_l  
ock acquired() (49): Exception during communicate with lock service"  
2022-05-31-18:23:54 microservice.nano-service "2022-05-31 18:23:54,069 [ERROR] <Thread-1:140388928400200> lock_service.py release() (6  
4): HTTPConnectionPool(host='api-gateway', port=8080): Max retries exceeded with url: /rest/vxm/internal/lockservice/v1/lock/release (6  
Caused by NewConnectionError('urllib3.connection.HTTPConnection object at 0x7faed3b2e828>; Failed to establish a new connection: [Err  
no -3] Temporary failure in name resolution'))"  
2022-05-31-18:23:54 microservice.nano-service "2022-05-31 18:23:54,069 [ERROR] <Thread-1:140388928400200> general_lock_service.py _re  
lease() (40): Exception during communicate with lock service"  
2022-05-31-18:24:48 microservice.ms-dayl-bringup "2022-05-31 18:24:48,916 [ERROR] <MainThread:140069886911808> hostquery.py call_do_q  
uery() (289): Query http://api-gateway:8080/rest/vxm/internal/do/v1/host/query failed, will not have extra info for hosts."  
2022-05-31-18:24:48 microservice.ms-dayl-bringup "2022-05-31 18:24:48,916 [ERROR] <MainThread:140069886911808> hostquery.py load_hosts  
for_ip_change() (280): Error get extra host info when calling DO service. cannot find the hosts."  
2022-05-31-18:24:48 microservice.ms-dayl-bringup "2022-05-31 18:24:48,917 [ERROR] <MainThread:140069886911808> vxm_ip_change_scheduler  
.py run_scheduler() (132): Hosts discover failed"  
2022-05-31-18:27:34 microservice.ms-dayl-bringup "2022-05-31 18:27:34,874 [ERROR] <Dummy-9:139625510778952> wfservice.py get_status_fr  
om wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-804  
0-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:34 microservice.ms-dayl-bringup "2022-05-31 18:27:34,906 [ERROR] <Dummy-9:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should be  
in node discovery stage of new workflow launching."  
2022-05-31-18:27:37 microservice.ms-dayl-bringup "2022-05-31 18:27:37,628 [ERROR] <Dummy-11:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:37 microservice.ms-dayl-bringup "2022-05-31 18:27:37,645 [ERROR] <Dummy-11:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:38 microservice.ms-dayl-bringup "2022-05-31 18:27:38,739 [ERROR] <Dummy-13:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:38 microservice.ms-dayl-bringup "2022-05-31 18:27:38,754 [ERROR] <Dummy-13:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:39 microservice.ms-dayl-bringup "2022-05-31 18:27:39,887 [ERROR] <Dummy-15:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:39 microservice.ms-dayl-bringup "2022-05-31 18:27:39,902 [ERROR] <Dummy-15:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:41 microservice.ms-dayl-bringup "2022-05-31 18:27:41,169 [ERROR] <Dummy-17:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:41 microservice.ms-dayl-bringup "2022-05-31 18:27:41,191 [ERROR] <Dummy-17:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:42 microservice.ms-dayl-bringup "2022-05-31 18:27:42,400 [ERROR] <Dummy-19:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:42 microservice.ms-dayl-bringup "2022-05-31 18:27:42,422 [ERROR] <Dummy-19:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:43 microservice.ms-dayl-bringup "2022-05-31 18:27:43,554 [ERROR] <Dummy-21:139625510778952> wfservice.py get_status_f  
rom wf() (617): Error get workflow progress status: http://api-gateway:8080/rest/vxm/internal/engine/v1/instance/a00133f7-c403-4878-80  
40-0126342a4c33 (status: 404, response body: {"error": "WFNotFound: 404 Not Found: instance a00133f7-c403-4878-8040-0126342a4c33 not  
found"})"  
2022-05-31-18:27:43 microservice.ms-dayl-bringup "2022-05-31 18:27:43,579 [ERROR] <Dummy-21:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance a00133f7-c403-4878-8040-0126342a4c33, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:46 microservice.ms-dayl-bringup "2022-05-31 18:27:46,114 [ERROR] <Dummy-24:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance 520fc5f4-d3ec-4c9b-b8dc-2b4593d151ba, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:49 microservice.ms-dayl-bringup "2022-05-31 18:27:49,153 [ERROR] <Dummy-25:139625510778952> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance 520fc5f4-d3ec-4c9b-b8dc-2b4593d151ba, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:52 microservice.ms-dayl-bringup "2022-05-31 18:27:52,132 [ERROR] <Dummy-27:139625510779720> progress_converter.py lo  
ad foreach_items_from_resource() (133): can not find resource.json file for instance 520fc5f4-d3ec-4c9b-b8dc-2b4593d151ba, it should b  
e in node discovery stage of new workflow launching."  
2022-05-31-18:27:57 microservice.vxm-agent "2022-05-31 18:27:57,411 [ERROR] <Thread-37:140451431503616> vxml_agent_utils.py run_vxm_c  
ommand() (66): run_vxm_command Fail. error code: 2, message: b"ls: is: cannot access '/var/lib/vmware-marvin/manifest.xml': No such file or  
directory\n""  
2022-05-31-18:27:57 microservice.vxm-agent "2022-05-31 18:27:57,411 [ERROR] <Thread-37:140451431503616> vxml_agent_utils.py run_vxm_c  
ommand() (66): run_vxm_command Fail. error code: 2, message: b"ls: is: cannot access '/var/lib/vmware-marvin/manifest.xml': No such file or  
directory\n""  
2022-05-31-18:27:57 microservice.vxm-agent "2022-05-31 18:27:57,411 [ERROR] <Thread-37:140451431503616> vxml_agent_utils.py handle_vxm_a  
gent_response() (33): http://vxml-agent:5000/vxm-agent/v1/vxm/services/command failed!"  
2022-05-31-18:28:04 microservice.ms-dayl-bringup "2022-05-31 18:28:04,842 [ERROR] <Dummy-30:139625510778696> vxml_agent.py handle_vxm_a  
gent_response() (33): http://vxml-agent:5000/vxm-agent/v1/vxm/services/command failed!"  
2022-05-31-18:28:04 microservice.vxm-agent "2022-05-31 18:28:04,839 [ERROR] <Thread-47:140451431503616> vxml_agent_utils.py run_vxm_c  
ommand() (66): run_vxm_command Fail. error code: 2, message: b"ls: is: cannot access '/data/store2/recovery/recoveryBundle-7.0.241.zip': No  
such file or directory\n""  
2022-05-31-18:28:04 microservice.vxm-agent "ERROR:utils.vxm_agent.utils:run_vxm_command Fail. error code: 2, message: b"ls: cannot ac  
cess '/data/store2/recovery/recoveryBundle-7.0.241.zip': No such file or directory\n""  
2022-05-31-18:28:07 microservice.vxm-agent "2022-05-31 18:28:07,611 [ERROR] <Thread-51:140451431503616> vxml_agent_utils.py run_vxm_c  
ommand() (66): run_vxm_command Fail. error code: 1, message: b'File transfer got error response: <Response [404]>\n"  
2022-05-31-18:28:07 microservice.vxm-agent "ERROR:utils.vxm_agent.utils:run_vxm_command Fail. error code: 1, message: b'File transfer  
got error response: <Response [404]>\n"  
2022-05-31-18:28:07 microservice.do-cluster "[2022-05-31 18:28:07,676: [ERROR/MainProcess] http://vxml-agent:5000/vxm-agent/v1/vxm/servi  
ces/command failed!"  
2022-05-31-18:28:07 microservice.do-cluster "[2022-05-31 18:28:07,676: [ERROR/MainProcess] Caught for log, will raise this exception ag  
ain."  
2022-05-31-18:28:07 microservice.do-cluster "[2022-05-31 18:28:07,683: [ERROR/MainProcess] Task worker.celery_task.rest_cluster.file_tr  
ansfer to vxml[35deb02d-5245-4667-97cc-925ae0642050] raised unexpected: ("code": "'DO_OPERATIONEXCEPTION'", "message": "'Exception(b'  
File transfer got error response: <Response [404]>\n'", "params": {}, "context": {}, "task": null})"  
2022-05-31-18:28:08 microservice.ms-dayl-bringup "2022-05-31 18:28:08,128 [ERROR] <Thread-34:139625510778440> transfer_handler.py down  
load_file() (159): error download /data/store2/recovery/recoveryBundle-7.0.241.zip from vxrail-datastore/recoveryBundle-7.0.241.zip  
2022-05-31-18:28:08 microservice.do-cluster "2022-05-31 18:28:08,126 [ERROR] <Dummy-139713334609736> async_task.py get() (398): Trac  
eback (most recent call last):  
2022-05-31-18:28:08 microservice.do-cluster "2022-05-31 18:28:08,126 [ERROR] <Dummy-8:139713334609736> sync_task.py get() (400): Task  
execution error: ('code': 'DO_OPERATIONEXCEPTION', 'message': "Exception(b'File transfer got error response: <Response [404]>\n',)"  
", 'params': {})"  
2022-05-31-18:28:15 microservice.vxm-agent "2022-05-31 18:28:15,271 [ERROR] <Thread-55:140451420649216> vxml_agent_utils.py run_vxm_c  
ommand() (66): run_vxm_command Fail. error code: 2, message: b"ls: is: cannot access '/var/lib/vmware-marvin/trust/lin': No such file or di  
rectory\n""  
2022-05-31-18:28:15 microservice.vxm-agent "ERROR:utils.vxm_agent.utils:run_vxm_command Fail. error code: 2, message: b"ls: cannot ac  
cess '/var/lib/vmware-marvin/trust/lin': No such file or directory\n""  
(2022-05-31-18:28:15,274 [ERROR] <Dummy-10:140388928400200> utils.py wrapper() (101): lo  
g_level 151, static.handle_vxm_agent_response raise exception: OperationException("message": "'Exception(b'ls: cannot access '/va  
r/lib/vmware-marvin/trust/lin'\n'", "bundle": "'", "prefix": "'", "common.exceptions.OperationException'"  
"key": "'", "field": "'", "error_code": "'000'", "exit_code": "'1'", "params": []})  
2022-05-31-18:28:15,274 [ERROR] <Dummy-10:140388928400200> utils.py wrapper() (102): lo  
g_level 151, static.handle_vxm_agent_response raise exception: OperationException("message": "'Exception(b'ls: cannot access '/va  
r/lib/vmware-marvin/trust/lin'\n'", "bundle": "'", "prefix": "'", "common.exceptions.OperationException'"  
"key": "'", "field": "'", "error_code": "'000'", "exit_code": "'1'", "params": []})
```

Dayone.log results for all errors

Search Results for "vmnic1 is down" Errors in Dayone.log

```
2022-05-31-18:45:23 microservice.nano-service["2022-05-31T18:45:23.381Z"] [ERROR] <Dummy-79:140388995301960> physical_link_live_validator.py add_error() (392): The pnic vmmci1 is down in host V073001.
2022-05-31-18:45:23 microservice.wrservice["INFO [wfengine] finish execute rest step {'result': {'result': 'FAILED', 'raw_result': None, 'name': 'PhysicalLinkLiveValidator', 'context': {'invalid_fields': ['network.vds.nic_mappings', 'config.validation.shared.network.vlan.setup']}, 'errors': [{'type': 'THOROUGH-VALIDATOR', 'field': 'network.vds.nic_mappings', 'code': 'E3100_VAL_62', 'placeholders': ['vmmci1', 'V073001']}, {'message': 'The pnic vmmci1 is down in host V073001.'}, 'warnings': []}]}"}
2022-05-31-18:45:23 microservice.nano-service["2022-05-31T18:45:24.454Z"] [ERROR] <Dummy-79:140388995301960> validator.py execute() (88): Validation errors: errors=[{'type': 'THOROUGH-VALIDATOR', 'field': 'network.vds.nic_mappings', 'code': 'E3100_VAL_62', 'placeholders': ['vmmci1', 'V073001']}, {'message': 'The pnic vmmci1 is down in host V073001.}]
2022-05-31-18:45:23 microservice.wrservice["INFO [wfengine.status] notify {'level': 'step', 'id': 'general_thorough_validation.thorough_validator.0.physical_link_live_validator', 'state': 'COMPLETED', 'progress': 60, 'status': '(id: 'physical link live validator', 'internal_id': 'general_thorough_validation.thorough_validator.0.physical_link_live_validator False 6a8071ad 0158 45 34e3fe64:ada8@eth1', 'internal_family': 'general_thorough_validation.thorough_validator.0.physical_link_live_validator', 'status': 'COMPLETED', 'startTtime': 165402273244, 'stage': '0', 'endtime': 165402273458, 'params': {'nic profile': 'VXRAIL_SUPPLIED_VDS', 'nic profile_list': ['device': 'vmmci0', 'key': 'key-vim.host.PhysicalNic-vmmci0', 'speed_mb': 10000}, {'device': 'vmmci1', 'key': 'key-vim.host.PhysicalNic-vmmci1', 'speed_mb': 0}, {'device': 'vmmci2', 'key': 'key-vim.host.PhysicalNic-vmmci2', 'speed_mb': 10000}, {'device': 'vmmci3', 'key': 'key-vim.host.PhysicalNic-vmmci3', 'speed_mb': 10000}, 'host_conn_info': {'host': 'fe80::250:56ff:fe64:ada8@eth1', 'username': 'root', '*****port': 443}, 'vds_list': ['[{"portgroups": [{"type": "MANAGEMENT", "vlan_id": 0, "vmk_mtu": 1500, "load_balance_policy": "LOADBALANCE_LOADBASED"}, {"failover_order": {"active": 'uplink1', "uplink2": "uplink1", "standby": []}, "name": "Management Network-fbd17031-bd5f-43fc-8b01-1e4811ea0962", "binding_type": "EPHEMERAL"}], "type": "VSAN", "vlan_id": 10, "vmk_mtu": 1500, "load_balance_policy": "LOADBALANCE_LOADBASED"}, {"failover_order": {"active": 'uplink3', "uplink4": "uplink4", "standby": []}, "name": "Virtual SAN-fbd17031-bd5f-43fc-8b01-1e4811ea0962", "binding_type": "EARLY_BINDING"}, {"type": "VMOTION", "vian_id": 20, "vmk_mtu": 1500, "load_balance_policy": "LOADBALANCE_LOADBASED"}, {"failover_order": {"active": 'uplink4', "uplink3": "uplink3", "standby": []}, "name": "VspHERE_vMotion-fbd17031-bd5f-43fc-8b01-1e4811ea0962", "binding_type": "EARLY_BINDING"}, {"type": "VXRAILDISCOVERY", "vian_id": 3939, "vmk_mtu": 1500, "load_balance_policy": "LOADBALANCE_LOADBASED"}, {"failover_order": {"active": 'uplink2', "uplink1": "uplink1", "standby": []}, "name": "VxRail Management-fbd17031-bd5f-43fc-8b01-1e4811ea0962", "binding_type": "EARLY_BINDING"}, {"type": "VXRAILSYSTEMVM", "vian_id": 0, "vmk_mtu": 1500, "load_balance_policy": "LOADBALANCE_LOADBASED"}, {"failover_order": {"active": 'uplink1', "uplink2": "uplink2", "standby": []}, "name": "vCenter Server Network-fbd17031-bd5f-43fc-8b01-1e4811ea0962", "binding_type": "EPHEMERAL"}, {"type": "CUSTOMERVM", "name": "VM Guest Network", "vian_id": 1761, "failover_order": {"active": 'uplink1', "uplink2": "uplink2", "standby": []}, "load_balance_policy": "LOADBALANCE_LOADBASED", "binding_type": "EARLY_BINDING"}, {"vmk_mtu": 1500, "nic mappings": [{"uplinks": [{"name": "uplink1", "physical_nic": "vmmci0"}, {"name": "uplink2", "physical_nic": "vmmci1"}, {"name": "uplink3", "physical_nic": "vmmci2"}, {"name": "uplink4", "physical_nic": "vmmci3"}]}, {"customer_supplied": False, 'name': 'VMware HCIA Distributed Switch VxRail-Cluster fbd1701', 'management_pgnname': 'Management Network-fbd17031-bd5f-43fc-8b01-1e4811ea0962'}, {"cluster_type": 'STANDARD', 'asset_tag': 'V073001', 'hw model': 'VxRail E560F', 'vc_conn_info': {'host': 'vcsa70.edu.local', 'username': 'administrator@vsphere.local', '*****port': 443}, 'datacenter_name': 'VxRail-DC1', 'invalid_fields': ['config.validation.shared.network.vlan.setup']}, {"network_prepare_params": {'vnxm_ip': '192.168.10.16', 'vnxm_netmask': '255.255.255.0', 'vnxm_gateway': '192.168.10.254', 'tld': 'edu.local', 'is_internal_dns': False, 'dns_servers': ['192.168.10.11'], 'vlnid': 0, 'host_conn_info': {'host': 'fe80::250:56ff:fe64:ada8@eth1', 'username': 'root', '*****port': 443}}}, 'result': {'result': 'FAILED', 'raw_result': None, 'name': 'PhysicalLinkLiveValidator', 'context': {'invalid_fields': ['network.vds.nic_mappings', 'config.validation.shared.network.vlan.setup']}, 'errors': [{"type": "THOROUGH-VALIDATOR", "field": "network.vds.nic_mappings", "code": "E3100_VAL_62", "placeholders": ['vmmci1', 'V073001']}, {"message": 'The pnic vmmci1 is down in host V073001.'}, 'warnings': []}]}"}
```

Dayone.log results for "vmnic1 is down" error

[External_Mgmt](#)

The external management VLAN is used for ESXi host management and for vCenter Server and VxRail Manager management. On a VxRail deployed VDS the Management Network port group and the vCenter Server Network port group use this VLAN ID.

[Glossary Term](#)

Example of a glossary term used in this course.

[Internal_Mgmt](#)

The internal management network is used for VxRail node discovery. On a VxRail deployed VDS the VxRail Management port group uses this VLAN ID.

[Link Aggregation Control Protocol \(LACP\)](#)

LACP is the protocol that enables the discovery, autoconfiguration, and management of the LAG relationship between the vSphere VDS and the adjacent physical ToR switches. Dynamic link aggregation requires an LACP policy to be configured on the VDS to establish the LAG relationship. LACP is the best practice for link aggregation because it offers support for more load balancing hashing algorithms and superior management capabilities.

[Spanning Tree Protocol \(STP\)](#)

STP is protocol to prevent network loops as defined in the IEEE 802.1d standard. STP forces the ports to go into five different states: Blocked, Listen, Learn, Forward, and Disabled. All ports start in the blocked mode to prevent the switch from creating a loop. STP runs by default on all ports of the switch. STP makes each port wait up to 50 s before data can be sent on the port. This delay in turn can cause problems with some applications or protocols including VxRail nodes. STP was revised to include the Rapid Spanning Tree Protocol (RSTP) as specified in the IEEE 802.1w standard.

[Test Plan](#)

The Dell or Dell partner implementation teams must complete the document after a VxRail deployment. The Test Plan is handed off to the customer at the conclusion of the implementation.

[Trunk mode](#)

Trunk and Access modes define how tagged and untagged packets are handled. A tagged packet contains the VLAN ID in the packet header. When a Trunk mode port receives a tagged packet, it passes the packet to the VLAN ID specified in the tag. If a Native (Access) VLAN is configured on Trunk mode ports, the ports accept untagged packets for that VLAN. Access mode ports only accept untagged packets for a single VLAN.