VXRAIL 8.0.XXX IMPLEMENTATION

DOWNLOADABLE CONTENT

Table of Contents

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. V xRail 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

Dell Technologies SolVe

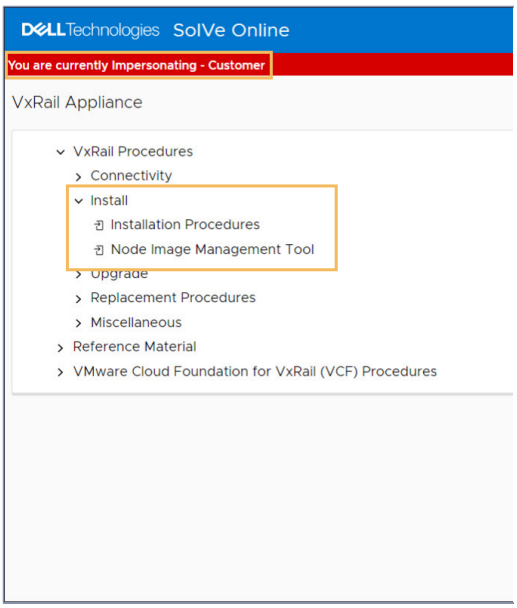
Dell Technologies SolVe is an interactive procedure generator that is used to create procedures for servicing Dell products.

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

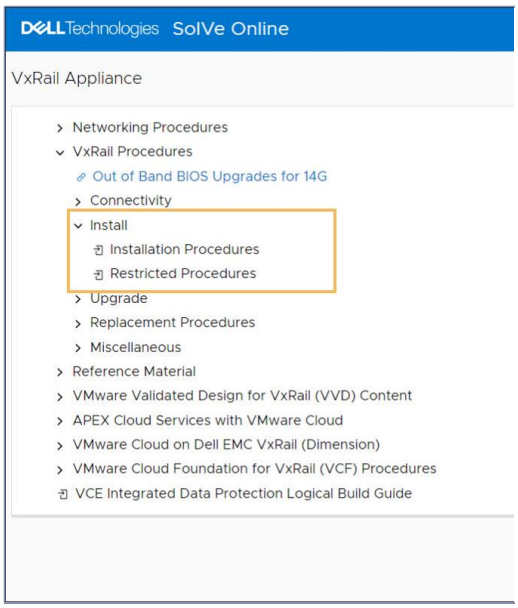
- SolVe Online - Web-based application
  - Can be accessed at - https://solve.dell.com/solve/home
  - Automatically updated procedures
- SolVe Desktop - User-installed Windows application
  - Can be downloaded from - https://solve.emc.com/desktopbinaries/setup.exe
  - Offline accessible
  - Manual update

The list of available procedures depends on the access level of the user: Dell Employee[2], Partner, or Customer.

[2] Dell Employees can impersonate all access levels.



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.

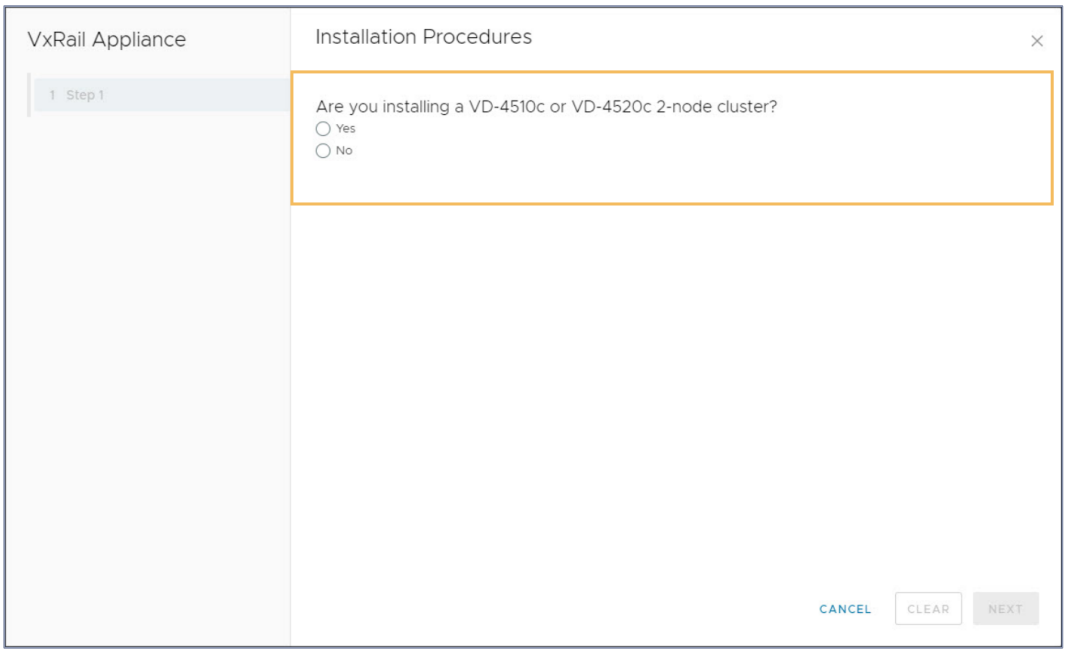
Generate VxRail Installation Procedures - Common Selections

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.

Cluster Verification

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

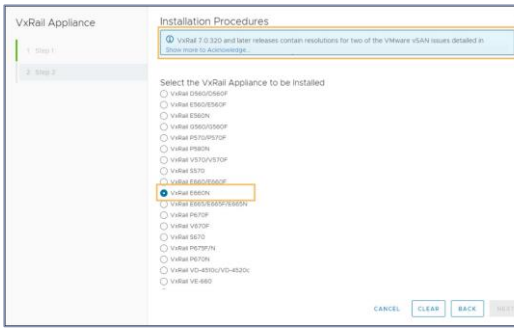


Customer View - Cluster verification

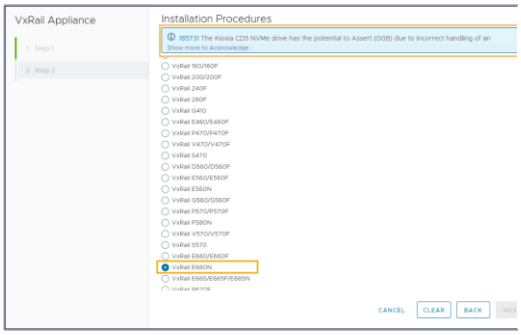
Model

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.



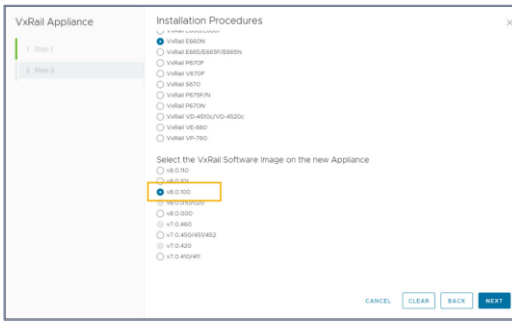
Customer View - Select VxRail model



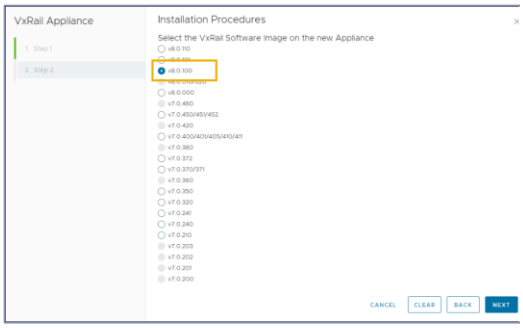
Internal or Partner View - Select VxRail model

Software Version

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



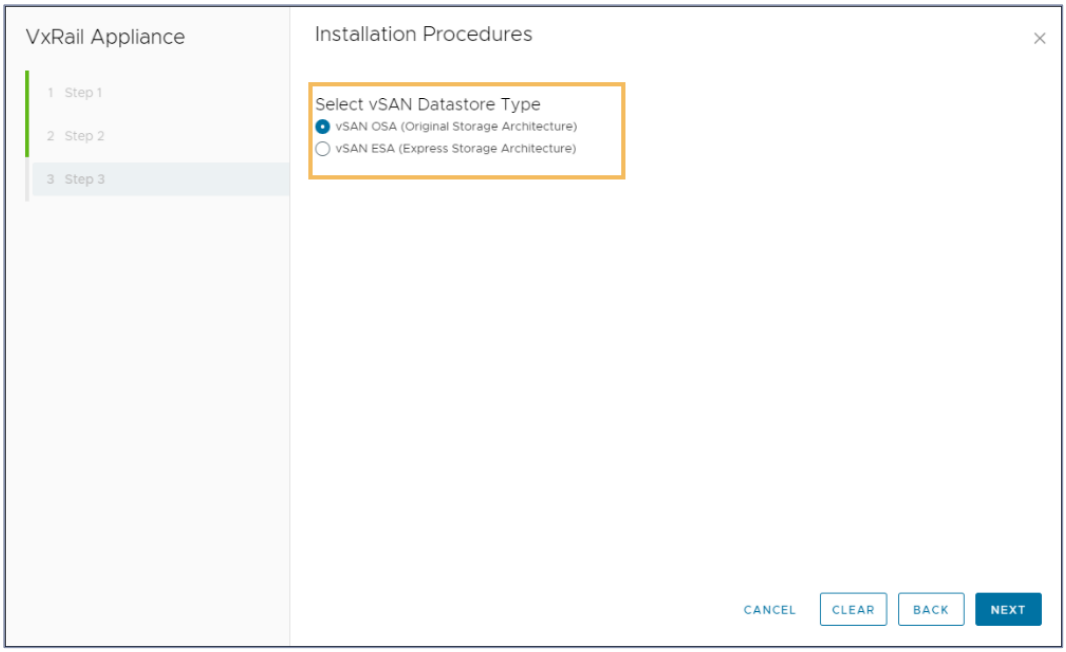
Customer View - Select VxRail software version



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.

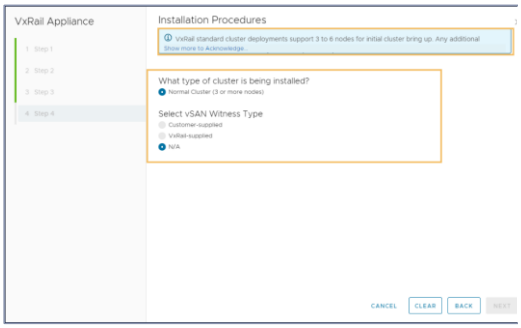


Customer View and Internal or Partner View - Select vSAN datastore type

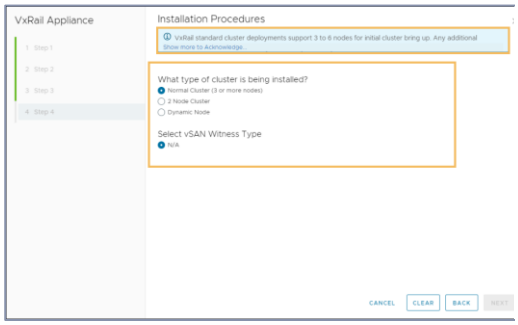
Cluster Type

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

Acknowledge the informational message to proceed.



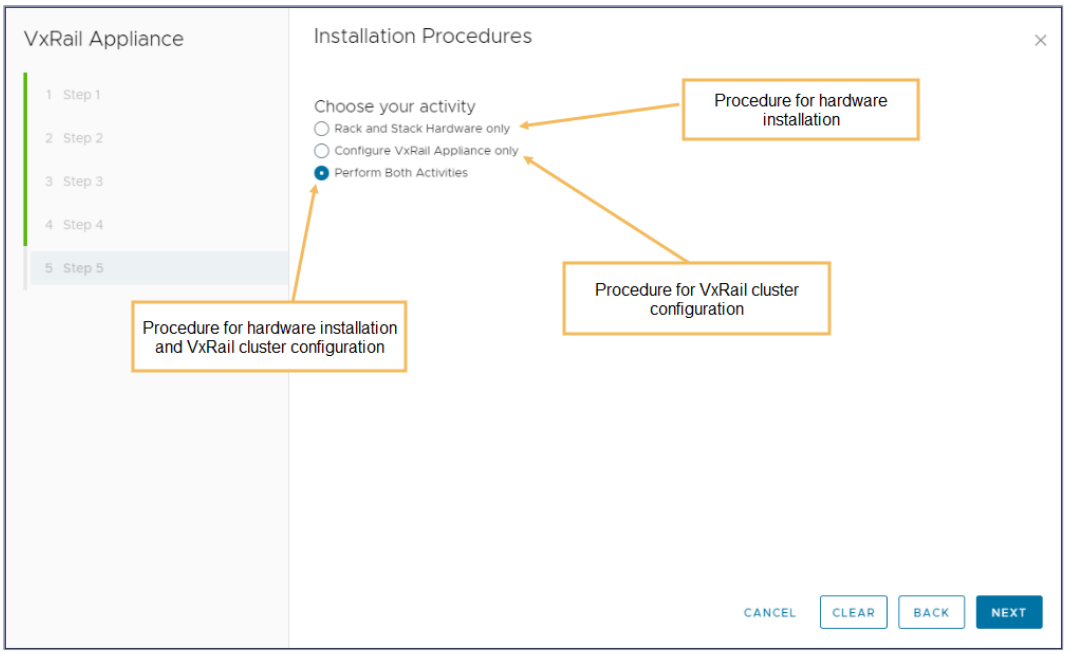
Customer View - Cluster and vSAN Witness type



Internal or Partner View - Cluster and vSAN Witness type

Activity

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



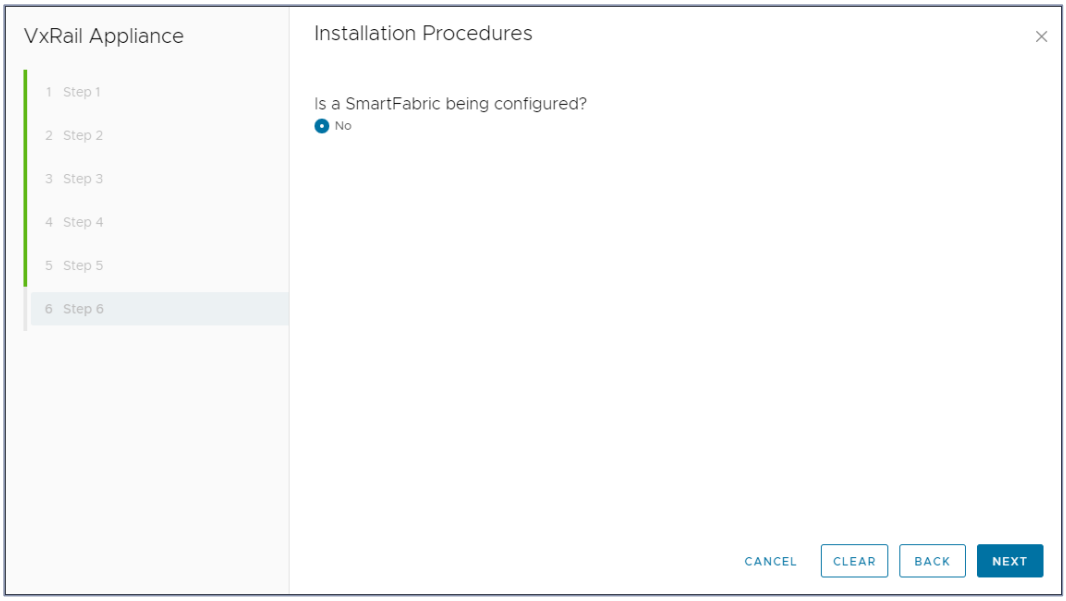
Customer View and Internal or Partner View - Select activity

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

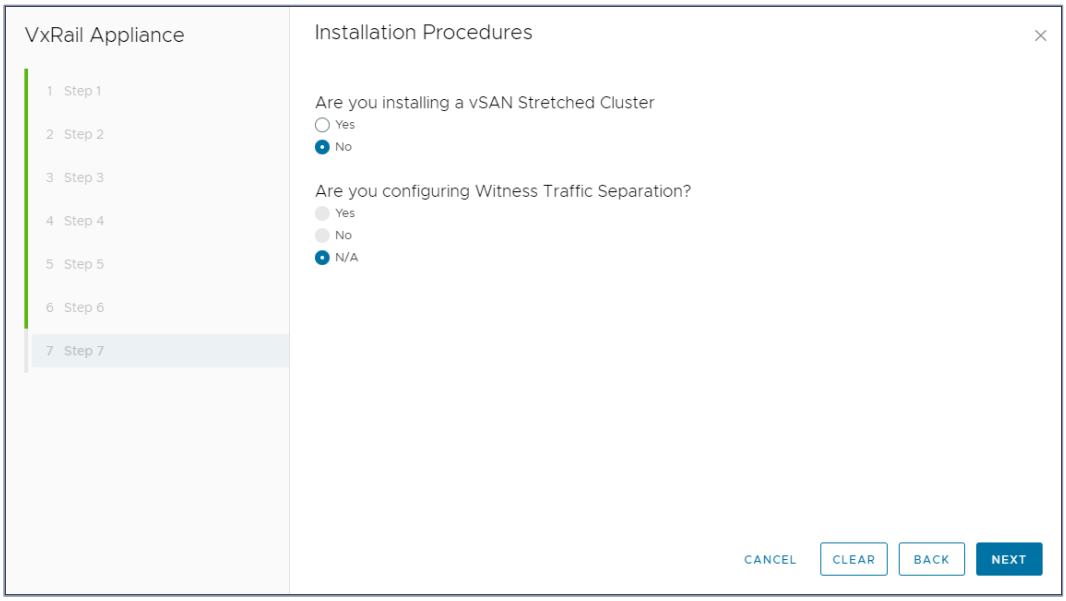
Select whether a configuration of SmartFabric is required.



Internal or Partner View - Select SmartFabric options

vSAN Stretched Cluster

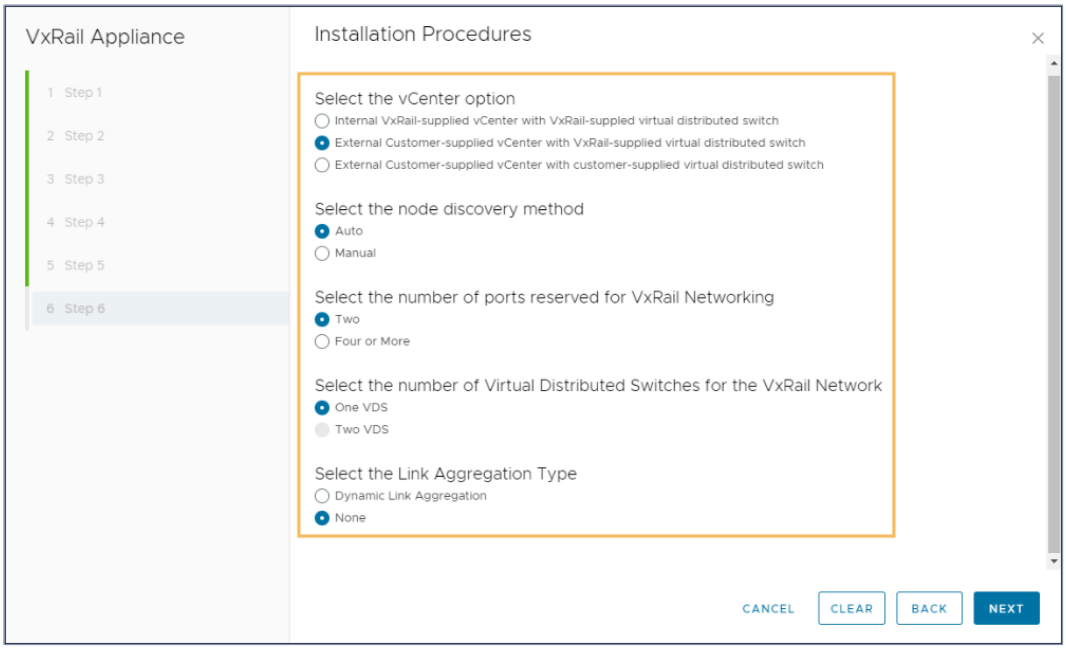
Select whether a vSAN Stretched Cluster is being implemented and whether Witness Traffic Separation is being configured.



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

vCenter Server and Networking Options

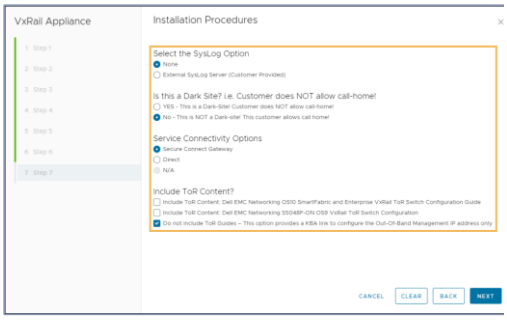
Select the vCenter Server Option, node discovery method, number of reserved ports for VxRail Networking, number of VMware Virtual Distributed Switch (VDS), and Link Aggregation Type. Some of the networking options depend on this selection.



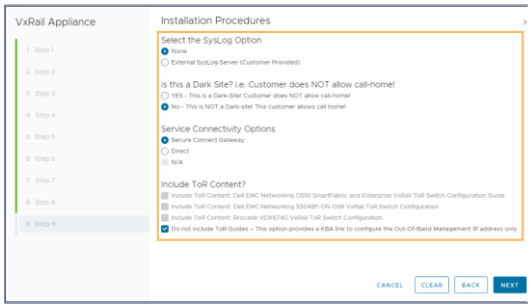
Customer View Internal or Partner View - Select vCenter, discovery, and networking options

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.



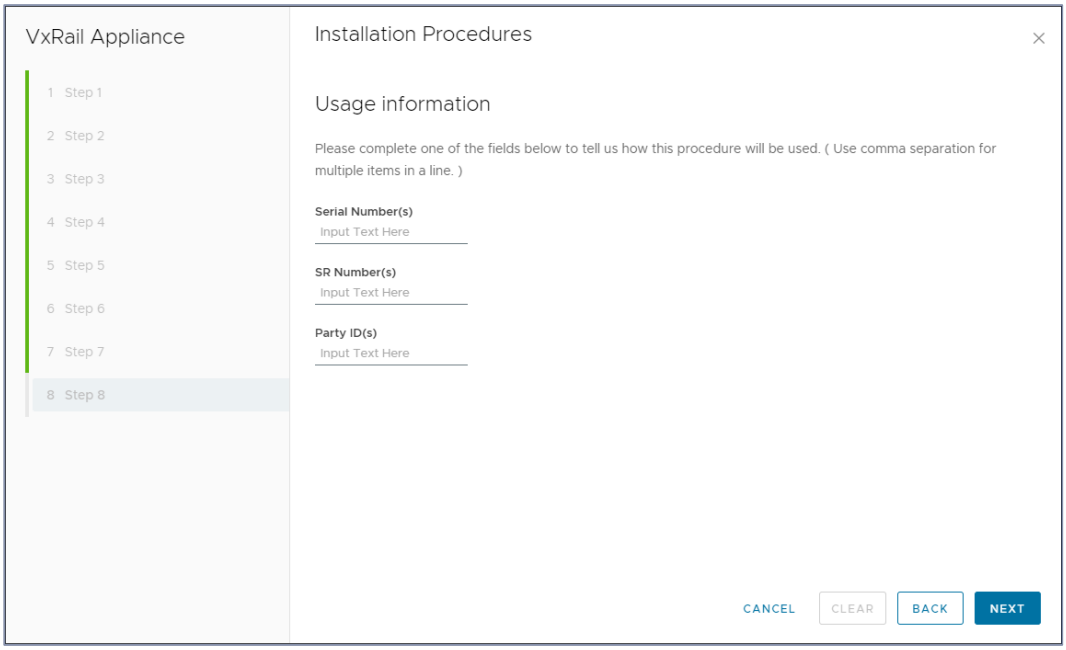
Customer view - Select connectivity options



Internal or Partner View - Select connectivity options

Procedure Usage

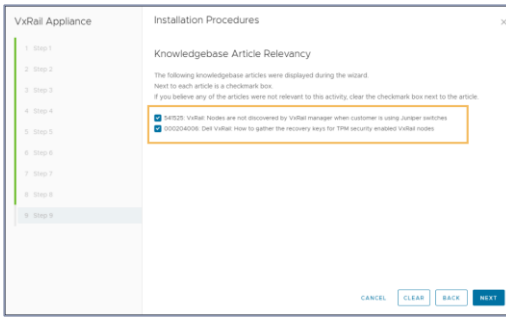
The usage information is an optional section. Enter the requested information about the VxRail nodes that this procedure has to be used on.



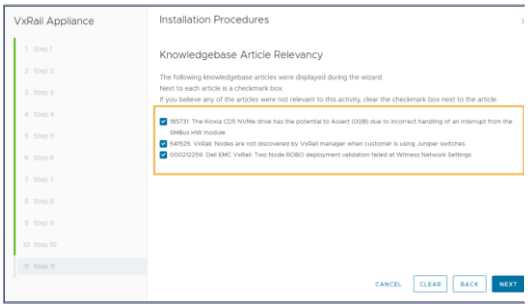
Customer and Internal or Partner View - Procedure usage information

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.



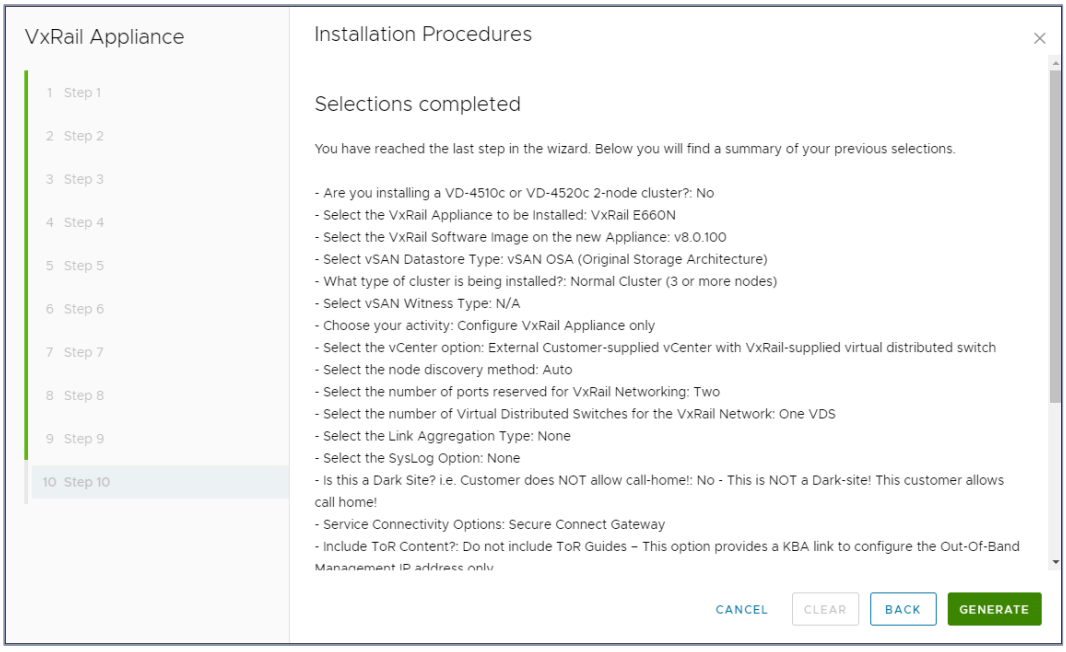
Customer view - Knowledgebase Article relevancy verification



Internal or Partner View - Knowledgebase Article relevancy verification

Summary and Generate Procedure

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



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

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.

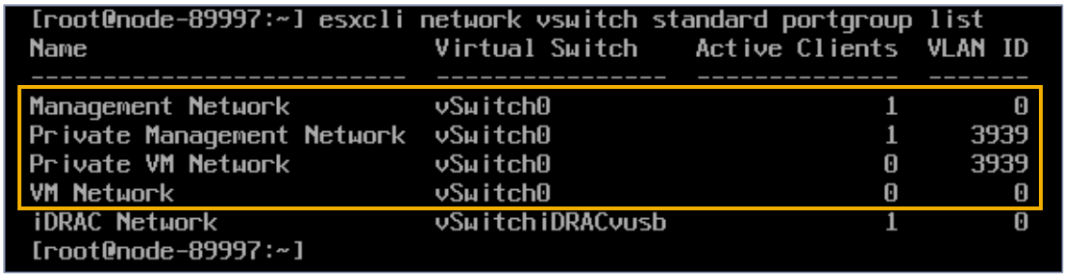
Lab Tasks

- 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:



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

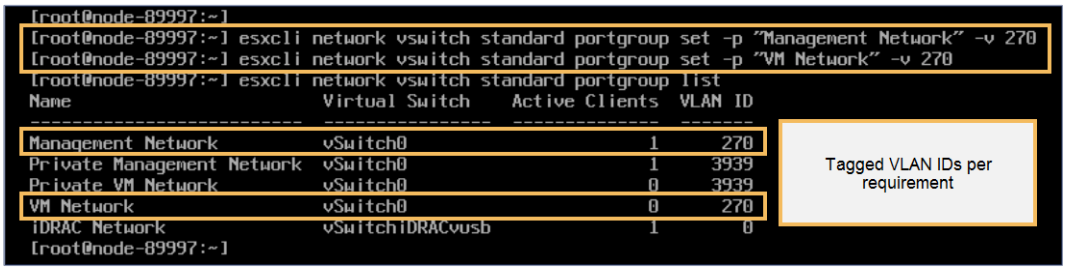
The default port group VLAN IDs can be modified by running the following ESXCLI command from the ESXi Shell of the node:

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:



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.

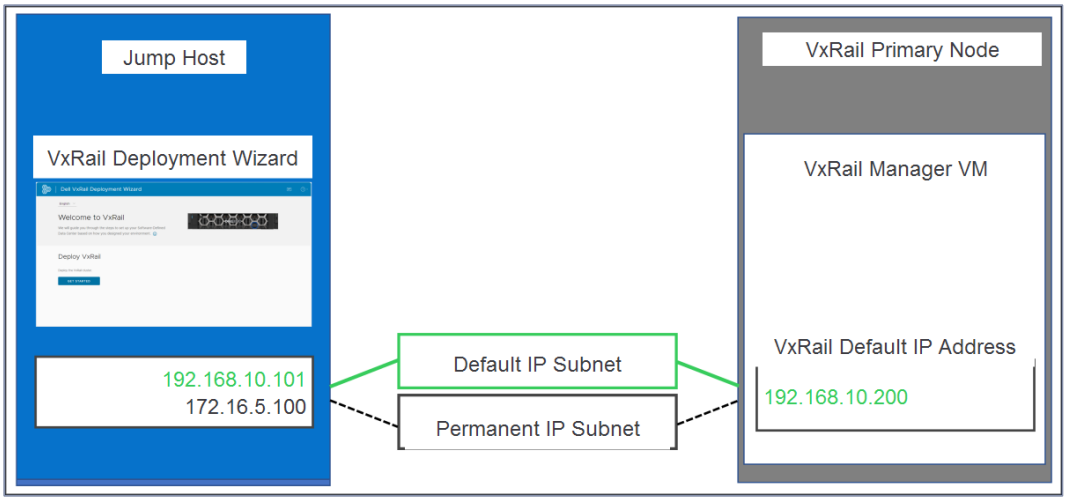
Network Access to the VxRail Manager VM

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

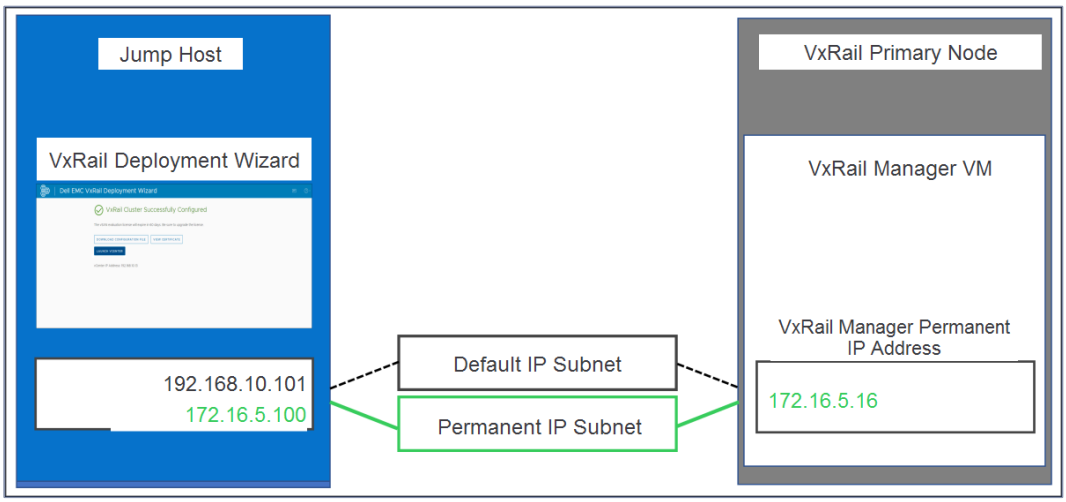
Configure the jump host with dual IP addresses. One IP address should be on the 192.168.10.x/24 subnet, and the other on the same subnet as the permanent IP address of the VxRail Manager. The jump host must be able to connect to the VxRail Manager default IP address at the start of the VxRail deployment.



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.



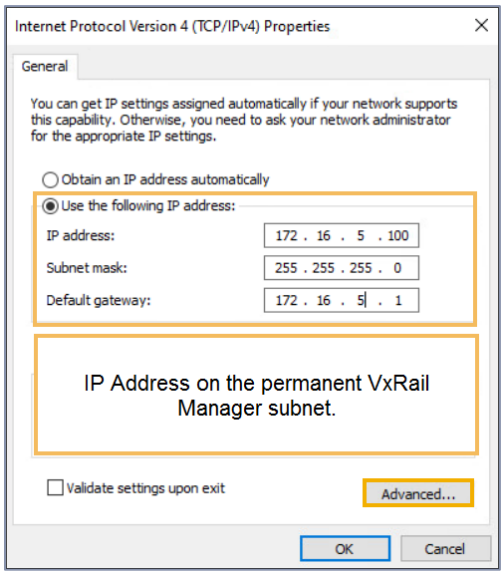
End of deployment - Jump host communicates with VxRail Manager with the permanent IP Address 172.16.5.16

Connect Service Laptop or Jump Host

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

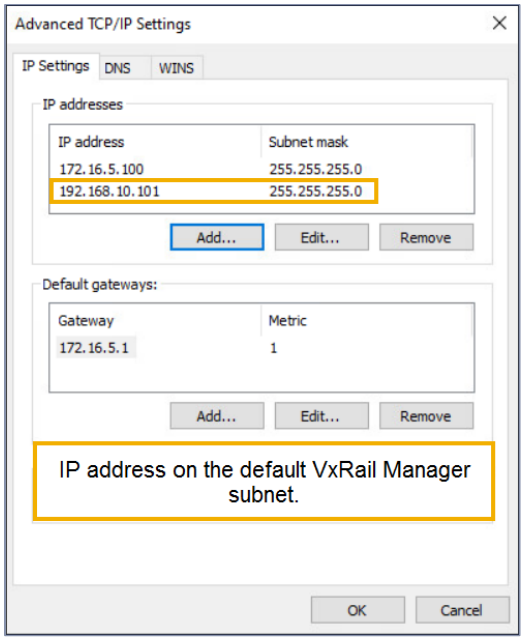
High-level steps run from a Windows jump host:

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.



Jump host - Advanced TCP/IP Settings

Configure VxRail Manager VM Network Settings

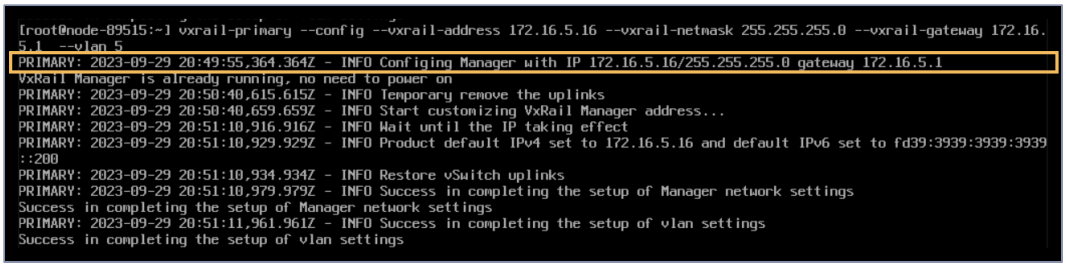
If deploying VxRail by connecting to the permanent IP address, there is no requirement for dual IP addresses on the jump host. The jump host only has to be able to connect to the permanent IP address, which must be configured before beginning the deployment.

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:



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

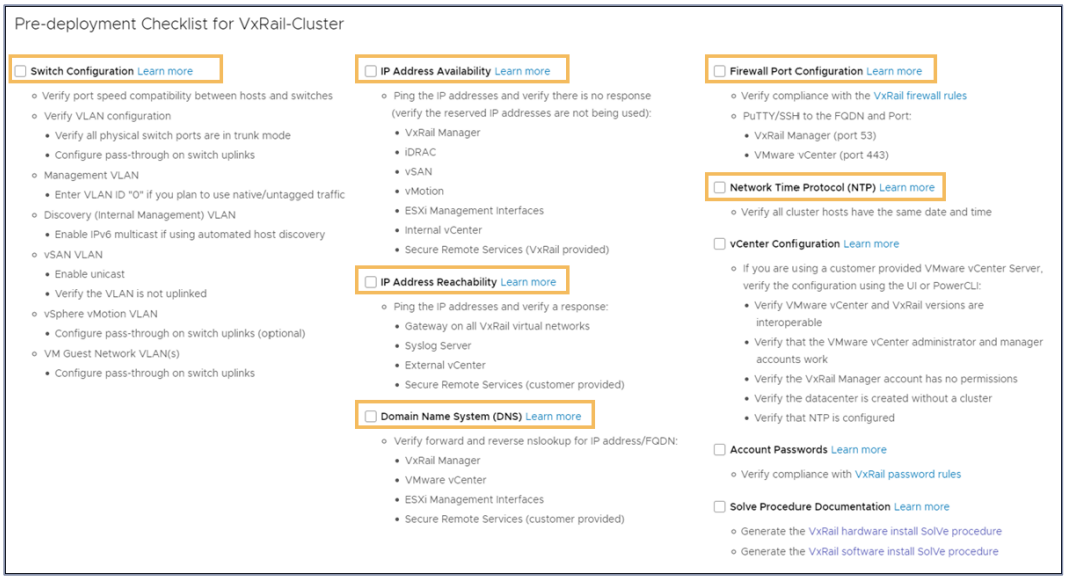
Manually Validate ToR Switch Configuration

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.



VxRail Configuration Portal - Pre-deployment Checklist

Perform network validations for:

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

- 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                                 A Eth1/1/17-1/1/18,1/1/20-1/1/32
    10     Active    vMotion                        T Eth1/1/1-1/1/16
    20     Active    vSAN                           T Eth1/1/1-1/1/16
    1751   Active    External_Mgmt                  A Eth1/1/1-1/1/16,1/1/19
    1761   Active    VM Customer Network            T 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.

```
DTES-VxRail-ToR# show interface status

------------------------------------------------------------------------------------------------
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.

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.

```
DTES-VxRail-ToR# show spanning-tree vlan 1751
Spanning tree enabled protocol rapid-pvst
VLAN 1751
Executing IEEE compatible Spanning Tree Protocol
Root ID     Priority 34519, Address 0c17.e76e.9d00
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 34519, Address 0c17.e76e.9d00
We are the root of VLAN 1751
Configured hello time 2, max age 20, forward delay 15
Flush Interval 200 centi-sec, Flush Invocations 6
Flush Indication threshold 5
Interface                                                    Designated
Name              PortID    Prio      Cost      Sts      Cost      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.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
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
Reply from 192.168.10.90: bytes=32 time<1ms TTL=64
Reply from 192.168.10.90: bytes=32 time<1ms TTL=64
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>
```

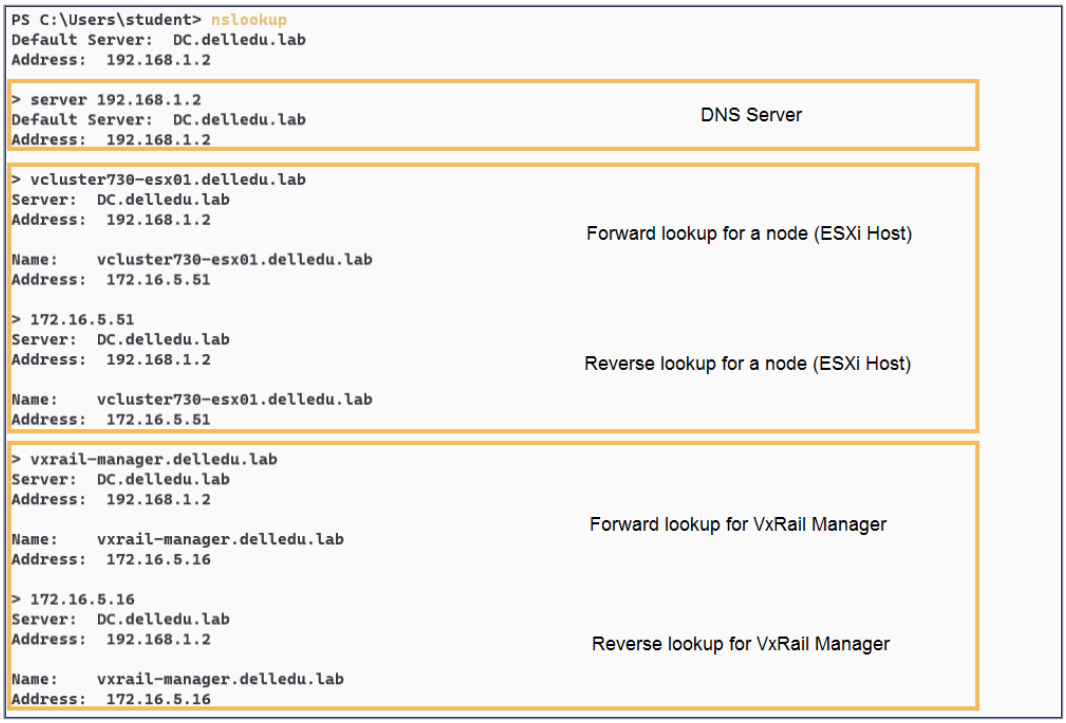
Example of a successful ping test

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

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.



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>

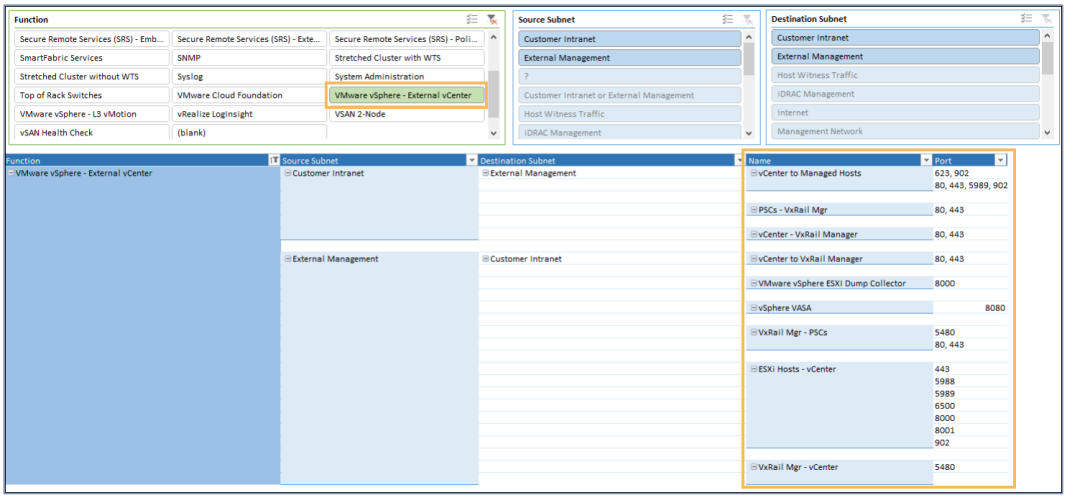
```
C:\Users\Administrator>w32tm /stripchart /computer:192.168.10.1 /samples:10
Tracking 192.168.10.1 [192.168.10.1:123].
Collecting 10 samples.
The current time is 2/11/2022 1:47:52 PM.
13:47:52, d:+00.0005321s o:+00.0001595s  [                       *                       ]
13:47:54, d:+00.0004377s 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.



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.

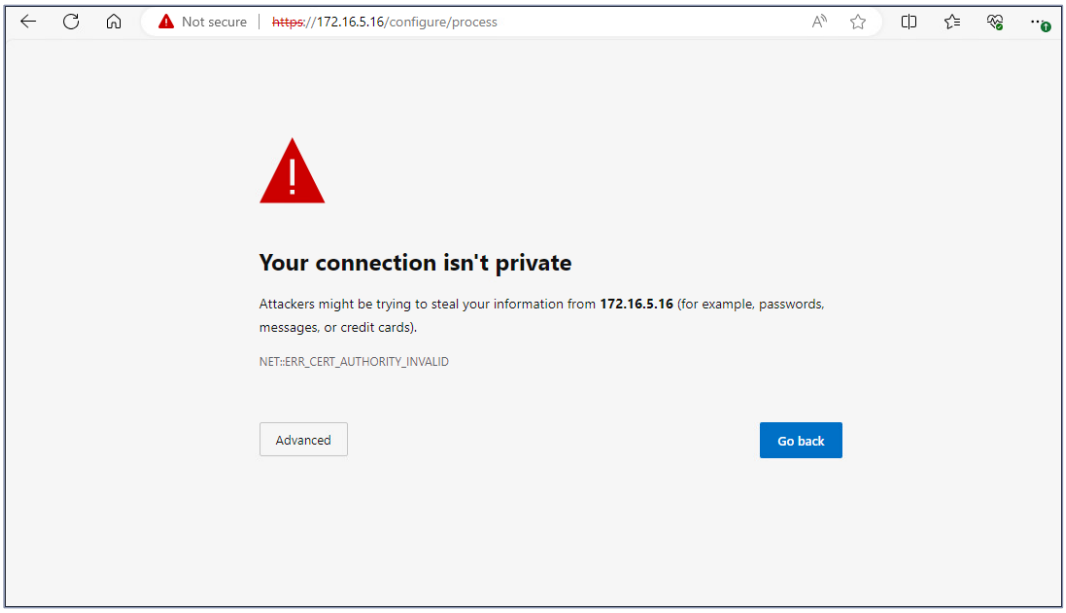
Lab Tasks

- 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.

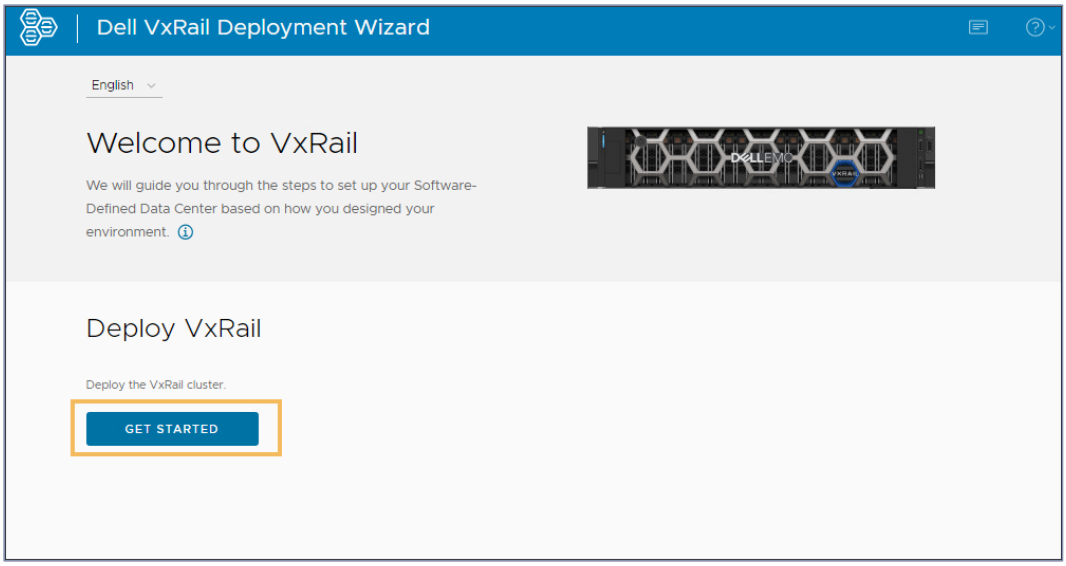


Browser Safety Warning - Chrome

VxRail Deployment Wizard Landing Page

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

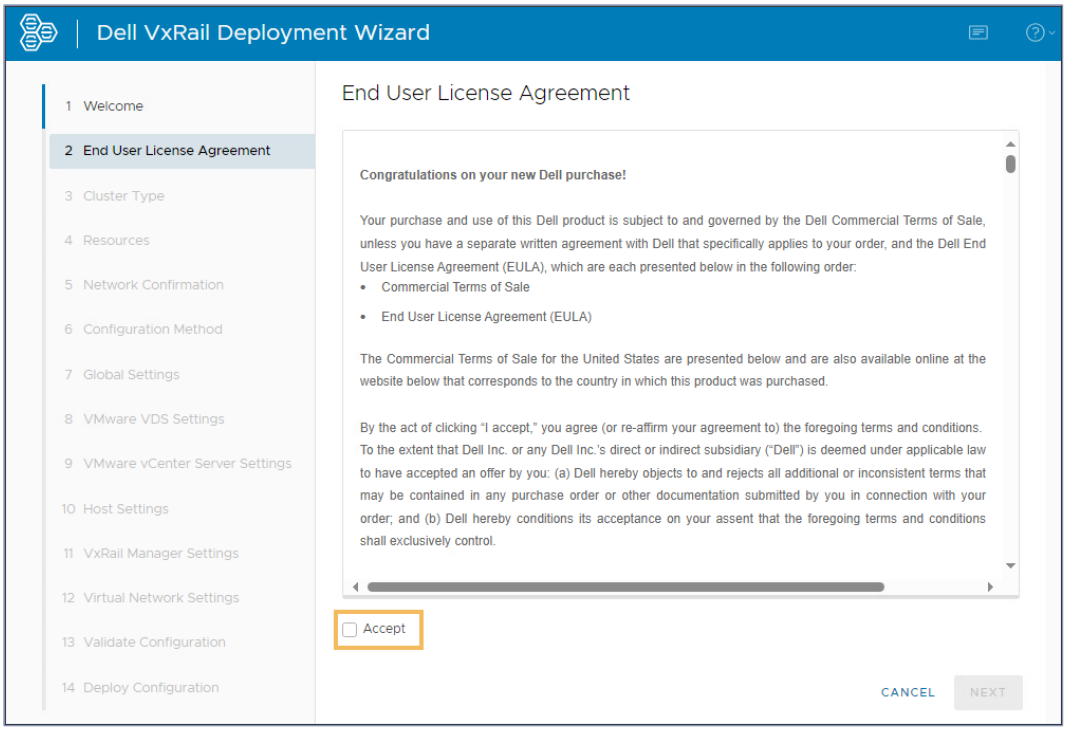
To start the VxRail configuration, click **GET STARTED**.



Deployment Wizard Landing Page

Software License and Maintenance Agreement

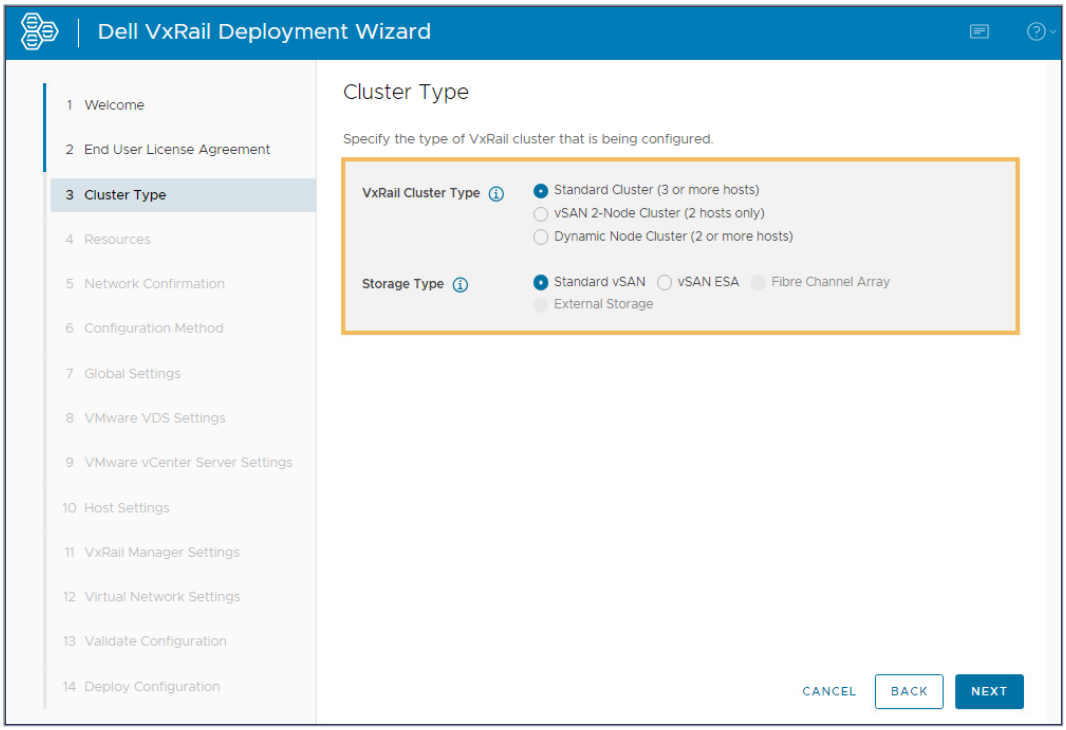
The **End User License Agreement** page of the wizard includes the Commercial Terms of Sale and the End User License Agreement (EULA). The EULA must be accepted to continue the configuration.



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.

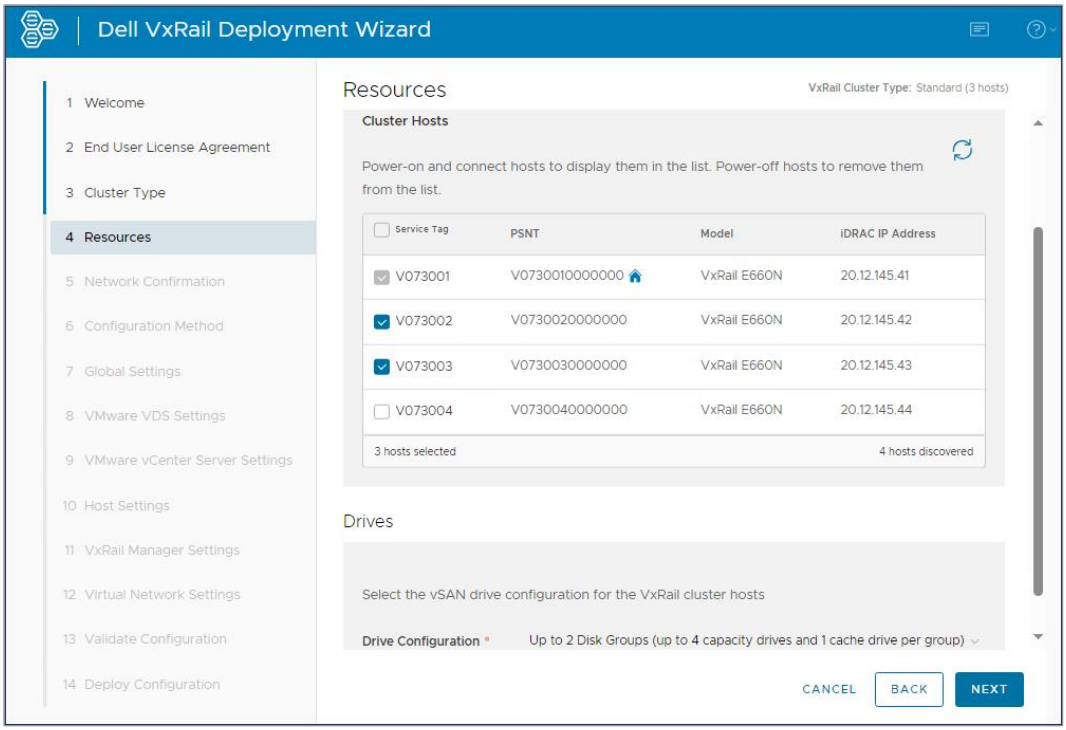


Cluster Type - Selections for a standard cluster

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.

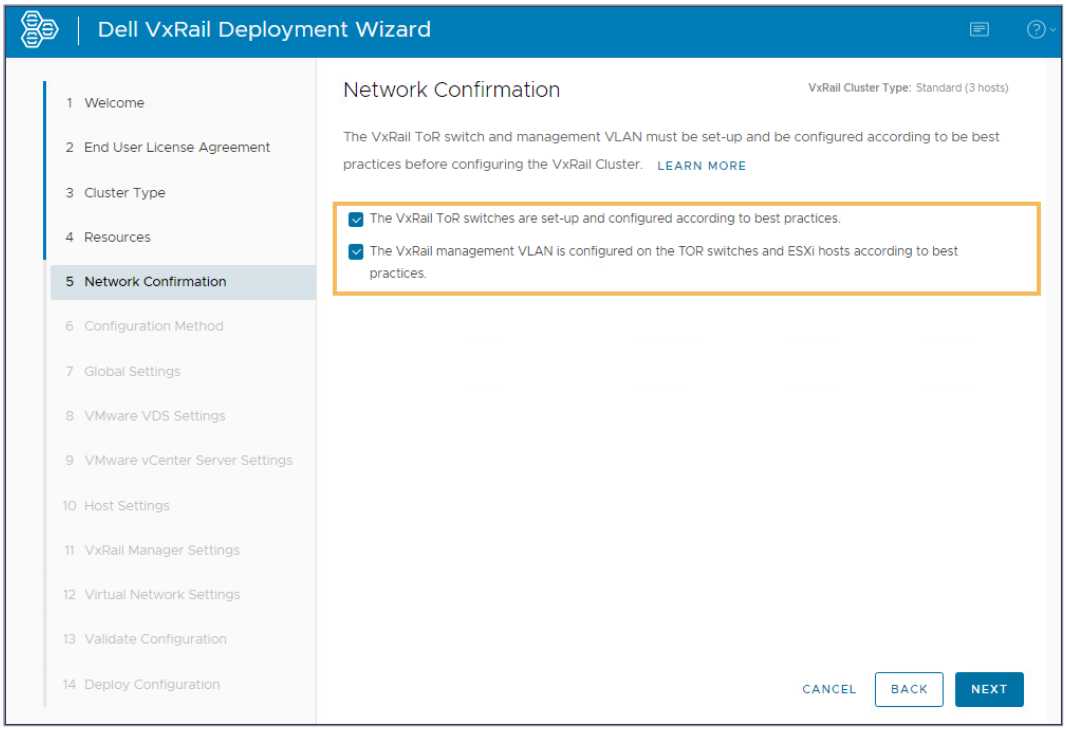


Discovered Resources

Network Confirmation

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

Select the checkboxes to acknowledge each statement.



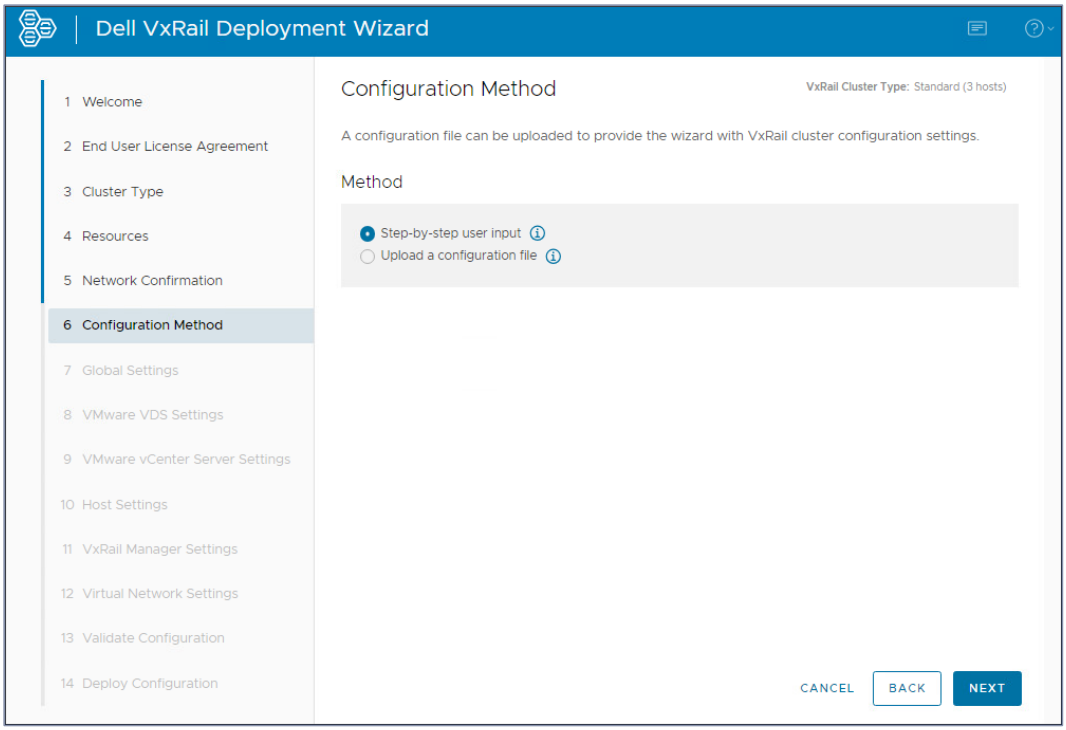
Network Confirmation

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.



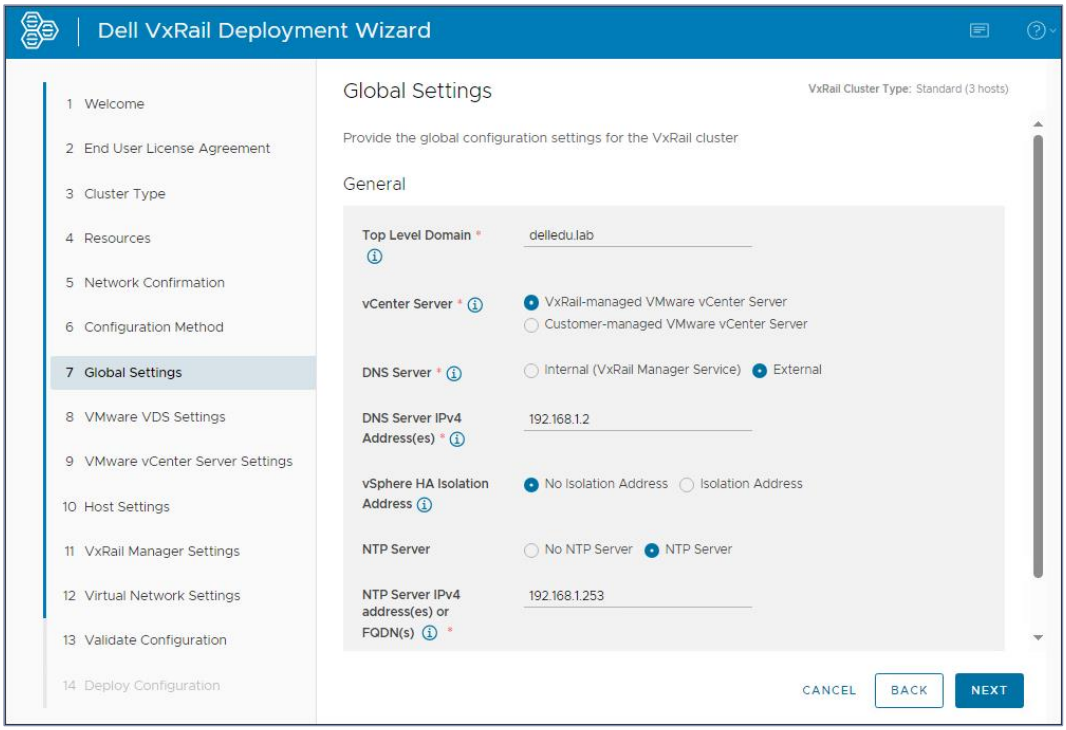
Configuration Method

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



Global Settings

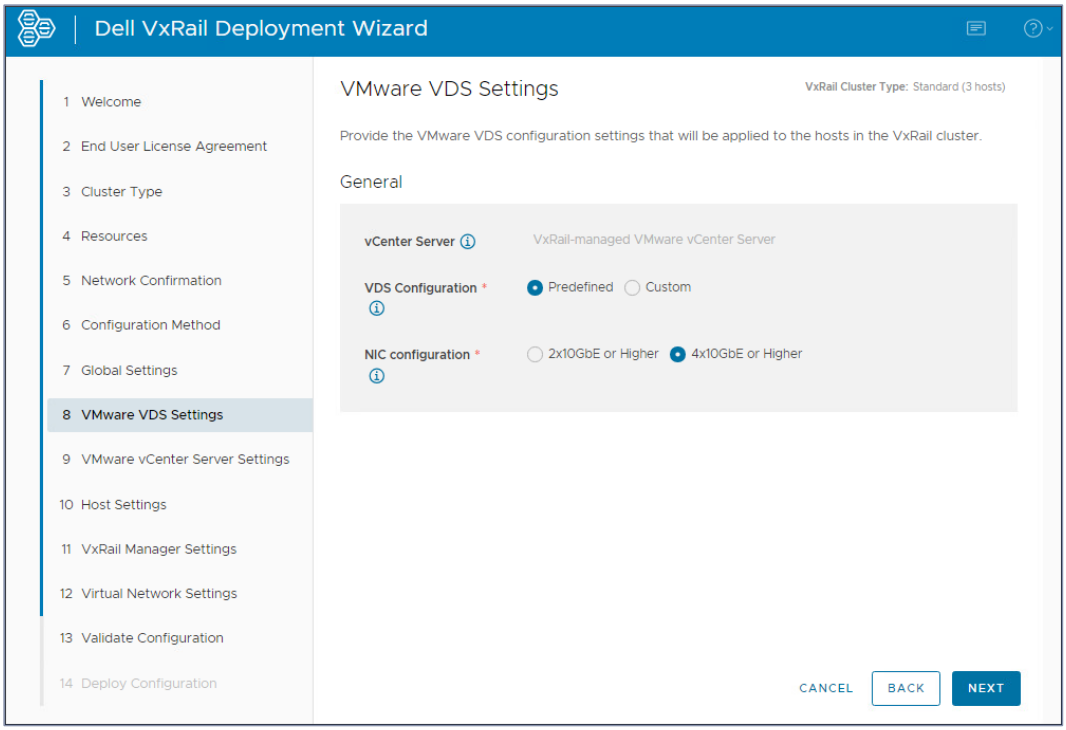
Tip: A comma-separated list of IP addresses (DNS, NTP, Syslog) or Hostnames (NTP and Syslog) can be used when entering multiple IP addresses.

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:

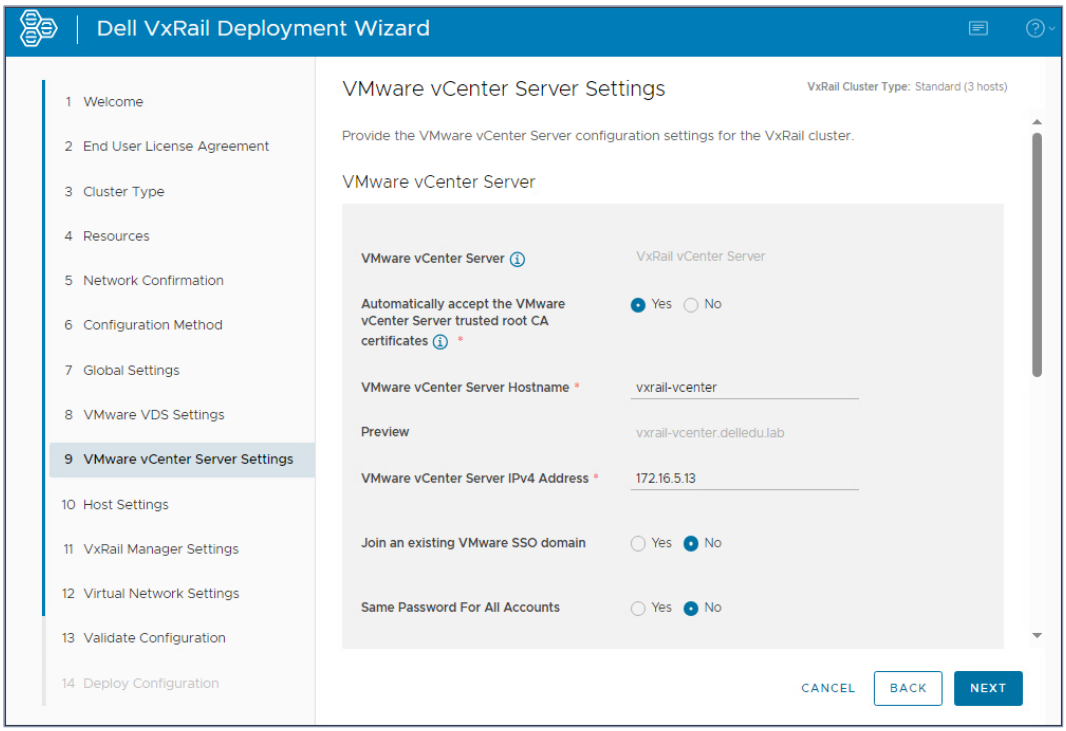
1. The **Predefined** VDS Configuration provides a default configuration that is based on the number of NICS selected.
2. The **Custom** VDS Configuration allows flexibility in the virtual network configuration.



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.



vCenter Server Settings

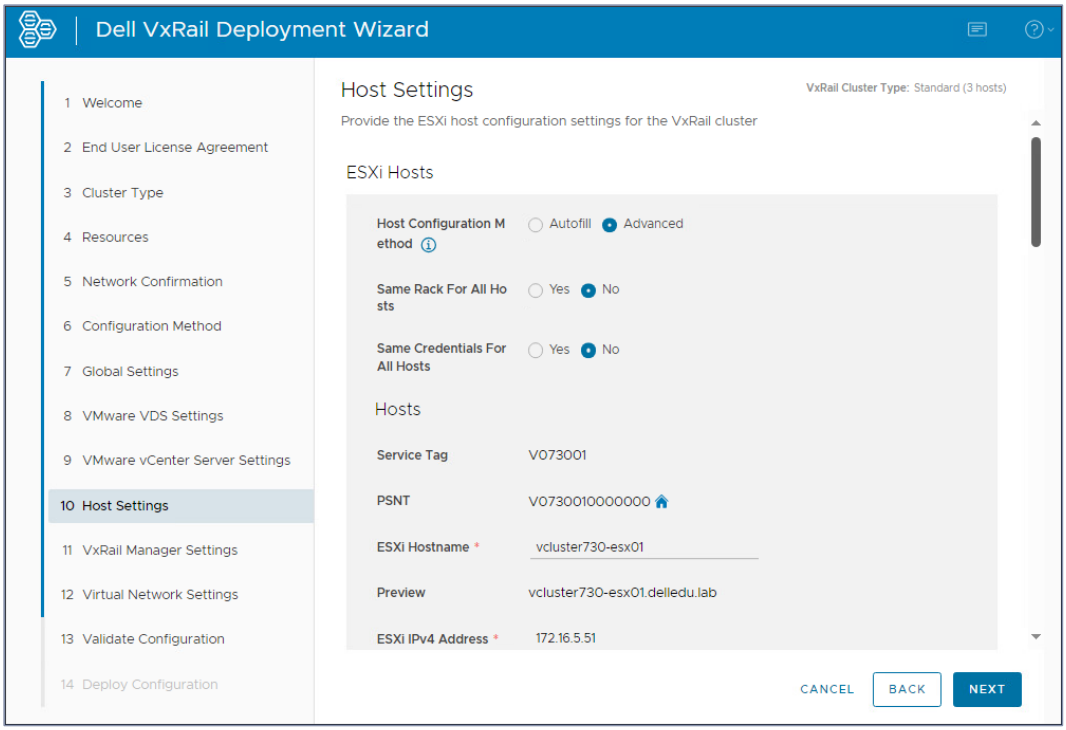
Important: If the configuration file is uploaded, the file will not have the passwords and would require manual entry.

Host Settings

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

There are two Host Configuration Methods:

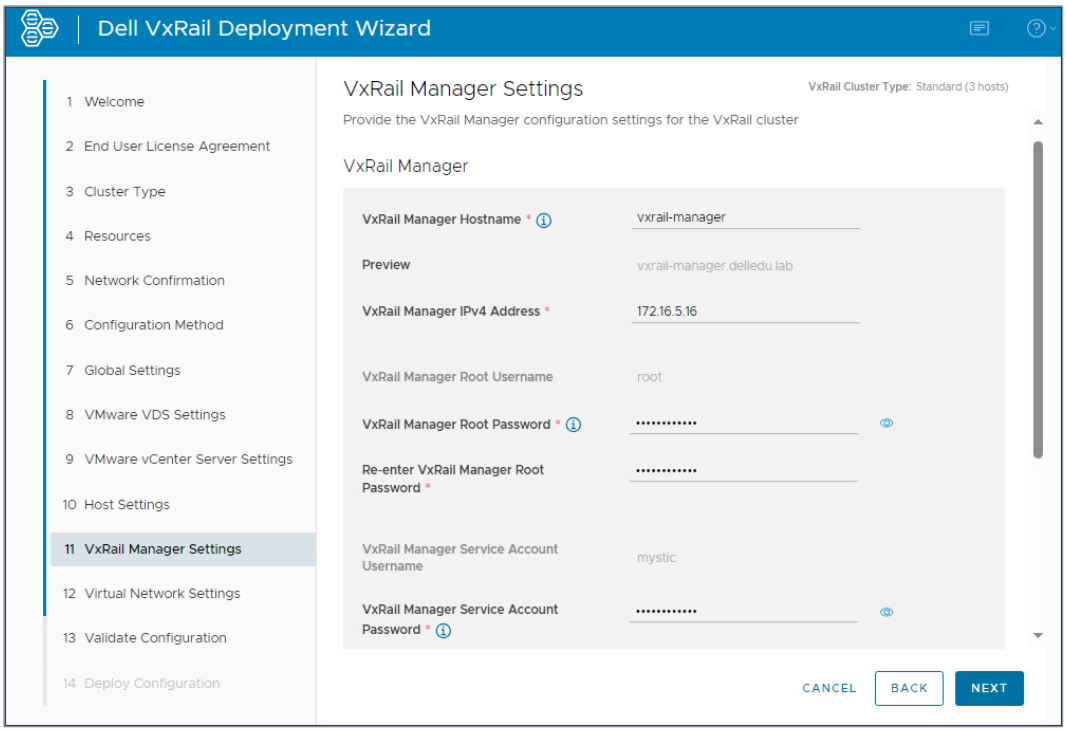
1. The **Autofill** method enables hostnames to be generated based on a pattern and assigns IP addresses sequentially from a starting IP address.
2. The **Advanced** method allows flexibility in the specification of the host configuration details, for example unique names or nonconsecutive IP addresses.



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.

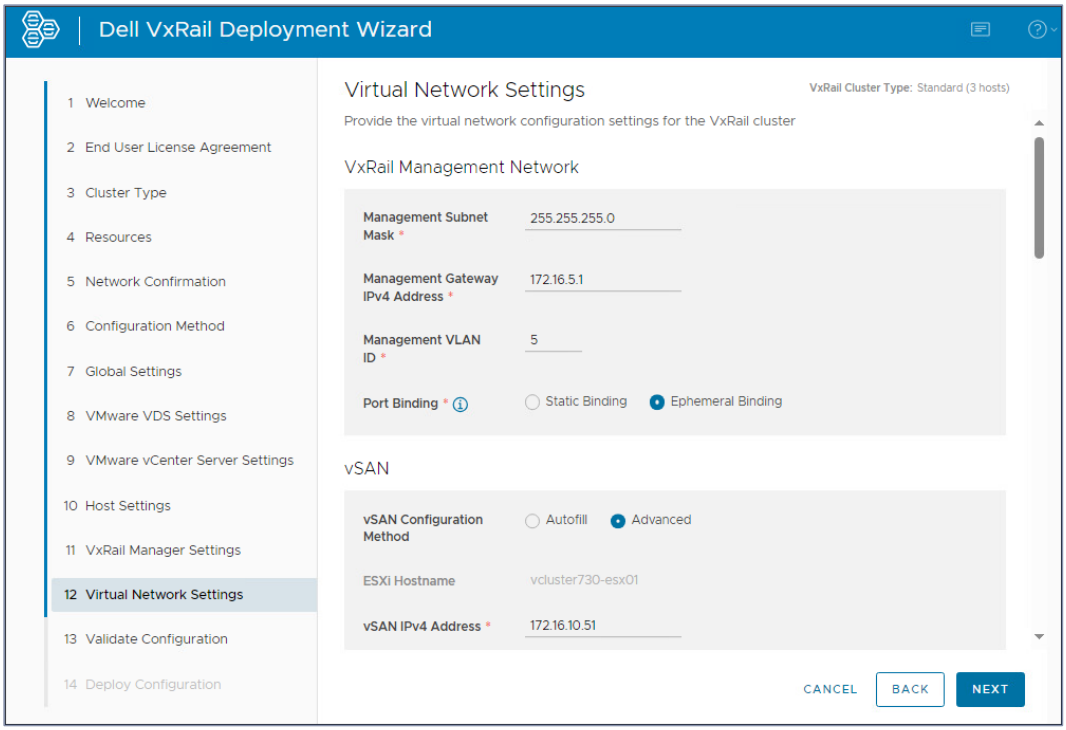


VxRail Manager Settings

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.

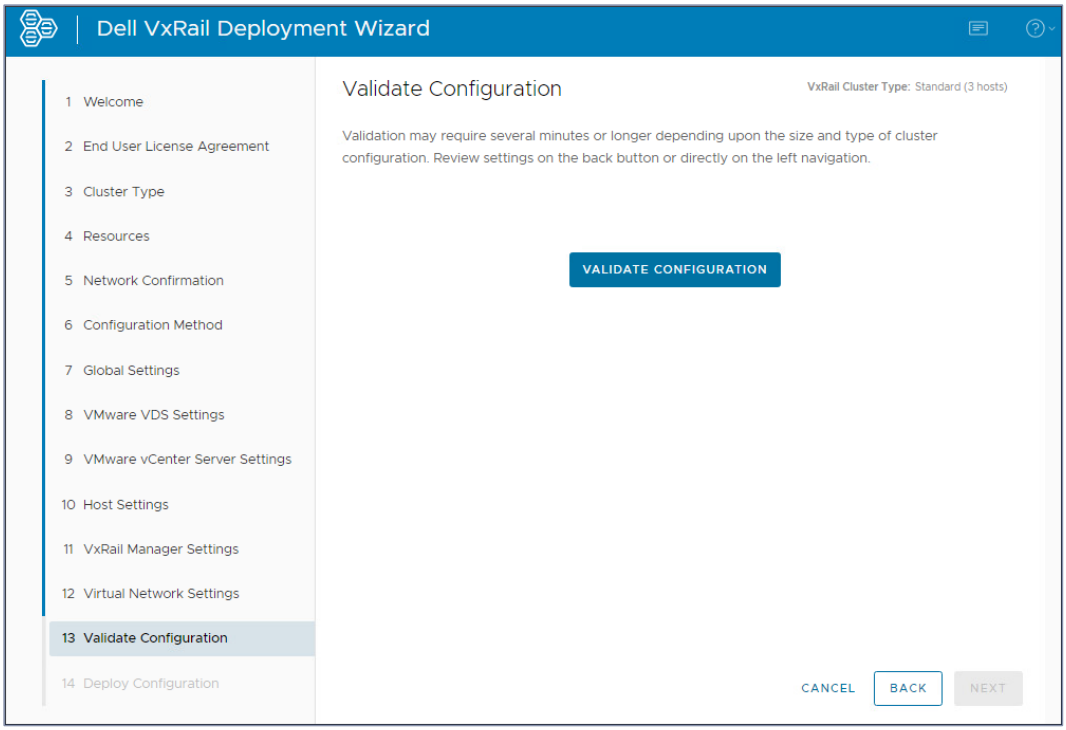


Virtual Network Settings

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.

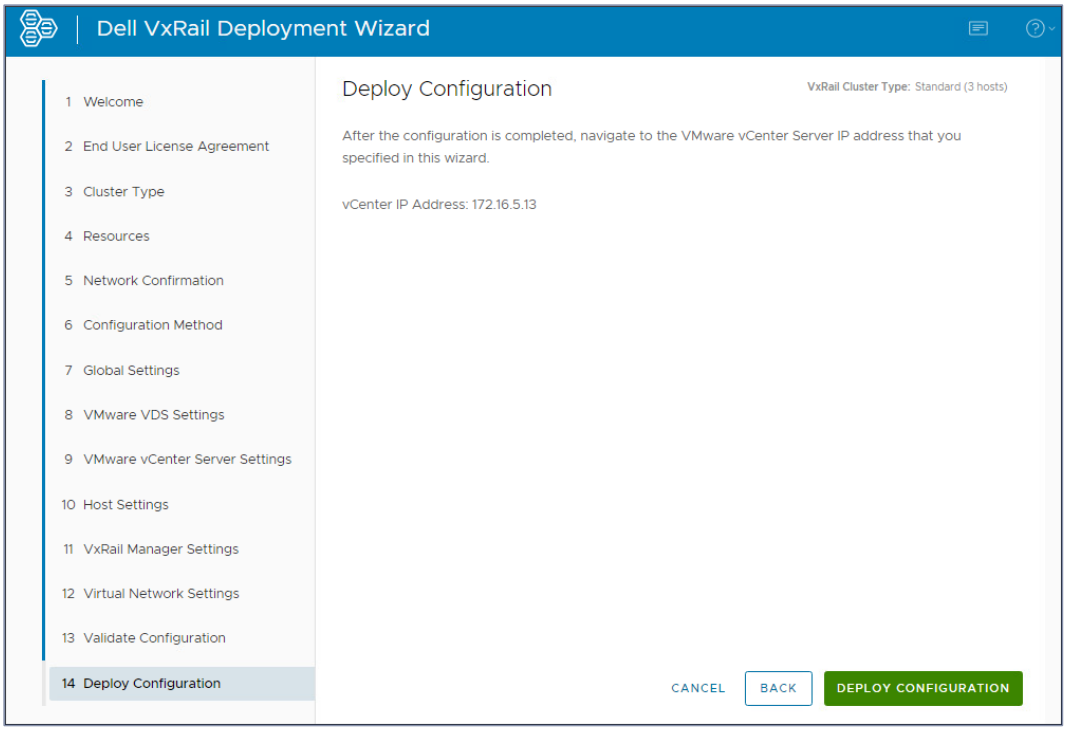


Validation Configuration

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.



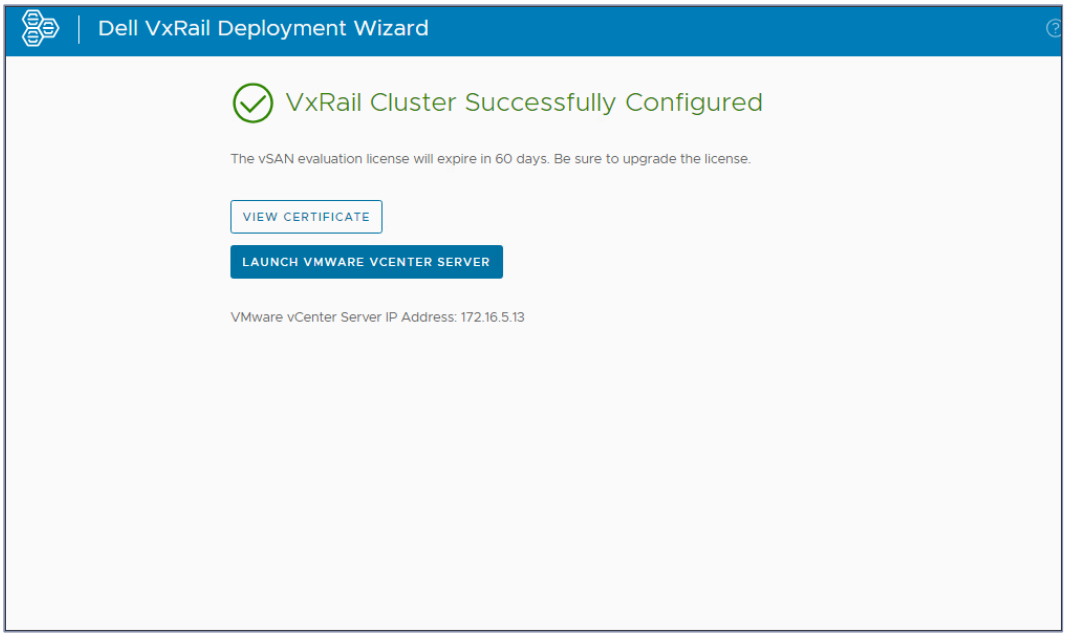
Deploy Configuration

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.



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

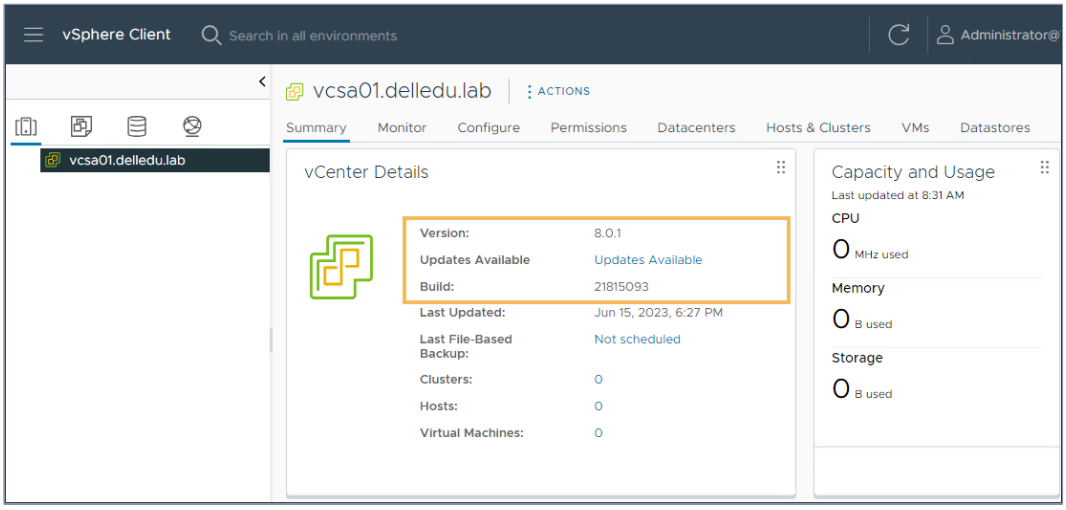
The details of the customer-supplied vCenter Server are documented in the VxRail Configuration Report that is available in the VxRail Configuration Portal. Example of a VxRail Configuration Report.

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

example, the recommended vCenter Server version for VxRail 8.0.100 is 8.0 U1a (8.0.1.00100) or later[1].

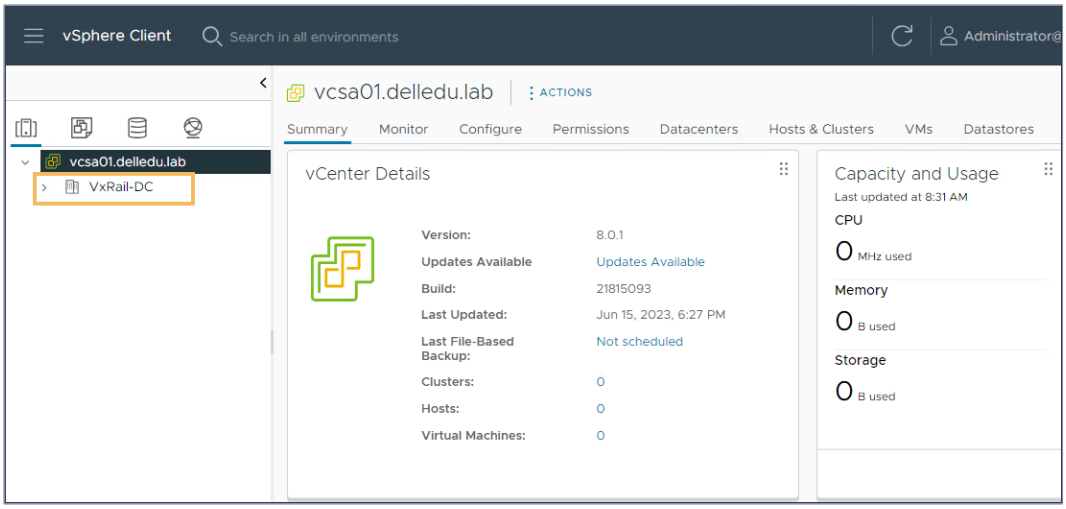


vCenter Server Version

[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.

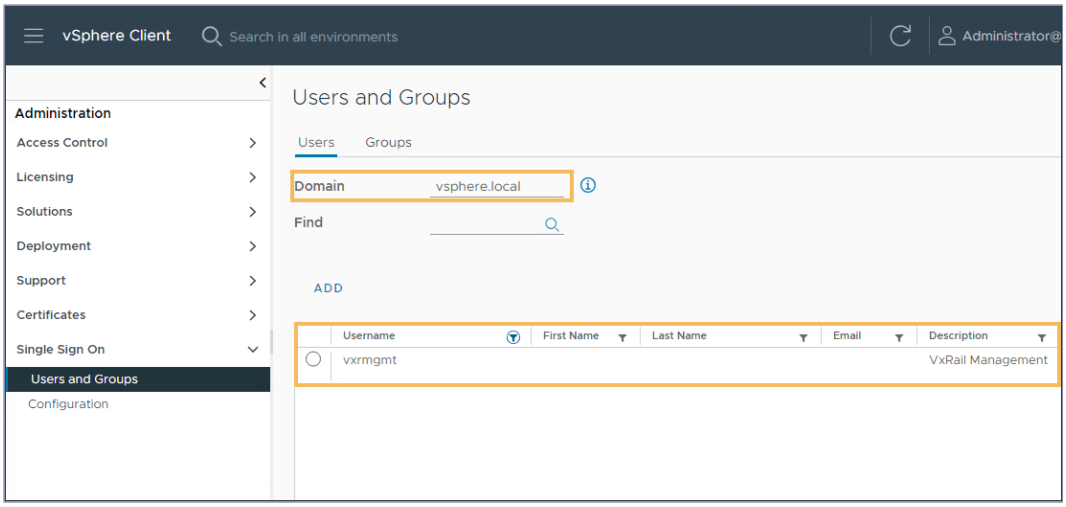


vCenter Server - Data Center created

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.



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.

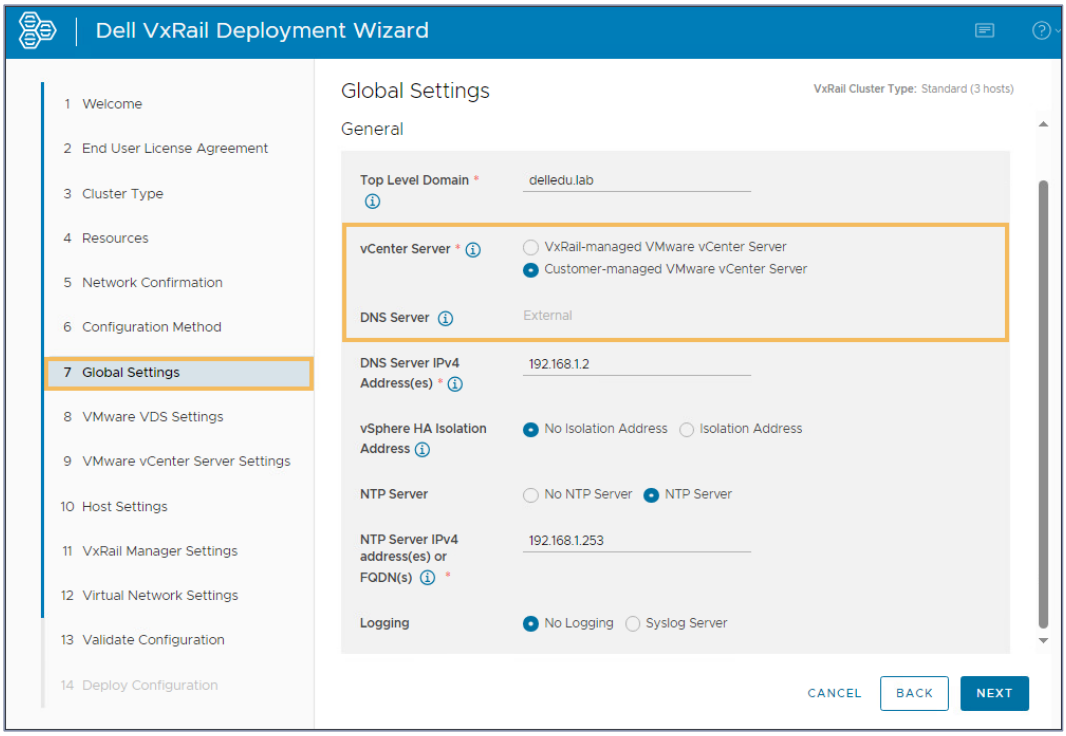
VxRail with customer-supplied vCenter Server - Deployment Wizard Settings

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**.

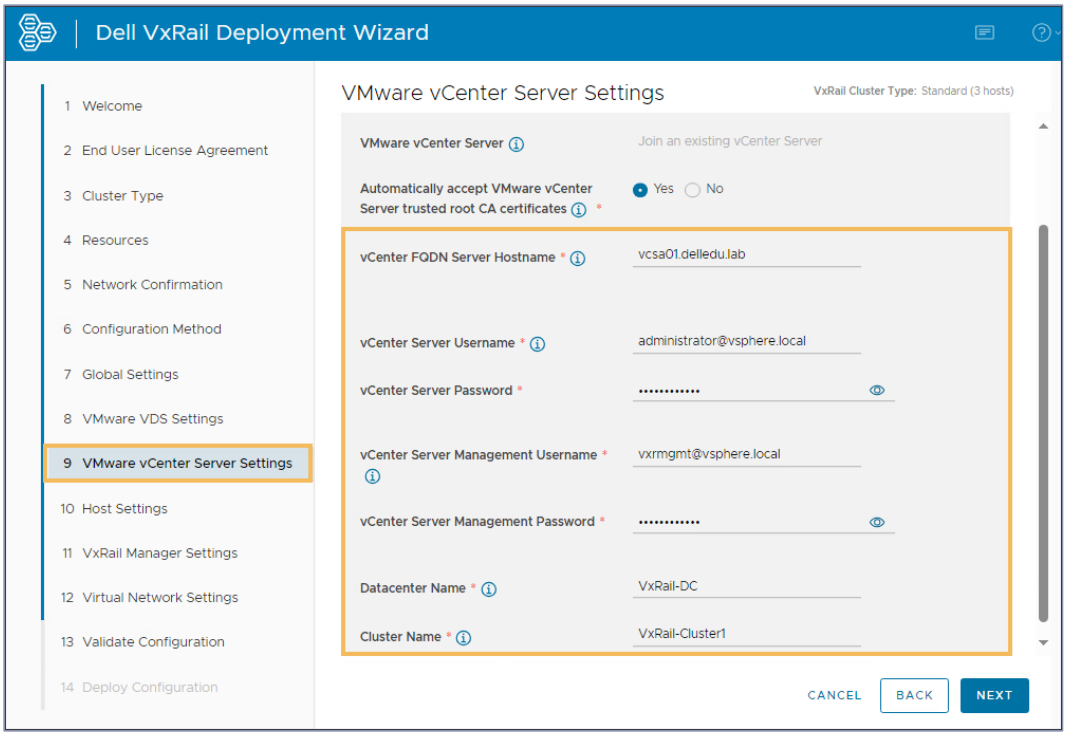


Global Settings for a customer-supplied vCenter Server

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



Customer-supplied vCenter Server Settings

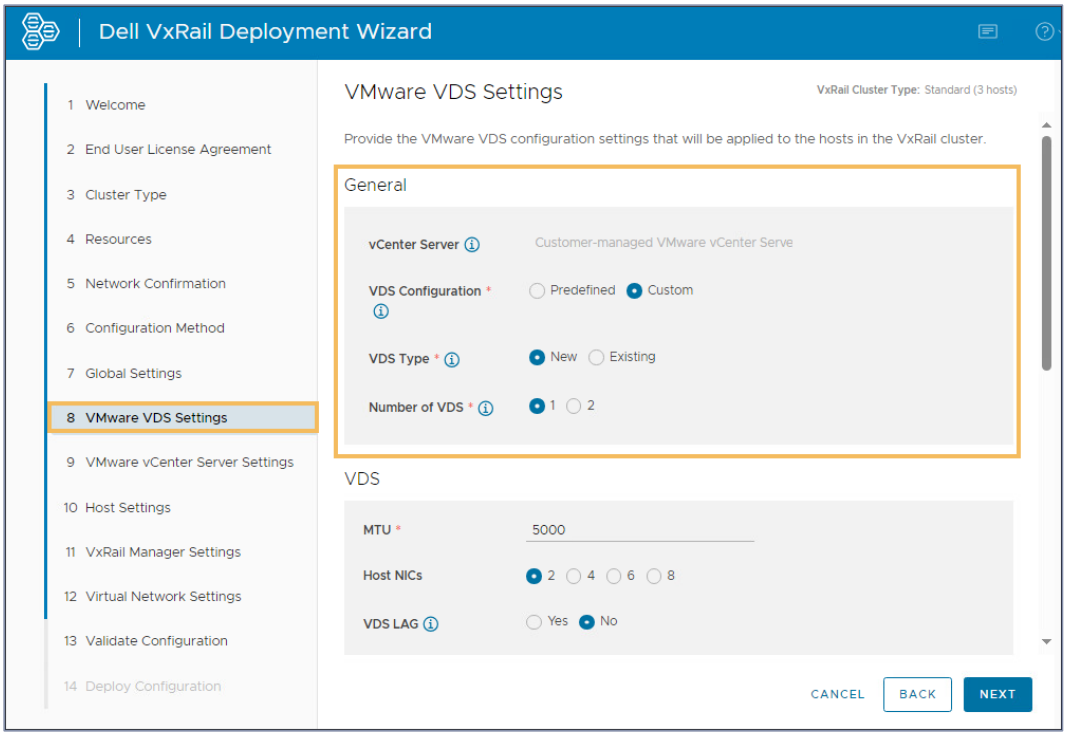
New Custom VDS - Deployment Wizard Settings

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**.

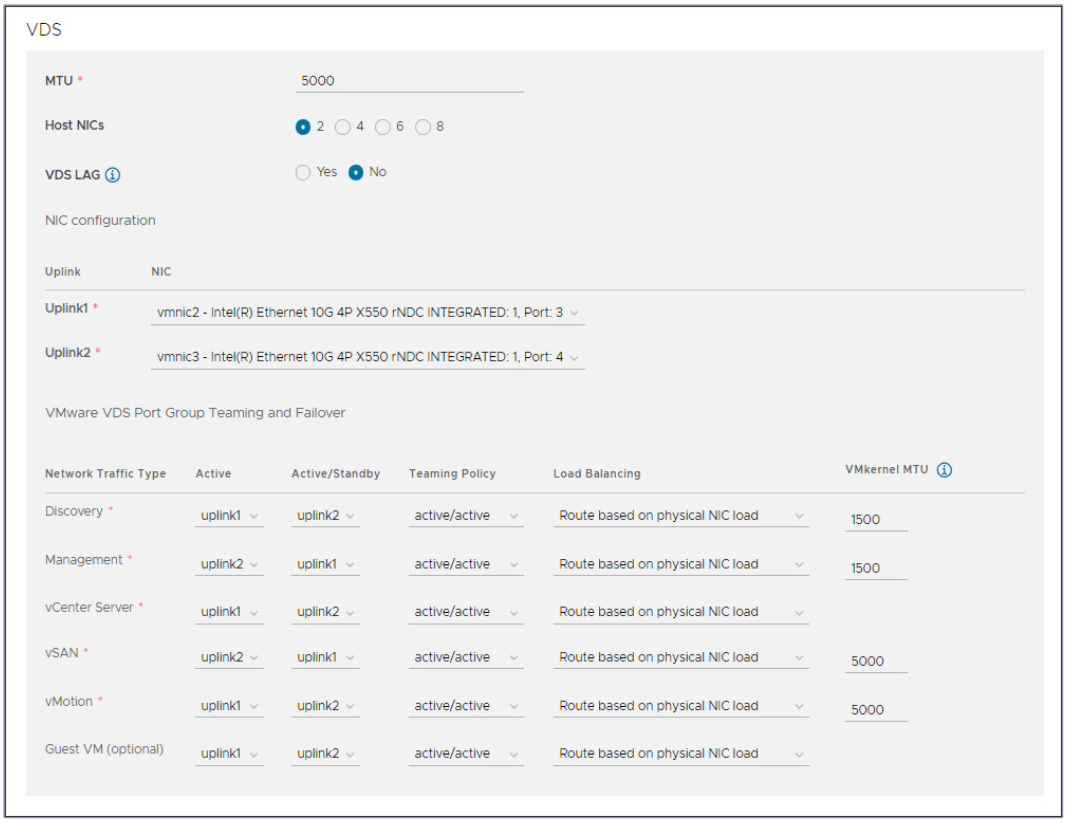


VMware Custom New VDS Settings - General

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.



VMware Custom New VDS Settings

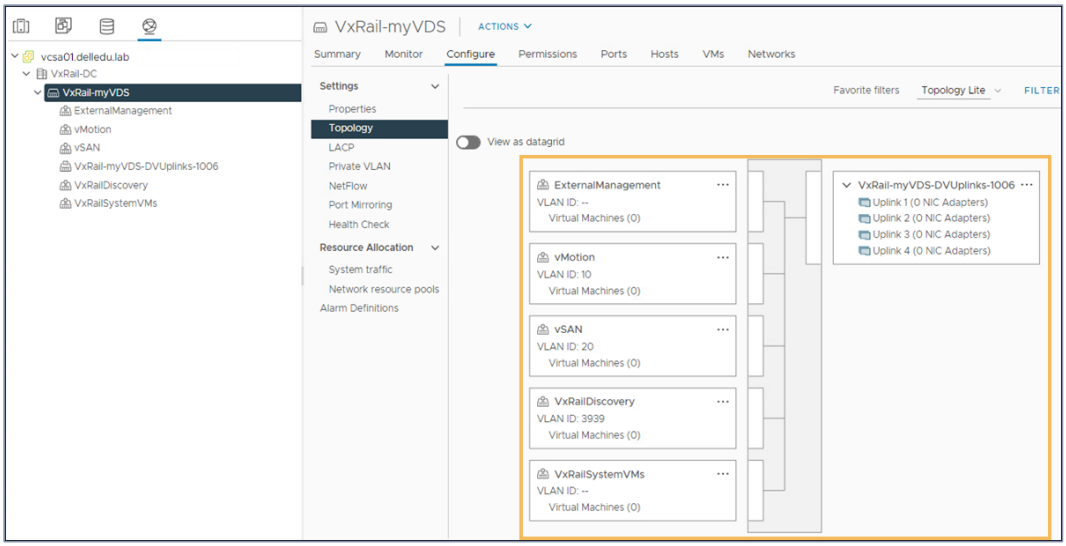
VxRail Deployment with Existing VDS

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



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

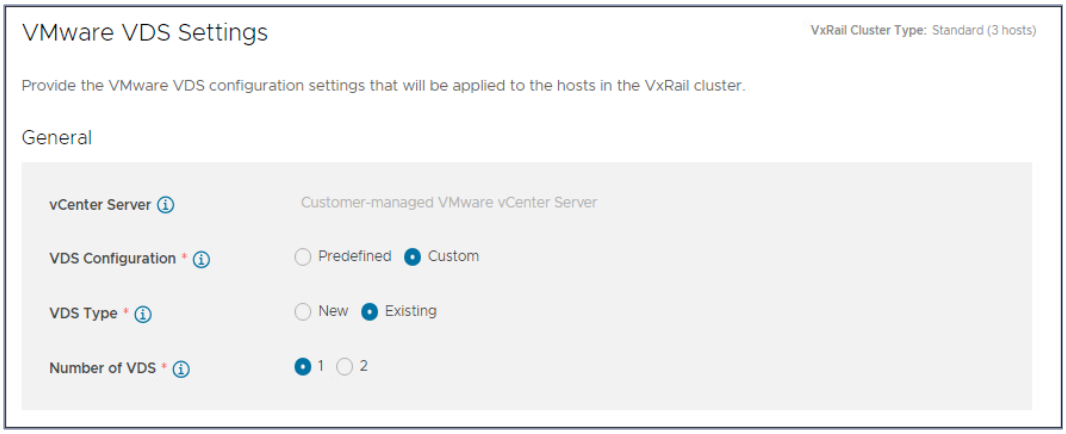
Existing Custom VDS - Deployment Wizard Settings

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**.



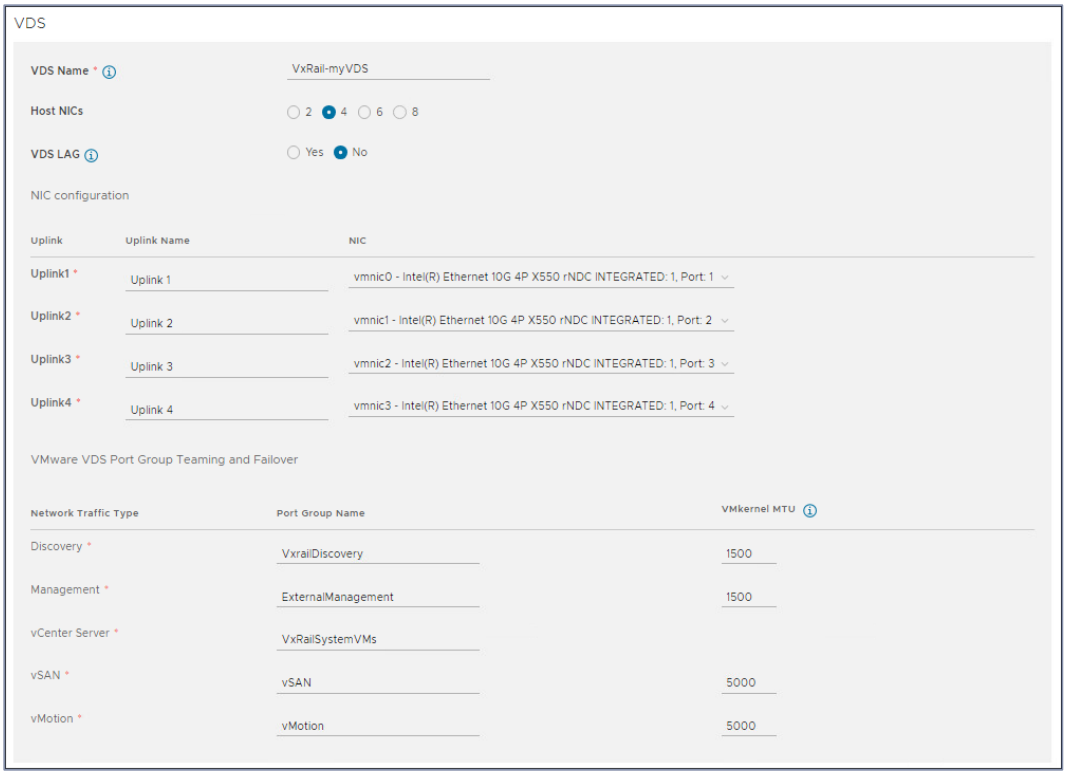
VMware Custom Existing VDS Settings - General

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.

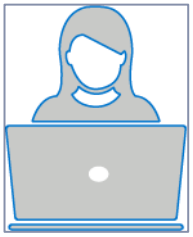


VMware Custom Existing VDS Settings - Four NICs, no LAG

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.

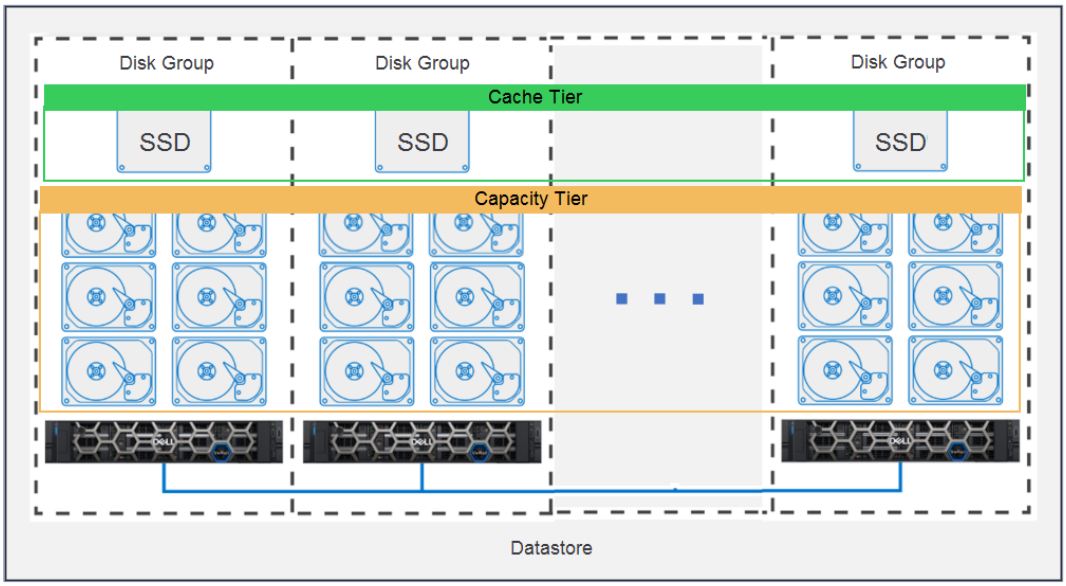
Deploy a Standard VxRail Cluster With vSAN ESA

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.

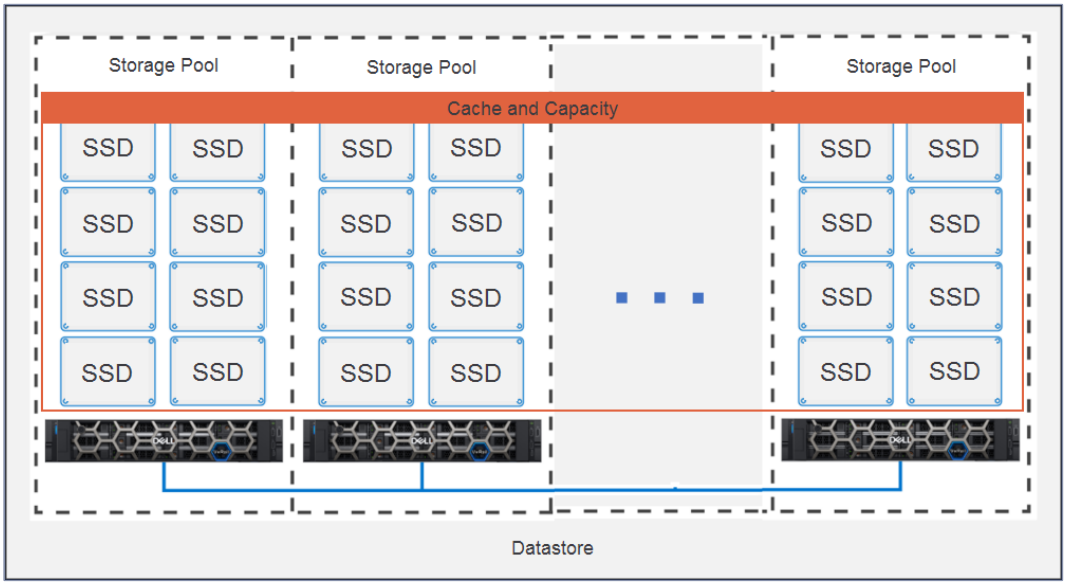


OSA Architecture

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

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.

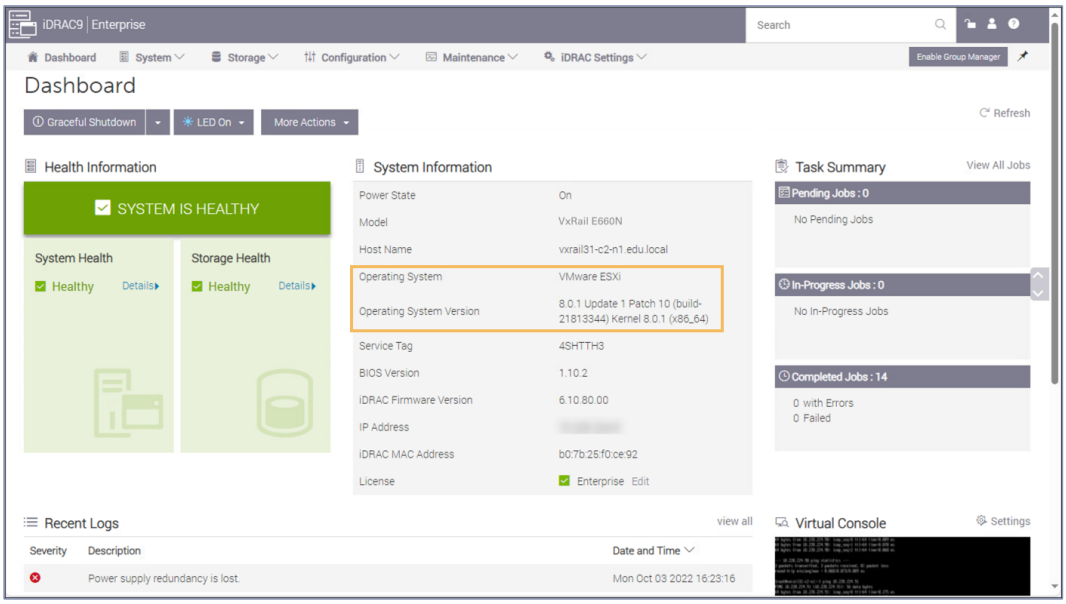
vSAN ESA Software Requirements

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.

vSphere ESXi

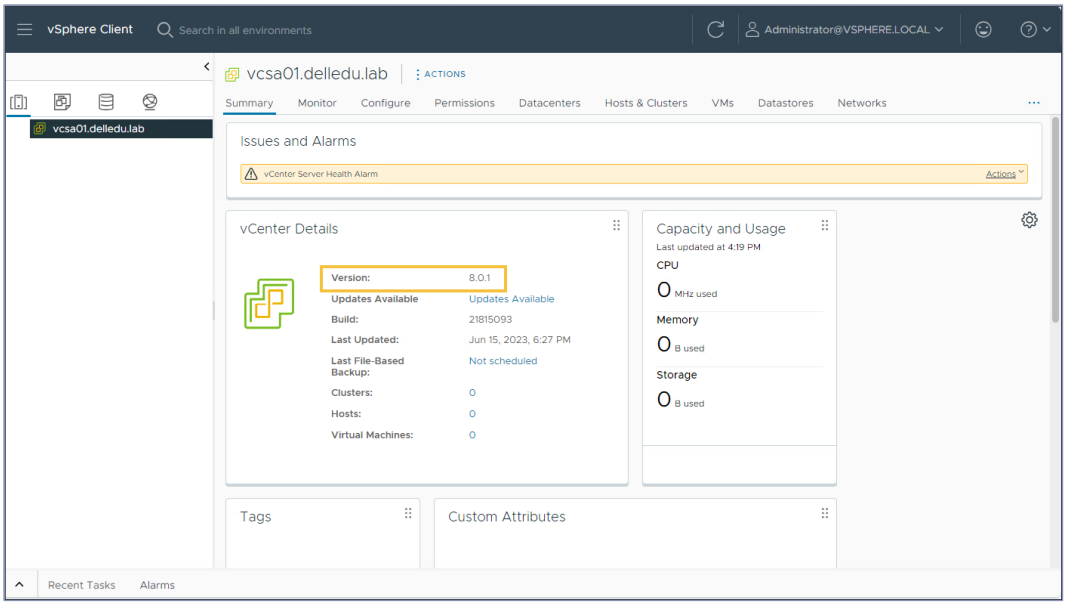
The current ESXi version on each node can be verified in the **System Information** section on the iDRAC **Dashboard**.



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.



vCenter appliance Summary tab with the vCenter 8.0 version identified

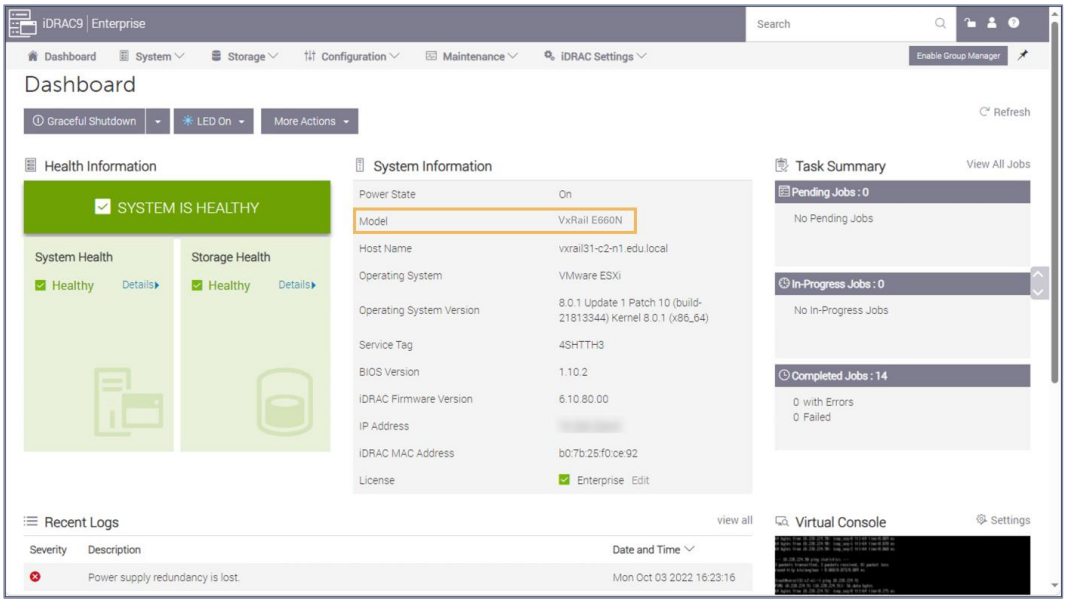
vSAN ESA Hardware Requirements

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

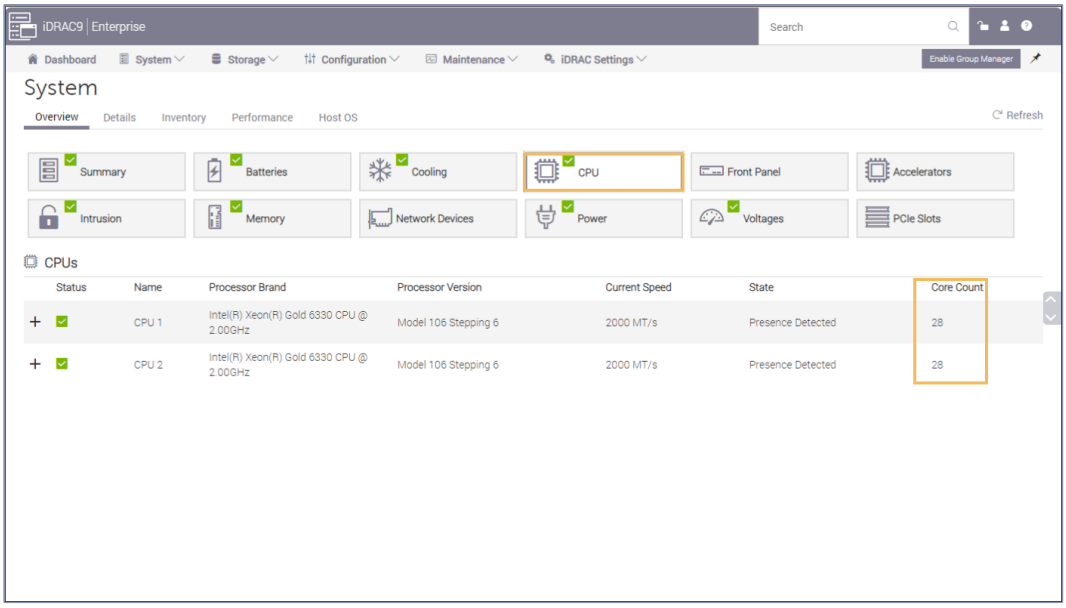
The VxRail model can be verified in the **System Information** section on the iDRAC **Dashboard**.



iDRAC Dashboard with the VxRail model identified

CPU

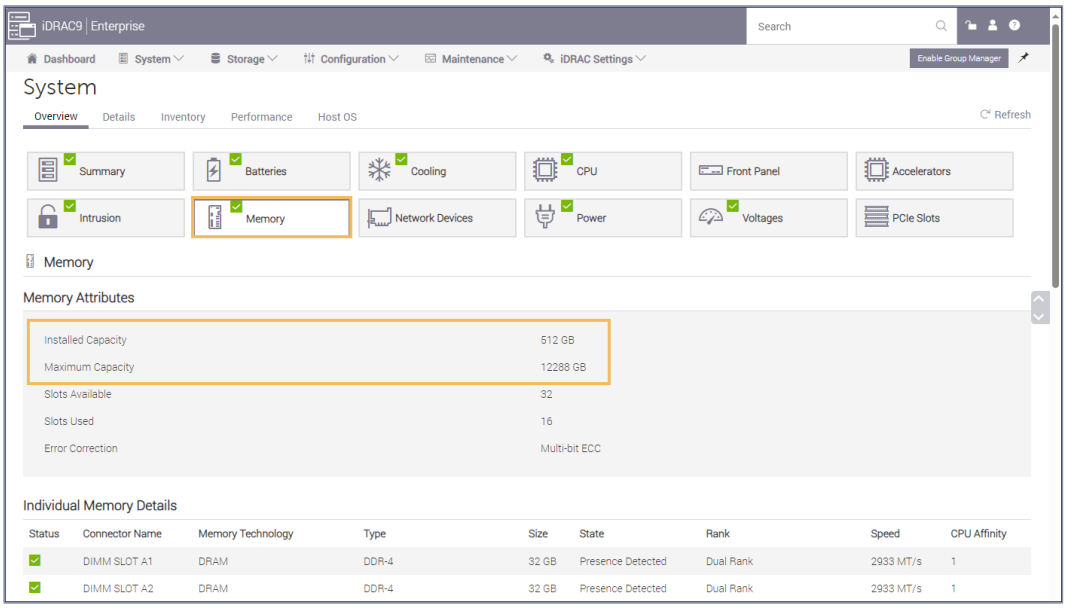
The number of CPU cores can be verified on the iDRAC **System > CPU** page. The image below shows a total of 56 cores in the node.



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

Memory

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



iDRAC System > Memory page with the memory capacity identified

vSAN ESA Drive Requirements

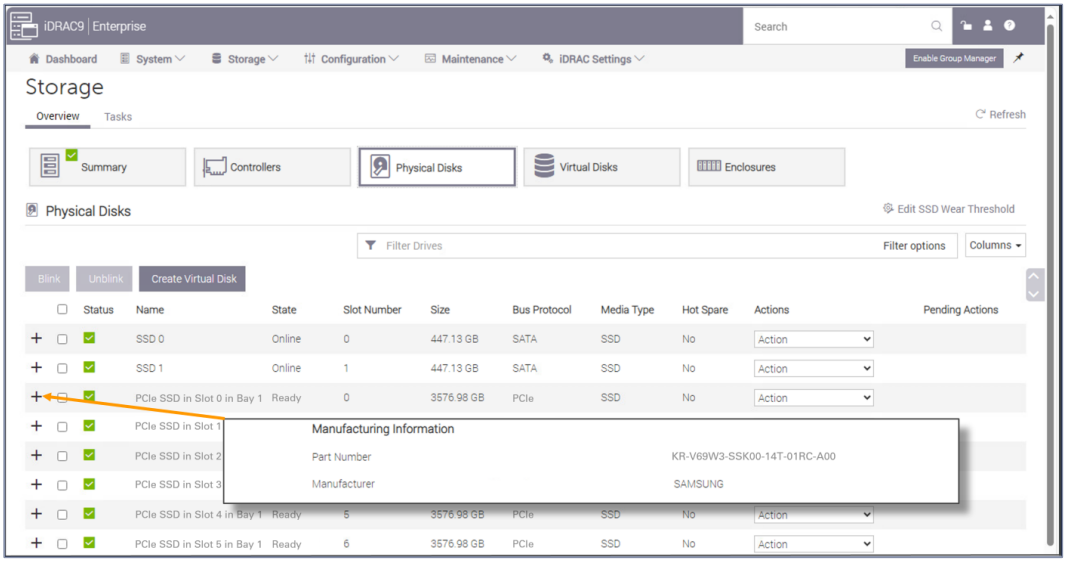
vSAN ESA is supported only with qualified NVMe drives. Depending on the VxRail model, ESA requires a minimum of four to six NVMe drives per VxRail node. Disk drives must populate the disk slots sequentially starting in slot 0. Bus protocol is PCIe for supported NVMe drives.

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**.

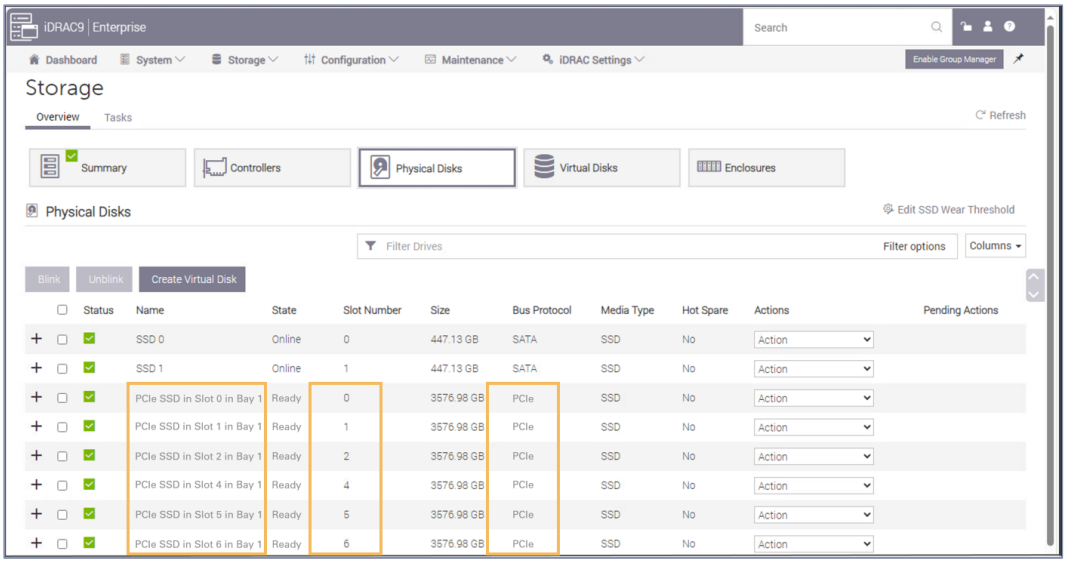
See the VxRail 8.X Support Matrix pg 57 for the complete list of supported NVMe manufacturers and models.



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.



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

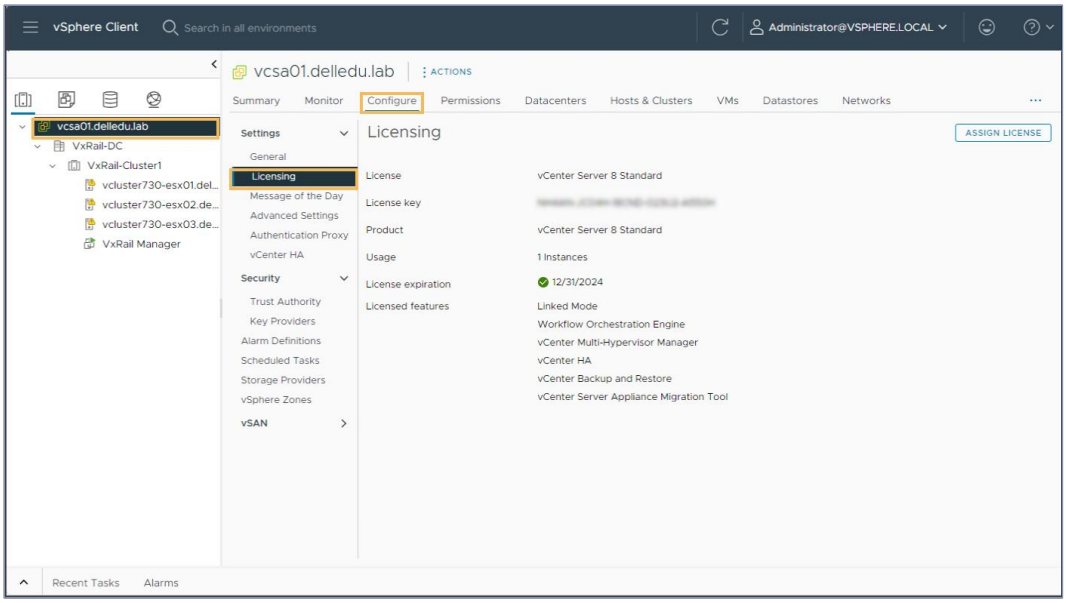
Verify vSAN ESA Licensing

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**.

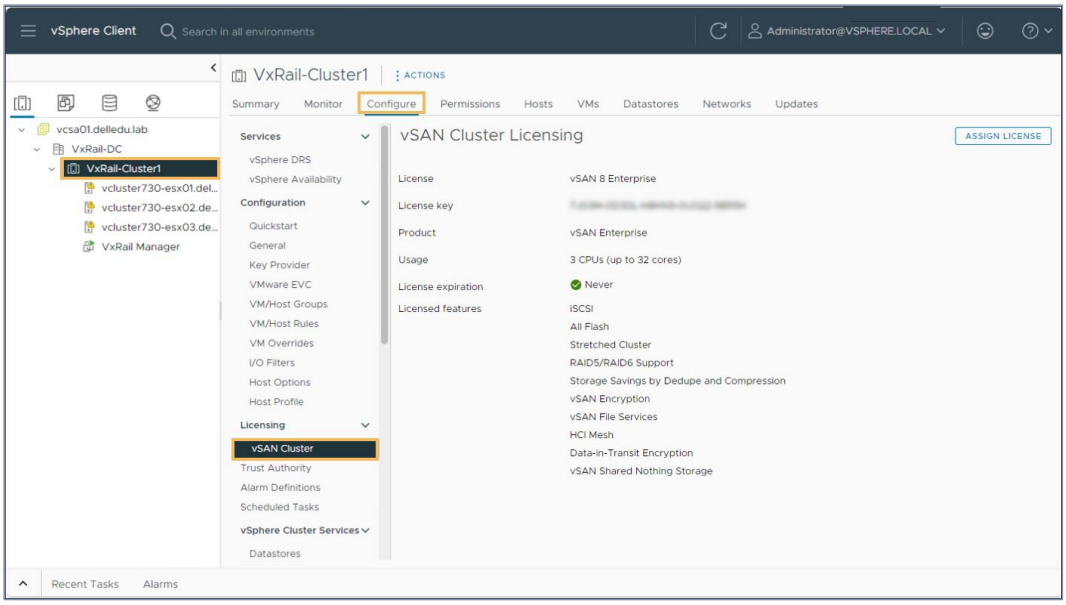


vCenter Server Configure Licensing page showing the vCenter license

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**.

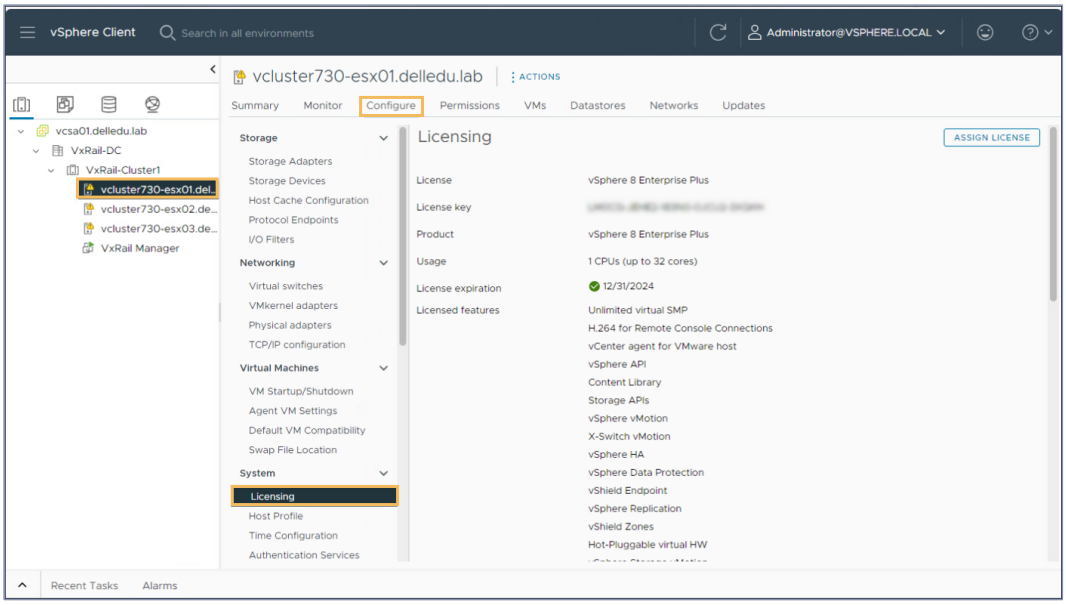


Cluster Configure vSAN Cluster page showing the vSAN license

vSphere License

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

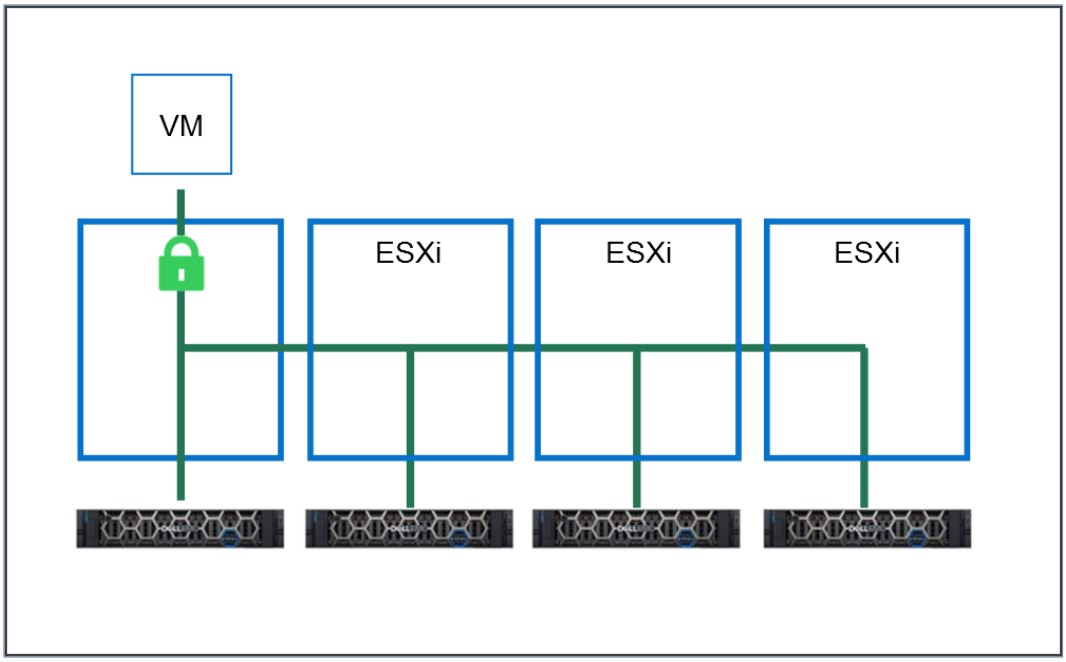
To verify the vSphere license, select each node and go to **Configure > System > Licensing**.



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

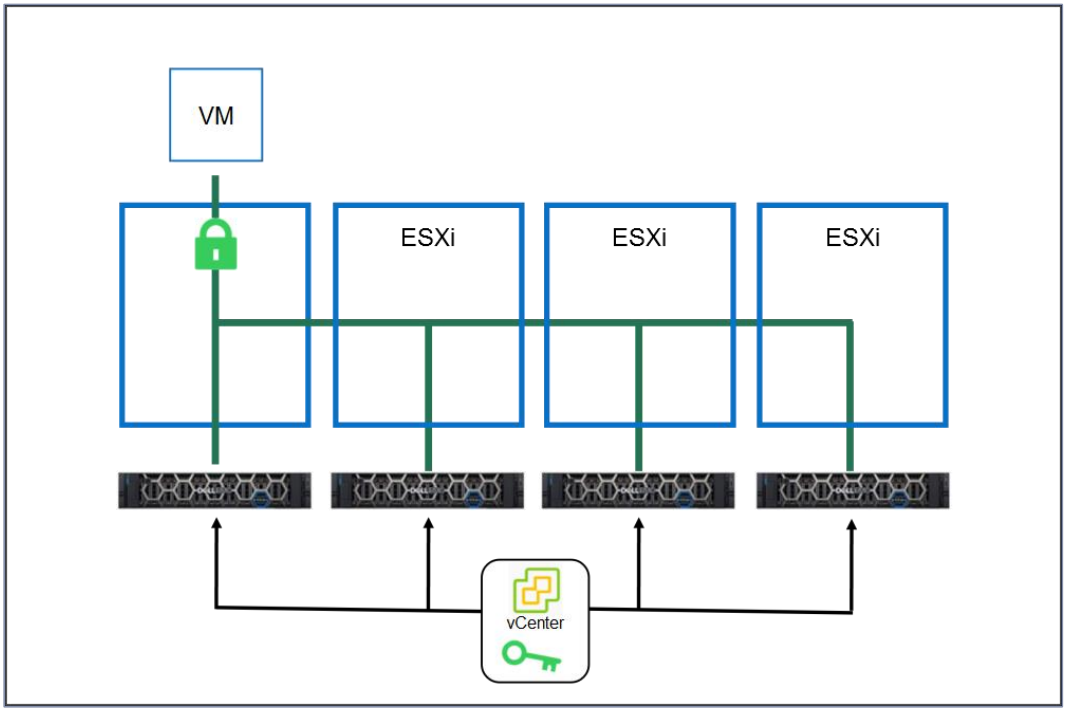
Encryption of a vSAN ESA datastore supports both the Native Key Provider and a Standard Key Provider.

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

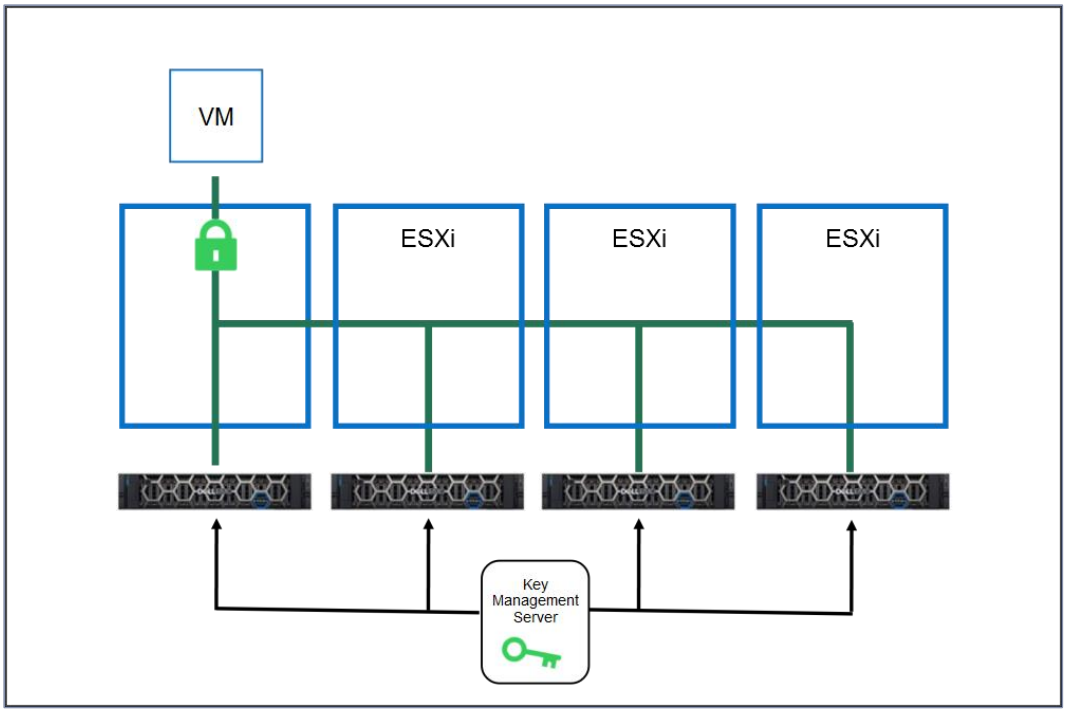
a vSAN Enterprise Plus license. Access to a backup of the primary key is required for data recovery, if vCenter is inaccessible.



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.

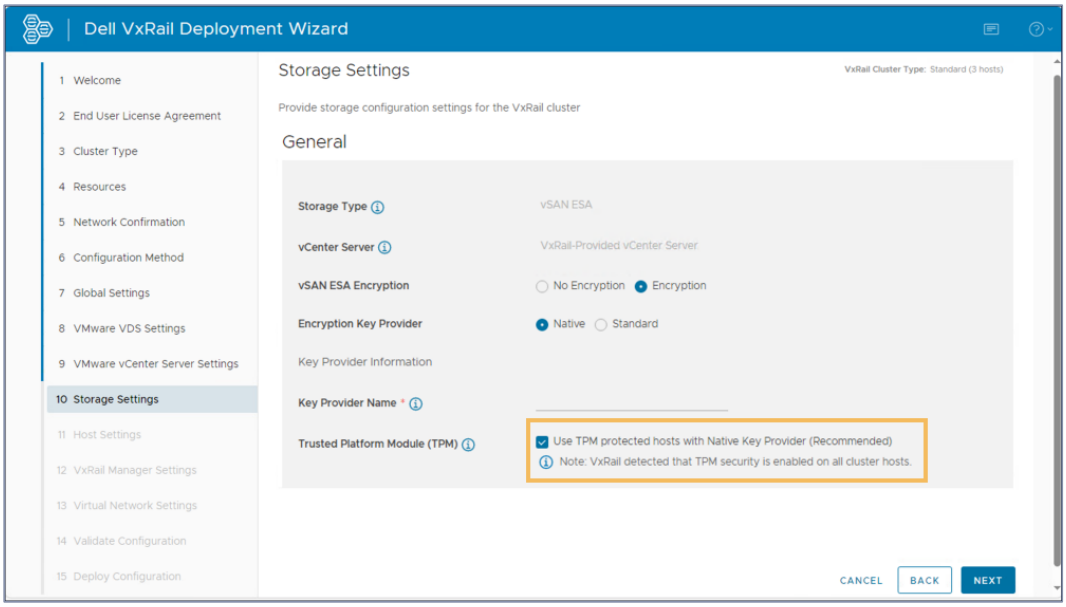


vSAN ESA Standard Key Provider

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.

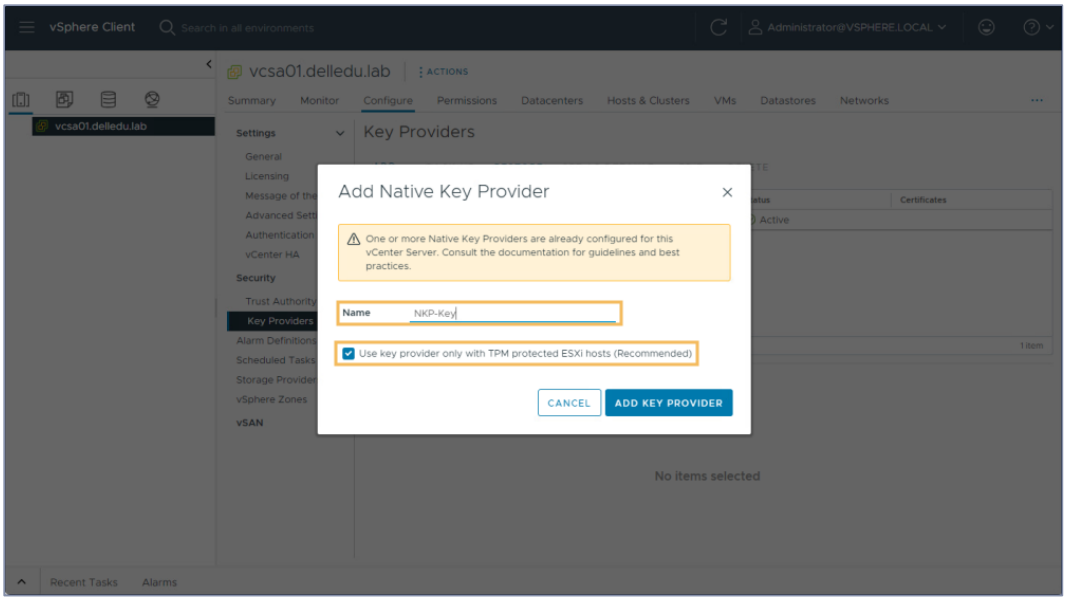


VxRail Deployment Wizard with the option to use TPM protected host selected

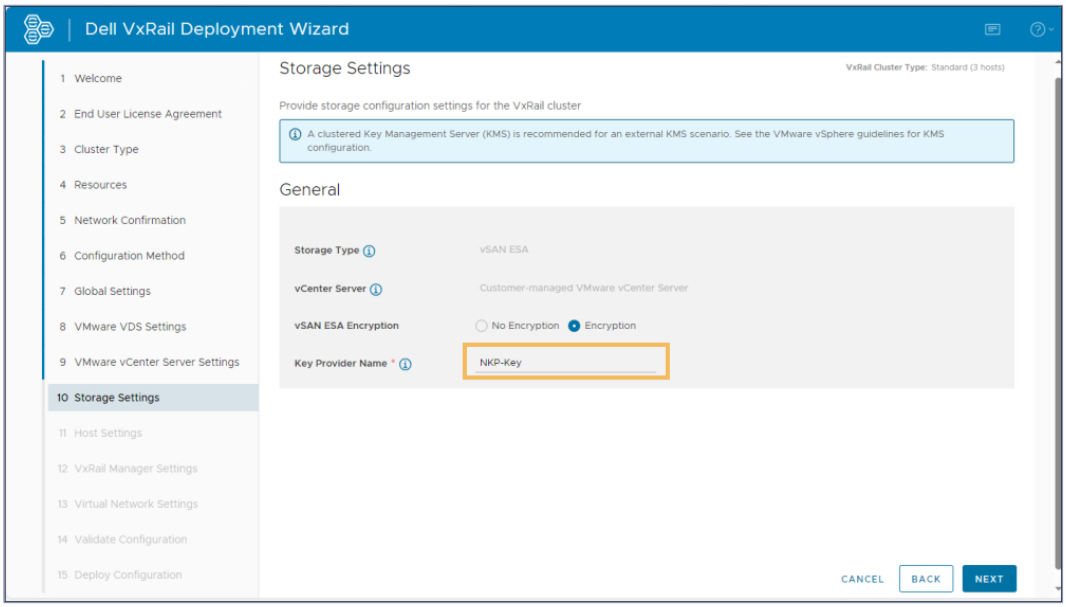
Tip: Enabling TPM 2.0 on the VxRail hosts to support encryption is recommended as a best practice, but not required.

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.



vCenter Add Native Key Provider Wizard showing the Key Provider Name



VxRail Deployment Wizard showing the Key Provider Name

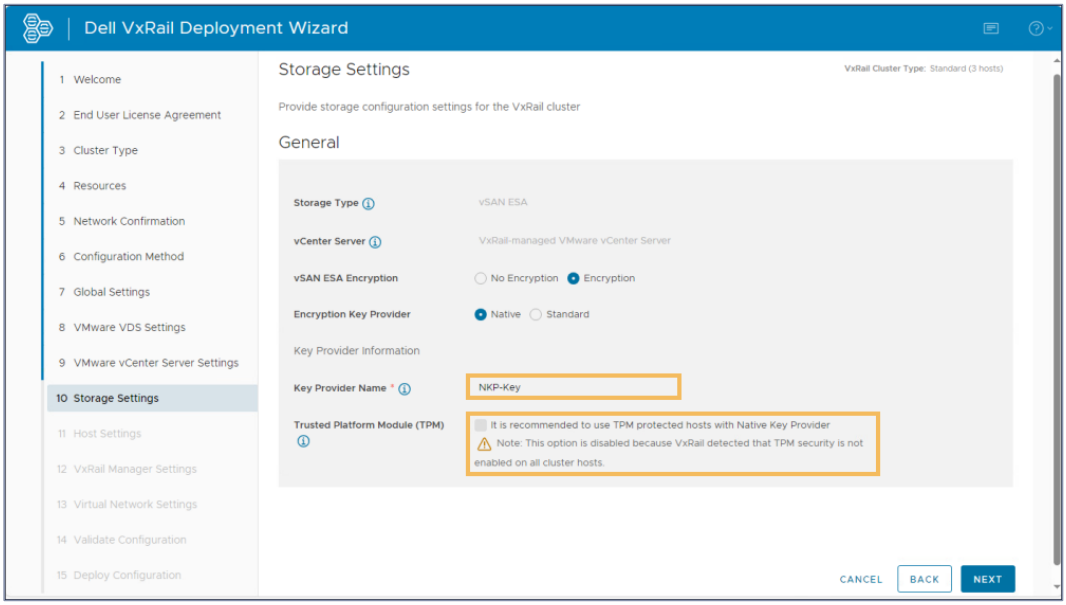
Configuring Key Providers on a VxRail-Managed vCenter Server

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

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

Native Key Provider

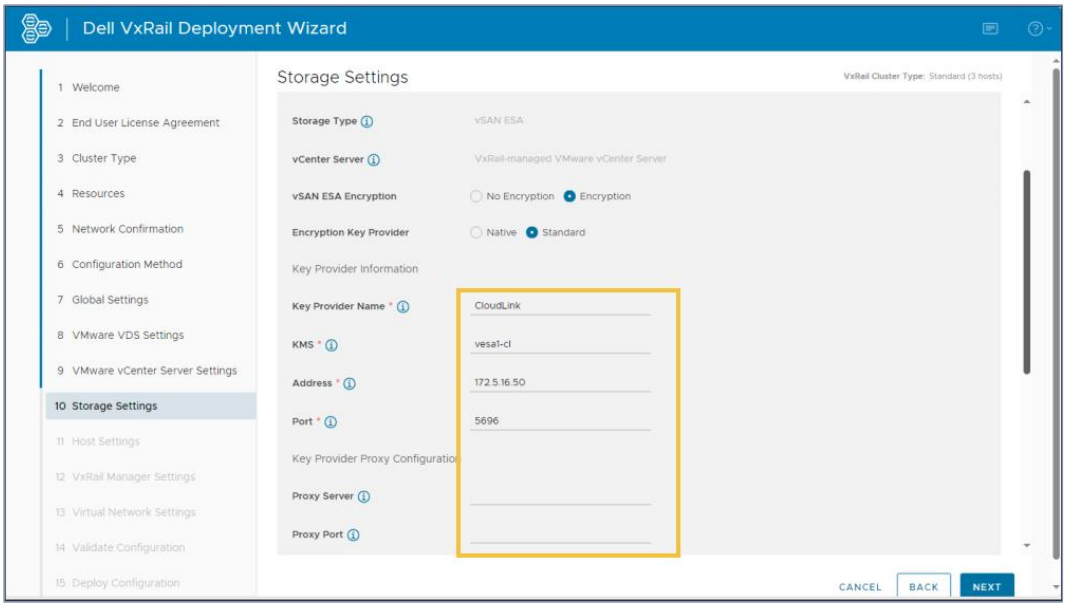
When a VxRail-managed vCenter Server is deployed, the Native Key Provider is configured on vCenter during the initial build. A name for the key provider is entered into the **VxRail Deployment Wizard**. If TPM is not enabled on all the hosts before the start of VxRail initial build, the **Trusted Platform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



VxRail Deployment Wizard showing KMS settings

Interaction: Add a Native Key Provider to the vCenter Server

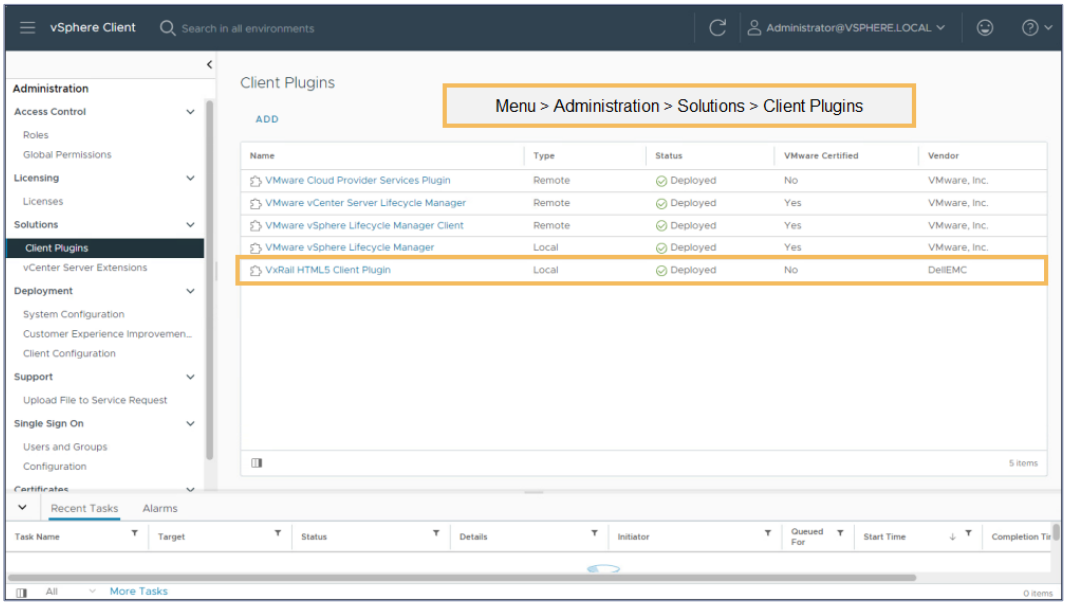
The web version of this content contains an interactive activity.

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



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

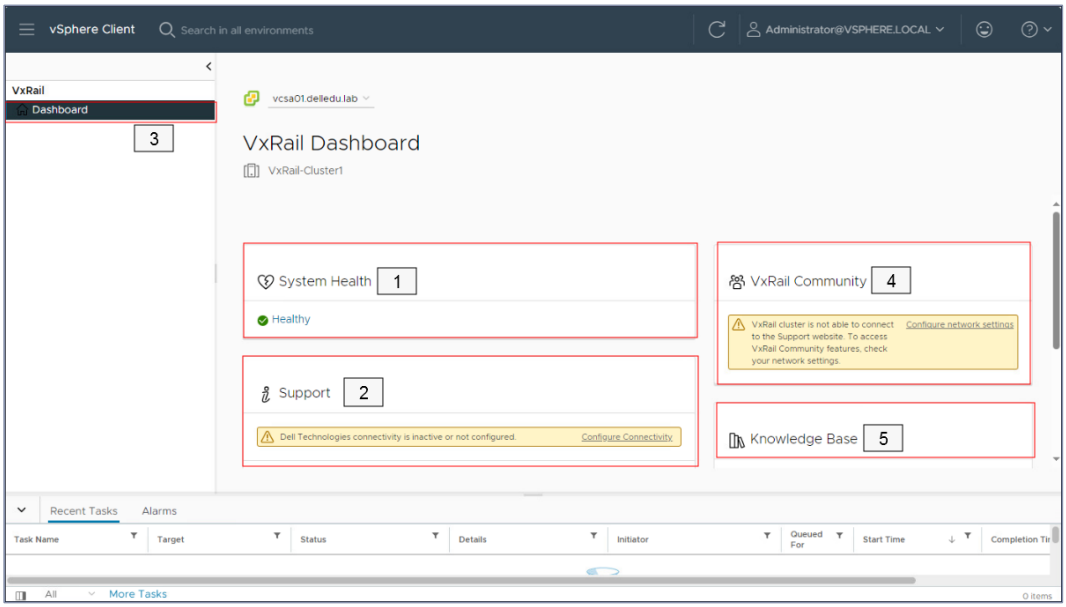
Tip: There are KB articles to help troubleshoot issues that are related to the VxRail Plugin, for example KB 193869.

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



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

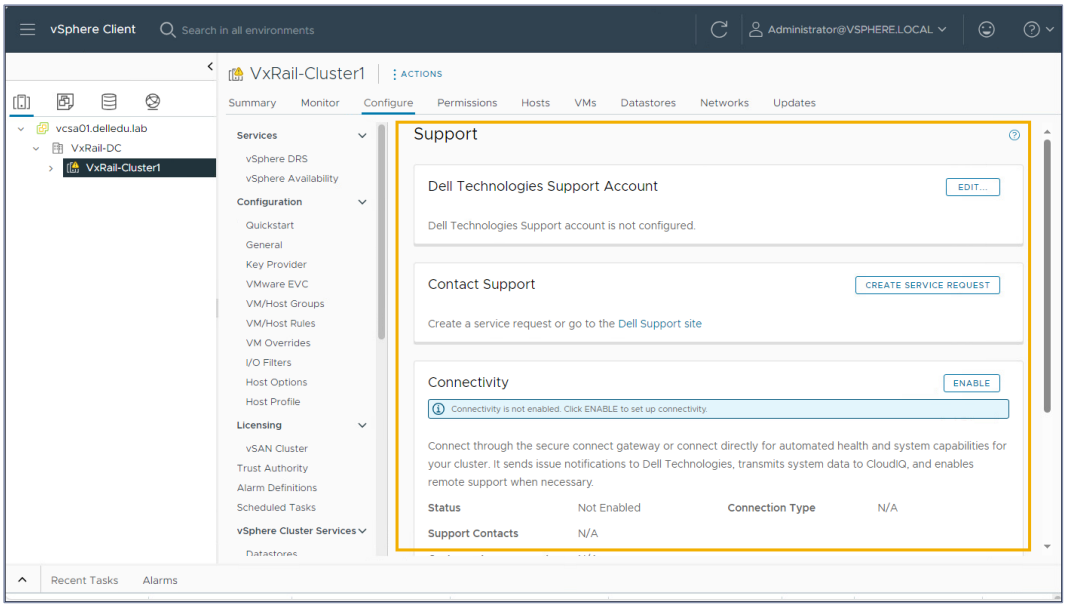
Clicking the health status link takes you to the Issues and Alarms view of the VxRail Cluster in the vSphere Client.

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.

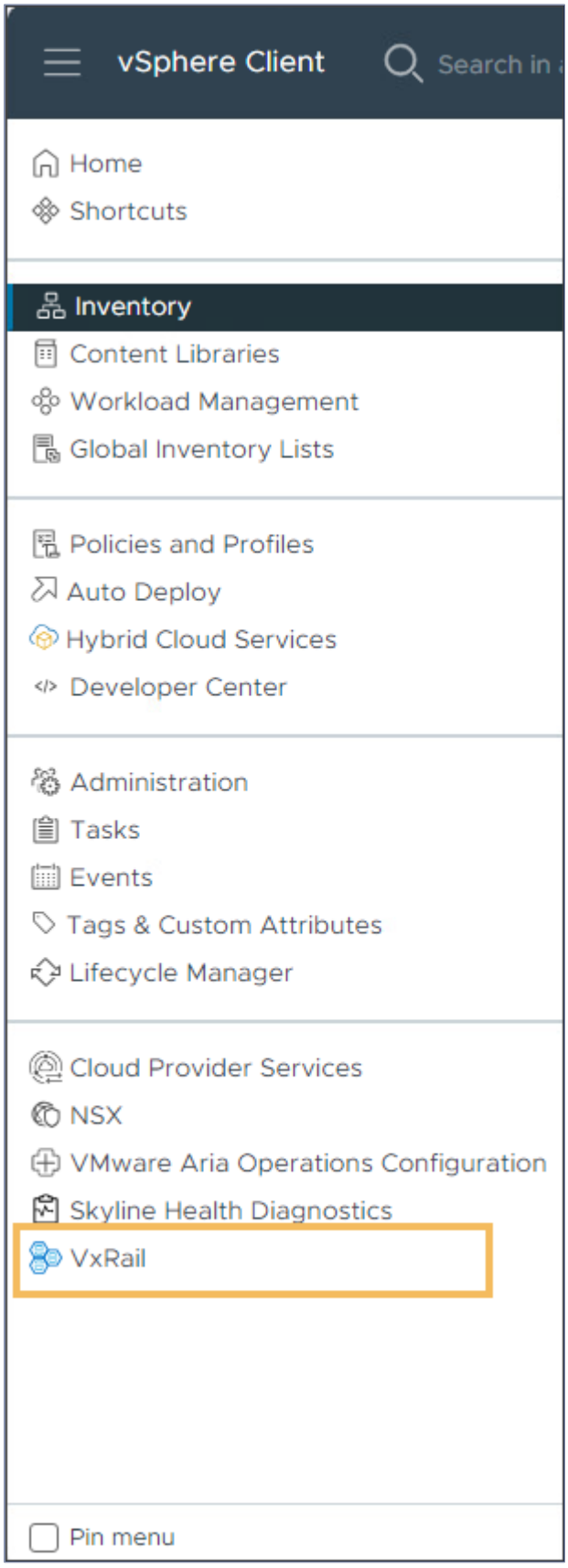
A valid Dell Support account that is associated with the VxRail system is required to engage Support resources. Clicking the **Configure Connectivity** link brings you to the VxRail Support page shown below. Use this page to configure the Dell Technologies Support Account and Secure Connect Gateway.



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**.



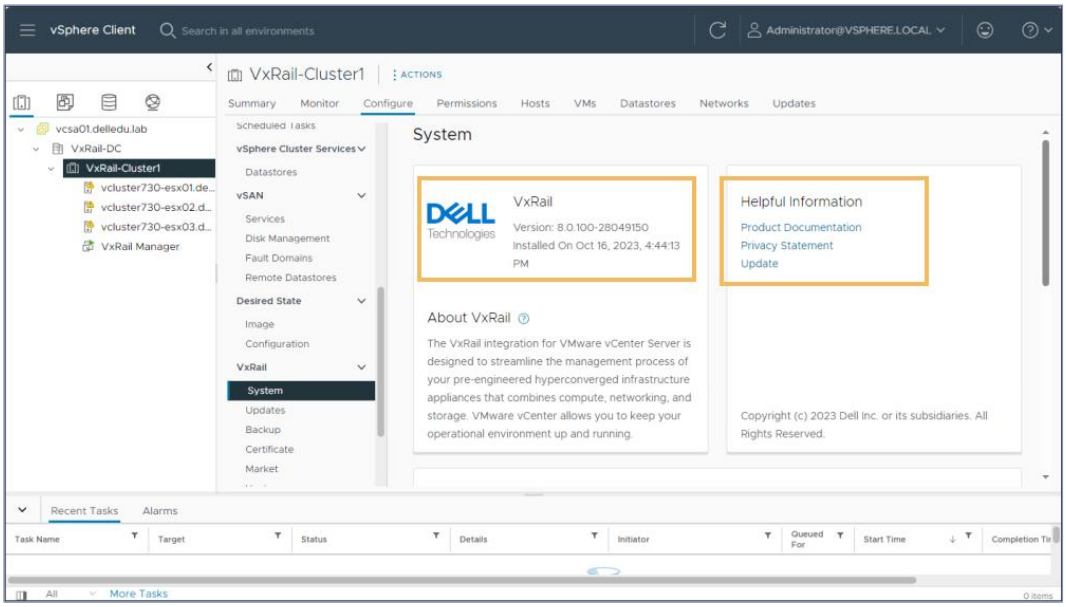
Menu > VxRail

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



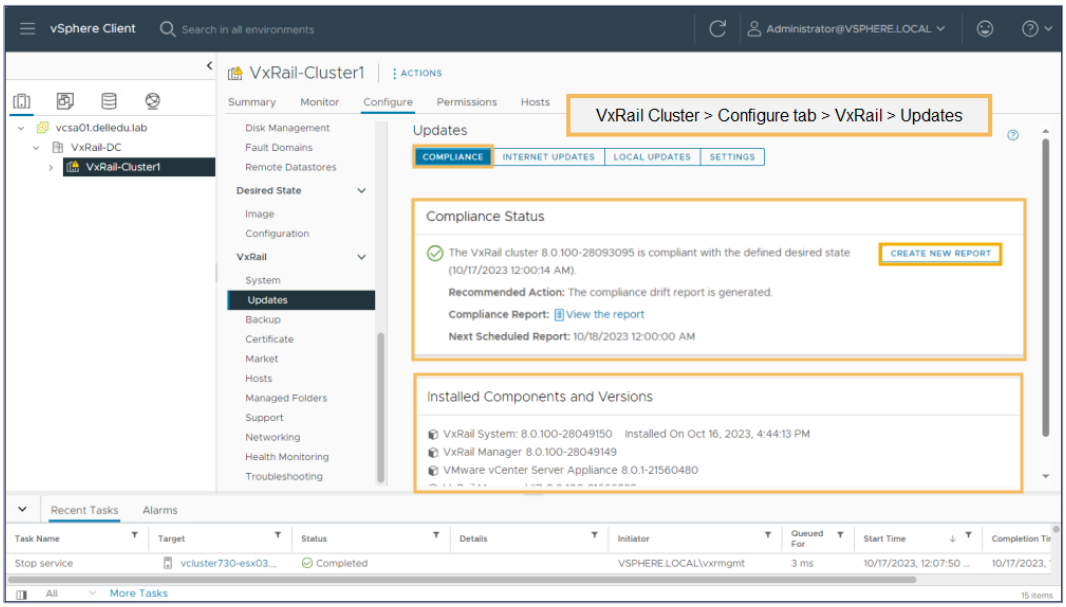
VxRail System Information page

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

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



VxRail Updates page - Compliance tab

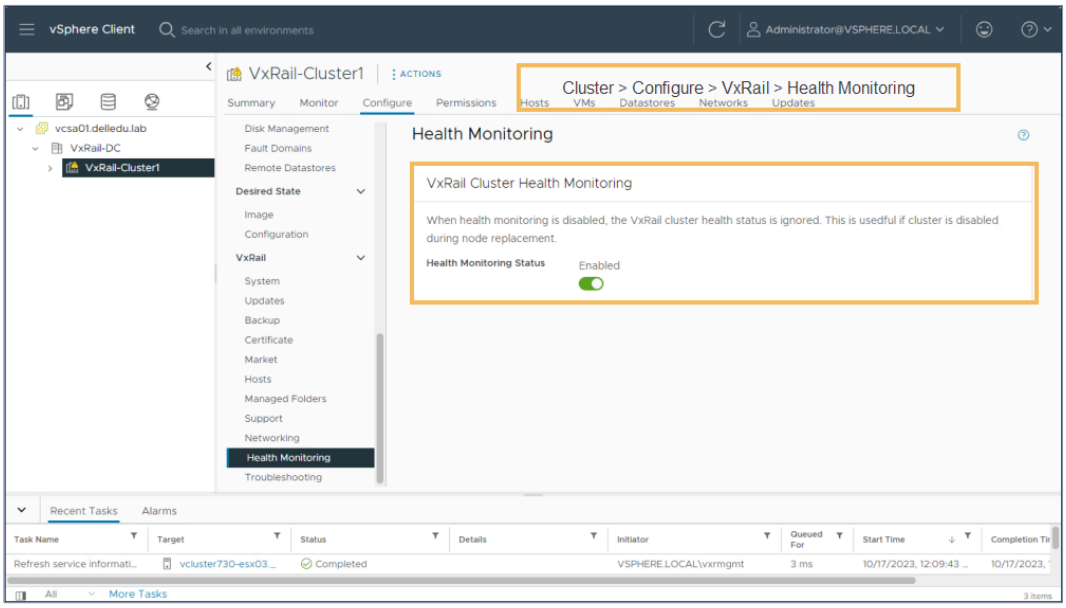
The installed components and versions are displayed on the **Compliance** tab of the **VxRail > Updates** page.

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

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

The compliance report runs automatically every 24 hours.

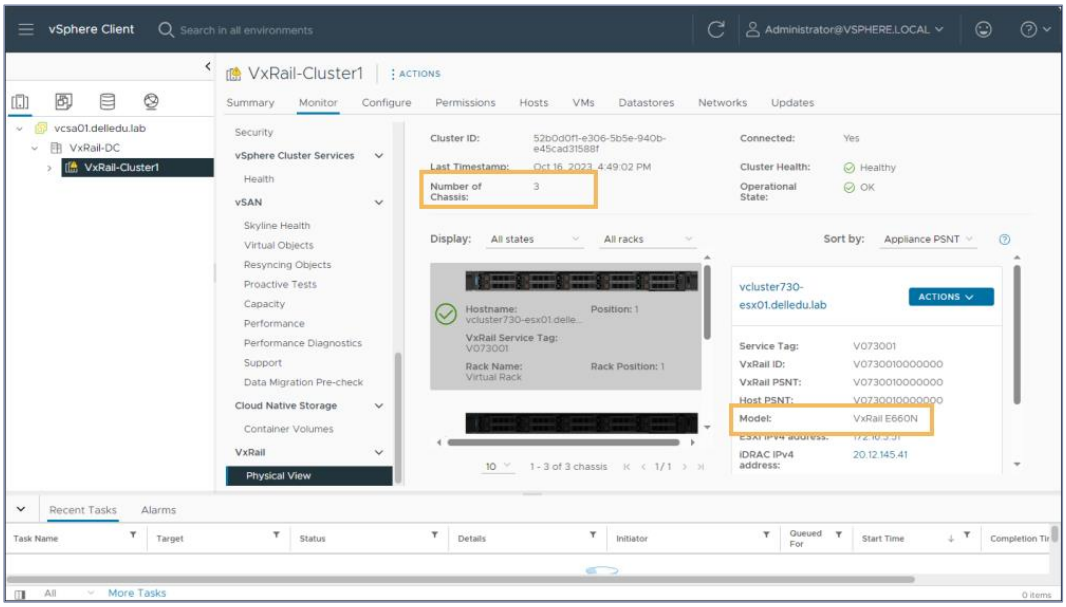
VxRail Cluster Health Monitoring Status



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.

VxRail Cluster - Physical View



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.

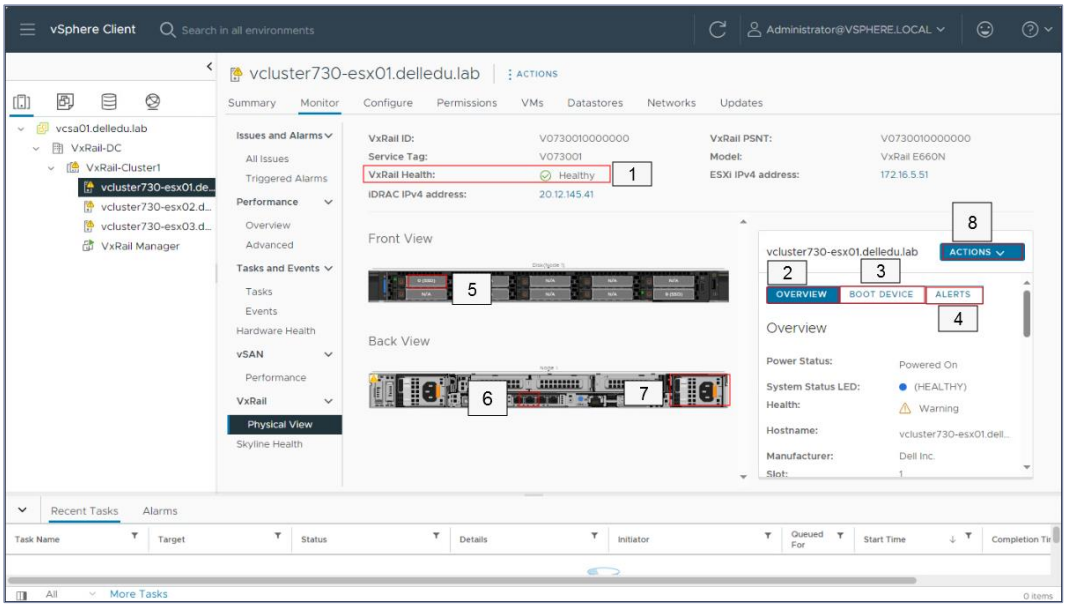
In the example shown, the cluster has three VxRail E660N nodes.

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.

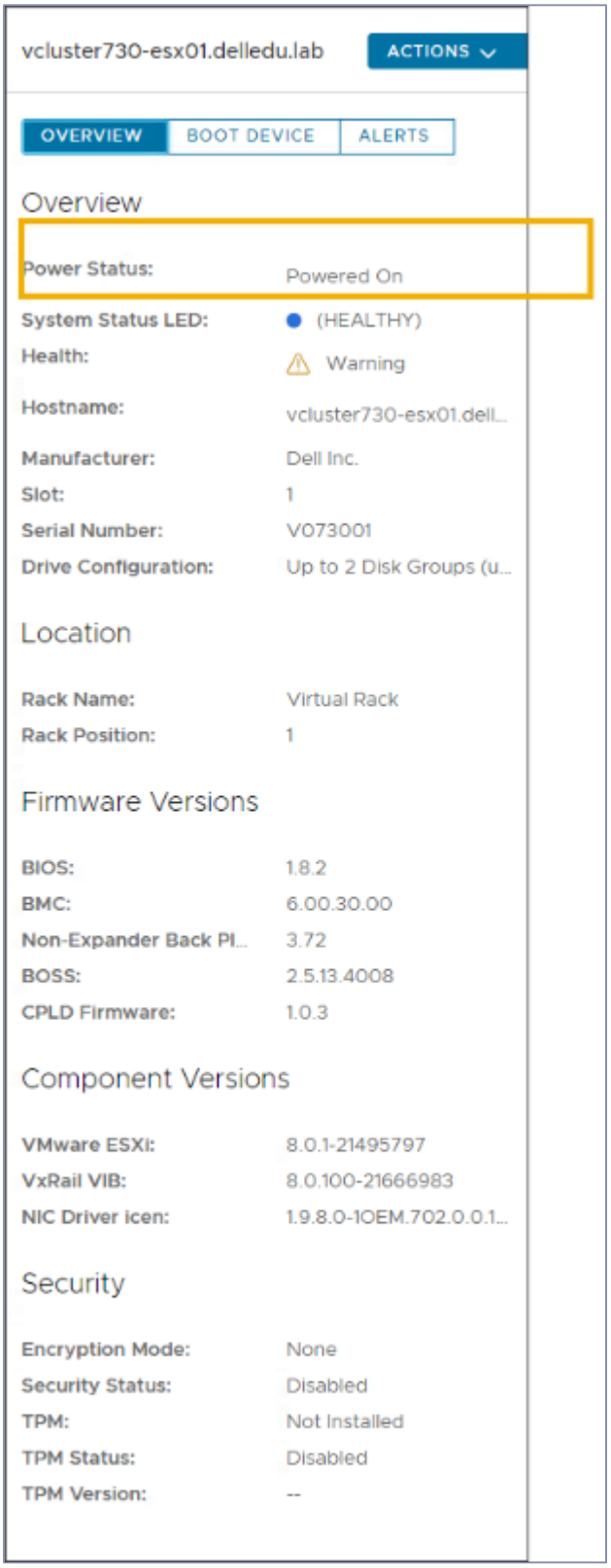
VxRail Node Physical View



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

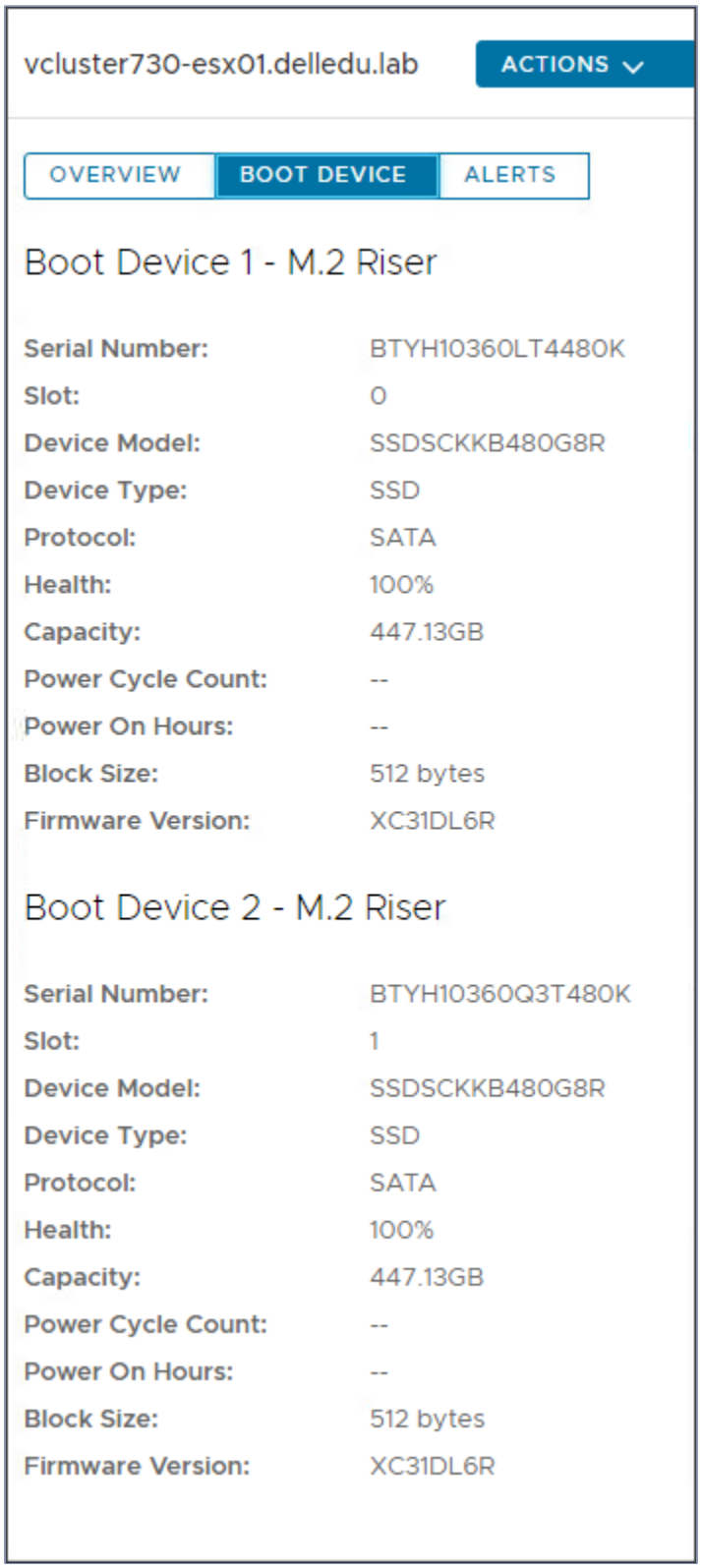
The **OVERVIEW** tab displays the power status, system LED status, health, hostname, node PSNT, serial number, location data, firmware versions, and component versions.



Node 1 Overview

3: BOOT DEVICE

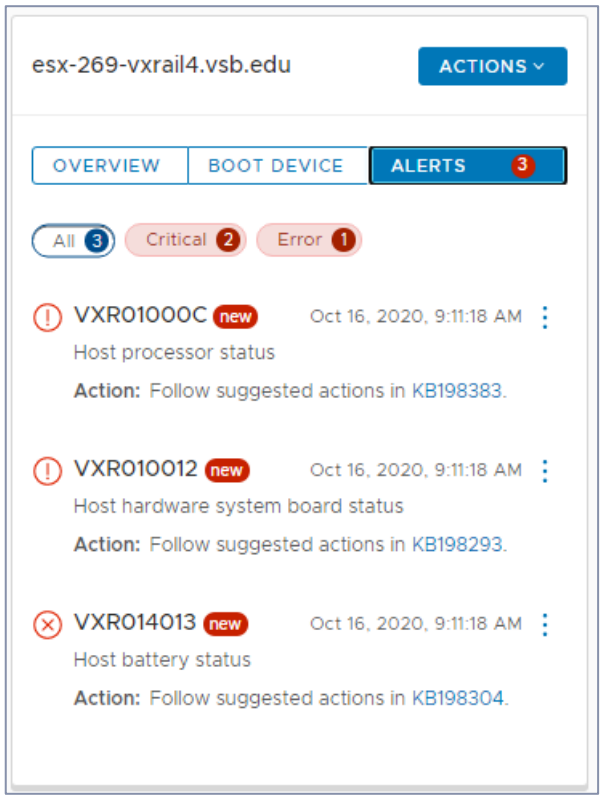
The **BOOT DEVICE** tab displays details about the boot device. The example that is shown is an E560F node.



Node 1 Boot Device

4: ALERTS

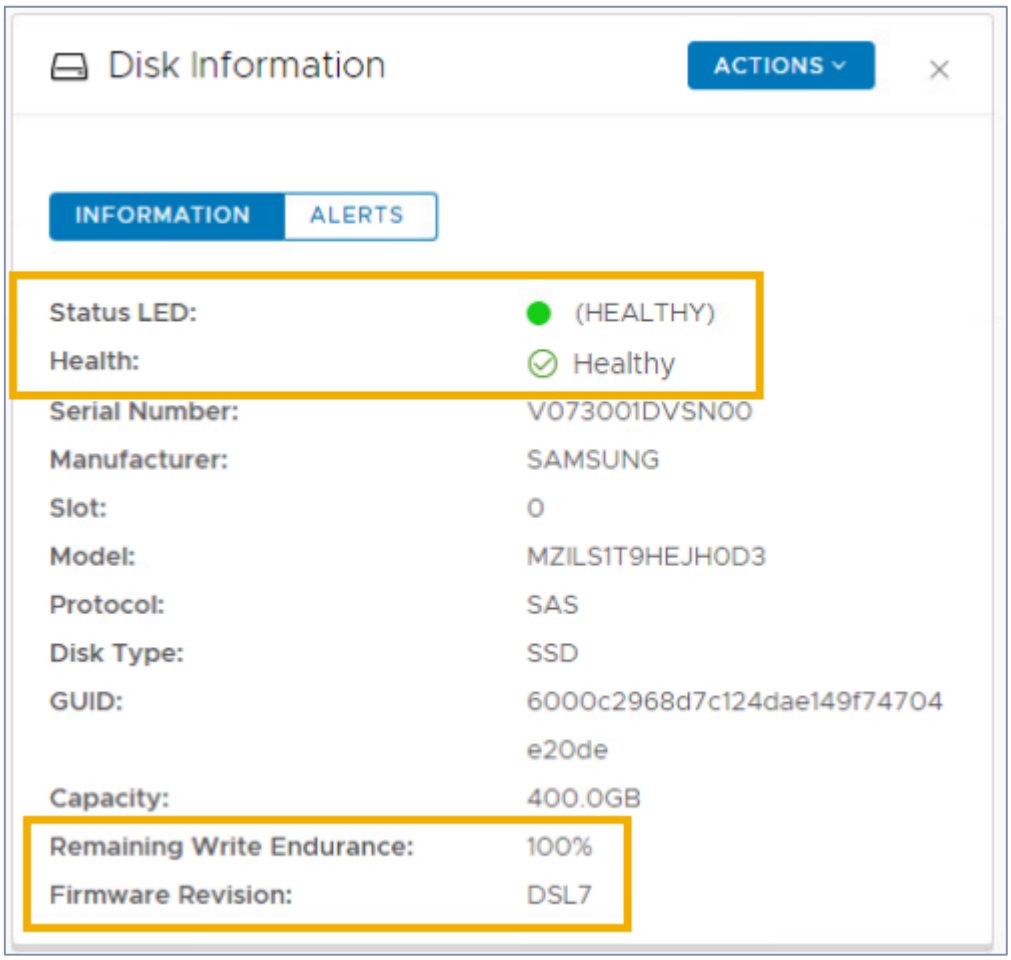
The **ALERTS** tab lists the triggered VxRail alerts specific to the node. All VxRail alerts start with VXR.



Example - A G560 node with three active alerts.

5: Disk Information

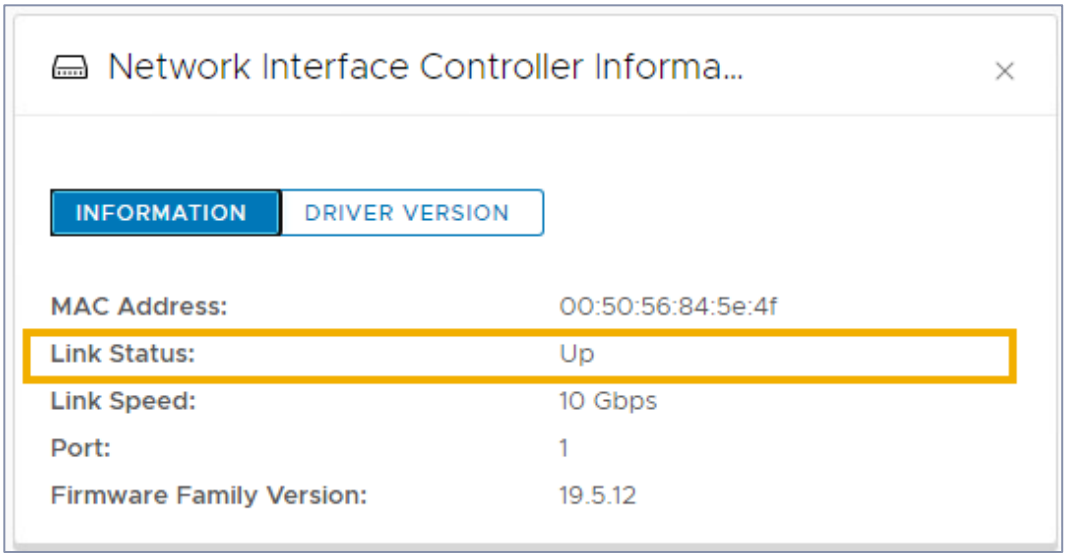
By clicking any of the active disks, you can find information about the disk health and monitoring. The **Actions** menu in this section would be used to replace an unhealthy drive.



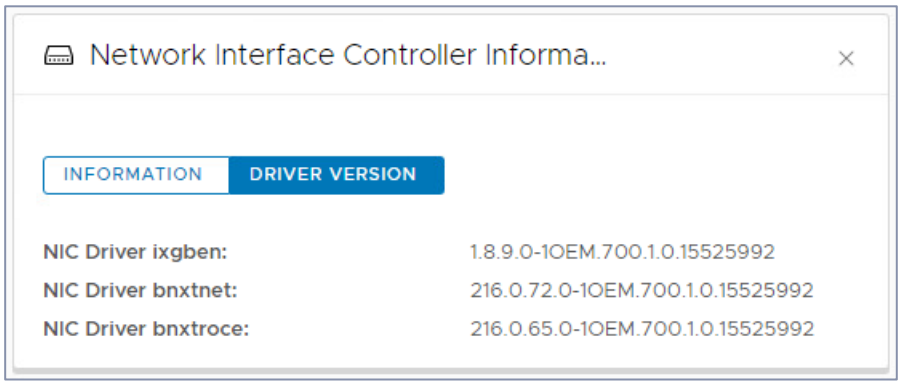
Disk information example - A E660N node with a healthy status

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.



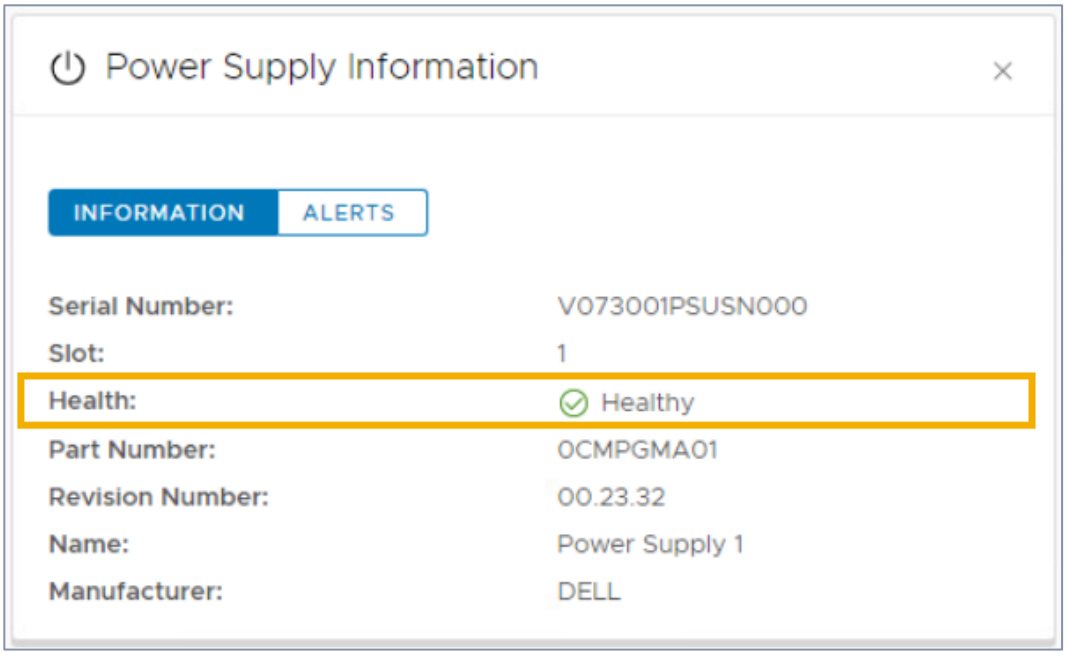
Node 1 NIC Information



Node 1 NIC Driver Version

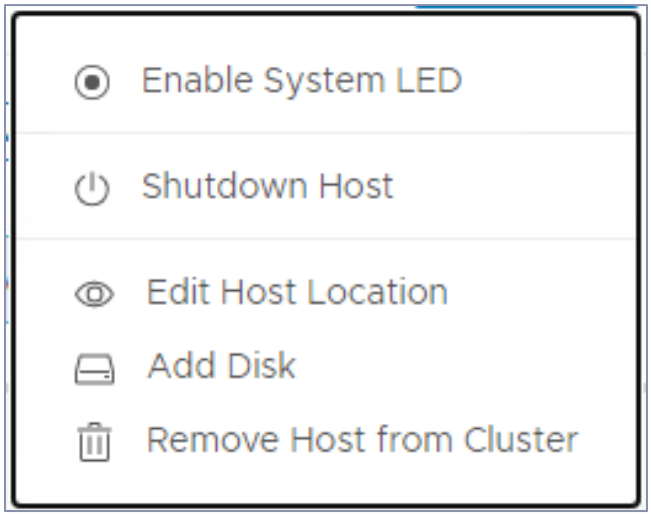
7: Power Supply Information

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



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.

Lab Tasks

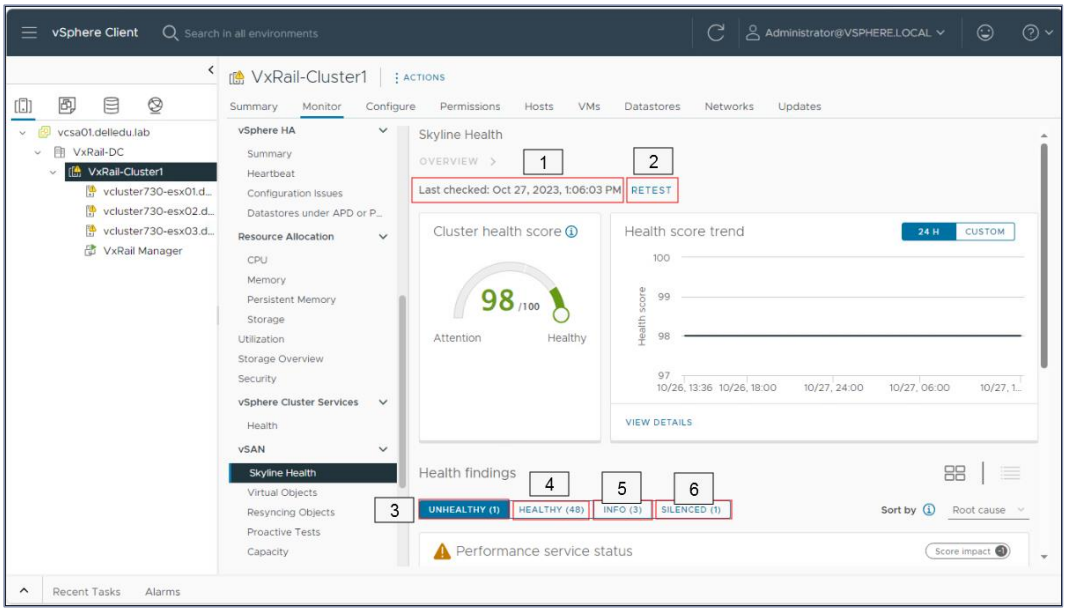
- Confirm that the VxRail Plugin has been deployed.
- Use the VxRail Plugin to validate:
  - Overall system health.
  - VxRail installed versions at a system and component level.
  - VxRail component information using the physical view for the cluster and node.

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



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.

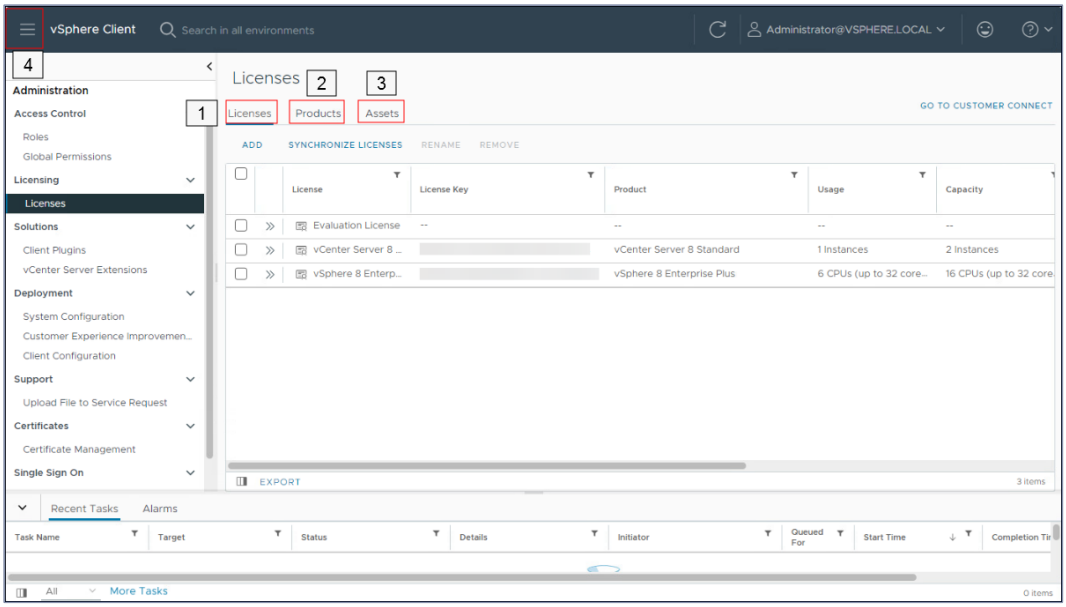
Examples of impact due to license expiration include:

- 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.

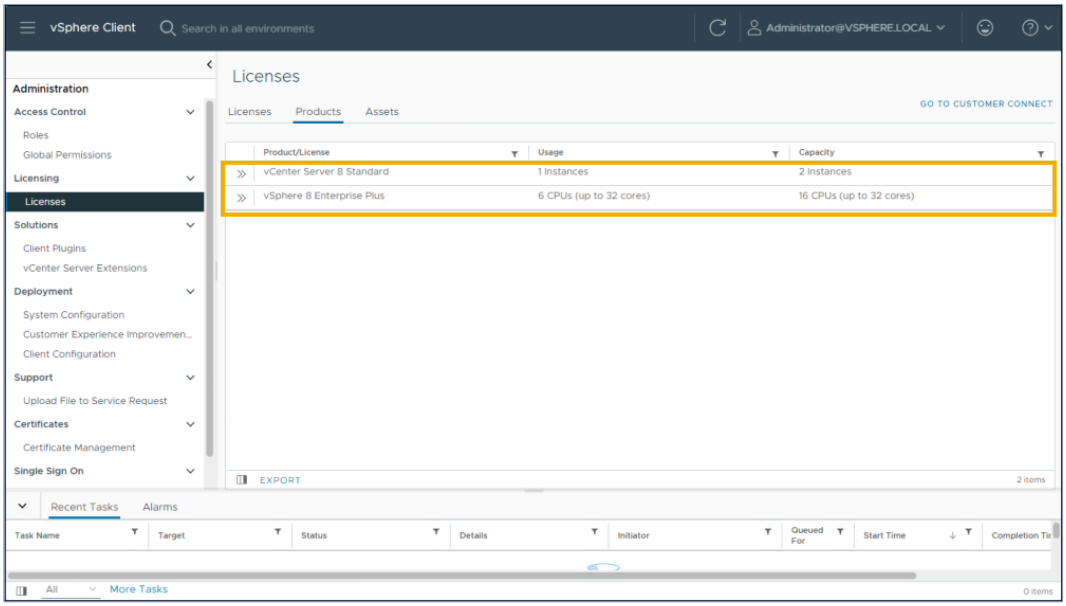
Licenses are viewed and added through the vSphere Client. To learn more about how to navigate licensing through the vSphere Client, select the four (4) red hotspots.

vSphere License Management



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.

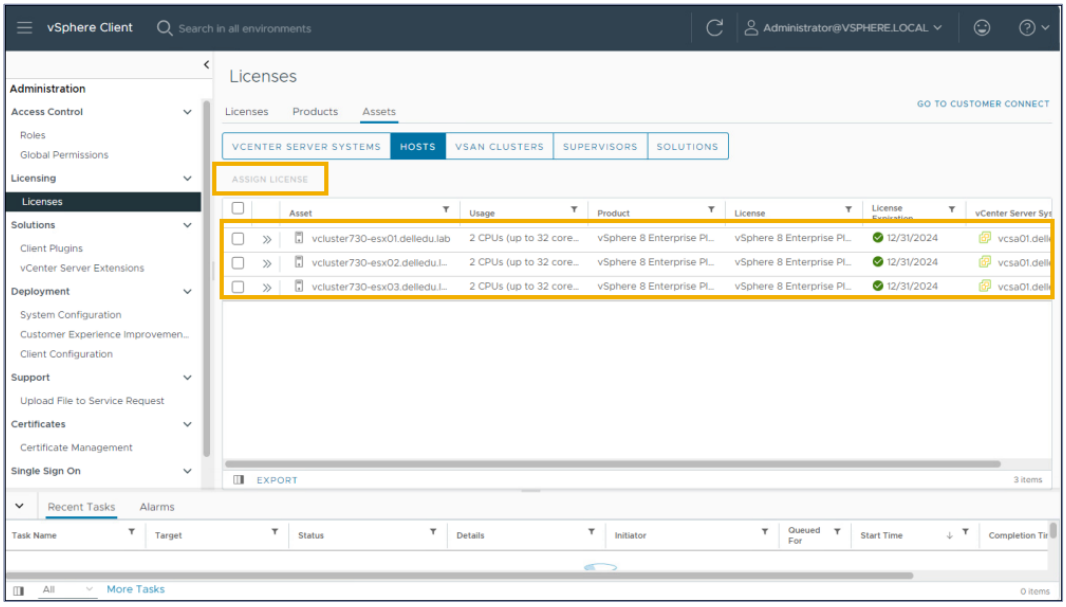
2: The **Products** tab displays the available product licenses.



Example that displays the Products tab with available licenses

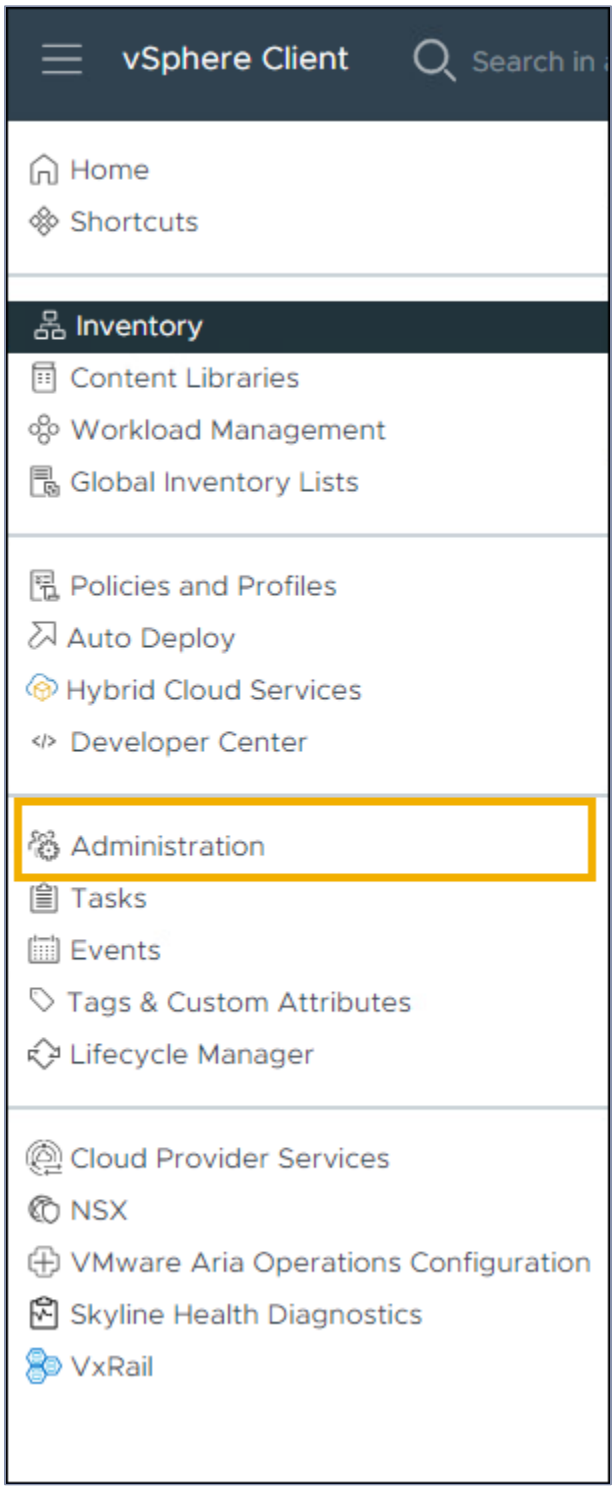
3: The **Assets** tab displays the license status of various assets like **vCenter Server Systems, Hosts, vSAN Clusters, Supervisor Clusters,** and **Solutions**. The **Asset** page is also used to assign available licenses

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



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.



Example presenting the Menu dropdown options available in the vSphere Client

Additional information:

- Software Licensing Options for VxRail

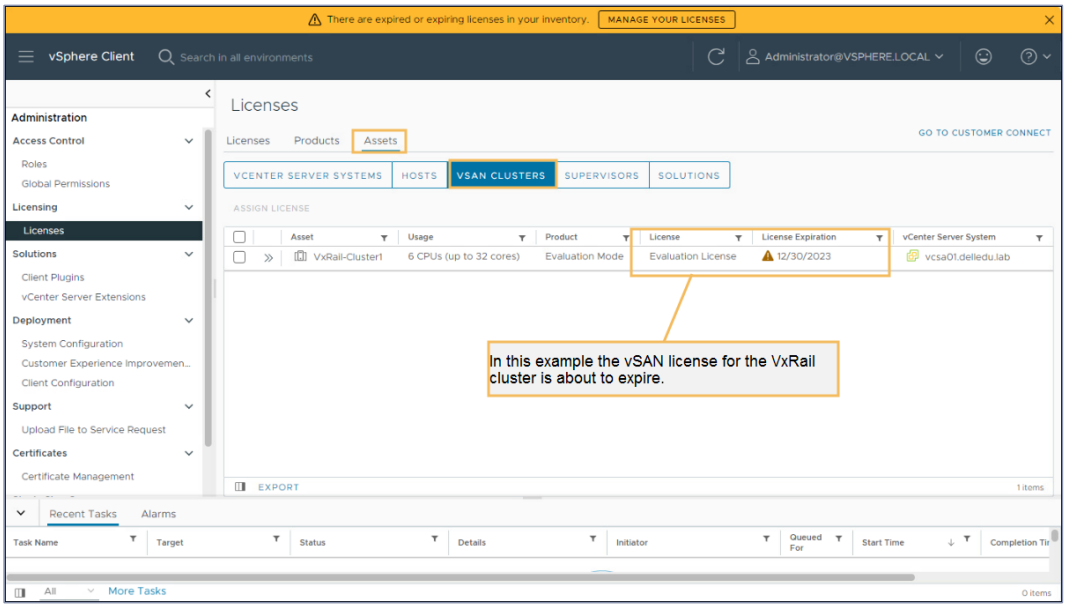
- VMware vSphere and vSAN Editions Feature Comparison
- About ESXi Evaluation and Licensed Modes
- How to activate Partner Activation Codes (PAC) for vSphere License

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

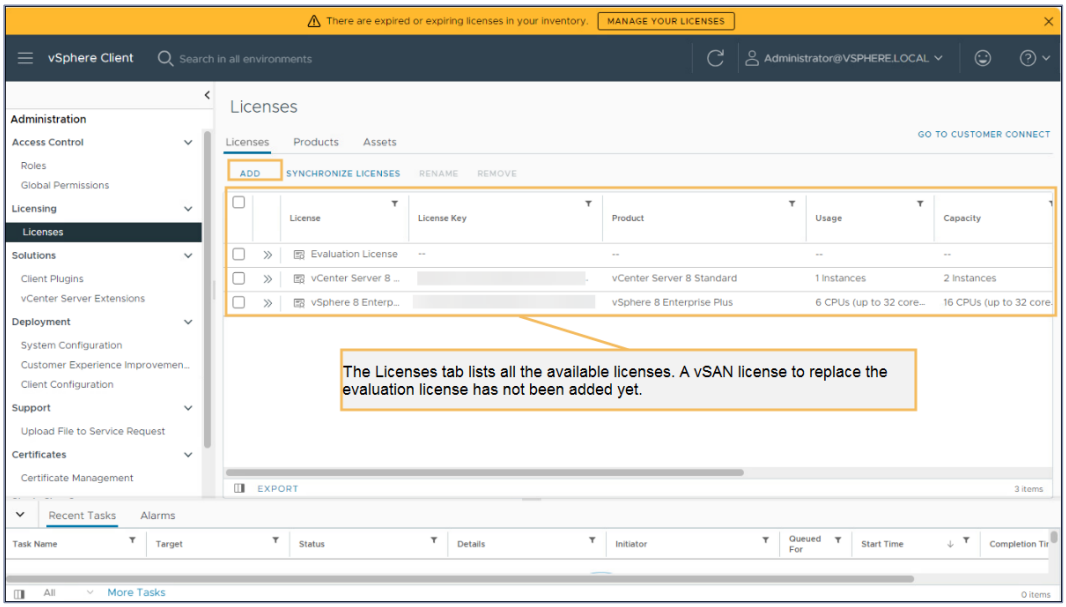
When a license is about to expire, a notification is displayed at the top of the vSphere Client page. Clicking the **MANAGE YOUR LICENSES** button launches the **Licenses** page, which can also be accessed by going to **Administration > Licensing**.



Manage Licenses

Add License

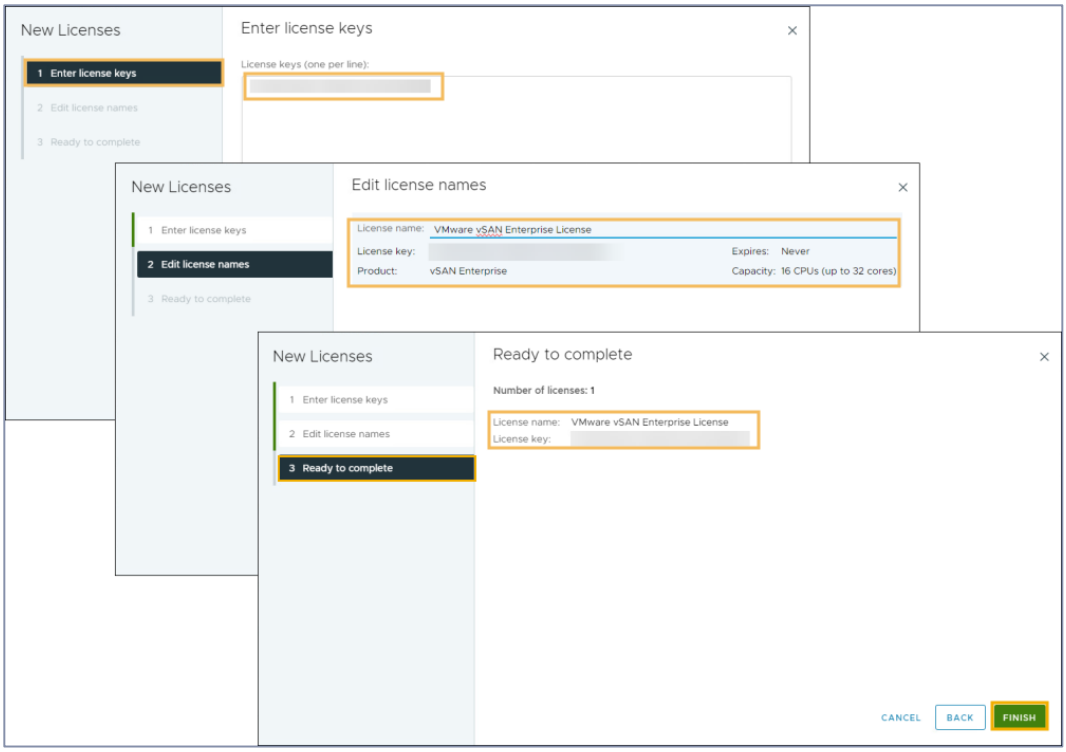
There are multiple ways to add a license. One of the ways is to go to the **Licenses** tab and click **ADD**. The **ADD** button allows multiple licenses for ESXi hosts, clusters, and solutions to be added. Clicking **ADD** launches the **New Licenses** wizard.



View and add Licenses

New License Wizard

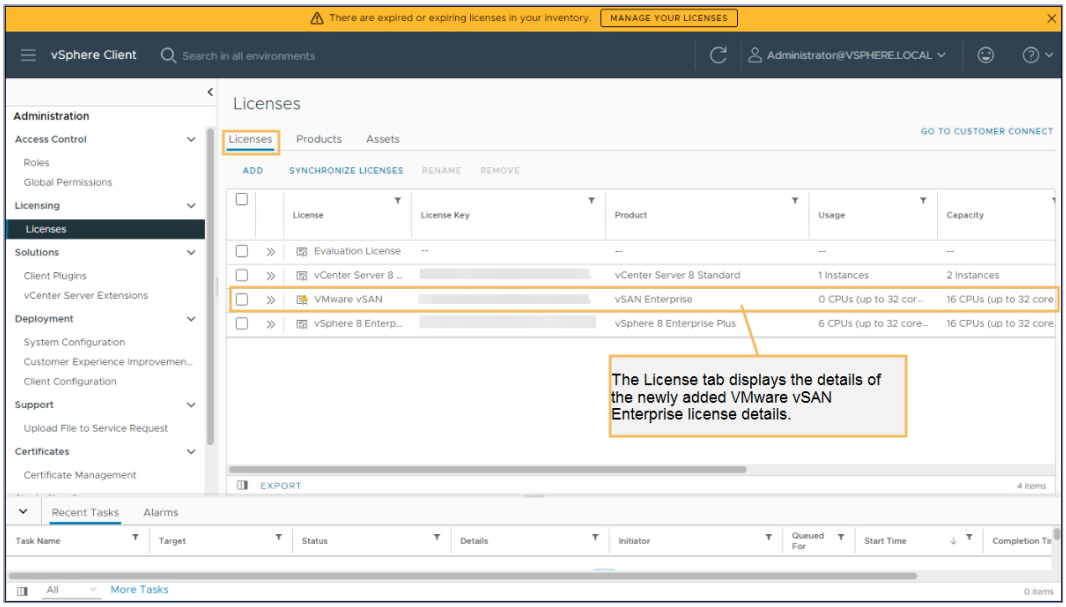
Follow the wizard to enter the license keys on the **Administration > Licenses** page.



New Licenses wizard

View Newly Added License

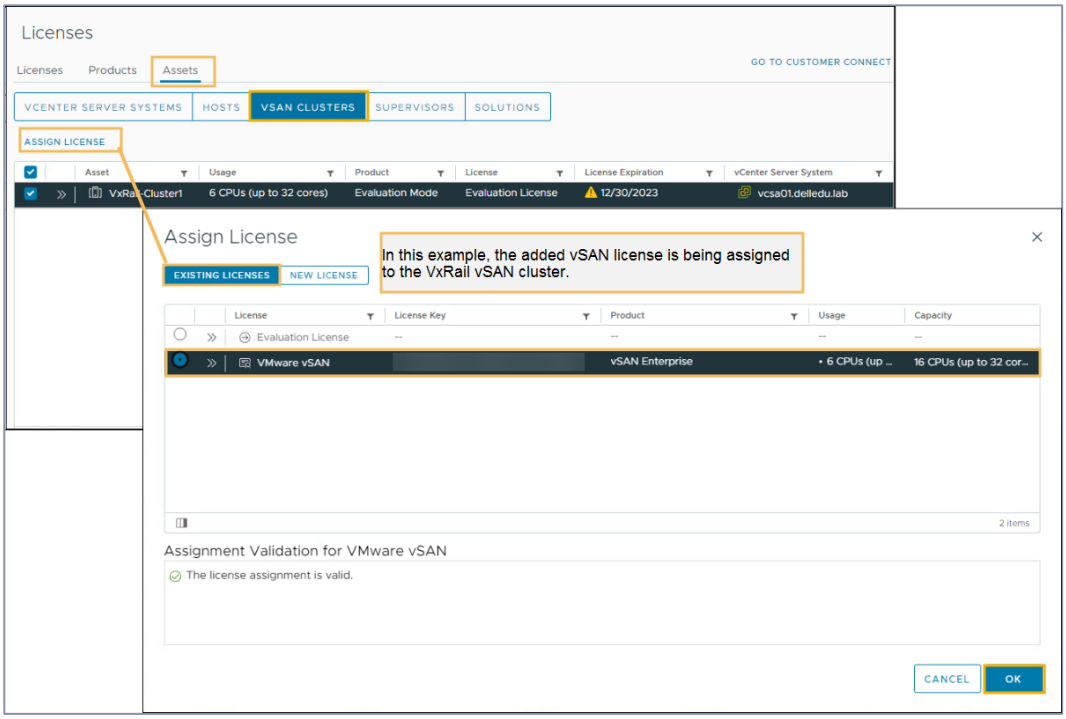
The newly added license can be viewed from the **Licenses** tab.



View newly added License

Assign License

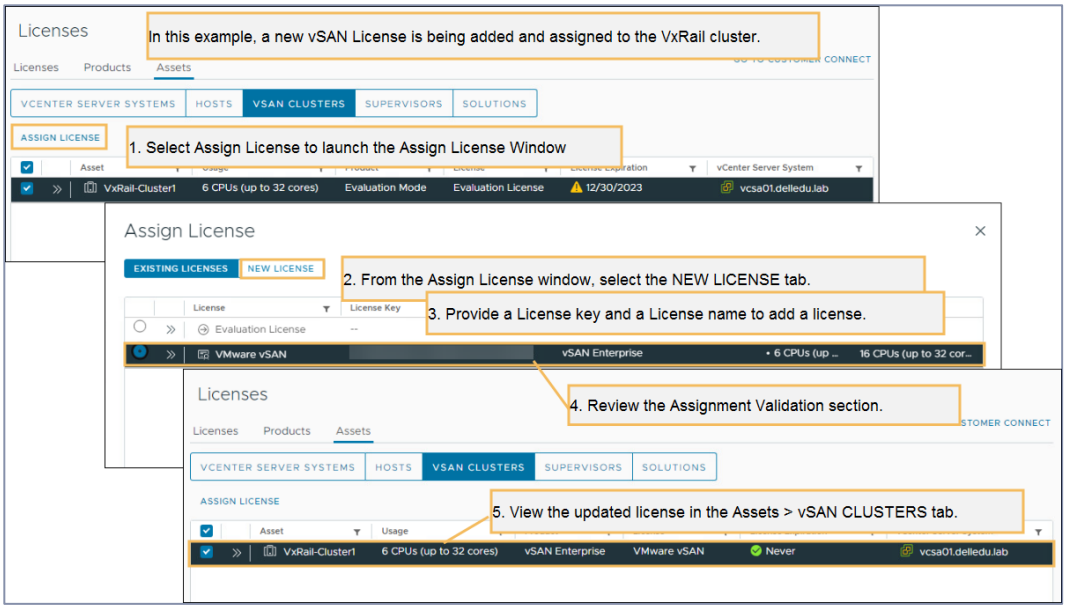
After the license keys are added, go to the **Assets** tab. Select **VSAN CLUSTERS** and then **VxRail-vSAN cluster1**. Clicking **ASSIGN LICENSE** launches the **Assign License** wizard. Assign the newly added vSAN license key to the VxRail vSAN cluster.



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.



An alternate way to add and assign License in vSphere

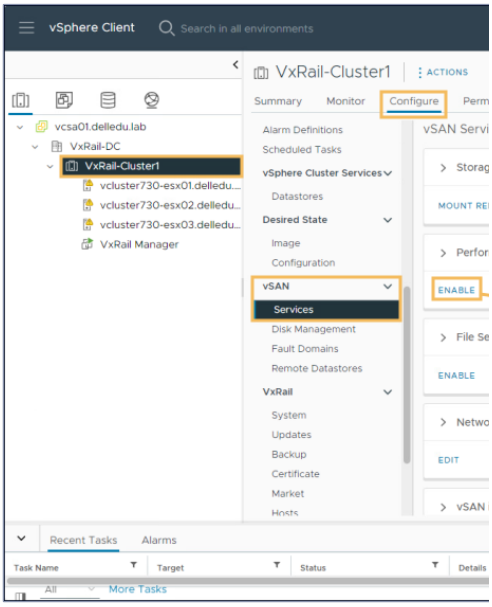
Configure vSAN Services

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.

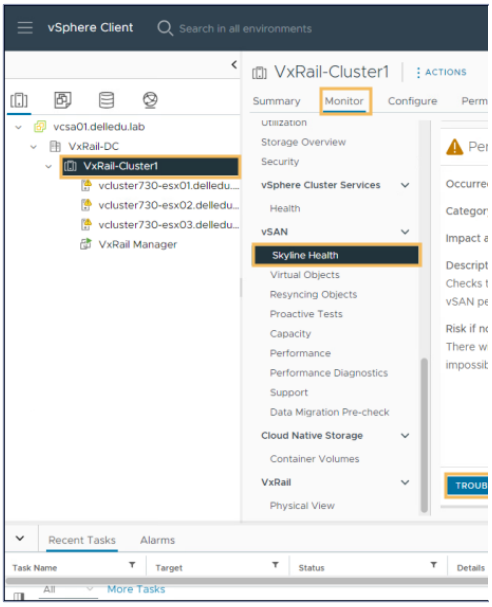
The vSAN Performance service is disabled by default. For VxRail deployments performed by Dell or Dell partners, the vSAN Performance service is manually enabled during the deployment process as required in the Test Plan. The Dell or Dell partner implementation teams must complete the document after a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

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.



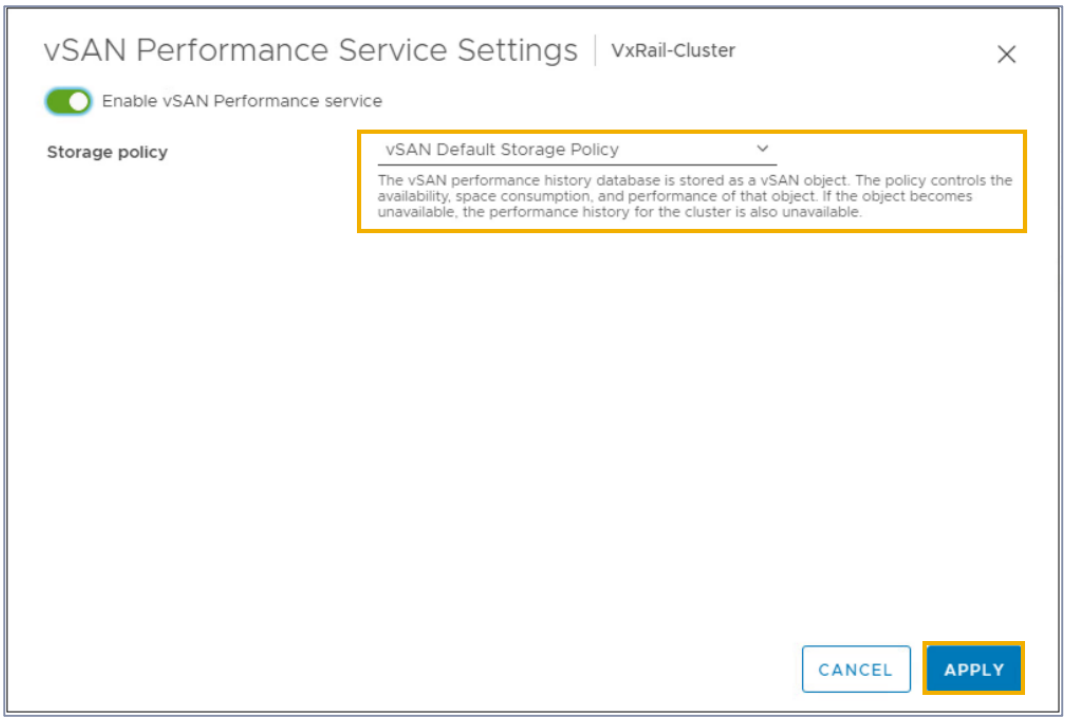
Enable vSAN Performance service through Configure > vSAN > Services

O R 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.



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

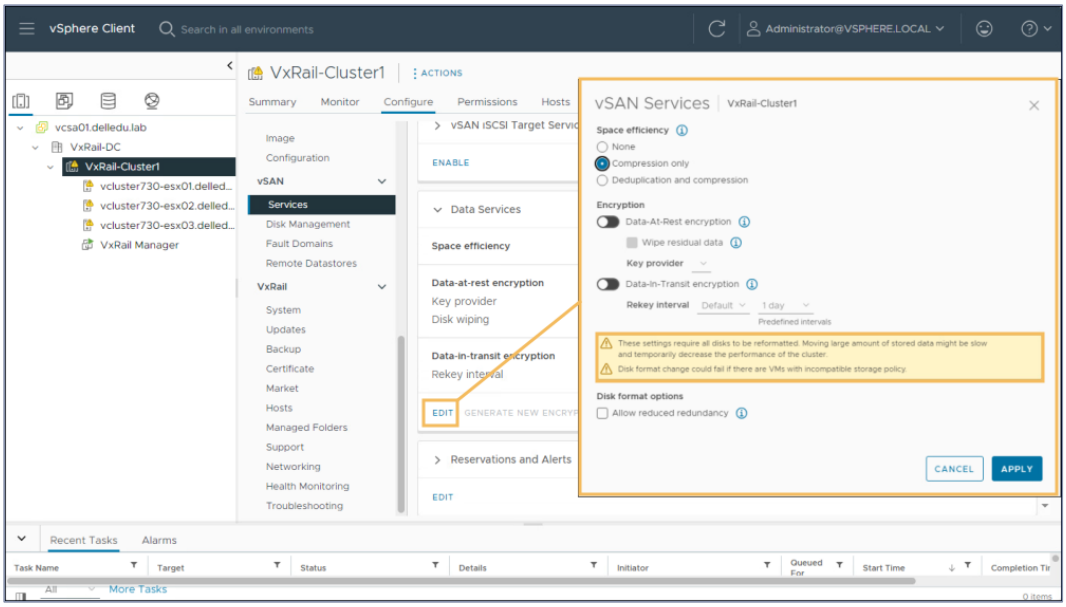
Go to: For more information about the vSAN Space Efficiency options, browse to: Using Deduplication and compression

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.



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.

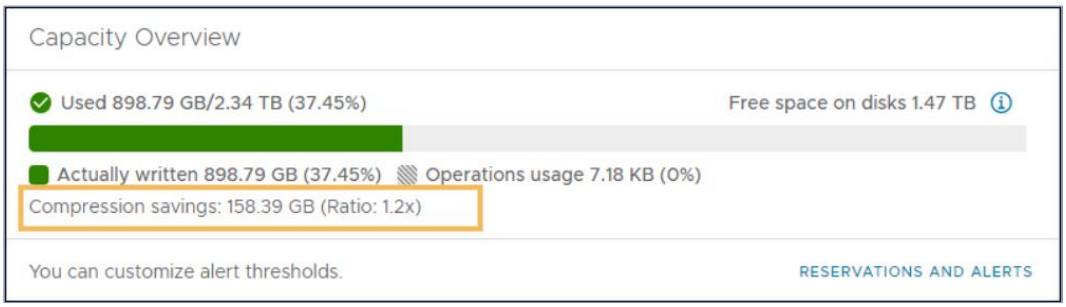
Capacity Overview

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.

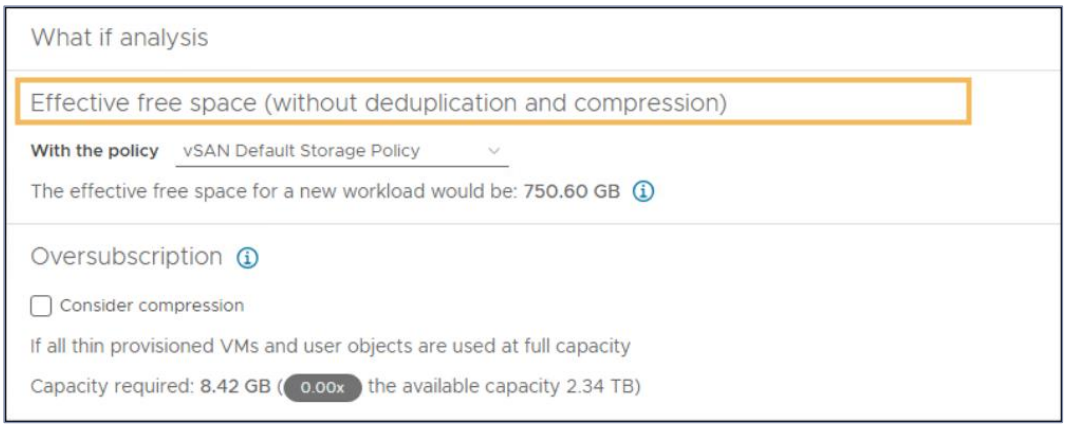
Example based on screenshot: (898.79+158.39)/898.79=1.1762 which rounds to 1.2.



vSAN Capacity Overview

What if analysis

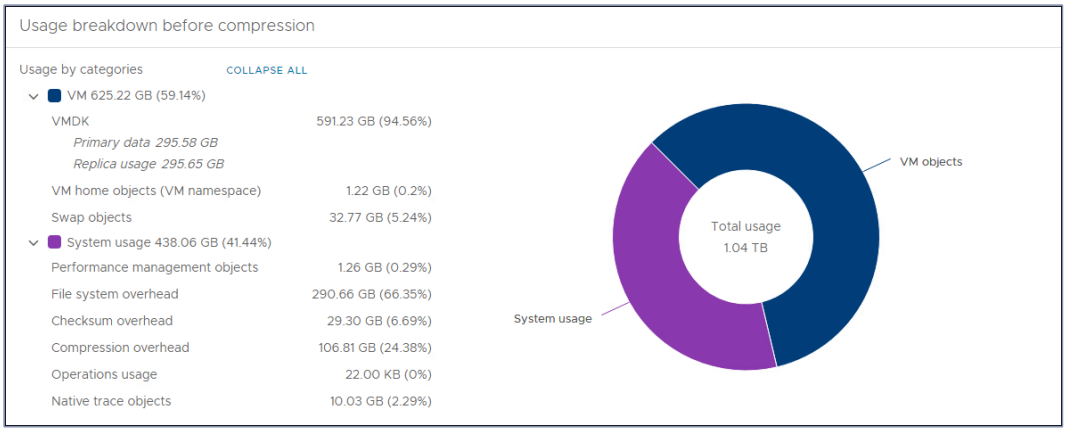
The **What if analysis** displays what would be the effective free space for a new workload without deduplication and compression, with the selected storage policy.



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

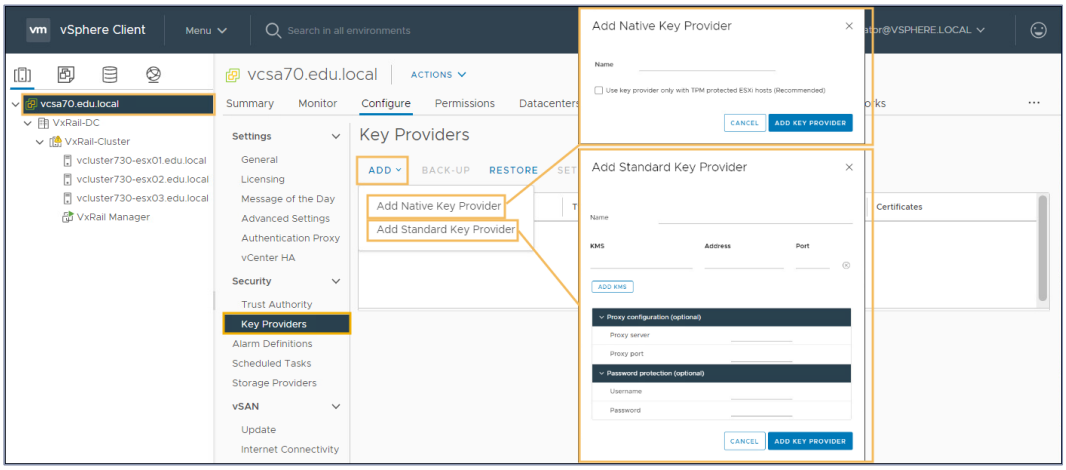
Data-At-Rest Encryption requires a key provider be added to the vCenter Server. Once a key provider is added, a trust must be established between the vCenter Server and the KMS before the encryption service is enabled.

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:

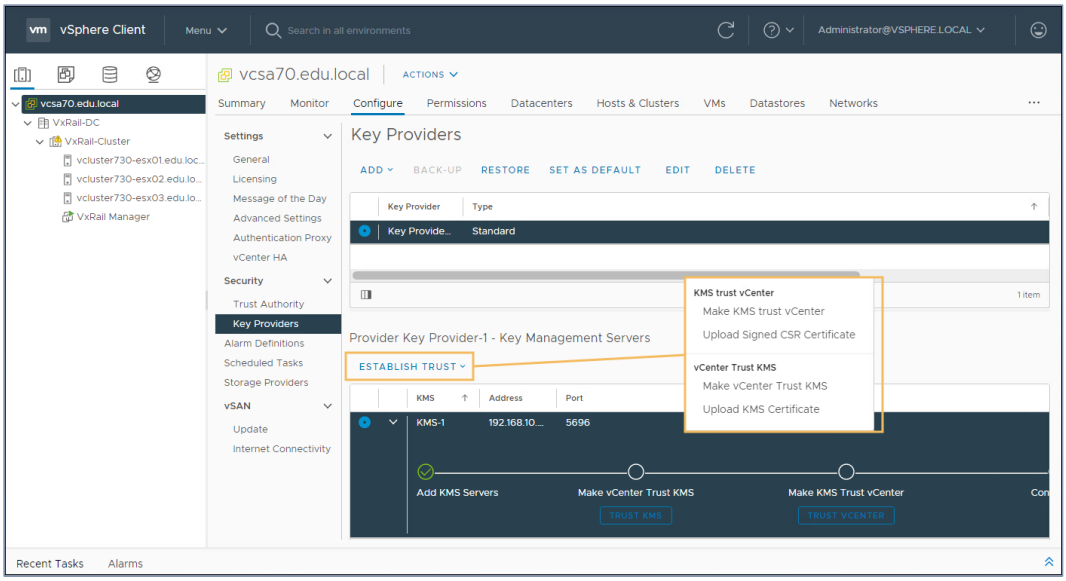
- A vSphere Native Key Provider (NKP) is an internal key provider.
- A Standard Key Provider is an external key provider.



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 Key Provider

Additional information:

- Set up the Standard Key Provider
- Set up a Native Key Provider
- VMware Certified Key Management Servers list

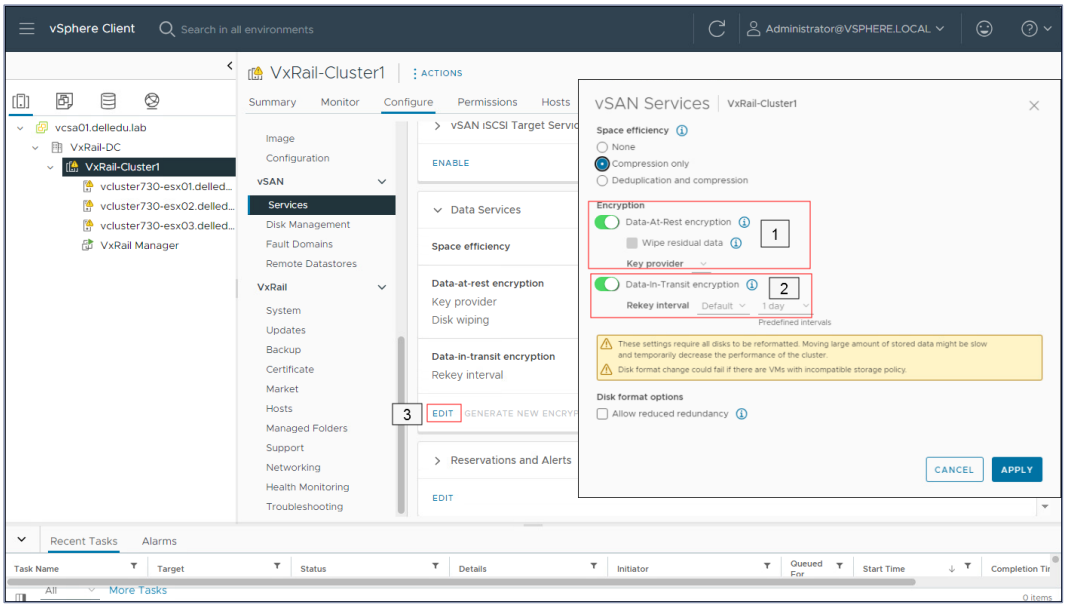
Enable vSAN OSA Encryption

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.

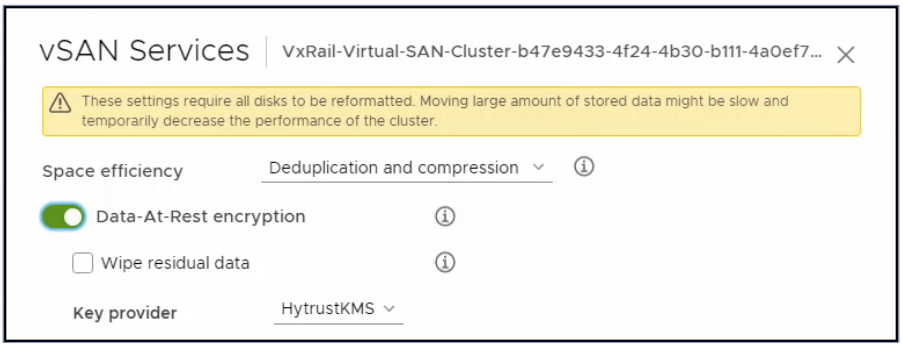
vSAN OSA encryption is enabled from the **vSAN Services** page. In the example, both **Data-at-Rest encryption** and **Data-in-Transit encryption** are enabled.

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

vSAN Services page with the vSAN Services dialog



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

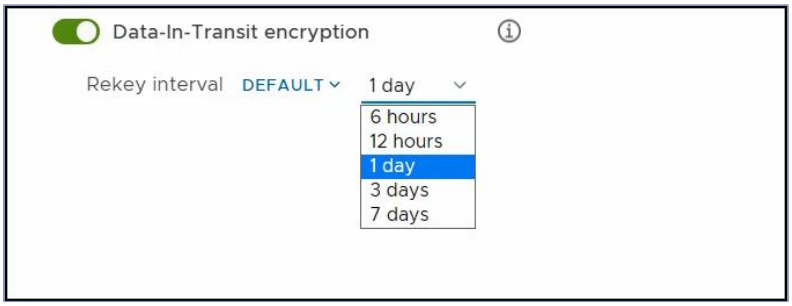


vSAN Services dialog with warning.

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.

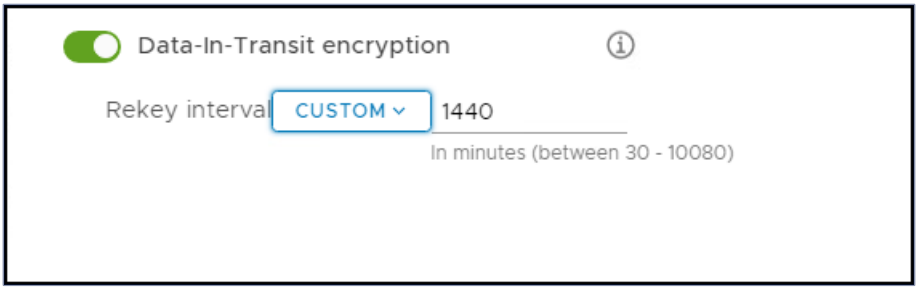
The **Key provider** defaults to the key provider that has been added to the vCenter Server.

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.



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

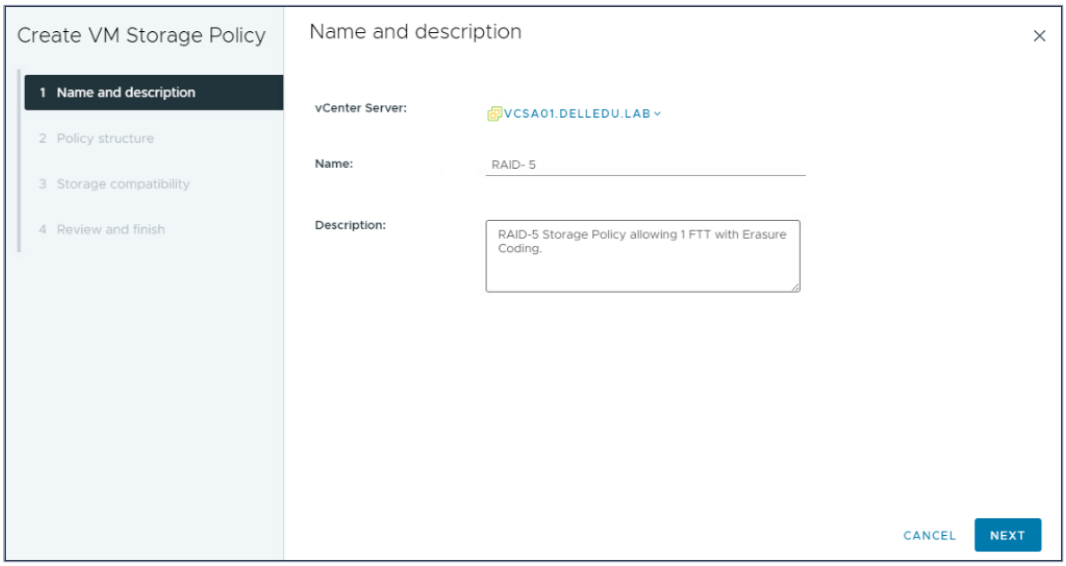
VM Storage Policies has vSAN specific attributes. A VM Storage Policy can be assigned to a vSAN datastore as the default policy.

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

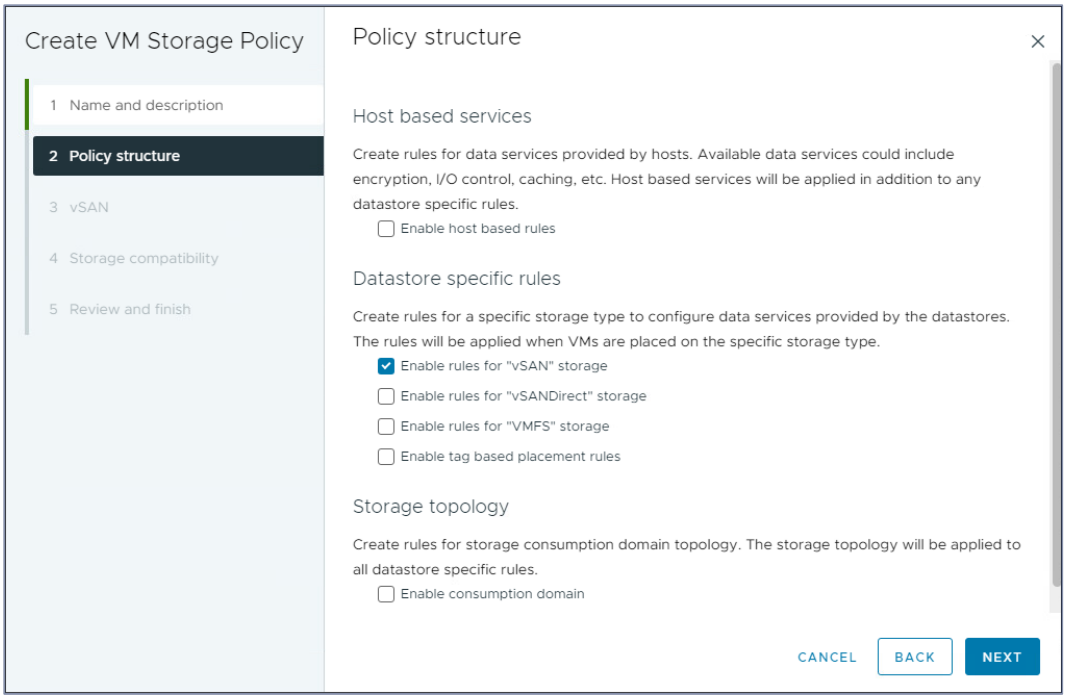
On the **Name and description** page, create a unique name and a description for the new policy.



Create VM Storage Policy wizard-Name and description

Policy structure

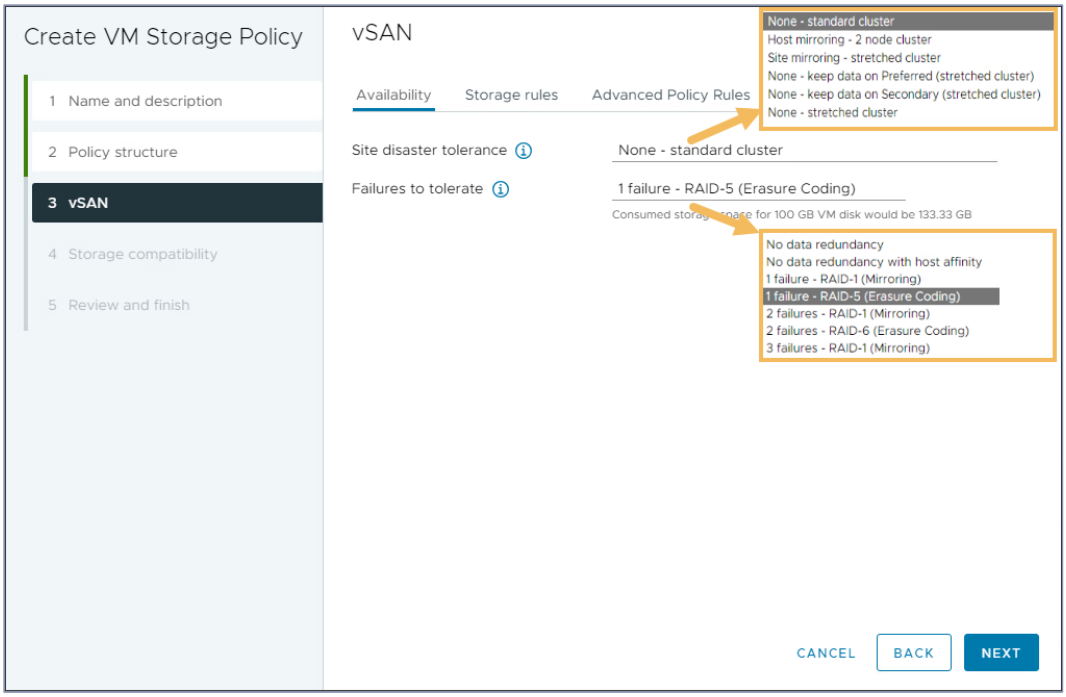
In the **Policy structure** page, check **Enable rules for "vSAN" storage**. A **vSAN** page is added to the wizard after enabling the rules for vSAN storage.



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 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.

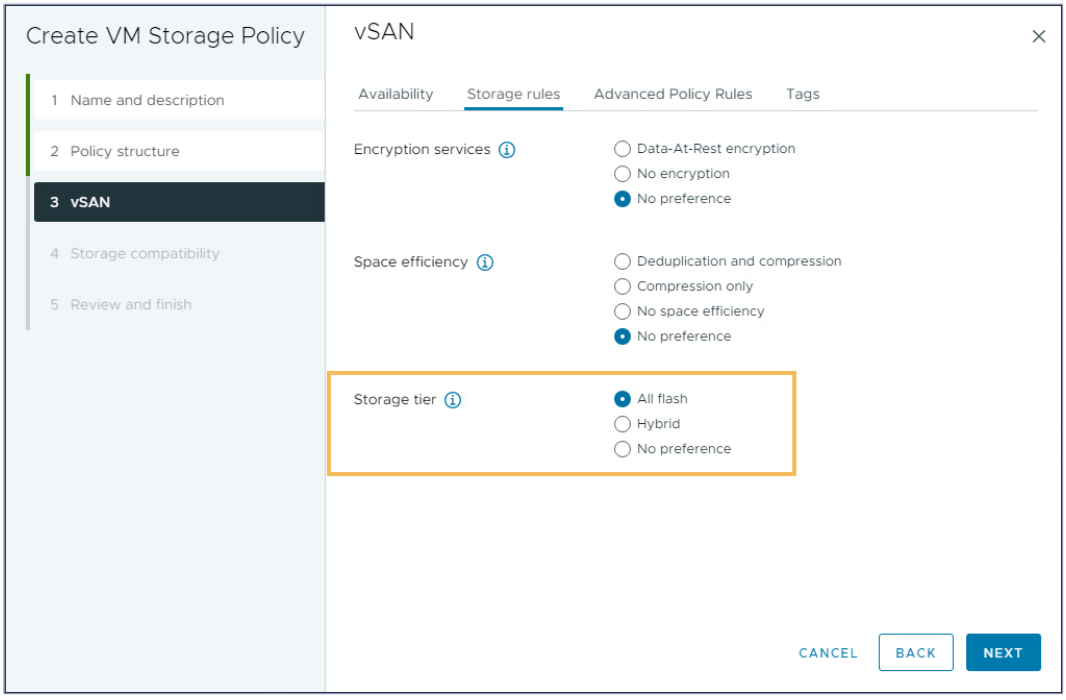
Erasure coding supports one Fault Domain failure with RAID-5 or two Fault Domain failures with RAID-6. Erasure coding is supported on All-flash systems only.

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).

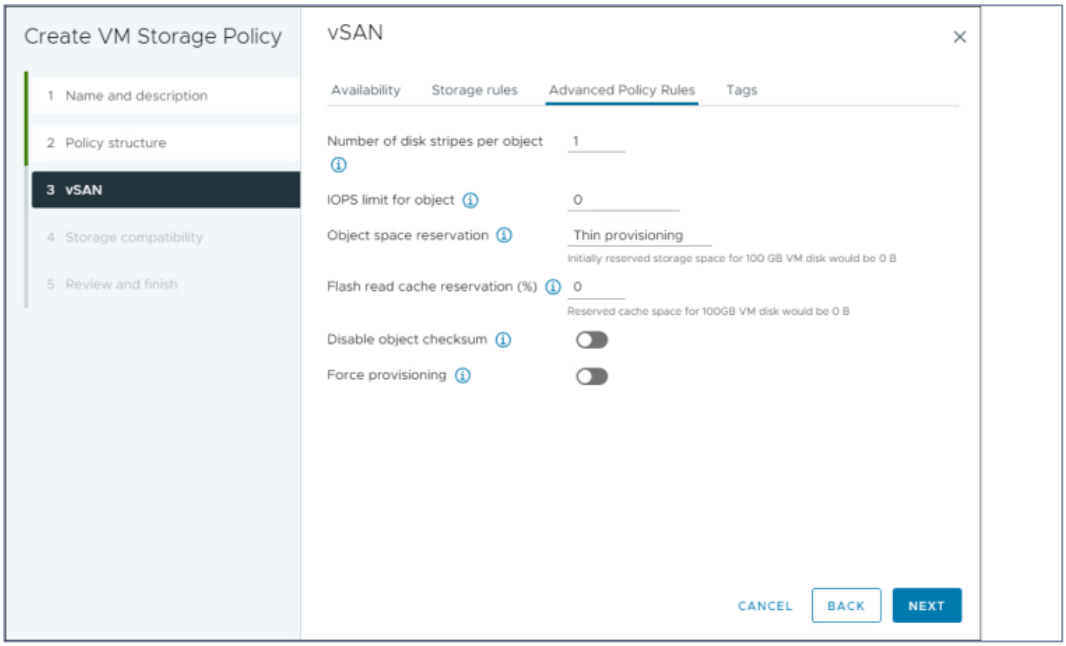
In the example below, the datastore must be on an **All flash** Storage tier and **No preference** for encryption services or space efficiency.



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

vSAN Advanced Policy Rules

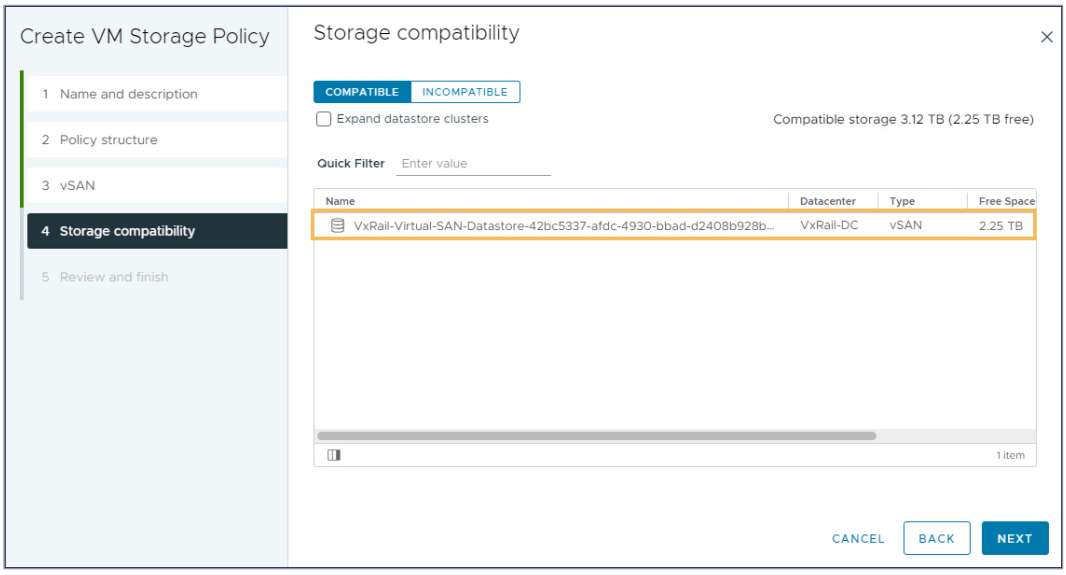
Under the **Advanced Policy Rules**, additional rules can be configured. For additional vSAN policy rules, see the vSAN Advanced Policy Rules. In this example, the default values have been selected.



Create 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.

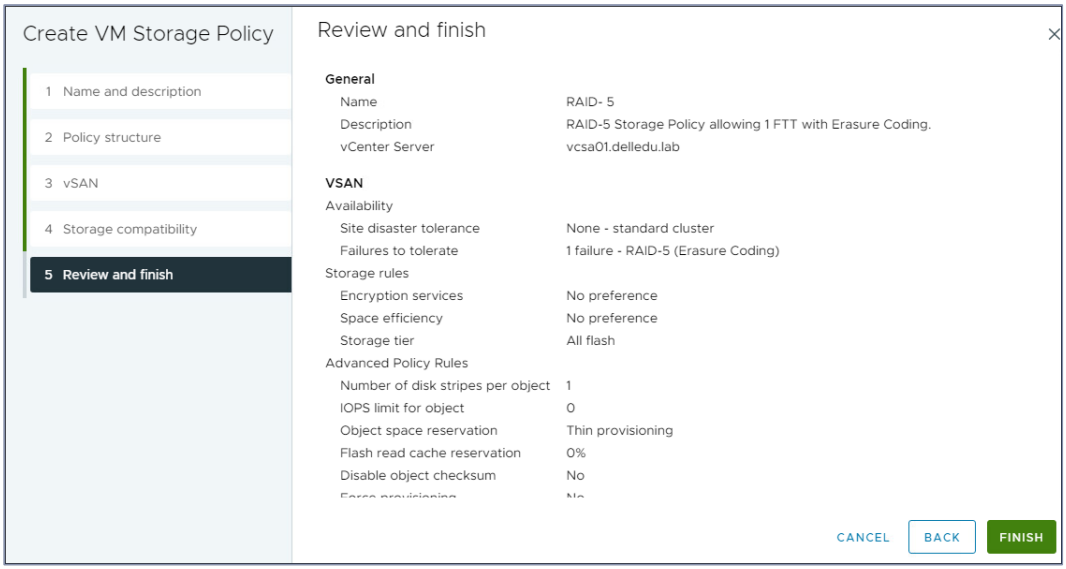


Create VM Storage Policy wizard-Storage compatibility

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

Review and finish

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



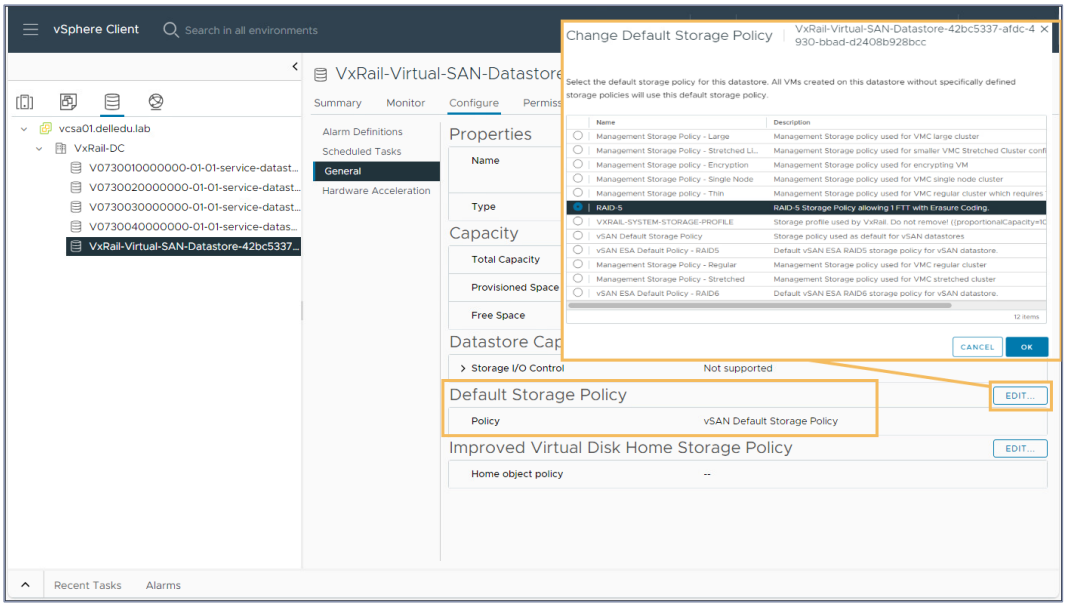
Create VM Storage Policy wizard-Review and finish

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.

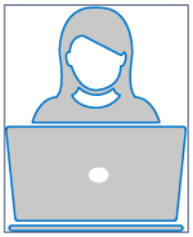


VxRail vSAN Datastore - Configure tab showing the Change Default Storage Policy wizard

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.

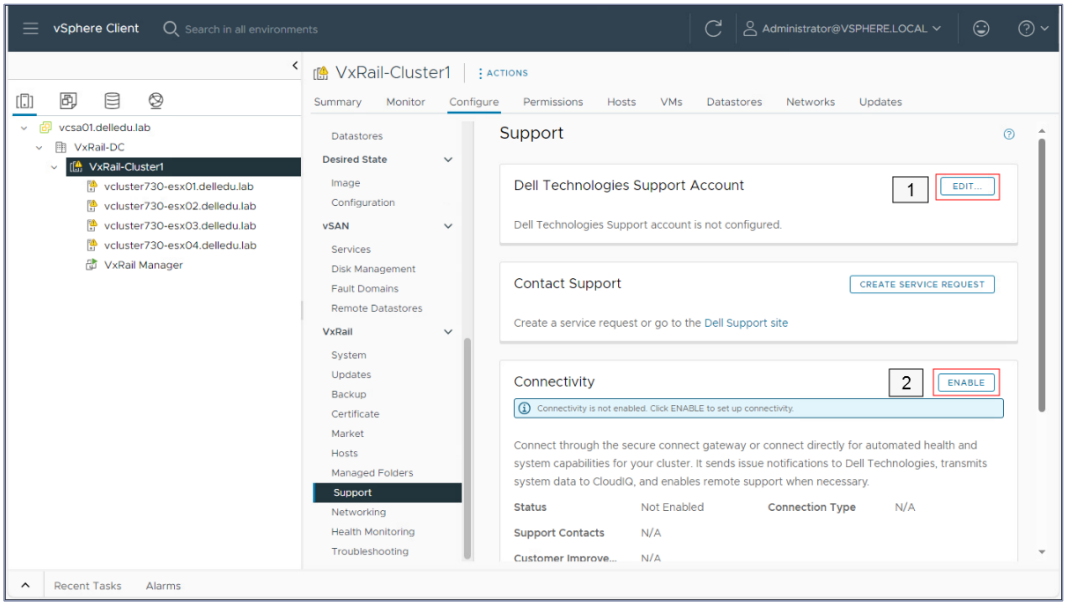
Configure Dell Support Account and Remote Support Connectivity

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.

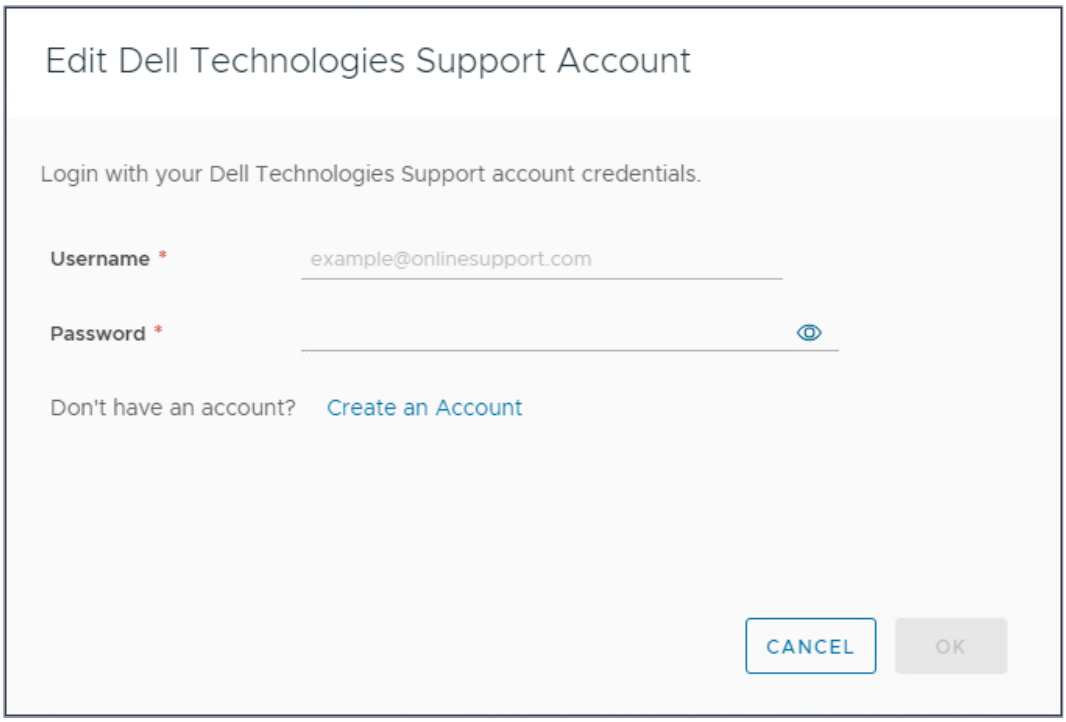
To access the **Support** page from the vSphere Client, select the **Configure** tab for the **VxRail-Cluster1**, then scroll down to **VxRail > Support**. To learn more about the configuration of support account and connectivity, select the two red hotspots.

VxRail Support page



1:

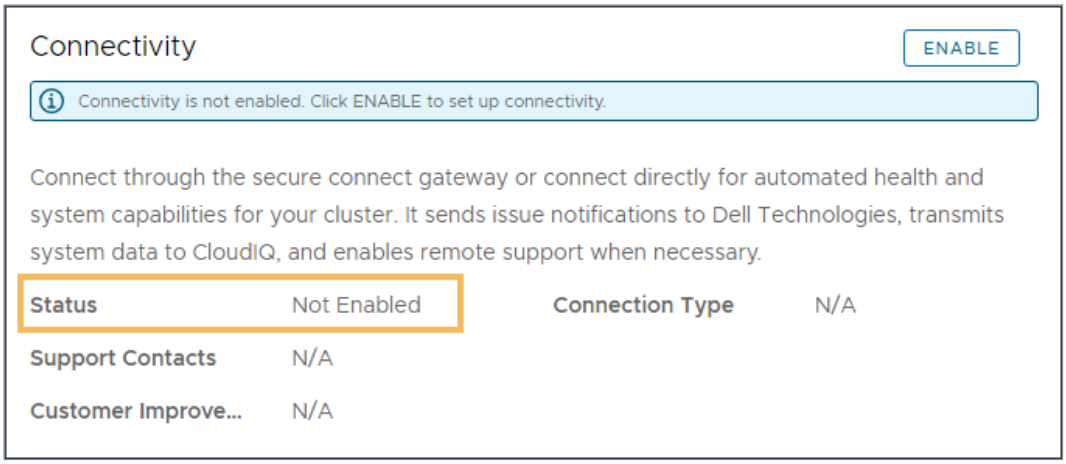
Enter the support account credentials on this screen to link the account with the VxRail system and allow access to support services. Before installation, obtain a support account from https://www.dell.com/myaccount/. The support account is used to:



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**.

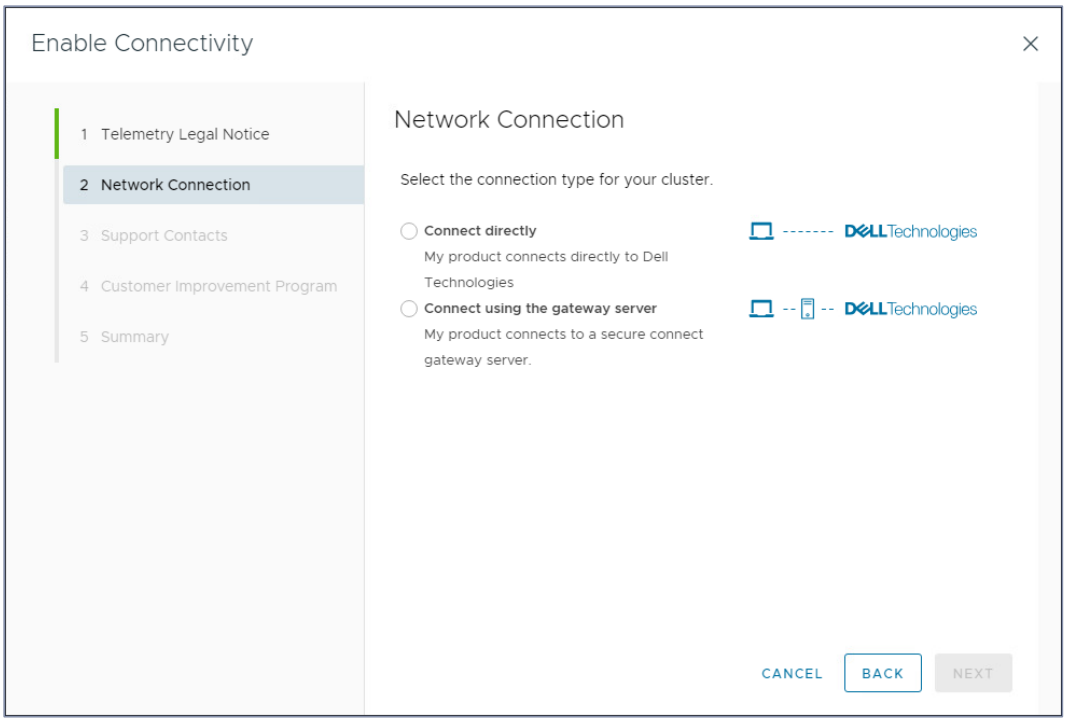


Connectivity Status window

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.



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

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.

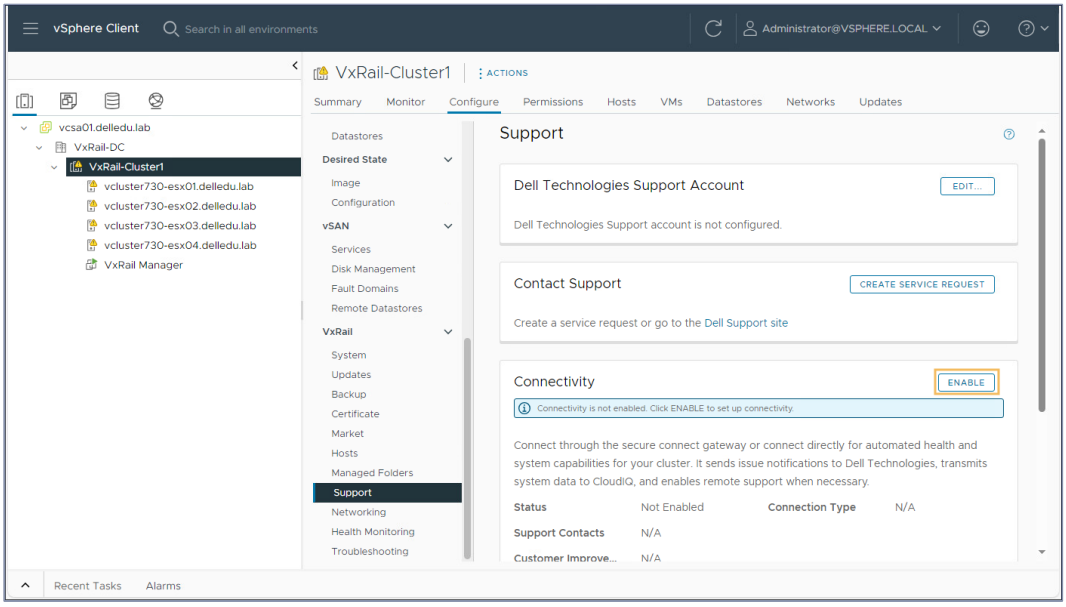
[1]For supported Secure Connect Gateway versions, see the VxRail 8.X Support Matrix. If Secure Connect Gateway is not installed, go to the Dell support page to download the installation files. The Secure Connect Gateway can be installed on the VxRail cluster or any other non-VxRail vSphere node.

Enable Remote Support Connectivity

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

Launch Enable Connectivity Wizard

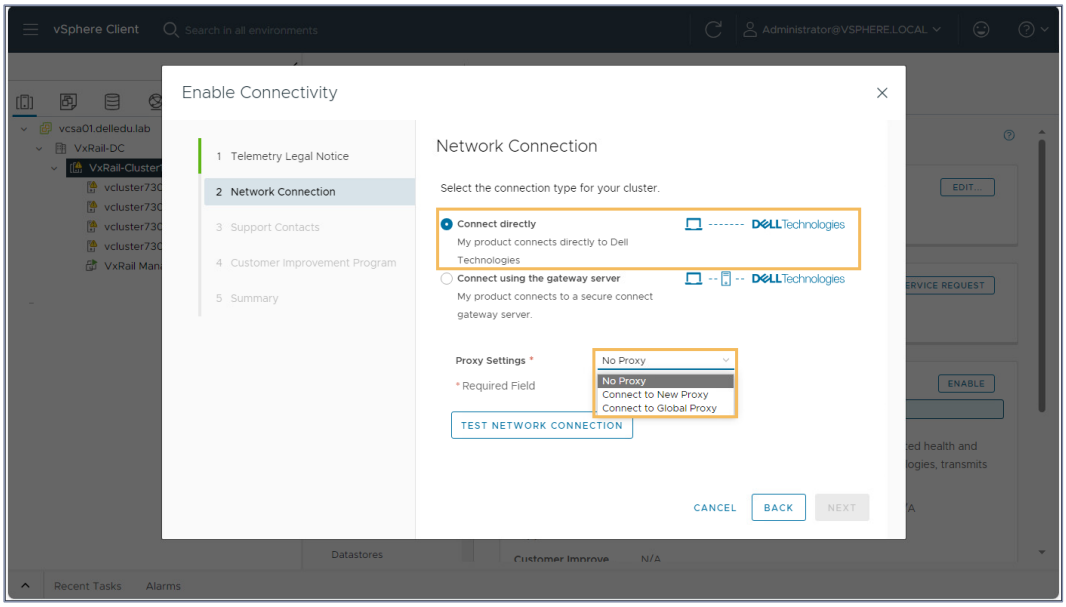
In the **Connectivity** section of the **VxRail > Support** page, select **ENABLE** to open the **Enable Connectivity** wizard. The Internet connection for VxRail Manager must be enabled on the **VxRail > Networking** page in order to enable Remote Connectivity here.



VxRail Plugin Support page with the Connectivity Enable button identified

Network Connection - Connect Directly

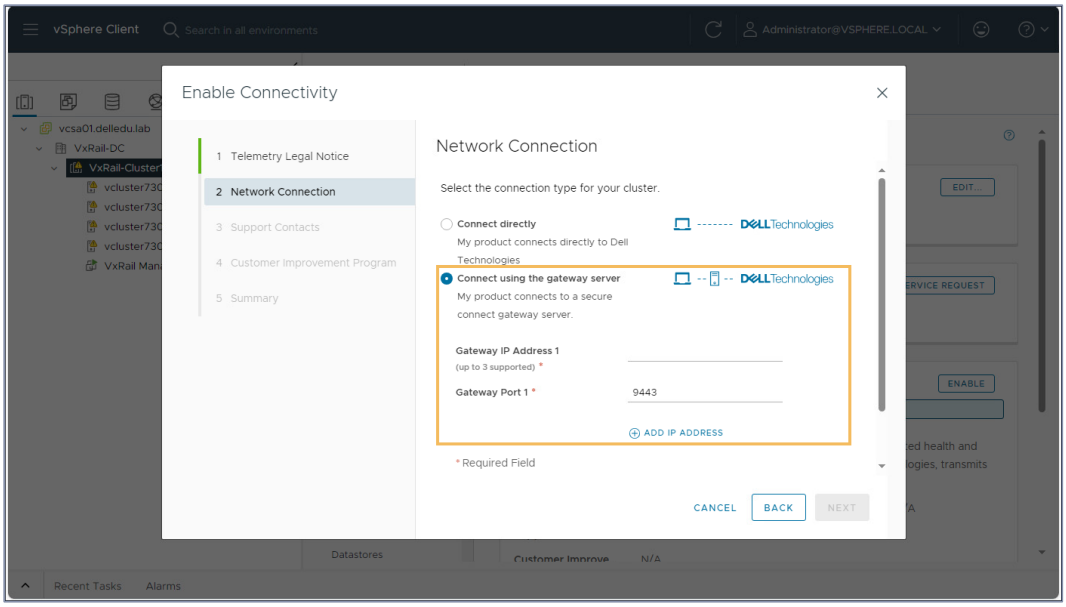
In the **Network Connection** step of the wizard, select **Connect directly,** if the VxRail system connects directly to Dell support. Administrators can choose **No Proxy, Connect to Global Proxy** that has been configured in the **VxRail > Networking** page or **Connect to New Proxy**.



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

Network Connection - Connect using Gateway

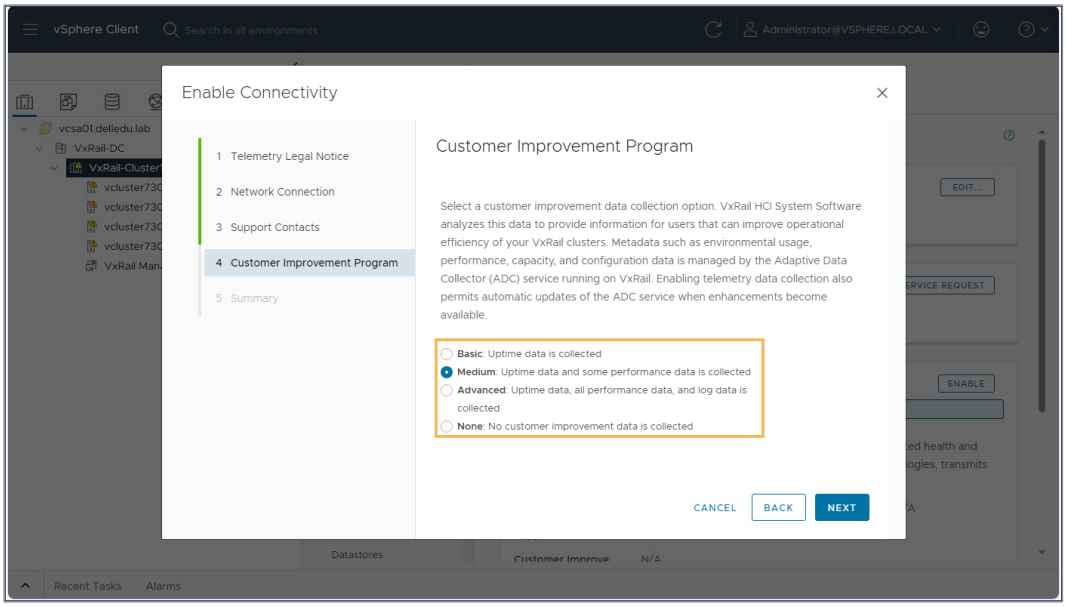
In the **Network Connection** step of the wizard, select **Connect using the gateway server,** if the VxRail system connects to an SCG. Enter the IP address and port for the gateway.



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.



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.

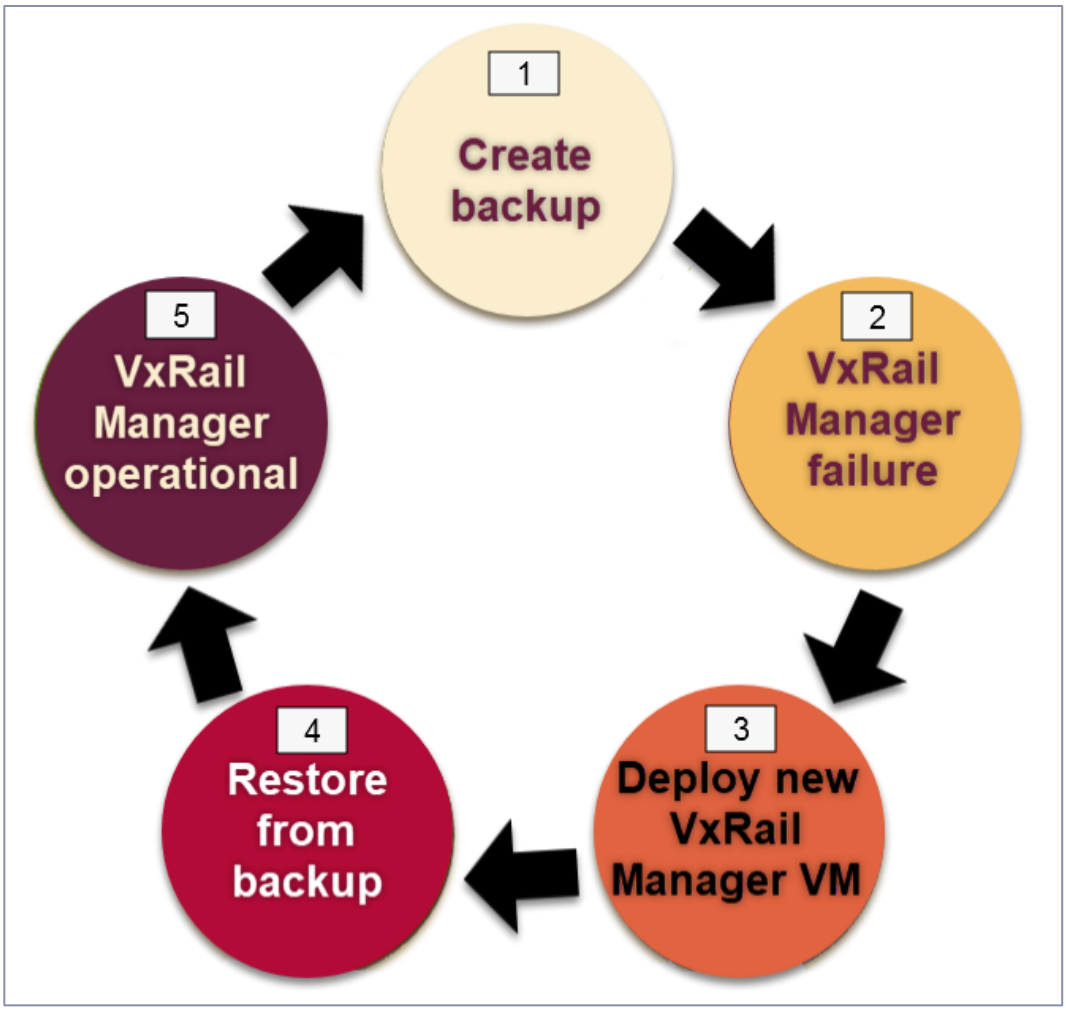
Configure VxRail Manager File-Based Backup

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



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.


```
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, --configmetwork   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 #
```

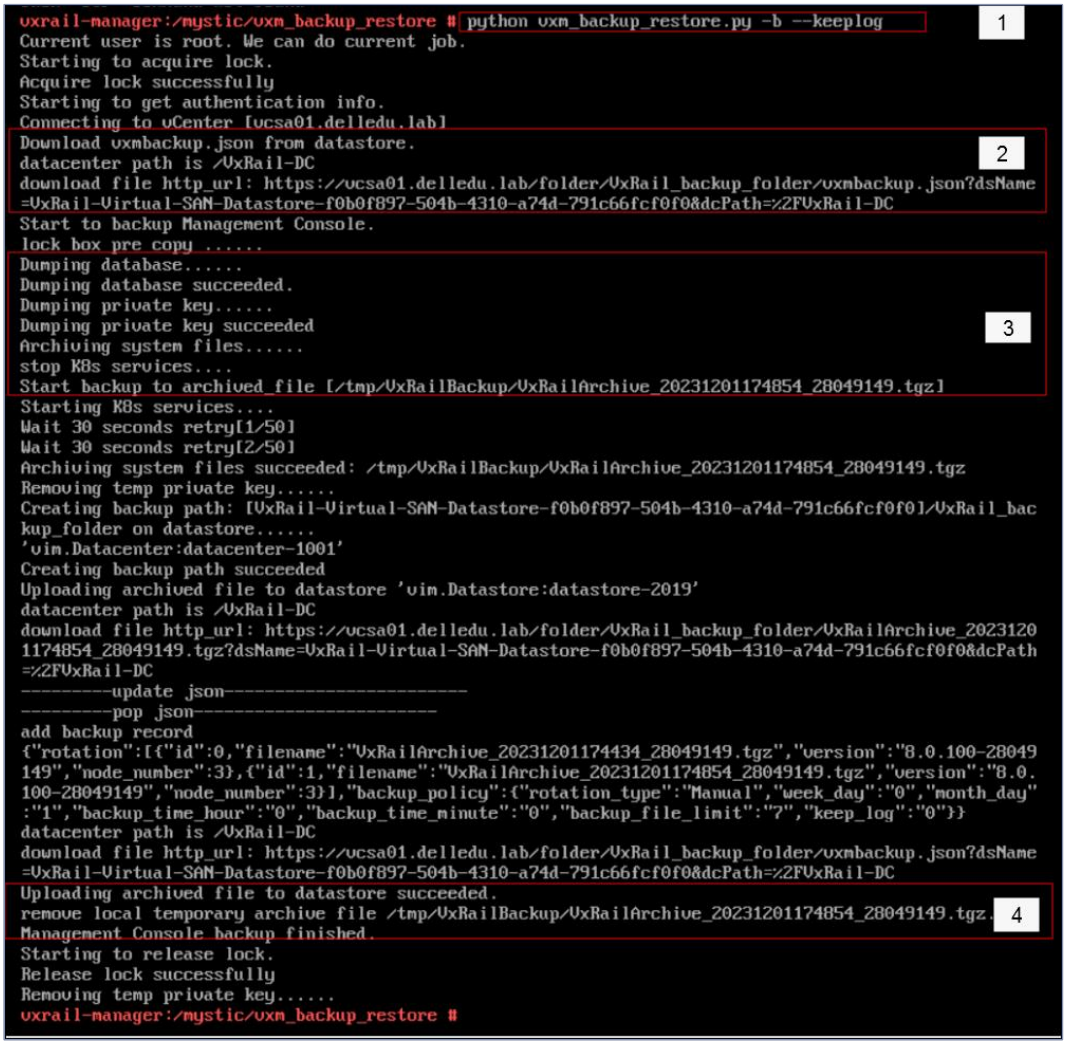
VxRail Manager backup and restore script - Syntax

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



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 ***vxmbackup.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

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

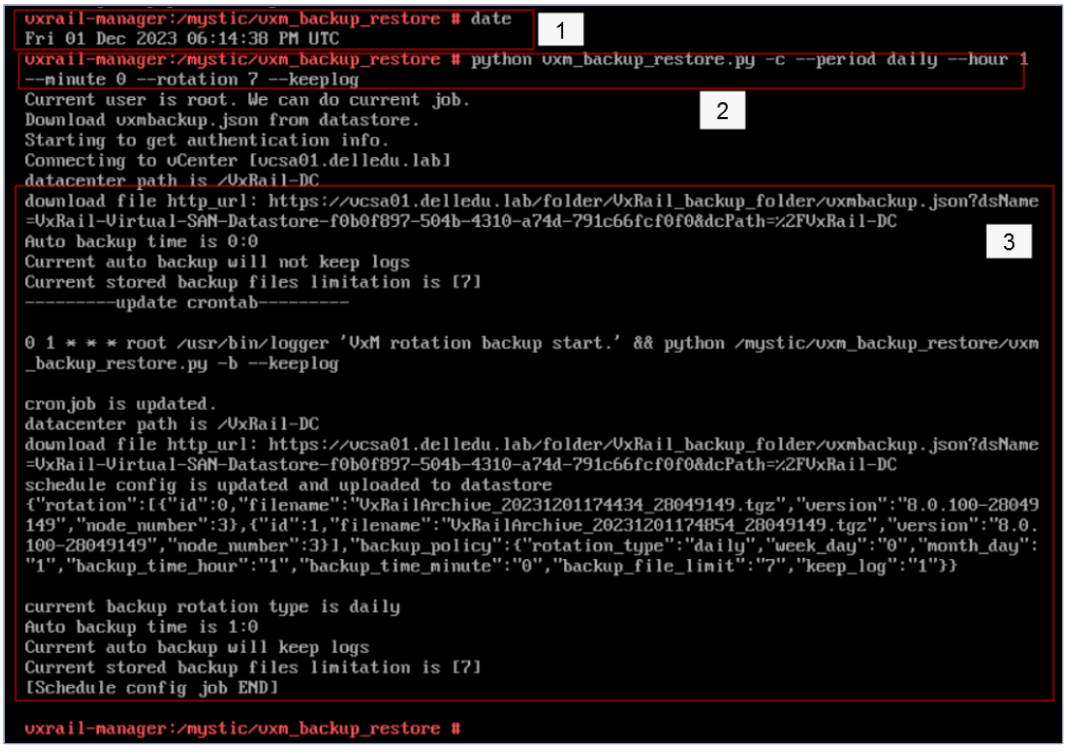
3: The script creates the backup archive locally on the VxRail Manager VM and then uploads the archive to the VxRail vSAN datastore.

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



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

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 ***vxmbackup.json*** file. The updated ***vxmbackup.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/v
olumes/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:HlIs40T0Ge0HALWR+Mq+kZzZXhdxK0CV55TBcca+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                                    100%   17MB  19.7MB/s   00:00
mystic@vxrail-manager:~>
```

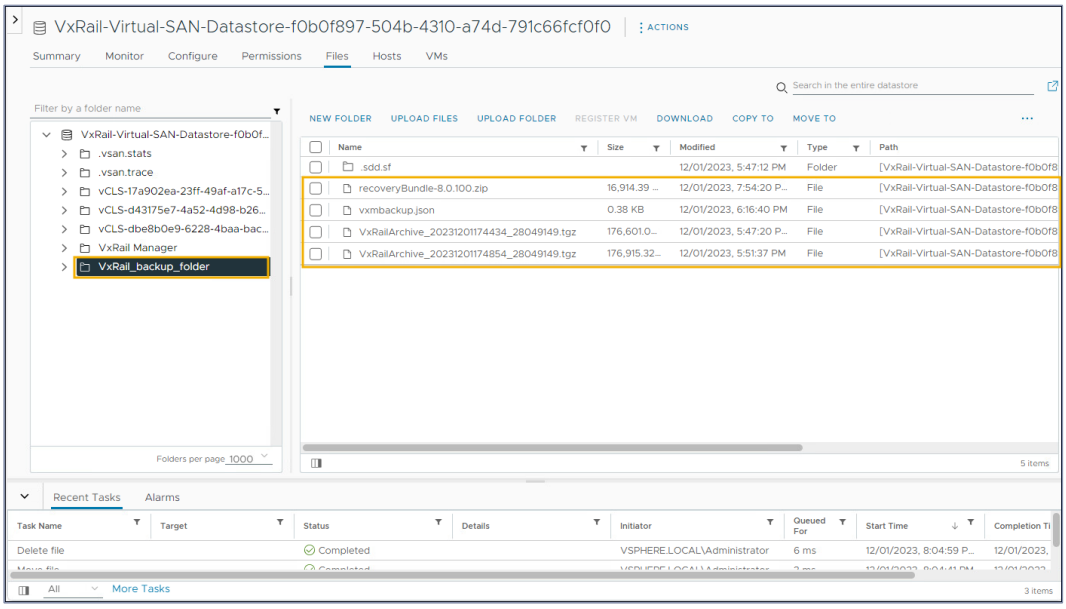
Example of copying the Recovery Bundle to the VxRail vSAN datastore

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 ***vxmbackup.json*** file, and two backup archives.



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

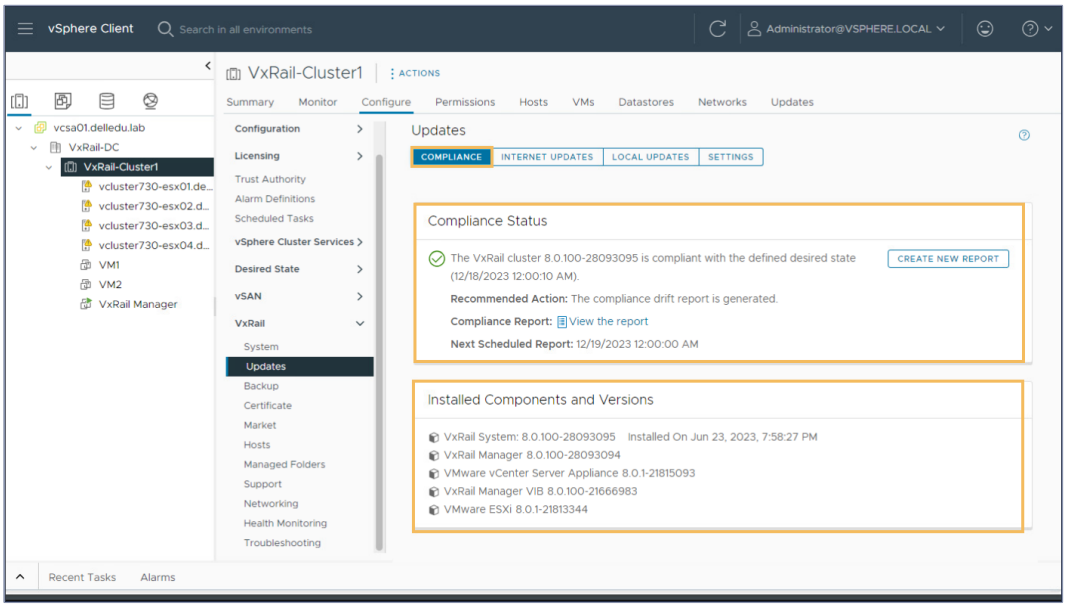
The VxRail software update is initiated from the VxRail Plugin. To initiate a software update, select the **Configure** tab for a cluster. In the middle pane, select **VxRail > Updates**.

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.

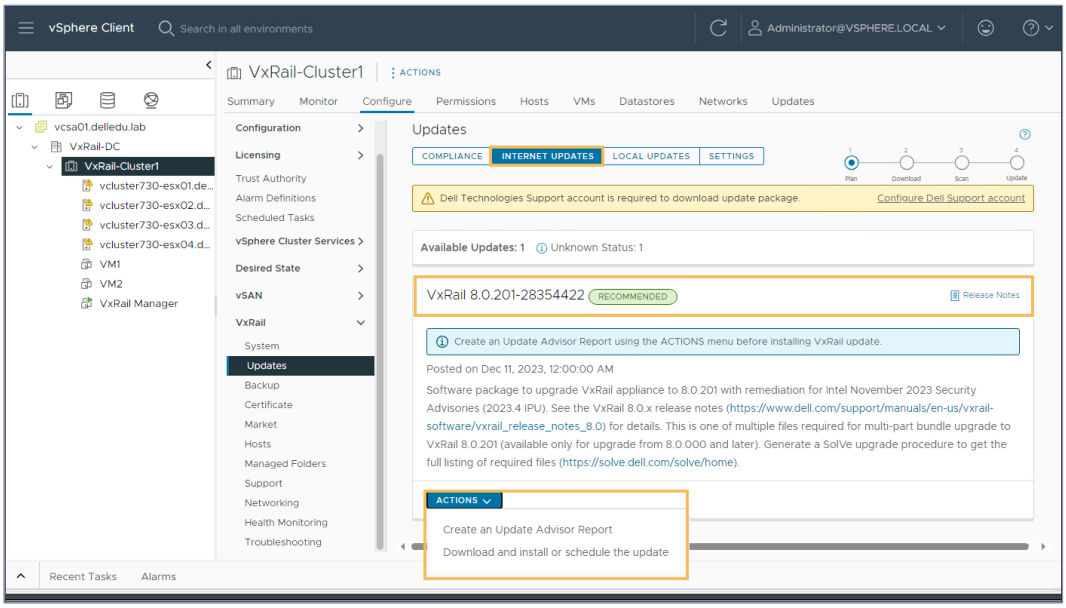


VxRail Plugin Updates COMPLIANCE tab

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.

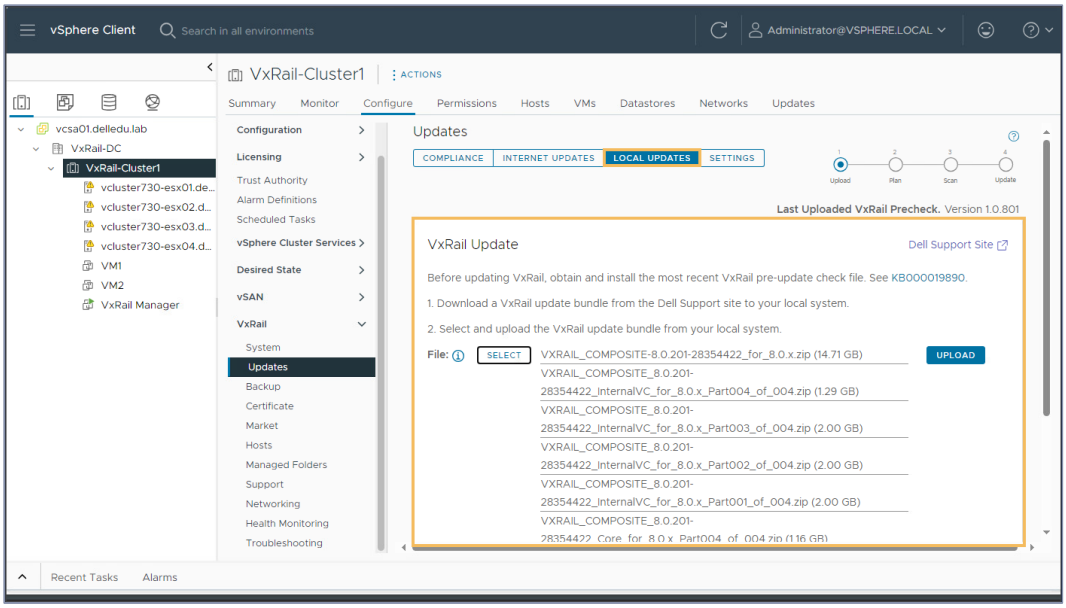


VxRail Plugin INTERNET UPDATES tab

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.



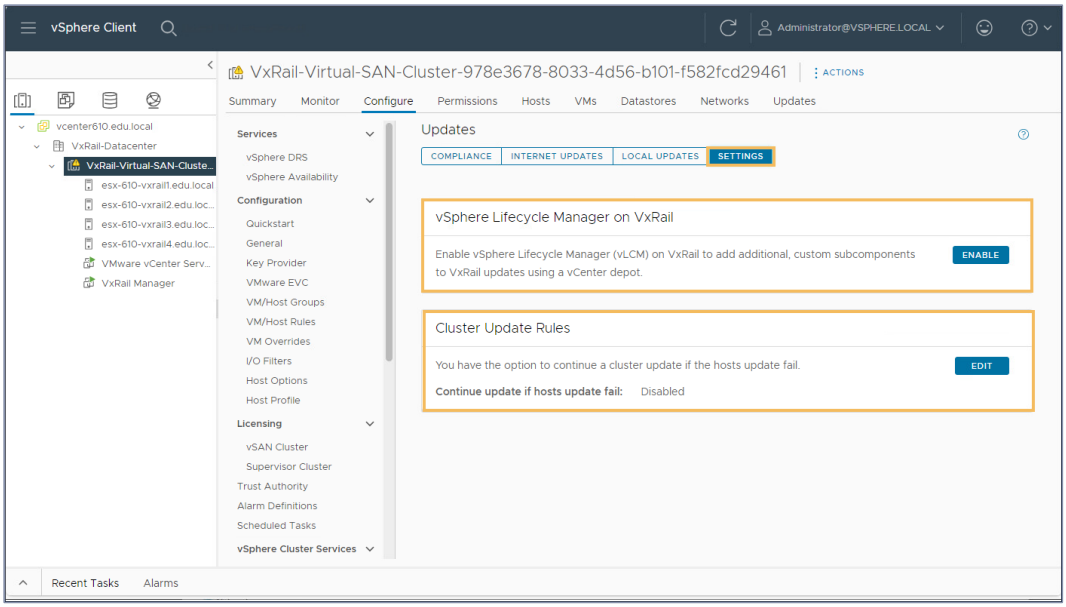
VxRail Plugin LOCAL UPDATES tab showing multiple files that are uploaded to VxRail

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.



VxRail Plugin Updates SETTINGS tab

Enabling vLCM

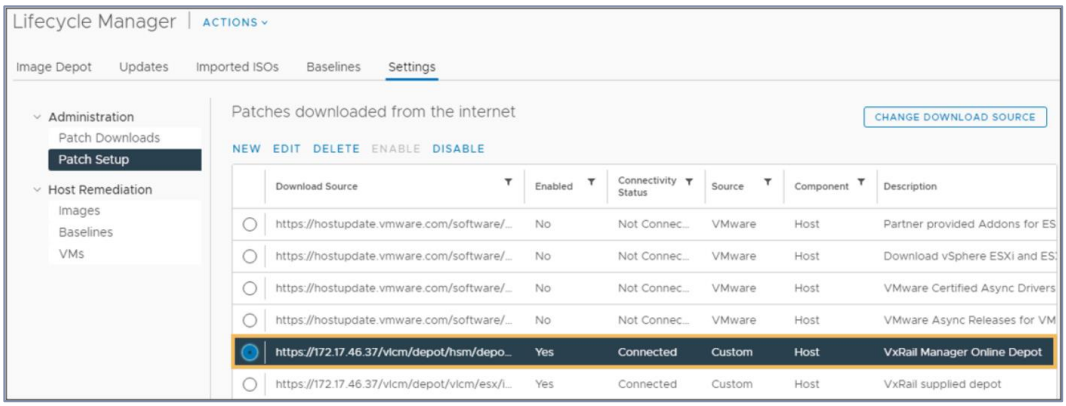
To learn about enabling vLCM on VxRail, select each tab.

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.

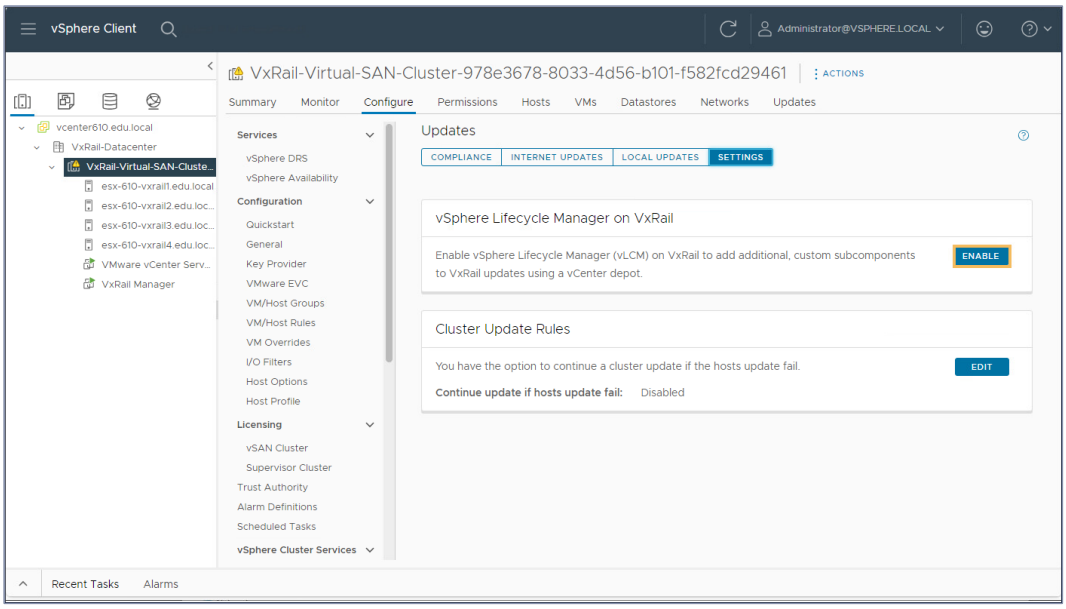
To disable the **Download Sources**, go to **vSphere Menu > Lifecycle Manager > Settings > Patch Setup**.



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.



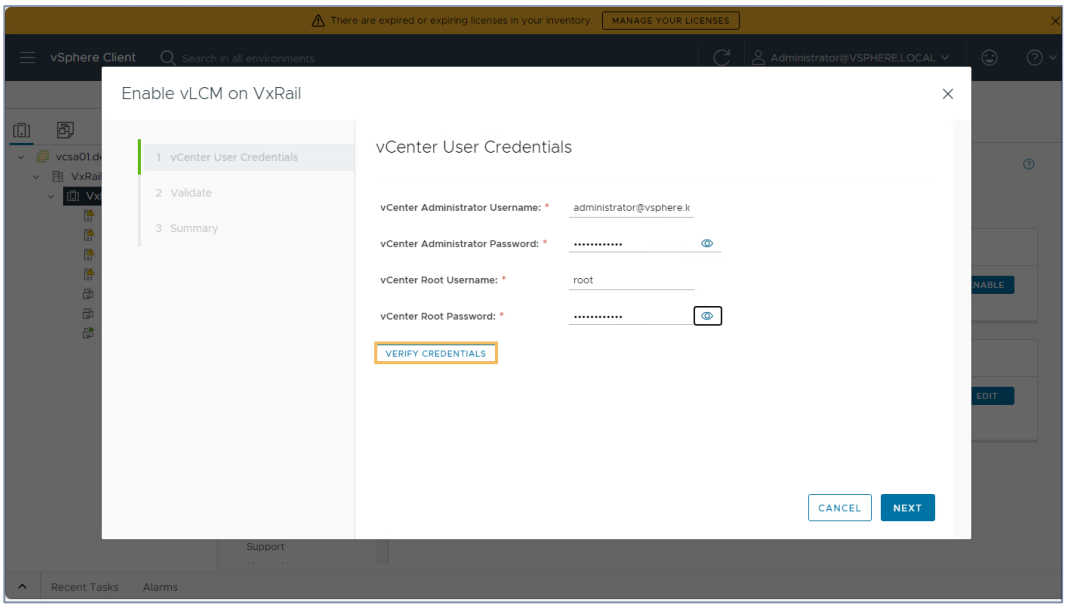
VxRail Plugin Updates SETTINGS tab with the vLCM on VxRail ENABLE button highlighted

Enter Credentials

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

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

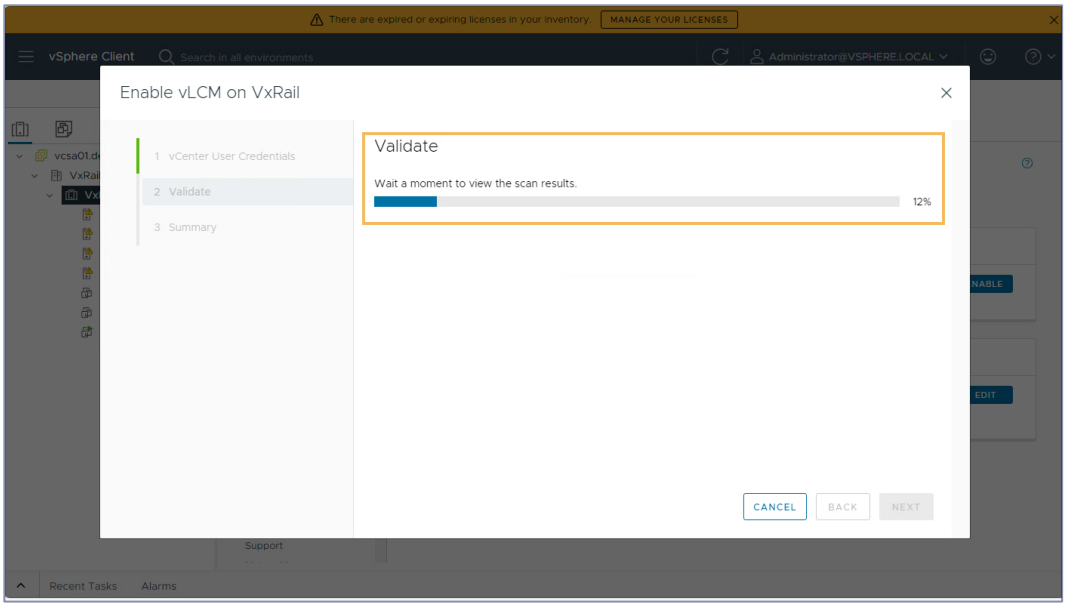
After the **VERIFY CREDENTIALS** button is selected, the system will request confirmation that a self-signed certificate can be added to the SSL Certificate folder on the vCenter Server.



Enable vLCM on VxRail Wizard vCenter User Credentials page

Validate

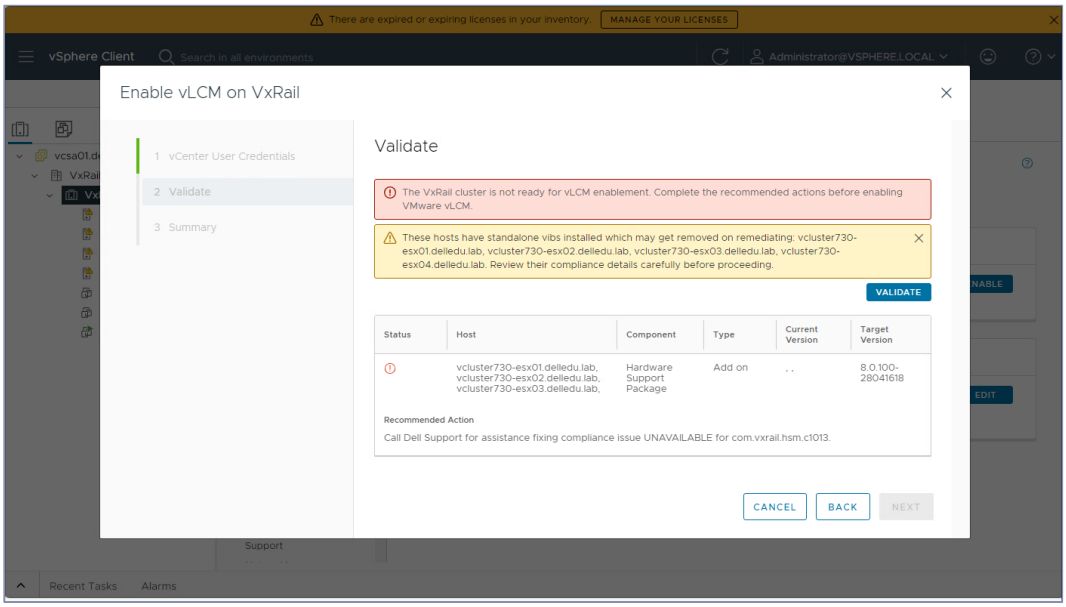
Once the credentials have been validated, the system will validate that the cluster is ready to enable vLCM on VxRail.



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 Lifecyle 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.

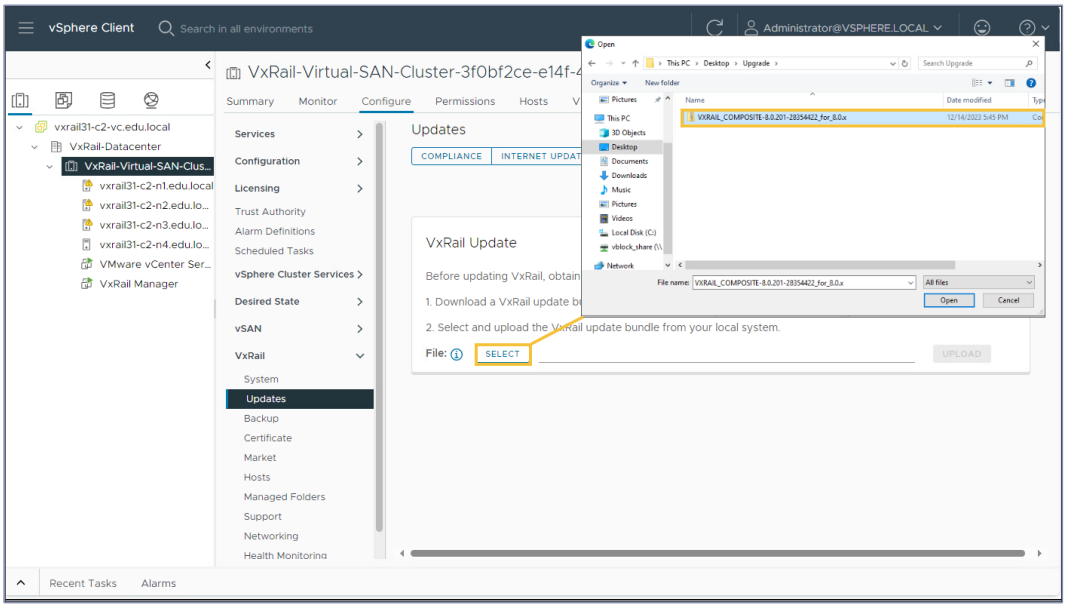
- Run VxVerify to check update readiness of the VxRail system.
- Ensure the cluster and vSAN are healthy.
- Take a snapshot of each service VM.
- Perform the upgrade.

VxRail Software Upgrade Using Local Updates

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

Select File

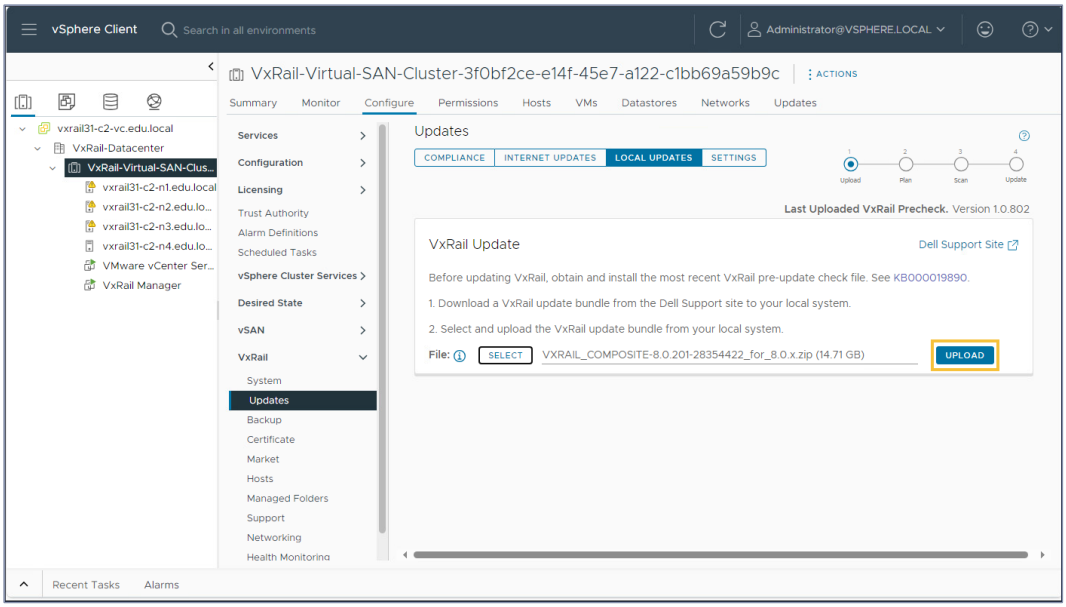
In the open file dialog, select the update file(s) that were previously downloaded and saved locally. If multipart files are used, ensure that all multipart files are uploaded at the same time and do not rename any of the files.



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.

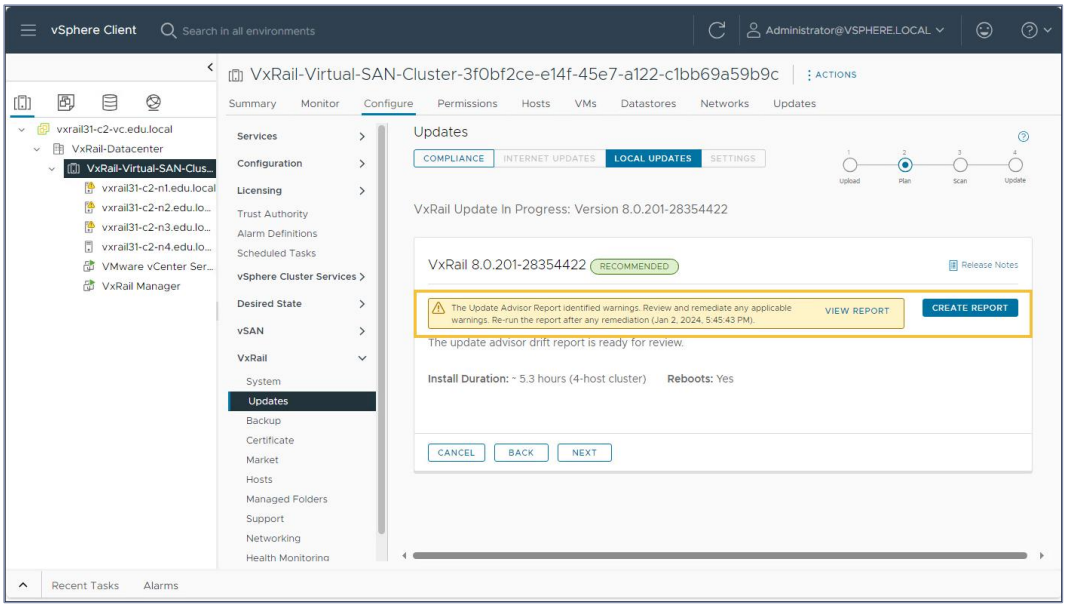


VxRail Local Updates page with the UPLOAD button highlighted

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.

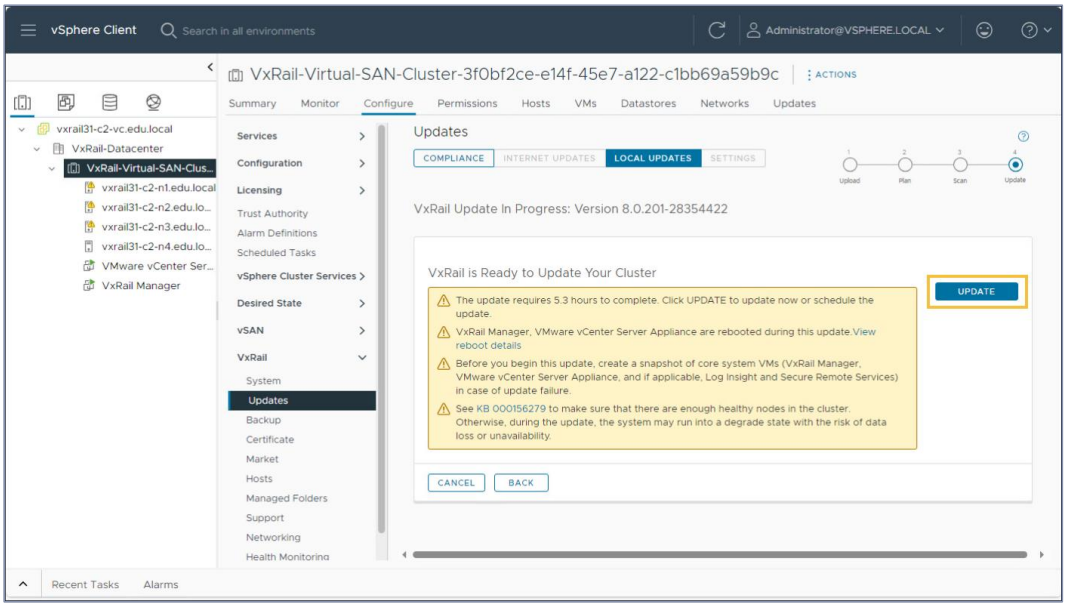
View a sample Advisory Report.



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.

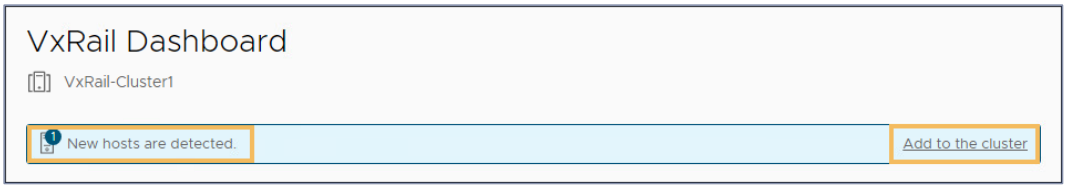
Follow the procedure to complete the node add process. High-level steps:

- 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

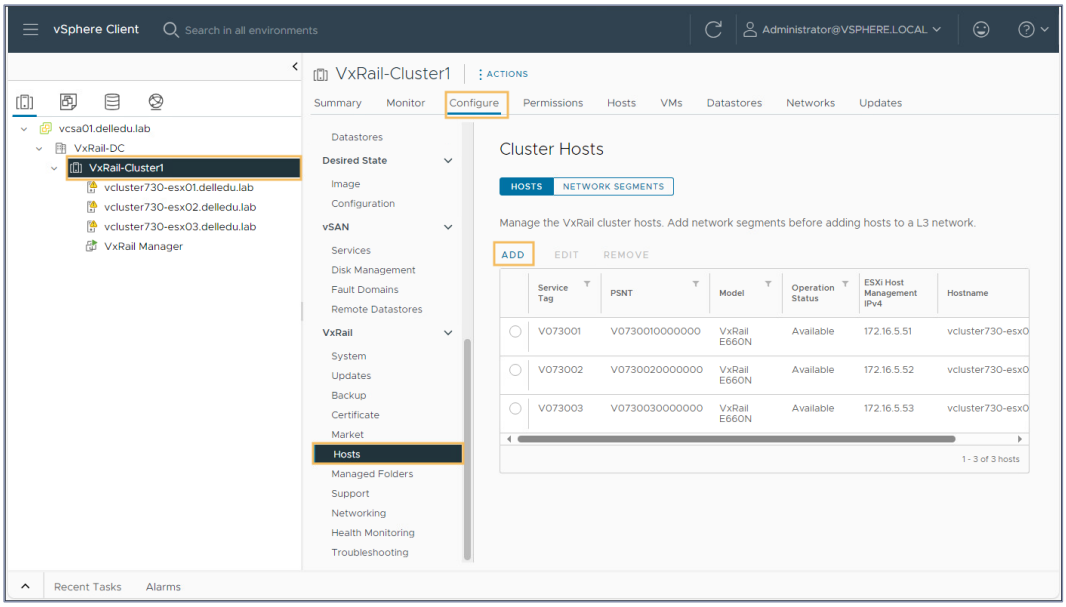
For VxRail clusters configured with automatic node discovery, the **VxRail Dashboard** displays a notification when new nodes are discovered.



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**.



VxRail Cluster Hosts page

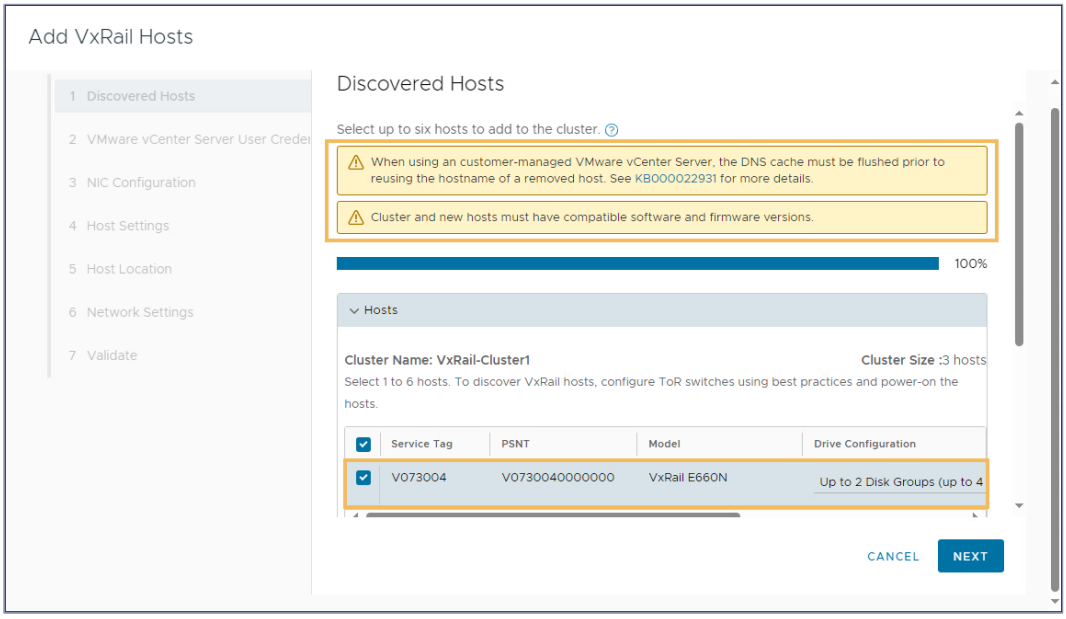
Add VxRail Hosts Wizard

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.

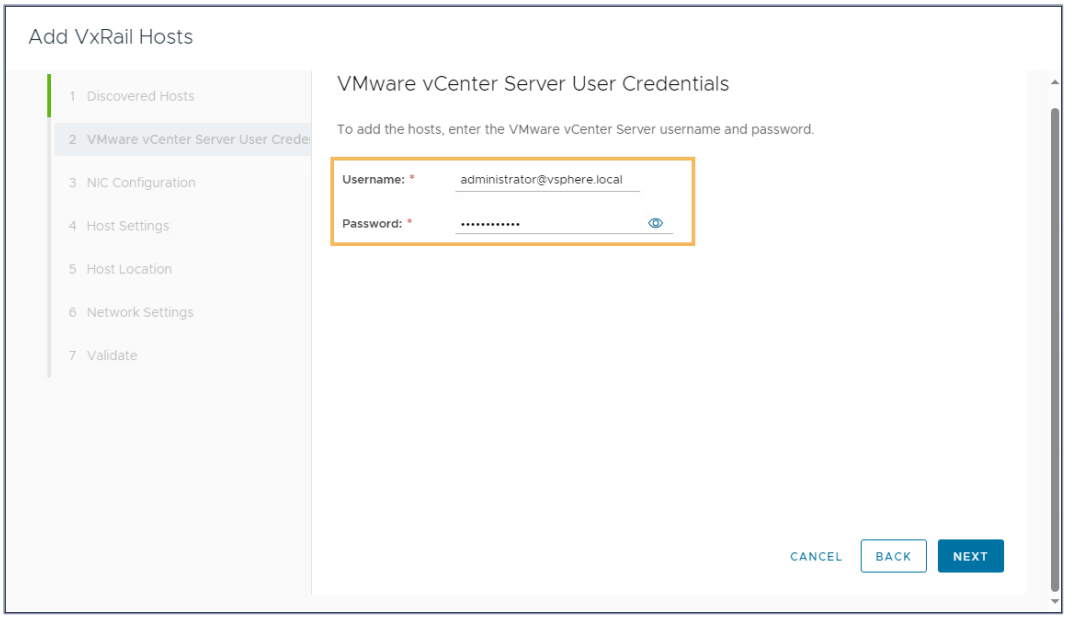
Select the nodes that should be added to the cluster. In the example, one compatible node has been discovered. Click **NEXT**.



Add VxRail Hosts wizard-Discovered Hosts

VMware vCenter Server User Credentials

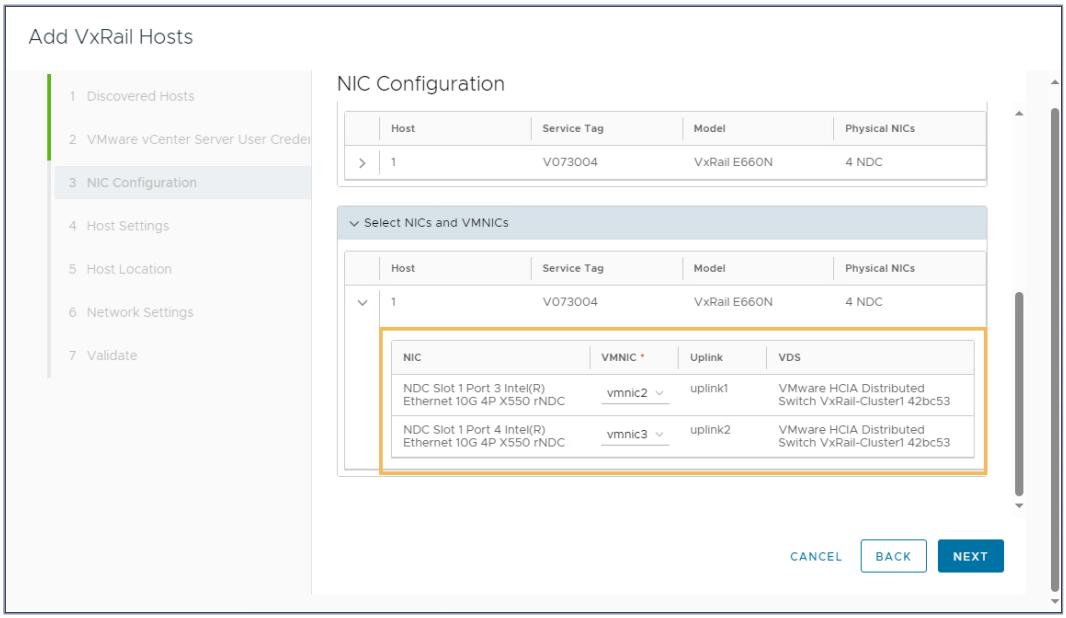
Provide the VMware vCenter user credentials. Click **NEXT**.



Add VxRail Hosts wizard-VMware vCenter Server User Credentials

NIC Configuration

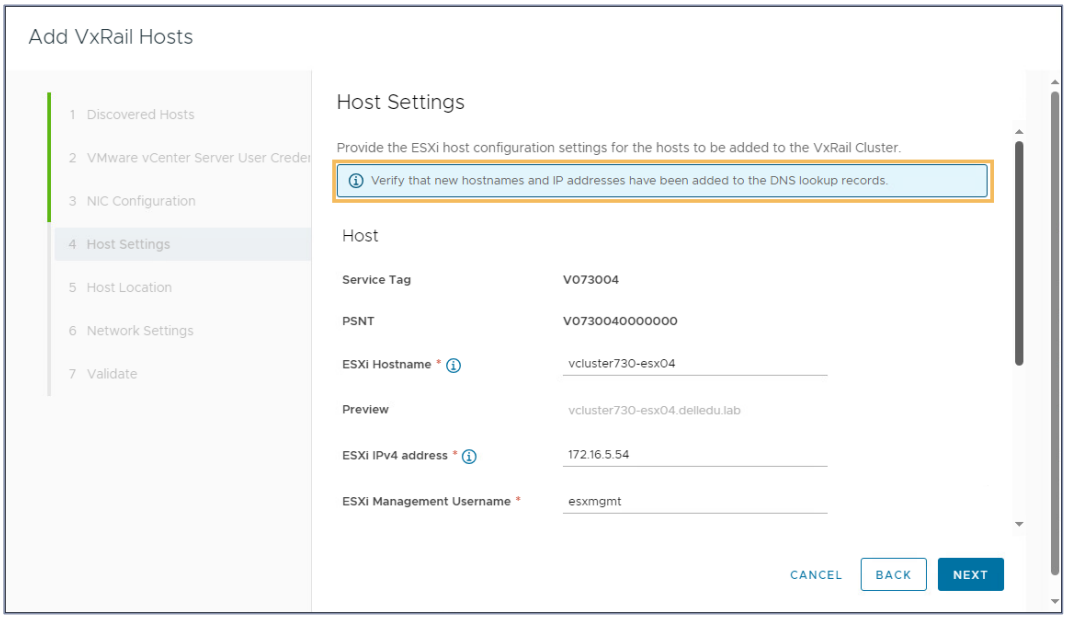
Map the physical NICs to the uplinks on the VDS. The NIC to uplink mapping defaults to that of the first node in the VxRail cluster. Click **NEXT**.



Add VxRail Hosts wizard-NIC Configuration

Host Settings

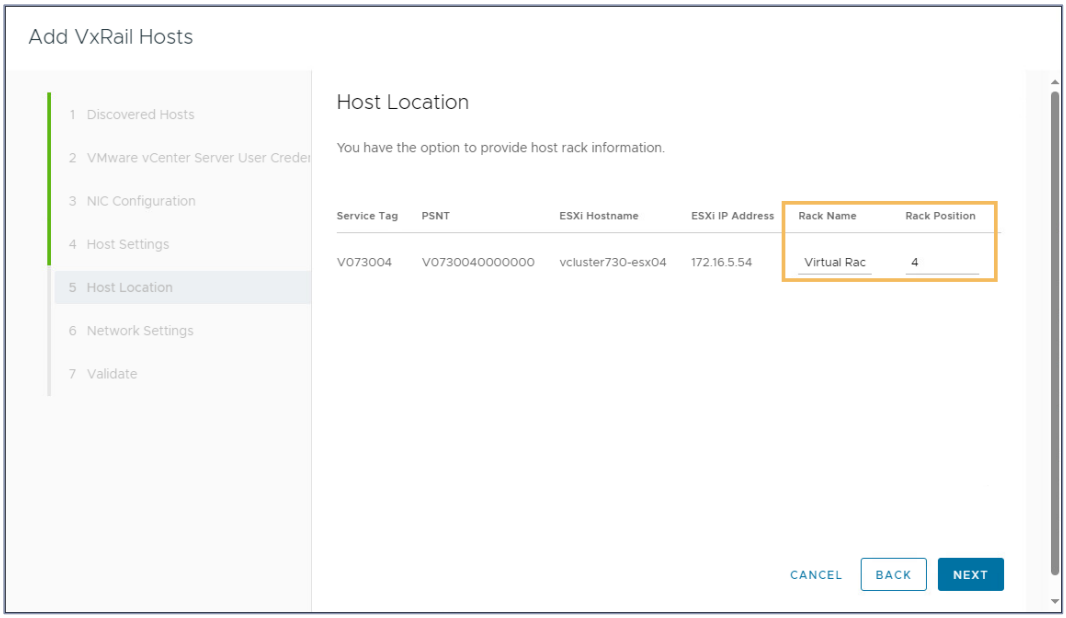
Provide the hostname, IP address, management username, management password, and root password. For VxRail implementations with an external DNS server, ensure that the forward and reverse Type A records have been added. Click **NEXT**.



Add VxRail Hosts wizard-Host Settings

Host Location

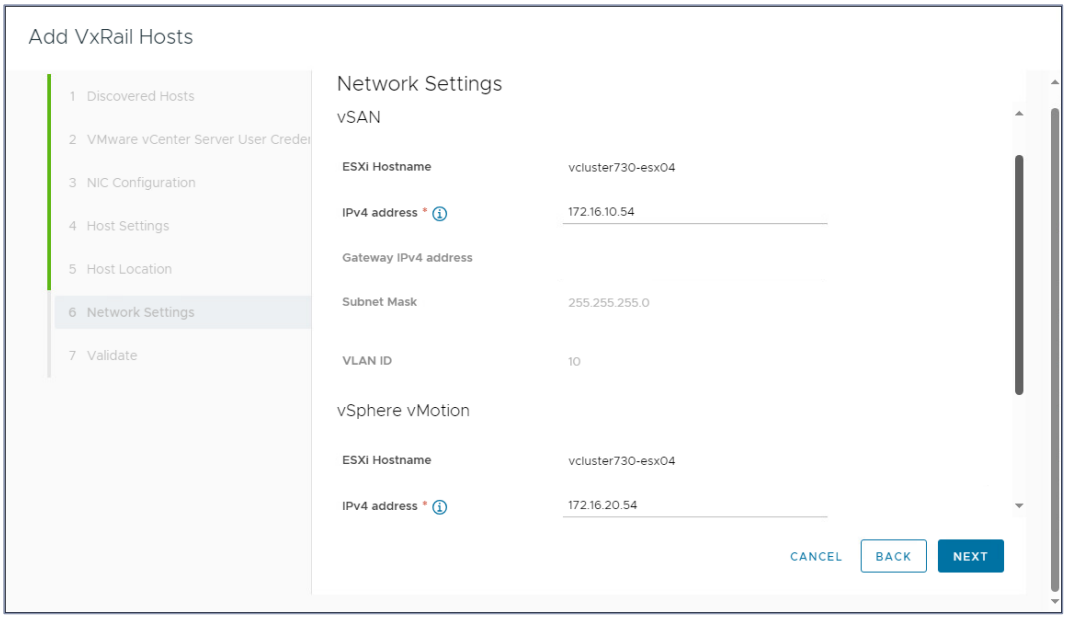
Optionally provide the rack name and position. Click **NEXT**.



Add VxRail Hosts wizard-Host Location

Network Settings

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

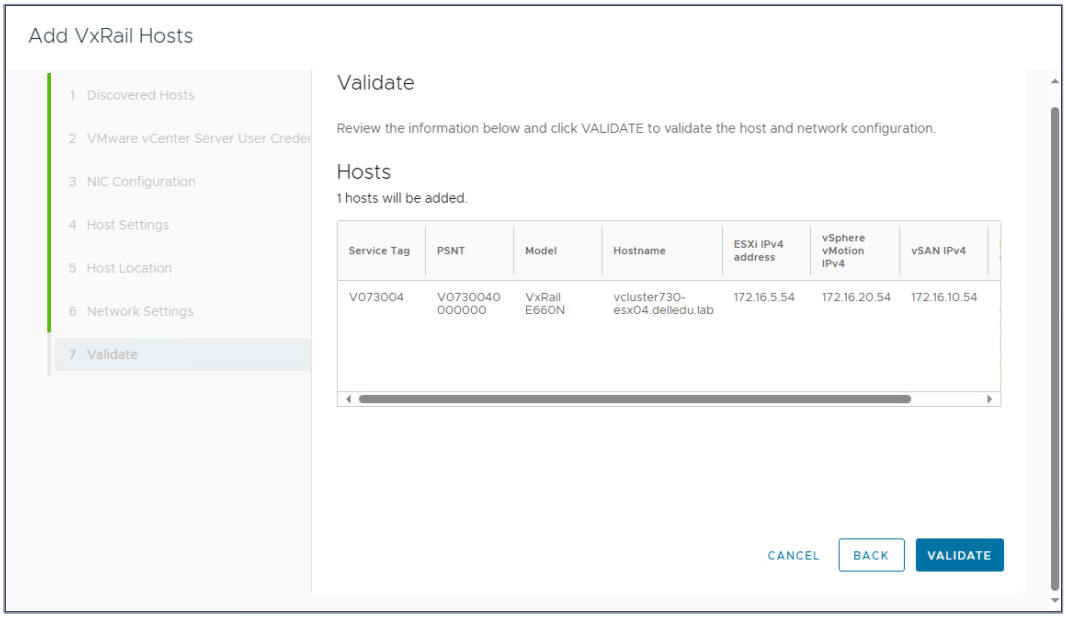


Add VxRail Hosts wizard Network Settings - vSAN and vMotion

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**.



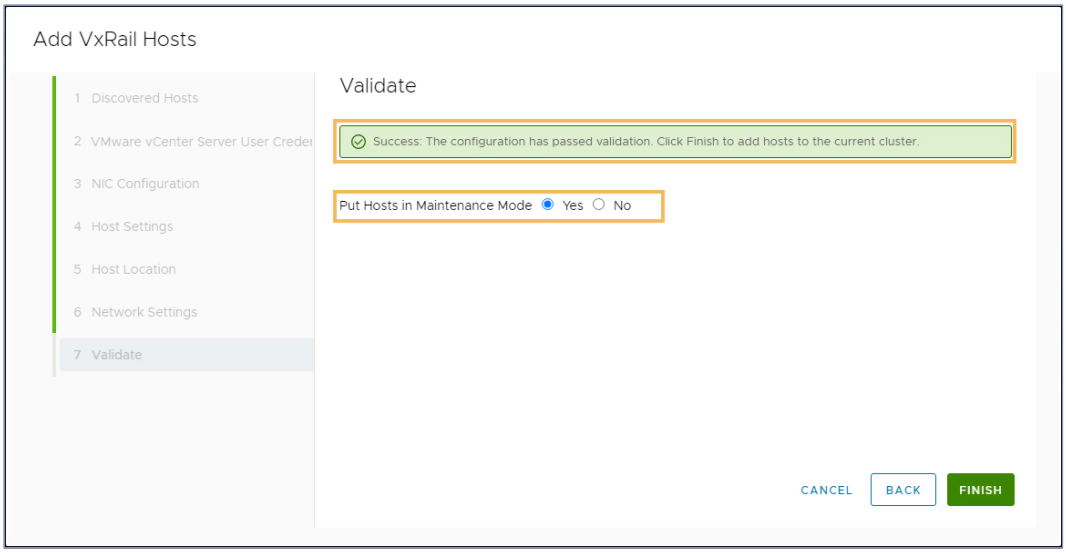
Add VxRail Hosts wizard-Validate

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**.

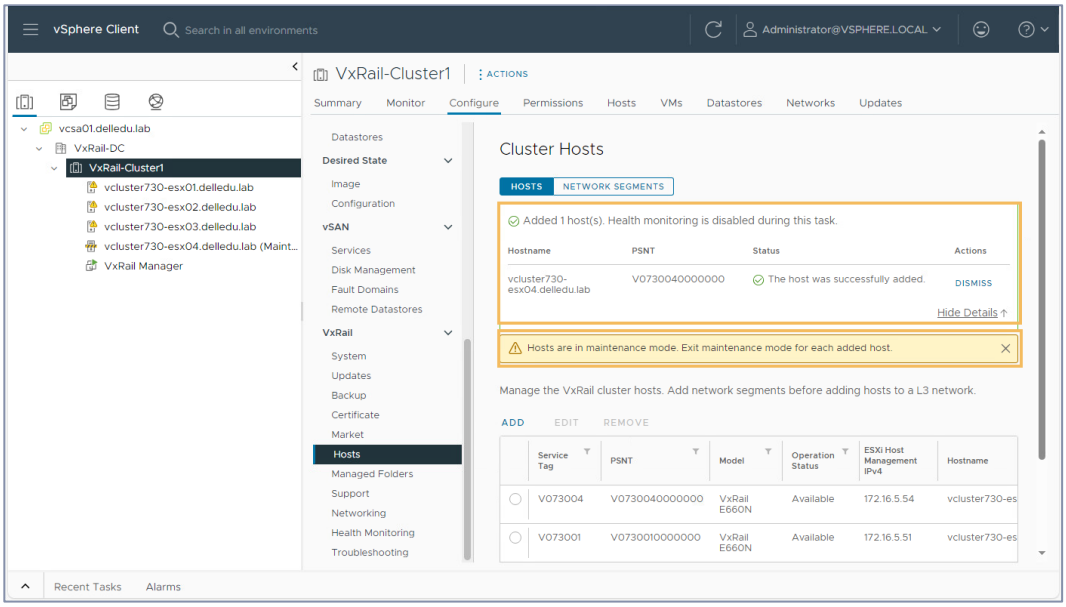


Successful validation

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.



Node added successfully to the VxRail cluster

Lab 14: Add a node to a VxRail cluster

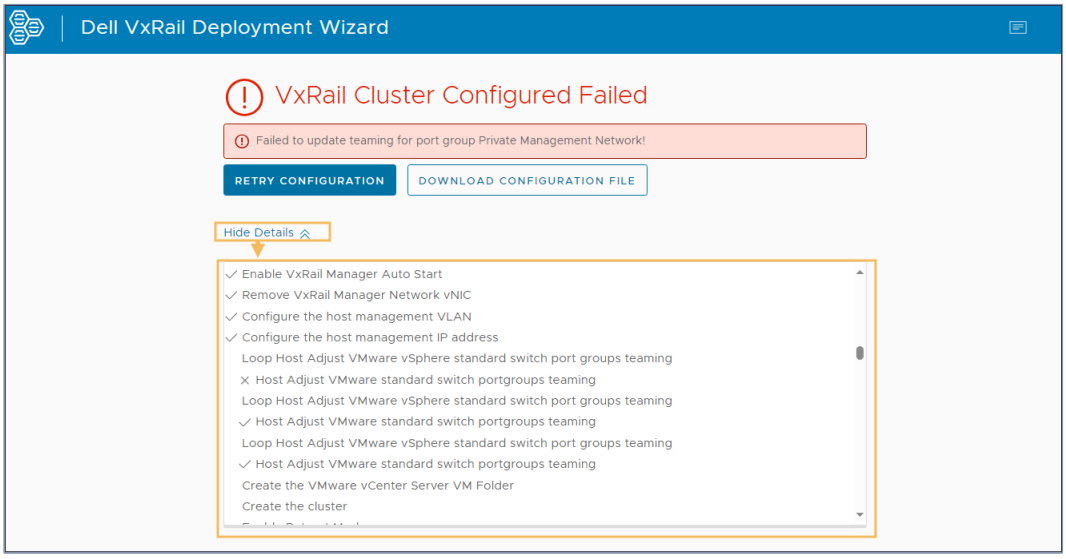
You are ready to add a VxRail node to a previously deployed VxRail cluster.

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:

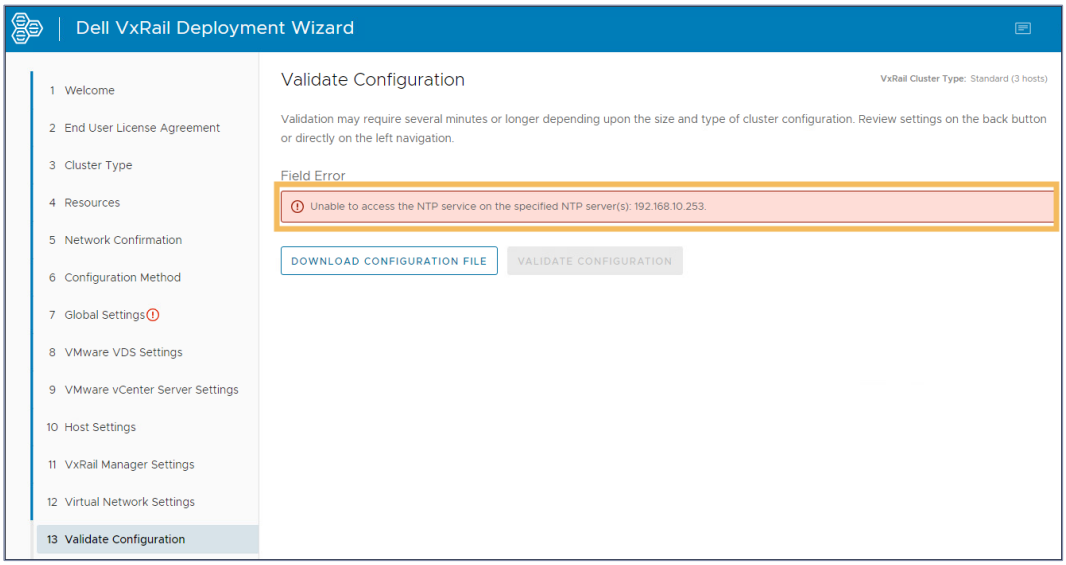
- Retry the installation to resolve issues that may be the result of a timeout during execution.
- Verify that the configuration wizard has the expected values after uploading a JSON file.
- Use the vSphere Client if vCenter is available, to determine the root cause and resolve issues.
- Use the VMware 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

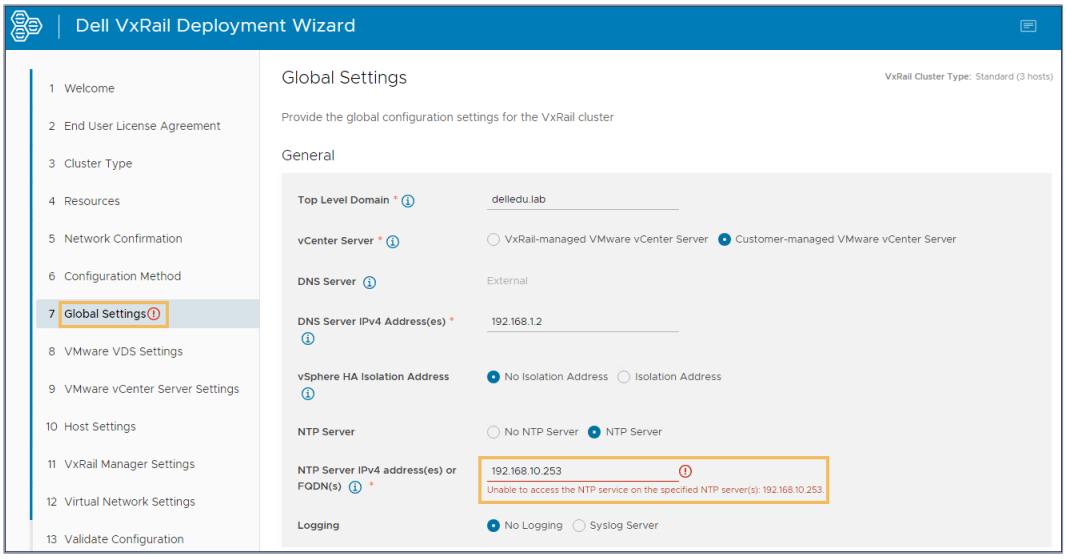
Review the error in the validation step of the VxRail Deployment Wizard.



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.



VxRail Deployment Wizard Global Settings Error

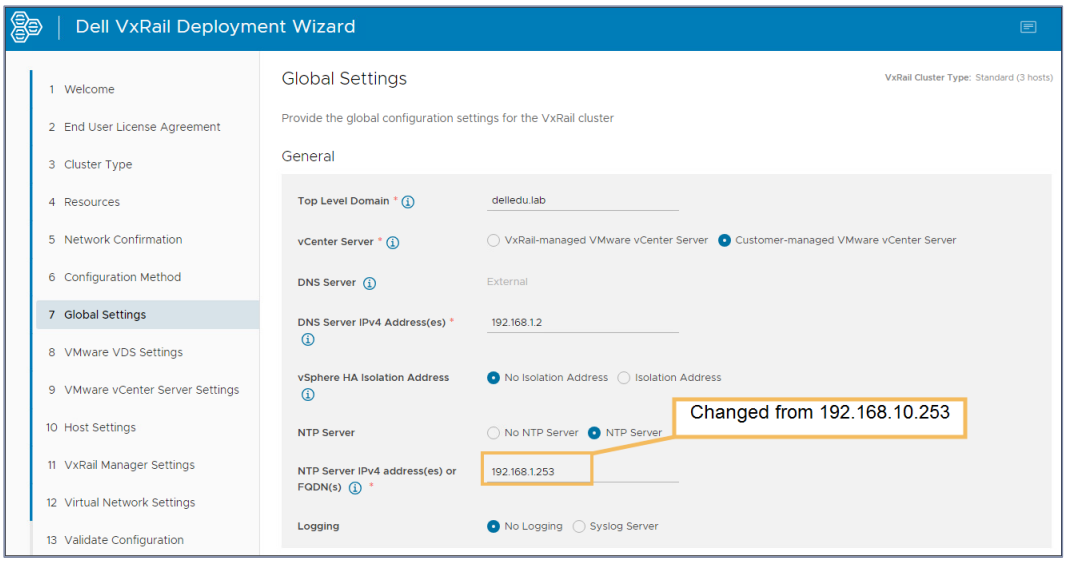
Perform Troubleshooting Steps

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.

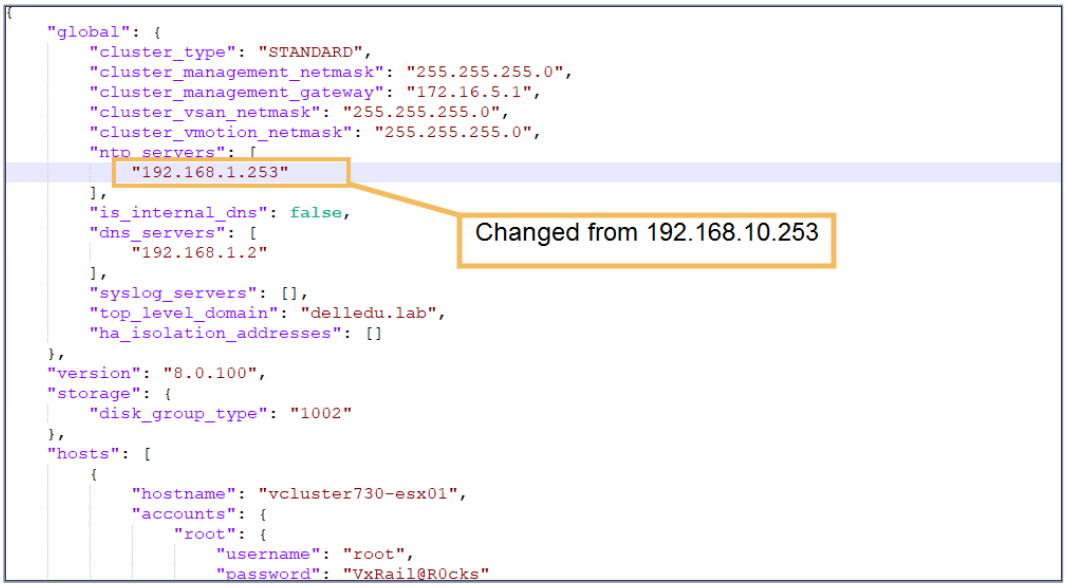
Update the VxRail Deployment Wizard

- 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.



VxRail Deployment Wizard Global Setting Corrected

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



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.

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

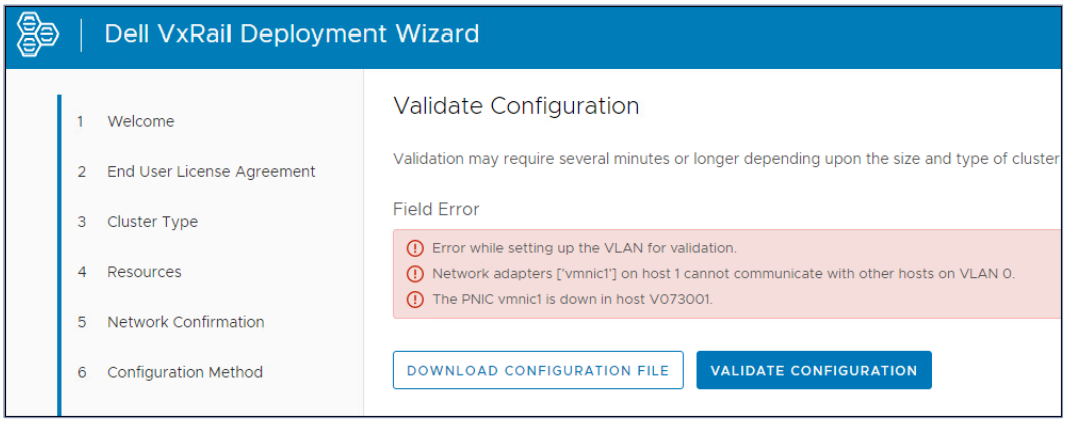
One method to view log files on the VxRail Manager VM, is to use an SSH client. When logging in, use the mystic account since root access is disabled for SSH. The IP address and password combination that is used during an SSH client session depends on the stage of the VxRail cluster installation:

- 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!)

– 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



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.

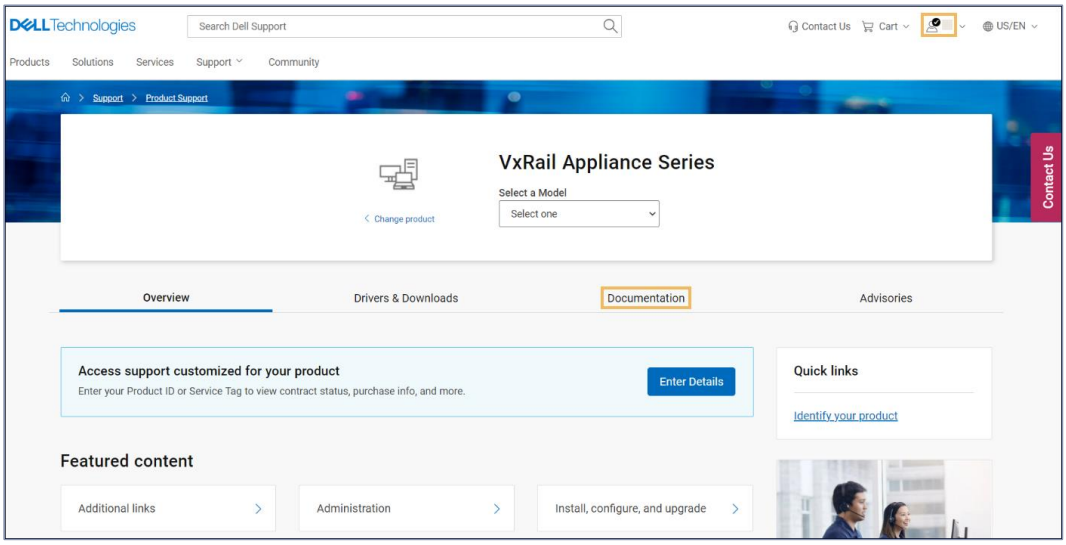
- ***cat /var/log/microservice_log/dayone.log | grep "vmnic1 is down"***

  Using more exact search criteria displays a more helpful output.

VxRail Knowledge Base (KB) Articles

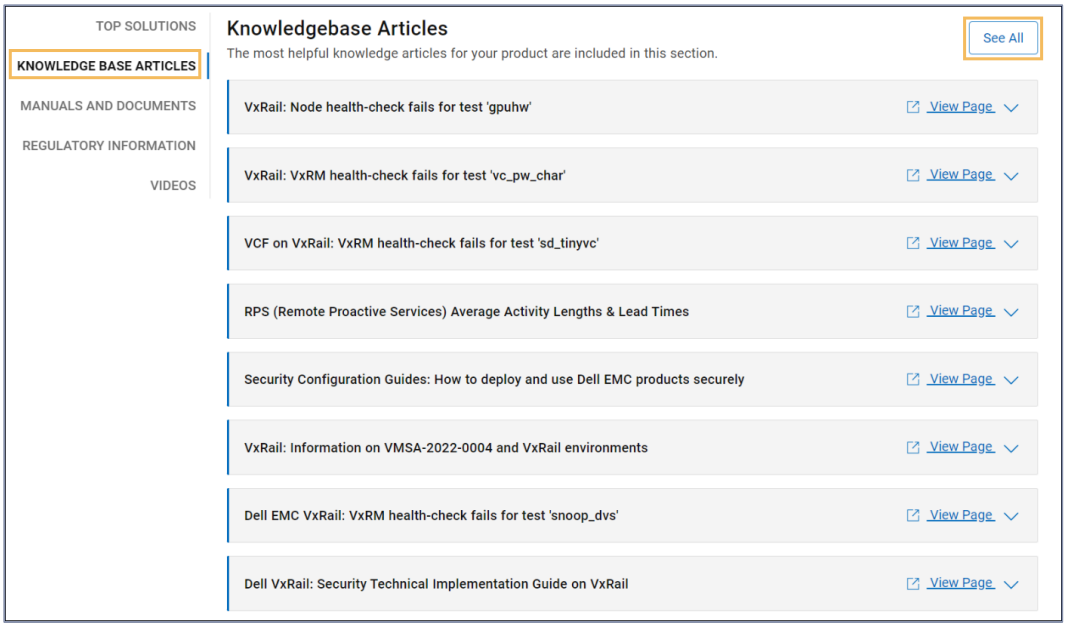
Links to KB articles that supplement the VxRail ecosystem can be found in SolVe procedures, VxRail Manager, and the Dell Support site. The **Documentation** tab on the VxRail Support page displays KB articles that are related to VxRail Manager.

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**.

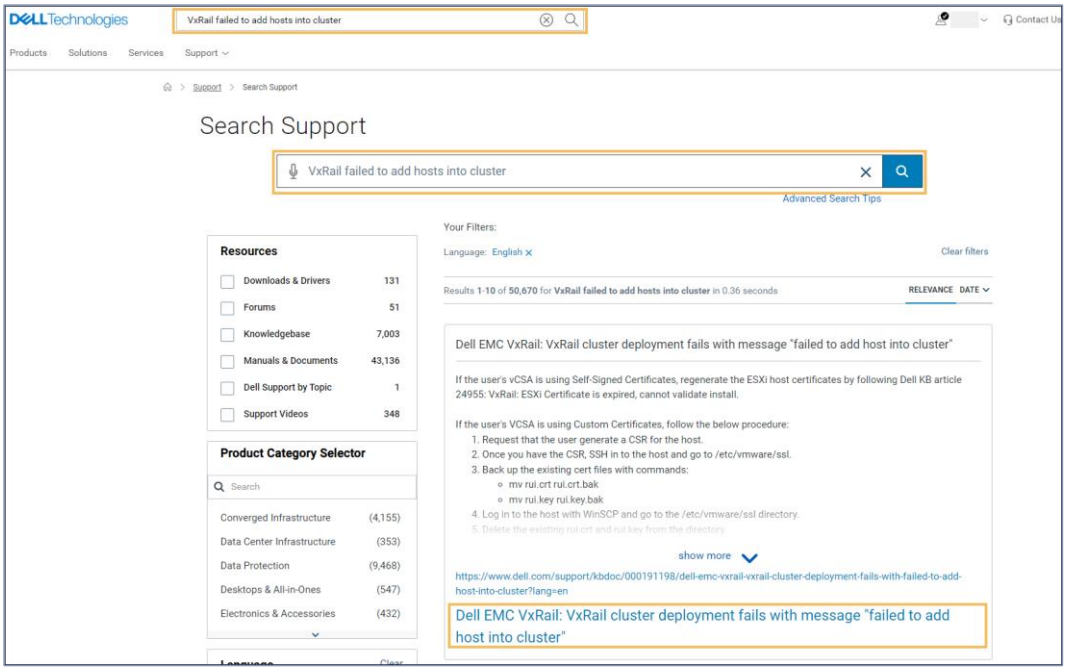


Knowledge Base Article list

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."



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.

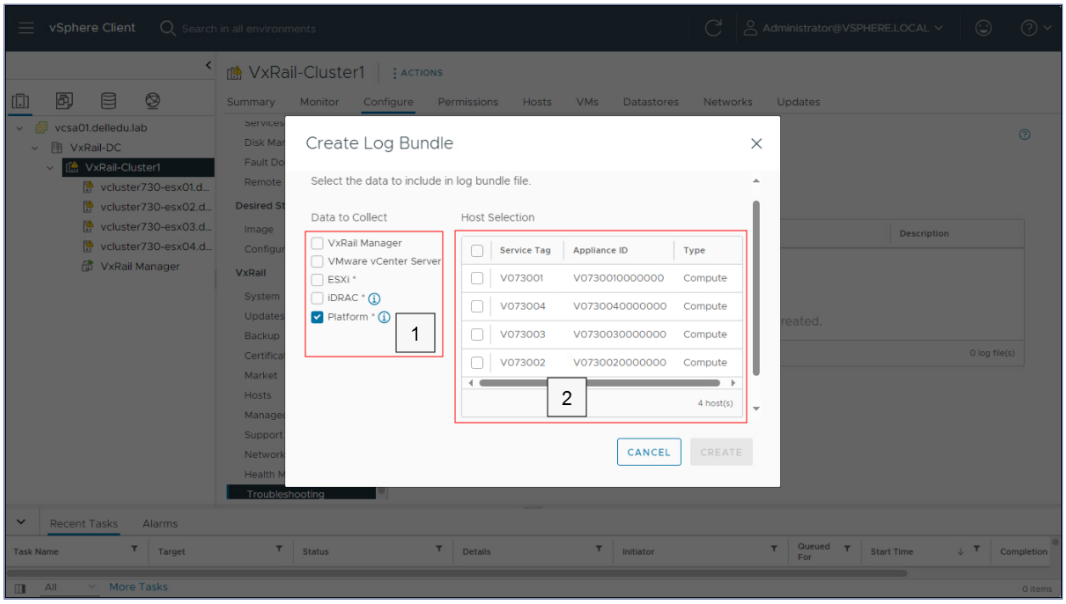
The Dell VxRail 8.0.x Administration Guide details the log bundle collection steps with the VxRail Plugin and with the VxRail Manager VM CLI scripts.

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.

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



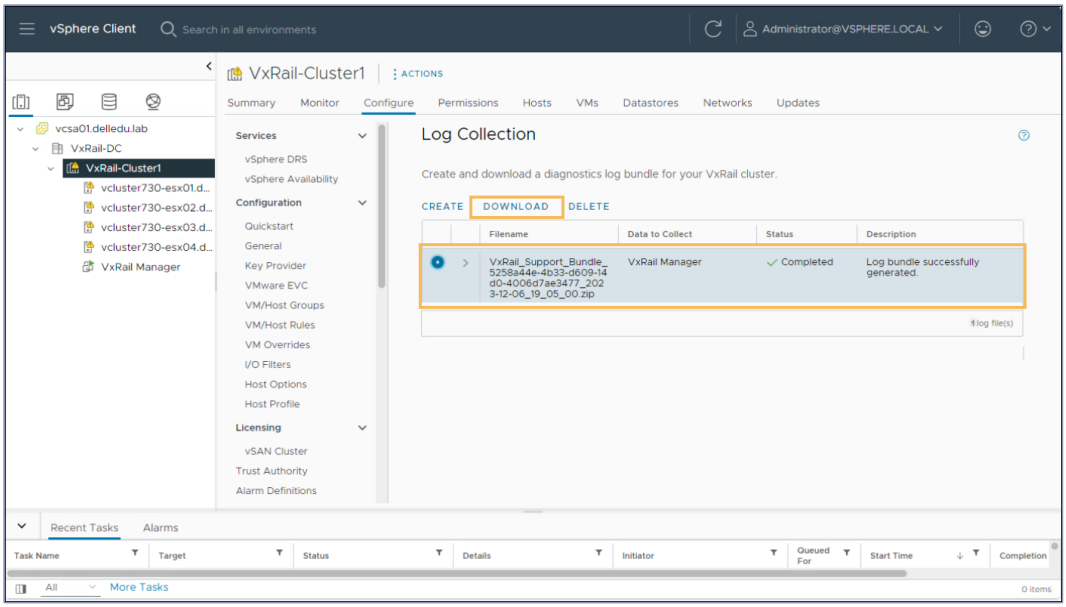
1: The Data to Collect section is used to select the required log bundles: VxRail Manager, vCenter, ESXi, iDRAC, and Platform.

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.



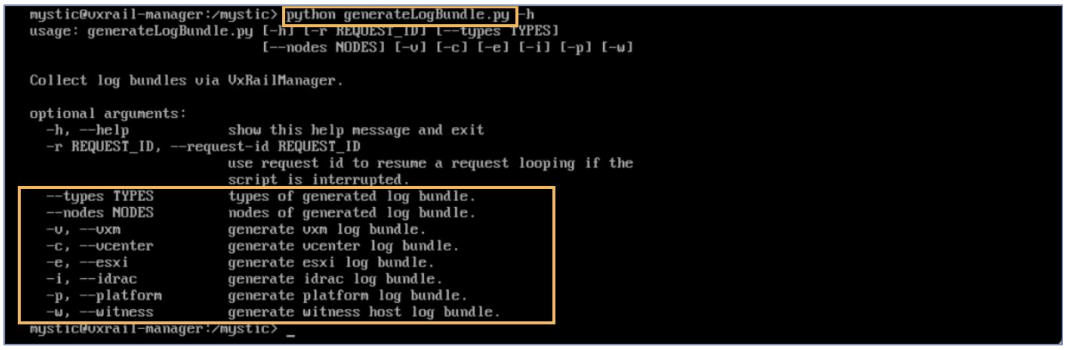
Log bundle generated successfully and available for download

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***



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

Request to generate a new log bundle	/v1/support/logs	**Types** - **`vxm, vcenter, esxi, iDrac`** **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

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.

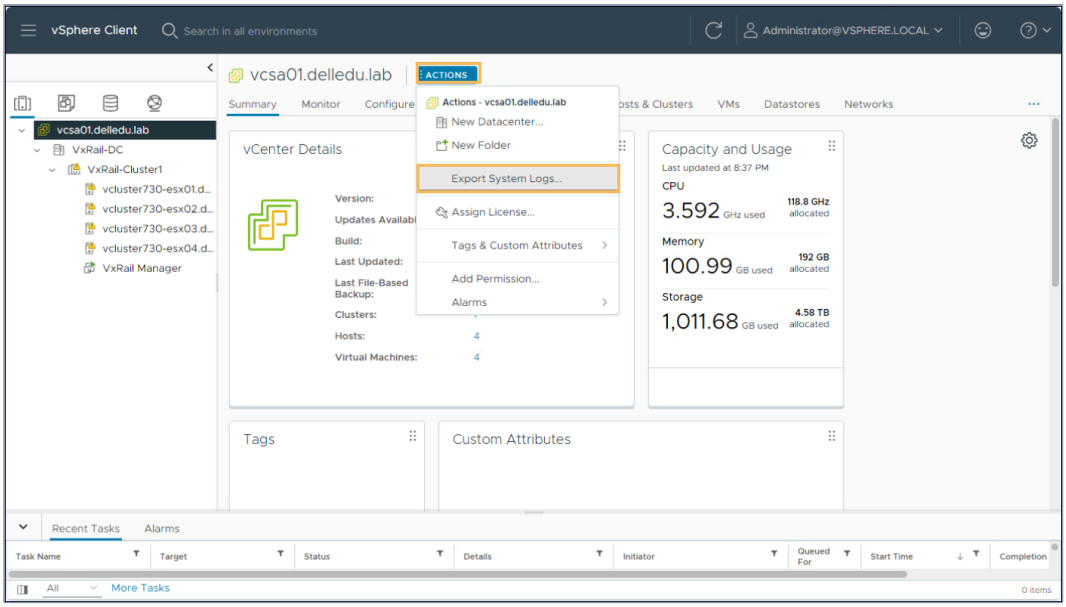
vCenter Server, ESXi, and vSAN Support Bundles

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

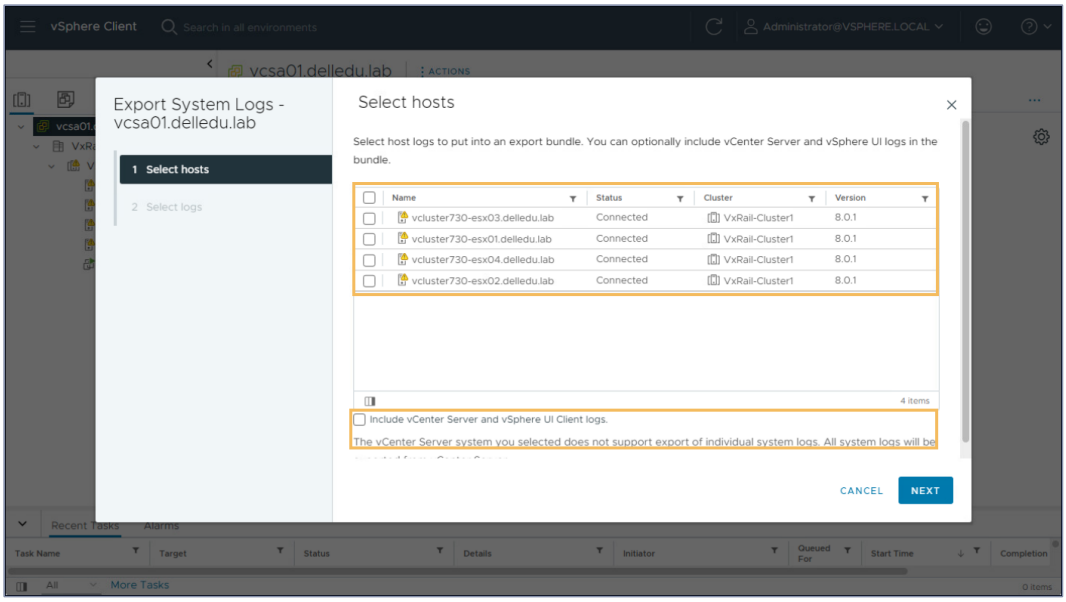
To export system logs from the vSphere Client, click the **ACTIONS** button and then select **Export System Logs**.



Export vCenter logs using the actions menu in the vSphere client

vSphere Client Export System Logs

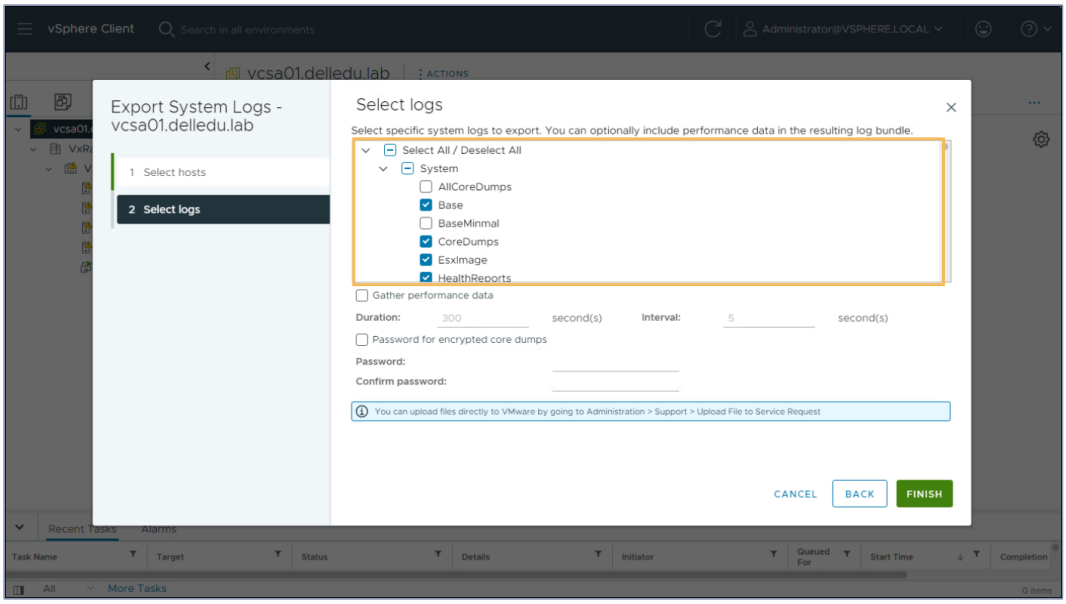
In the **Export System Logs** dialog, select the relevant ESXi hosts. Optionally, select the **Include vCenter Server and vSphere UI Client logs**.



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**.**



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

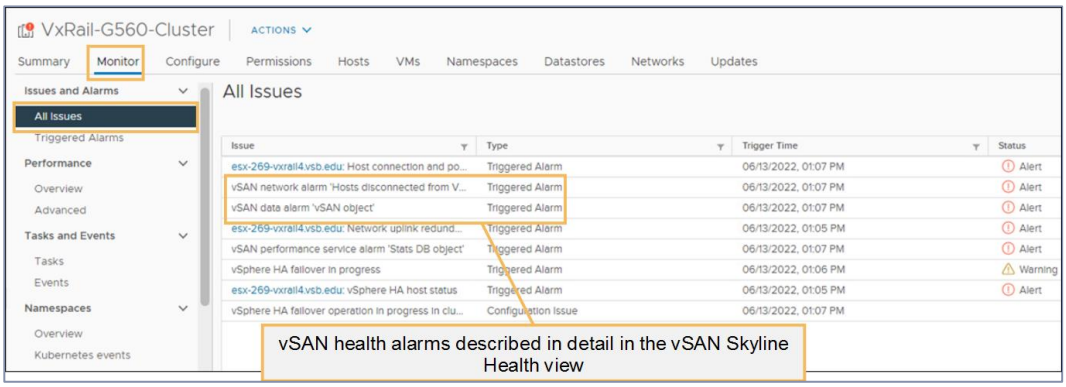
vSAN troubleshooting is typically performed using one or more of the following resources:

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

- 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

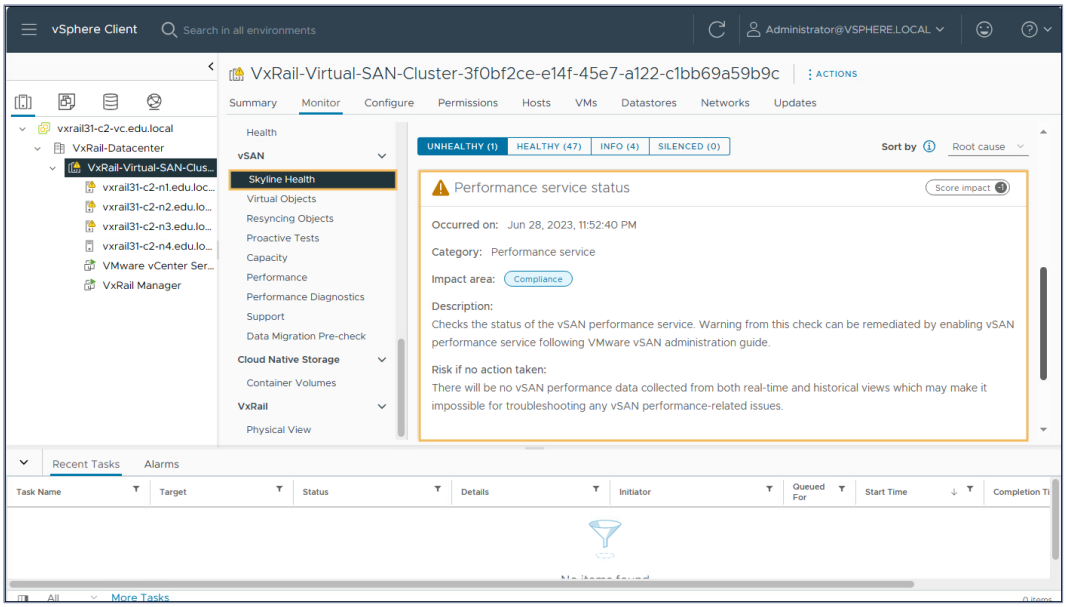
The **All Issues** view shows all triggered alarms relevant to the cluster. vSAN alarms start with vSAN, and VxRail related alarms have VXR in the event code.



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.



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.

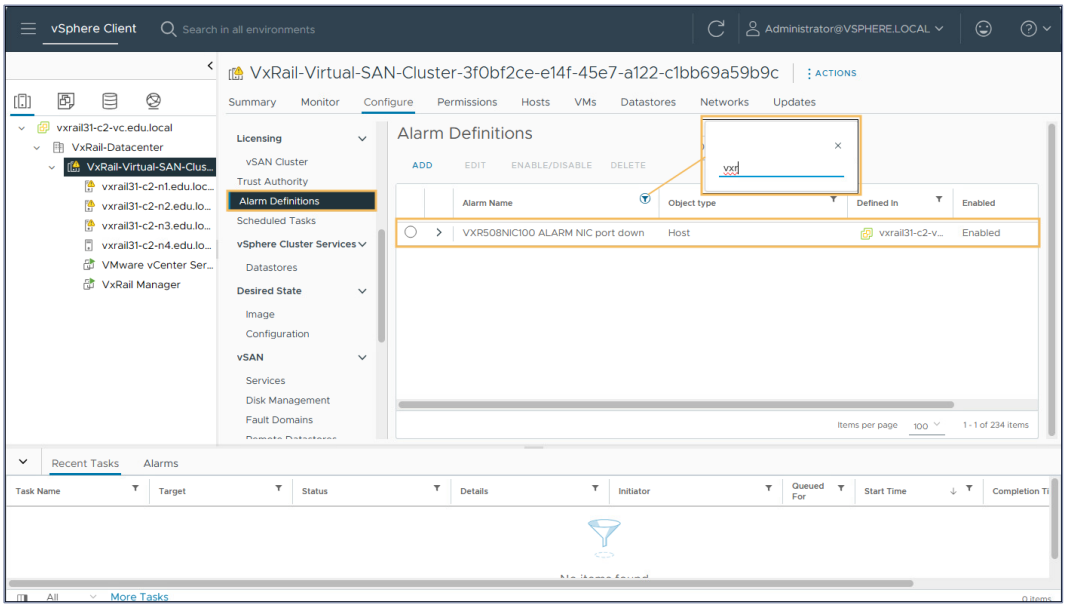
VXR014020 MYSTIC014020	Error	Network uplink redundancy lost: Failure of the network cable, disconnect of cable, failure of the physical network card, failure of network switch/ port/etc. Lost uplink redundancy on DVPort(s). Physical NIC is down. Lost uplink redundancy on a virtual switch. Physical NIC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



Filtered VXR Alarm Definitions example

vSAN Proactive Tests

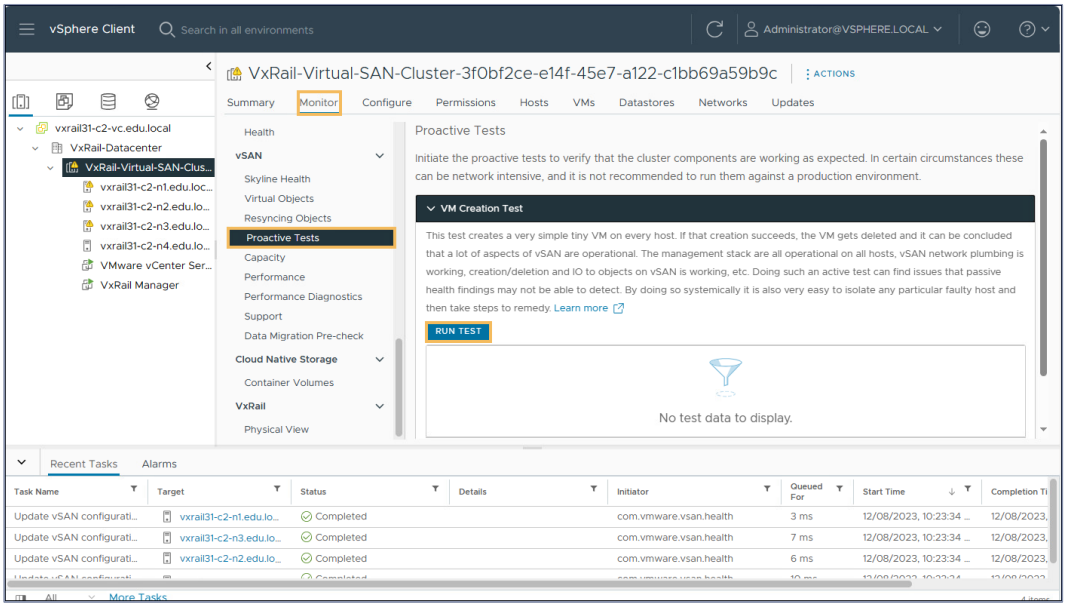
vSAN includes two proactive tests to validate the cluster: the **VM Creation Test** and the **Network Performance Test**. The vSAN proactive tests are available under the **Monitor** tab of the VxRail cluster. To learn about vSAN Proactive Tests select each tab.

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

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**.

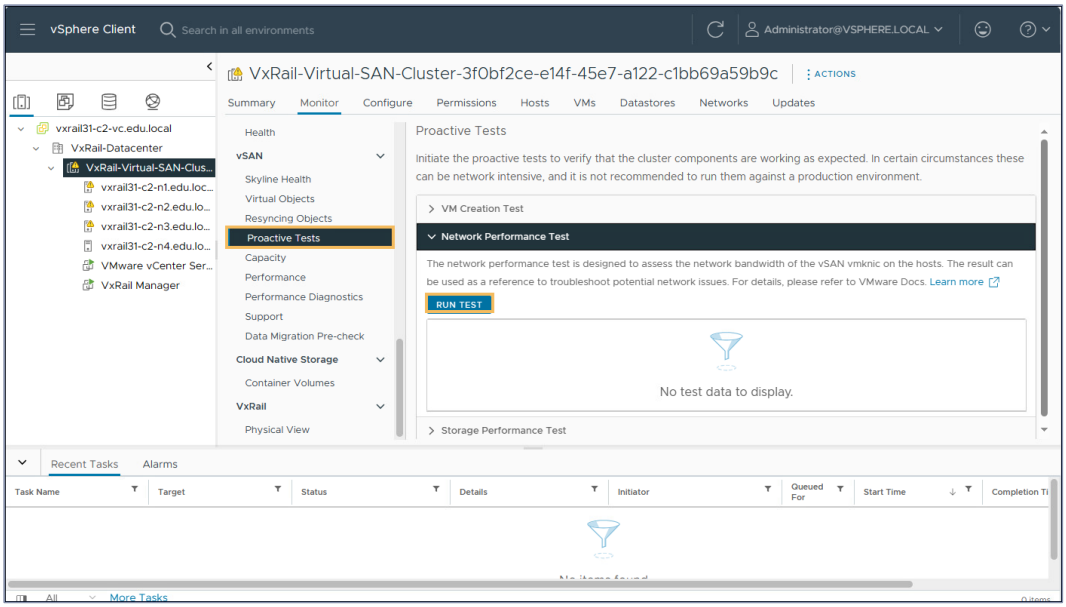


Virtual machine creation test example

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.**



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`***


```
   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                                         green
  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                                   green
  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.clusterpartitior

Partition list
Host            Partition     Host UUID
--------------------------------------------------------------------
172.16.40.84    1             64513e12-0d54-18d3-ae89-e43d1ad99790
172.16.40.83    1             6451430a-ada5-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

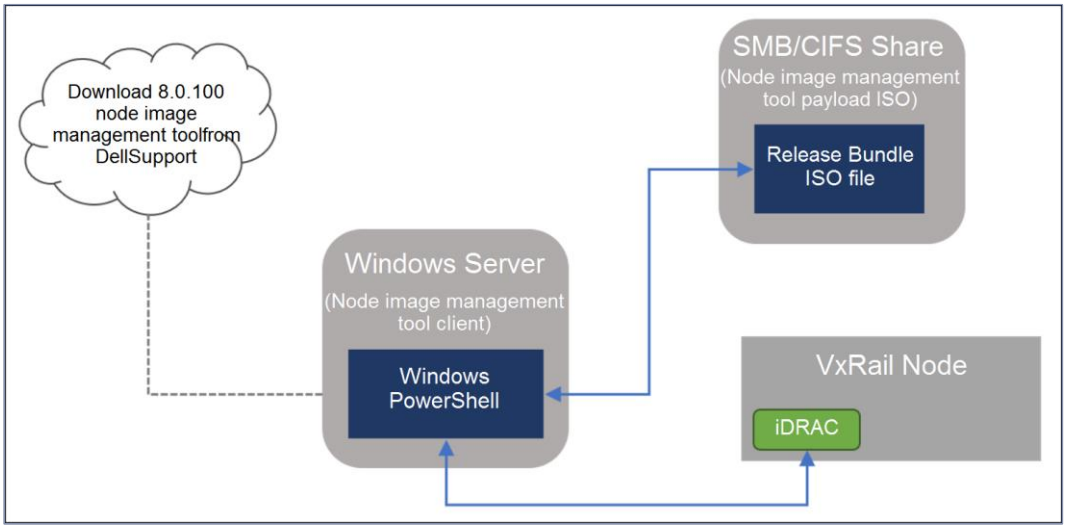
Example - Status of the health of vSAN objects - ***esxcli vsan debug object health summary get***


```
[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:

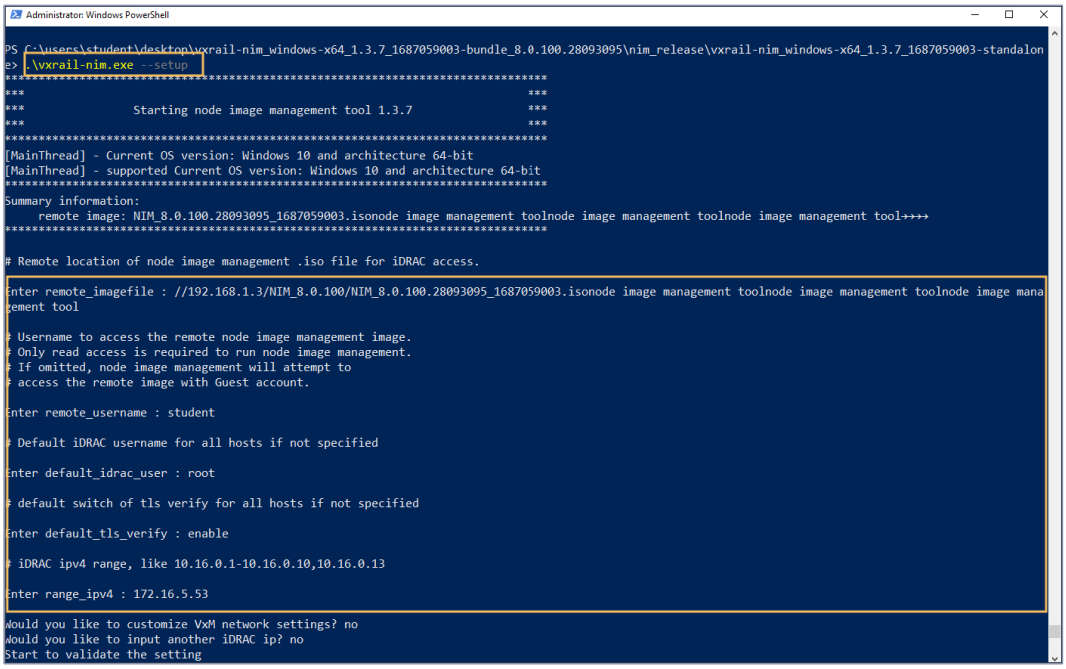
Node image management tool client: An executable CLI tool to enable the user to image VxRail nodes. The tool, with a few parameters, builds connections to the iDRAC on the target VxRail nodes, and consumes the node image management tool payload ISO.

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.



Performing a reimage 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.

- 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.

```
DTES-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

VxRail Configuration Report

Cluster Configuration Summary:

Configuration Status: SUCCESS

Report Timestamp (UTC): 2023-08-10 16:05:06

Project Name: University Deployment 1

Cluster Name: VxRail-Cluster

Datacenter Name: VxRail-DC

Top Level Domain: delledu.lab

VxRail Version: 8.0.100

Cluster Type: STANDARD

VCF on VxRail: NO

Number of Cluster Hosts: 3

SmartFabric Services: NO

Join Existing Single Sign On: NO

VDS Configuration: Custom

VDS Type: New

Number of VDS: 1

Host NICs: 6

Disk Group Type: Up to 2 Disk Groups (up to 4 capacity drives and 1 cache drive per group)

Accept VC Cert: YES

Storage Type: Standard vSAN

MTU: 5000

vSAN Storage Policy:

Stretched Cluster:
Number of Expansion Hosts:

Deduplication:

Compression:

Encryption:

Infrastructure

Component	Component Supplier	Component IP Address	Component Hostname
VxRail Manager	VxRail	172.16.5.16	vxrail-manager
vCenter	Customer		vcsa01.delledu.lab
DNS Servers	Customer	192.168.1.2	
NTP Servers	Customer	192.168.1.253	
Log Servers			
vSphere HA Isolation Addresses			
Secure Remote Services			

Hosts

Host Name	Host Model	Service Tag	Serial Number (PSNT)	Management IP Address	vSAN IP Address	vMotion IP Address	IDRAC IP Address	Rack Name	Rack Position
vcluster730-esx01	E660N			172.16.5.51	172.16.10.51	172.16.20.51		Rack 1	1
vcluster730-esx02	E660N			172.16.5.52	172.16.10.52	172.16.20.52		Rack 1	2
vcluster730-esx03	E660N			172.16.5.53	172.16.10.53	172.16.20.53		Rack 1	3

Credentials

Server	Management Username	Management Password	Root Username	Root Password	Administrator Username	Administrator Password	Remote Service Username	Remote Service Password
vCenter Server	vxrmgmt@vsphere.local				administrator@vsphere.local			
VxRailManager VM	mystic		root				service	
vcluster730-esx01	esxmgmt		root					
vcluster730-esx02	esxmgmt		root					
vcluster730-esx03	esxmgmt		root					

Network

Network Name	VLAN	Subnet IP Address	Netmask IP Address	Gateway IP Address
Management Network	5	172.16.5.0	255.255.255.0	172.16.5.1
vSAN Network	10	172.16.10.0	255.255.255.0	
vMotion Network	20	172.16.20.0	255.255.255.0	
VxRail Node Discovery Network	3939			
vCenter Server Network	5			
iDRAC				

Virtual Distributed Switch: VMware HCIA Distributed Switch

Port Group Name	TYPE	VLAN	Active Uplink<-> VMNIC	Standby/Active Uplink<-> VMNIC	Teaming Policy	Load Balancing	VMkernel MTU	Binding Mode

Example of a VxRail Configuration Report

VxRail Configuration JSON - Existing VDS Details


```
"network": {
    "nic_profile": "ADVANCED_CUSTOMER_SUPPLIED_VDS",
    "vds": [
        {
            "name": "VxRail-myVDS",
            "nic_mappings": [
                {
                    "uplinks": [
                        {
                            "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": [
                {
                    "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
                }
```

VDS name

Uplink names and physical NICs

Port group names, types, VLAN IDs, and MTU

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 Server[5]
- VMware vSphere and VMware vSAN - 60-day evaluation licenses
- RecoverPoint for Virtual Machines - five licenses per node
- CloudIQ SaaS multicluster management Tier 1[6]

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 vSAN[7] - 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		✓	✓	✓
RAID 5/6 Erasure Coding		✓	✓	✓
Data-at-rest and Data-in-transit Encryption			✓	✓
Stretched Cluster			✓	✓
File Services			✓	✓
VMware HCI Mesh			✓	✓
vSAN Express Storage Architecture		✓	✓	✓

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

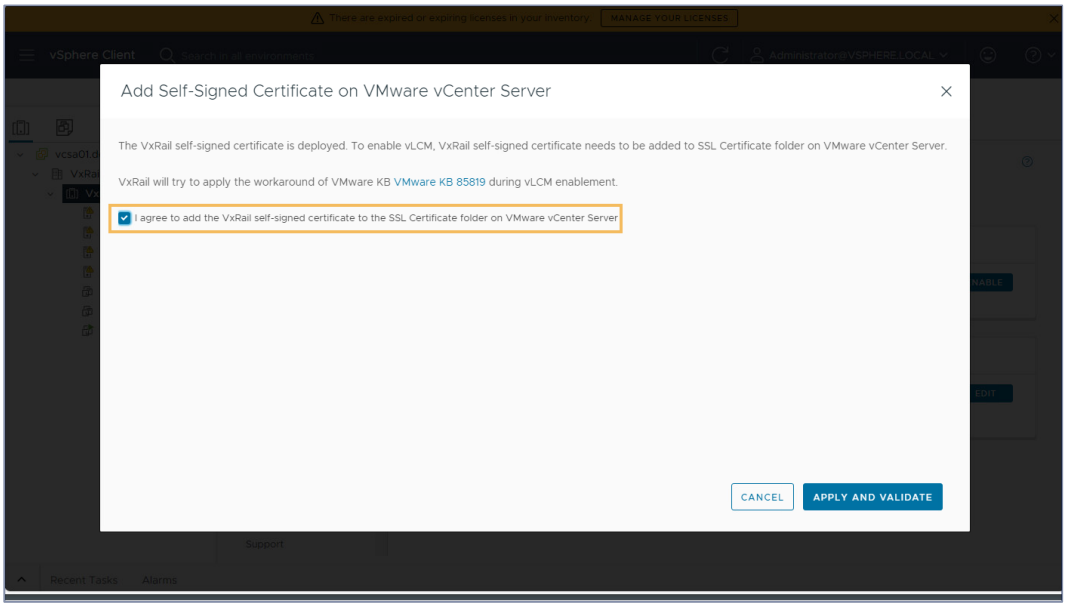
vSAN Advanced Policy Rules

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

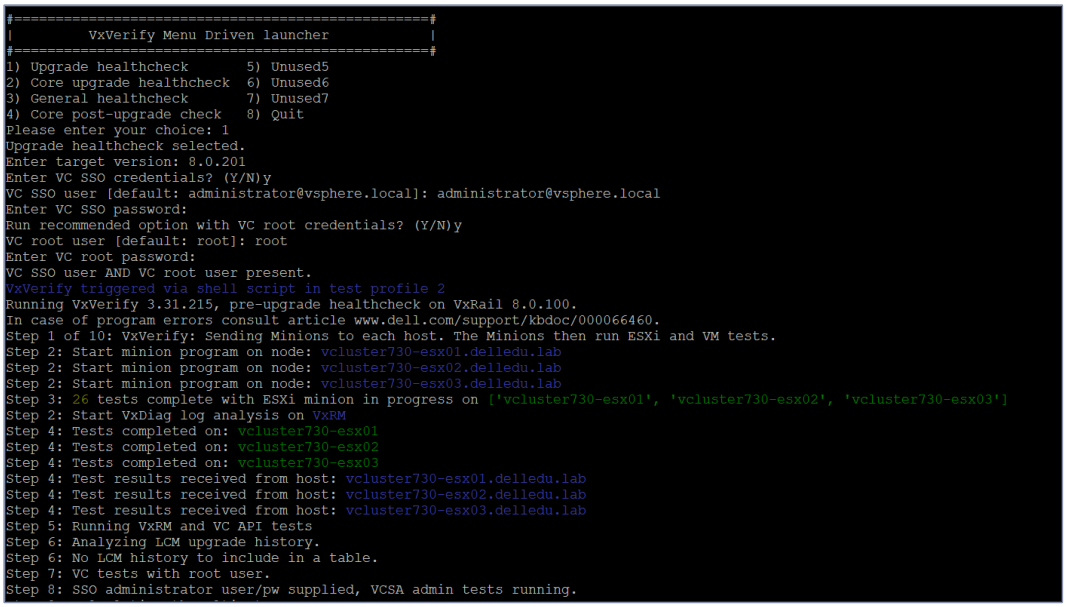


Add Self-Signed Certificate on VMware vCenter Server confirmation

VxVerify

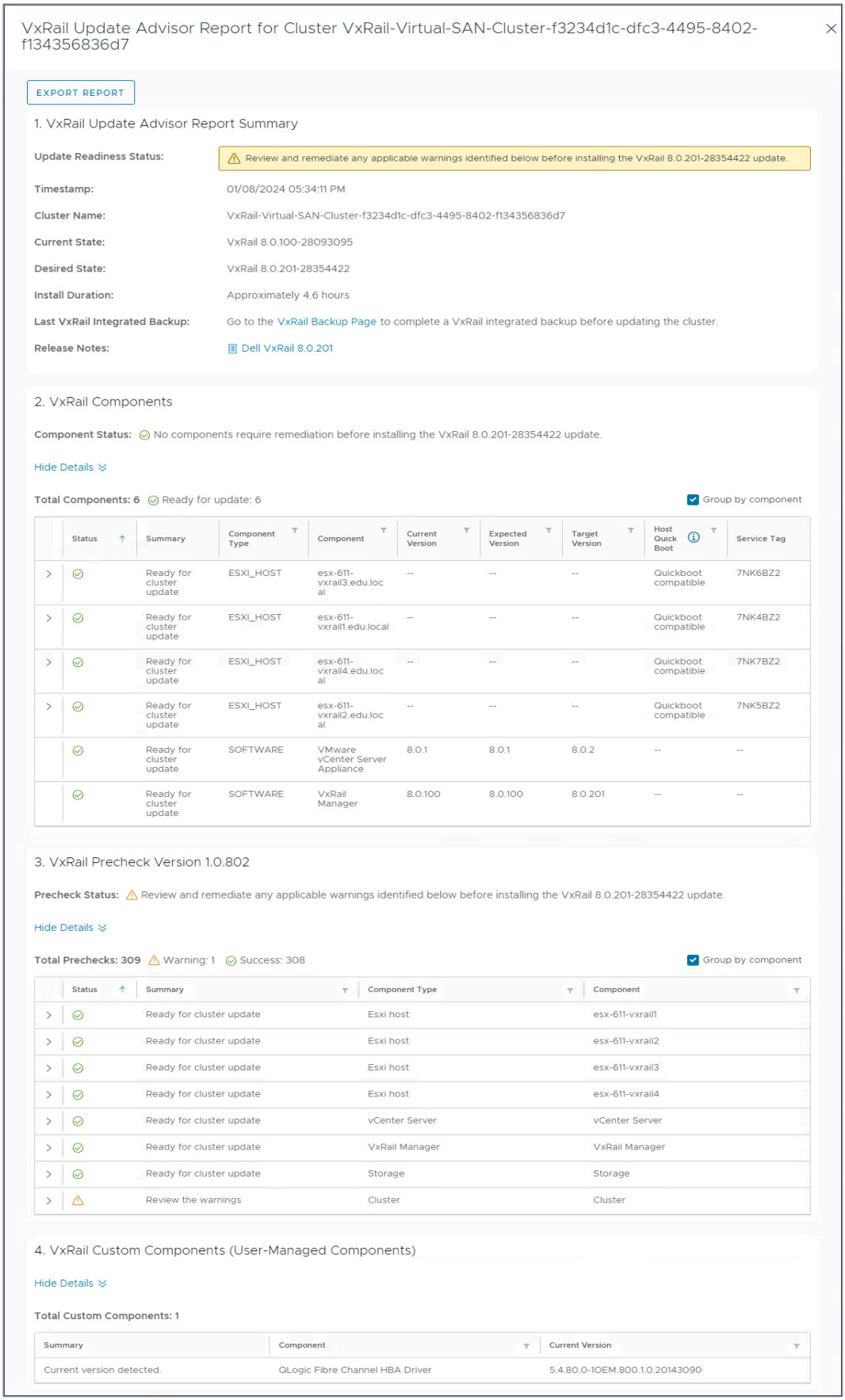
VxVerify is a tool for checking the health of the nodes and the service VMs. It is designed to detect issues that could cause complications or failures during VxRail LCM upgrades. VxVerify is run from the VxRail Manager. It automatically uploads and runs scripts against each ESXi node and system VM and 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.



Output of VxVerify python script

Sample Advisory Report



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.	QLogic Fibre Channel HBA Driver	5.4.80.0-1OEM.800.1.0.20143090

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.

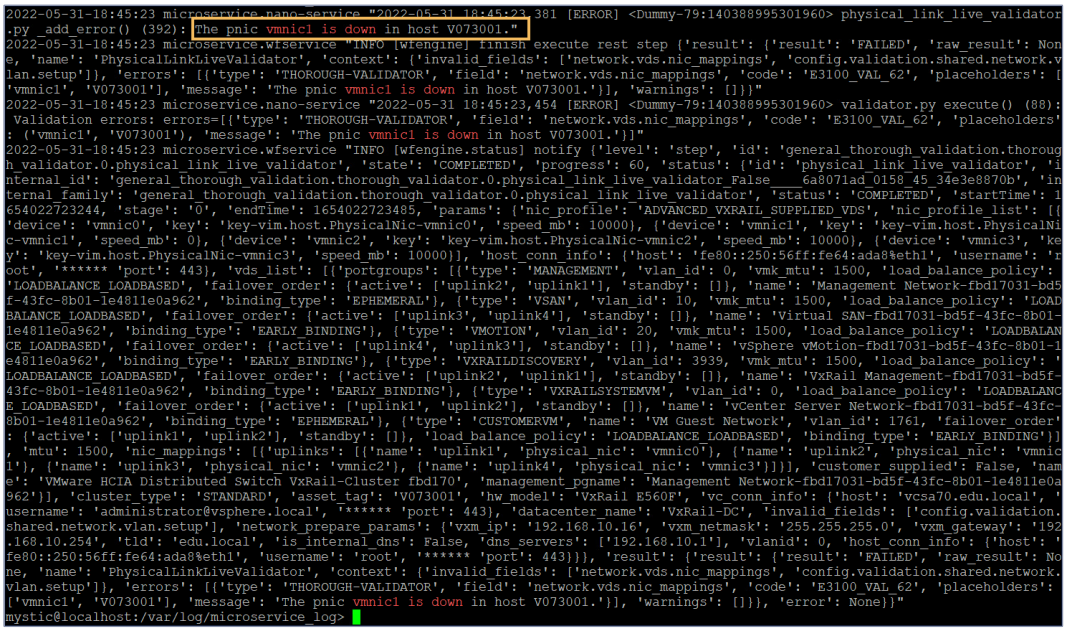
Search Results for All Errors in Dayone.log

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 (
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 (
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 _rel
ease() (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

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 (
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 _rel
ease() (40): Exception during communicate with lock service"
2022-05-31-18:24:48 microservice.ms-day1-bringup "2022-05-31 18:24:48,916 [ERROR] <MainThread:140069886911808> hostquery.py call_do_qu
ery() (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-day1-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-day1-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-day1-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-day1-bringup "2022-05-31 18:27:34,906 [ERROR] <Dummy-9:139625510778952> progress_converter.py _loa
d_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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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-day1-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 520f5cf4-d3ec-4c9b-b8dc-2b4593d151ba, it should b
e in node discovery stage of new workflow launching."
2022-05-31-18:27:49 microservice.ms-day1-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 520f5cf4-d3ec-4c9b-b8dc-2b4593d151ba, it should b
e in node discovery stage of new workflow launching."
2022-05-31-18:27:52 microservice.ms-day1-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 520f5cf4-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> vxm_agent_utils.py run_vxm_com
mand() (66): run_vxm_command Fail. error code: 2, message: b""ls: cannot access '/var/lib/vmware-marvin/manifest.xml': No such file or
 directory\n""""
2022-05-31-18:27:57 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/manifest.xml': No such file or directory\n""""
2022-05-31-18:27:57 microservice.ms-day1-bringup "2022-05-31 18:27:57,413 [ERROR] <Dummy-30:139625510778696> vxm_agent.py handle_vxm_a
gent_response() (33): http://vxm-agent:5000/vxm-agent/v1/vxm/services/command failed!"
2022-05-31-18:28:04 microservice.ms-day1-bringup "2022-05-31 18:28:04,842 [ERROR] <Dummy-30:139625510778696> vxm_agent.py handle_vxm_a
gent_response() (33): http://vxm-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> vxm_agent_utils.py run_vxm_com
mand() (66): run_vxm_command Fail. error code: 2, message: b""ls: 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 18:28:07,671 [ERROR] <Thread-51:140451431503616> vxm_agent_utils.py run_vxm_com
mand() (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://vxm-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_vxm[35d6b02d-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-day1-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-8:139713334609736> 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> async_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> vxm_agent_utils.py run_vxm_com
mand() (66): run_vxm_command Fail. error code: 2, message: b""ls: 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 microservice.nano-service "2022-05-31 18:28:15,274 [ERROR] <Dummy-10:140388928400200> utils.py wrapper() (101): lo
g_call 151, static.handle_vxm_agent_response raise exception: OperationException: {""message"": ""Exception(b\""ls: cannot access '/va
r/lib/vmware-marvin/trust/lin': No such file or directory\\n\"",)"", ""bundle"": """", ""prefix"": ""common.exceptions.OperationExcept
ion"", ""key"": """", ""field"": """", ""error_code"": ""0"", ""exit_code"": ""-1"", ""params"": []}"
```

Dayone.log results for all errors

Search Results for "vmnic1 is down" Errors in Dayone.log



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.

