Abstract
This is a planning and consideration guide for VxRail Appliances. It can be used to better understand the networking requirements for VxRail implementation. This document does not replace the implementation services with VxRail Appliances requirements and should not be used to implement networking for VxRail Appliances.

October 2019
Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>1st inclusion of this version history table</td>
</tr>
<tr>
<td></td>
<td>Support of VMware Cloud Foundation on VxRail</td>
</tr>
<tr>
<td>June 2019</td>
<td>Support for VxRail 4.7.210 and updates to 25 Gb networking</td>
</tr>
<tr>
<td>October 2019</td>
<td>Support for VxRail 4.7.300 with Layer 3 VxRail networks</td>
</tr>
</tbody>
</table>

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

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

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [10/14/2019] [Planning Guide] [H15300.11]
# Table of contents

Revision history .................................................................................................................. 2

Table of contents .................................................................................................................. 3

1 Introduction to VxRail ....................................................................................................... 6

2 Planning your datacenter network for VxRail ................................................................. 7

   2.1 VxRail hardware and the physical network infrastructure .................................. 7
   2.2 VxRail clusters, appliances, and nodes .............................................................. 7
   2.3 Network switch ..................................................................................................... 9
   2.4 Data Center Network ............................................................................................ 9
   2.4.1 Data Center Services ...................................................................................... 9
   2.4.2 Routing Services ............................................................................................ 10
   2.5 VxRail node connectivity options ...................................................................... 10
   2.6 VxRail networking rules and restrictions .......................................................... 12
   2.7 Topology and connections .................................................................................. 12
   2.8 Out-of-band management (optional) ................................................................ 13

3 VxRail feature-driven decision points .......................................................................... 14

   3.1 Software-defined data center .............................................................................. 14
   3.2 Dell EMC SmartFabric network mode .............................................................. 15
   3.3 vSAN stretched-cluster ..................................................................................... 16
   3.4 2-Node cluster .................................................................................................... 17

4 VxRail hardware and switch selection decision points .................................................. 18

5 Planning the VxRail Implementation ............................................................................. 19

   5.1 Plan Data Center Routing Services..................................................................... 19
   5.2 Decide on VxRail single point of management .................................................. 20
   5.3 Plan the VxRail logical network ........................................................................ 21
   5.4 Plan network settings for VxRail management components .............................. 24
   5.5 Identify unique hostnames for VxRail management components ...................... 27
       5.5.1 Select top-level domain ............................................................................. 27
       5.5.2 Select ESXi hostnames .............................................................................. 27
       5.5.3 Select VxRail Manager hostname ............................................................. 28
       5.5.4 Select VxRail vCenter Server hostname ................................................ 28
       5.5.5 Select Log Insight hostname .................................................................... 28
5.6 Identify external applications and settings for VxRail ......................................................... 29
5.6.1 Set time zone and NTP server ......................................................................................... 29
5.6.2 Create DNS Records for VxRail Management Components ........................................ 29
5.7 Prepare customer-supplied vCenter server ........................................................................ 30
5.8 Reserve IP addresses for VxRail vMotion and vSAN networks ........................................ 32
5.9 Decide on VxRail logging solution ..................................................................................... 32
5.10 Assign passwords for VxRail management ...................................................................... 33
5.11 Prepare for Dell EMC SmartFabric services enablement ................................................ 34

6 Configure the upstream network for VxRail ................................................................. 36
6.1 Setting up the network switch for VxRail connectivity ..................................................... 37
6.1.1 Plan switch configuration ............................................................................................... 37
6.1.2 Plan switch port configuration ....................................................................................... 39
6.1.3 Configure ports and VLANs on your switch(es) ............................................................. 41
6.2 Confirm your datacenter network ..................................................................................... 43
6.3 Confirm your firewall settings ........................................................................................... 43
6.4 Confirm your datacenter environment .............................................................................. 44

7 Preparing to build the VxRail cluster .............................................................................. 45
7.1 Configuring a workstation/laptop for VxRail initialization ............................................. 45
7.2 Perform initialization to create a VxRail cluster ................................................................. 46

8 After VxRail initialization network considerations .......................................................... 48
8.1 Support for NSX ................................................................................................................. 48
8.2 Using unassigned VxRail physical ports .......................................................................... 48

A VxRail Network Configuration Table .............................................................................. 49
B VxRail Passwords ................................................................................................................ 51
C VxRail Setup Checklist ....................................................................................................... 52
D NSX Support on VxRail ........................................................................................................ 54
E VxRail Open Ports Requirements ..................................................................................... 57
F Physical Network Switch Examples ................................................................................... 59
Intended use and audience

This guide discusses the essential network details for VxRail deployment planning purposes only. It introduces best practices, recommendations, and requirements for both physical and virtual network environments. This document has been prepared for anyone involved in planning, installing, and maintaining VxRail, including Dell EMC field engineers, and customer system and network administrators. This guide should not be used to perform the actual installation and set-up of VxRail. Work with your Dell EMC service representative to perform the actual installation.
1 Introduction to VxRail

Dell EMC VxRail™ Appliances are a hyper-converged infrastructure (HCI) solution that consolidates compute, storage and network into a single, highly available, unified system. With careful planning, VxRail Appliances can be rapidly deployed into an existing datacenter environment, and the end-product is immediately available to deploy applications and services.

VxRail is not a server. It is an appliance based on a collection of nodes and switches integrated as a cluster under a single point of management. All physical compute, network and storage resources in the appliance are managed as a single shared pool and allocated to applications and services based on customer-defined business and operational requirements.

The compute nodes are based on Dell EMC PowerEdge servers. The G Series consists of up to four nodes in a single chassis, whereas all other models are based on a single node. An Ethernet switch is required, at speeds of either 1/10/25 Gb, depending on the VxRail infrastructure deployed. A workstation/laptop for the VxRail user interface is also required.

VxRail has a simple, scale-out architecture, leveraging VMware vSphere® and VMware vSAN™ to provide server virtualization and software-defined storage, with simplified deployment, upgrades, and maintenance through VxRail Manager. Fundamental to the VxRail clustered architecture is network connectivity. It is through the logical and physical networks that individual nodes act as a single system providing scalability, resiliency, and workload balance.

The VxRail software bundle is preloaded onto the compute nodes, and consists of the following components (specific software versions not shown):

- VxRail Manager
- VMware vCenter Server™
- VMware vRealize Log Insight™
- VMware vSAN
- VMware vSphere
- Dell EMC Secure Remote Support (SRS)/VE

Licenses are required for VMware vSphere and VMware vSAN. The vSphere licenses can be purchased from Dell EMC, VMware, or your preferred VMware reseller partner.

The VxRail Appliances also include the following licenses for software that can be downloaded, installed and configured:

- Dell EMC RecoverPoint for Virtual Machines (RP4VM) - 5 full VM licenses per single node
- VxRail appliance (15 for the G Series appliance)
Planning your datacenter network for VxRail

The network considerations for VxRail are no different than those of any enterprise IT infrastructure: availability, performance, and extensibility. VxRail Appliances are delivered to your datacenter ready for deployment. The nodes in the appliance can attach to any compatible network infrastructure at 1/10/25 GbE speeds with either RJ45 or SFP+ ports. Models with single processors can attach to compatible 1 GbE network infrastructure. Most production VxRail network topologies use dual top-of-the-rack (ToR) switches to eliminate the switch as a single point of failure. This document guides you through the key phases and decision points for a successful VxRail implementation. The key phases are:

**Step 1.** Select the VxRail hardware and physical network infrastructure that best aligns with your business and operational objectives.

**Step 2.** Plan and prepare for VxRail implementation in your datacenter before product delivery.

**Step 3.** Set up the network switch infrastructure in your datacenter for VxRail before product delivery.

**Step 4.** Prepare for physical installation and VxRail initialization into the final product.

**Note:** Follow all the guidance and decision point described in this document; otherwise, VxRail will not implement properly, and it will not function correctly in the future. If you have separate teams for network and servers in your datacenter, you will need to work together to design the network and configure the switch(es).

VxRail hardware and the physical network infrastructure

VxRail nodes connect to one or more network switches, with the final product forming a VxRail cluster. VxRail communicates with the physical datacenter network through a virtual distributed switch deployed in the VxRail cluster. The virtual distributed switch and physical network infrastructure integration provide connectivity for the virtual infrastructure, and enable virtual network traffic to pass through the physical switch infrastructure. In this relationship, the physical switch infrastructure serves as a backplane, supporting network traffic between virtual machines in the cluster, and enabling virtual machine mobility and resiliency. In addition, the physical network infrastructure enables I/O operations between the storage objects in the VxRail vSAN datastore, and provides connectivity to applications and end-users outside of the VxRail cluster.

This section describes the physical components and selection criteria for VxRail clusters:

- VxRail clusters, appliances and nodes
- Network switch
- Data Center Network
- Topology and connections
- Workstation/laptop
- Out-of-band management (optional)

VxRail clusters, appliances, and nodes

A VxRail appliance consists of a set of server nodes that are designed and engineered for VxRail. A VxRail physical node starts as a standard Dell PowerEdge server. The Dell PowerEdge server next goes through a manufacturing process following VxRail product engineering specifications to produce a VxRail node ready for shipment. A set of prepared VxRail nodes is delivered to the customer site based on a purchase order. The set of VxRail nodes is delivered ready for datacenter installation and connectivity into the datacenter network infrastructure.
Once the datacenter installation and network connectivity are complete, and the equipment is powered on, the VxRail management interface is used to perform the initialization process, which forms the final product: a VxRail cluster.

A standard VxRail cluster starts with a minimum of three nodes and can scale to a maximum of 64 nodes. The selection of the VxRail nodes to form a cluster is primarily driven by planned business use cases, and factors such as performance and capacity. Five series of VxRail models are offered, each targeting specific objectives:

<table>
<thead>
<tr>
<th>VxRail Series</th>
<th>Target Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Series</td>
<td>Balanced Compute &amp; Storage, Space Optimized (1U1N chassis)</td>
</tr>
<tr>
<td>V-Series</td>
<td>Virtual Desktop Enablement</td>
</tr>
<tr>
<td>P-Series</td>
<td>High Performance</td>
</tr>
<tr>
<td>S-Series</td>
<td>Storage Dense</td>
</tr>
<tr>
<td>G-Series</td>
<td>Compute Dense, Space Optimized (2U4N chassis)</td>
</tr>
</tbody>
</table>

Each VxRail model series offers choices for network connectivity. The following illustrations show some of the physical network port options for the VxRail models.

![Back view of VxRail E-Series on Dell 14th Generation PowerEdge server](image1)

Figure 1 Back view of VxRail E-Series on Dell 14th Generation PowerEdge server

![Back view of VxRail V-, P-, S-Series on Dell 14th Generation PowerEdge server](image2)

Figure 2 Back view of VxRail V-, P-, S-Series on Dell 14th Generation PowerEdge server

![Back view of VxRail G-Series on Dell 14th Generation PowerEdge server](image3)

Figure 3 Back view of VxRail G-Series on Dell 14th Generation PowerEdge server

In addition to network connectivity, review the physical power, space and cooling requirements for your planned infrastructure to ensure datacenter compatibility.
2.3 Network switch

VxRail is broadly compatible with most networks and Ethernet switches, including Dell network switch products.

2.3.1 Basic Switch requirements

- The switch(es) must support both IPv4 and IPv6 network protocols.
- The switch(es) connected directly to VxRail nodes must support multicast on switch ports for all models of VxRail.
  - VxRail releases earlier than v4.5.0: both IPv4 and IPv6 multicast pass-through must be supported.
  - VxRail releases starting with v4.5.0: IPv6 multicast pass-through and IPv4 unicast must be supported.
  - Layer 3 multicast is not required.

Note: IPv6 multicast needs to be enabled on the switch ports connected to VxRail Appliances only. The multicast traffic required by VxRail is limited to those switch ports that service VxRail.

- Layer 3 support is not required on the switch(es) directly connected to VxRail nodes.

2.3.2 Advanced switch requirements

In certain instances, additional switch features and functionality are necessary to support specific use cases or requirements.

- If your plans include deploying all-flash storage on your VxRail cluster, then 10 Gb network switches are the minimum requirement for this feature. Dell-EMC recommends a 25 Gb network if that is supported in your data center infrastructure.
- Enabling advanced features on the switches planned for the VxRail cluster, such as Layer 3 routing services, can cause resource contention and consume buffer space. To avoid resource contention, select switches with sufficient resources and buffer capacity.
- For very large VxRail clusters with demanding performance requirements and advanced switch services enabled, consider switches with sufficient resource capacity and deep buffer capacity. A switch buffer of 16 MB is recommended in these use cases, with 1 GB of shared switch buffer for very demanding, high-performance workloads.

2.4 Data Center Network

VxRail is dependent on specific data center services to implement the cluster and for day-to-day operations. The top-of-rack switches will need to be configured to the upstream network to enable connectivity to these data center services, and to enable connectivity to the end-user community.

2.4.1 Data Center Services

- Domain Naming Services (DNS) is required to deploy the VxRail cluster and for ongoing operations.
- VxRail cluster depends on Network Time Protocol (NTP) to keep the clock settings on the various VxRail components synchronized. Dell-EMC recommends a reliable global timing service be used for VxRail.
- VxRail depends on VMware vCenter for cluster management and operations. You can use either the embedded vCenter instance that is included with VxRail, or an external vCenter instance in your data center.
2.4.2 Routing Services

VxRail cluster operations depend on a set of networks that run on both the virtual network inside of the cluster and on the adjoining physical network switches. Some of these networks, specifically for VxRail management and for end-user access, must be passed to the upstream network, while other VxRail networks will stay isolated on the adjoining network switches.

You will be required to specify a set of VLAN (Virtual LAN) IDs in your data center network that will be assigned to support the VxRail networks. All of the VLANs must be configured on the adjoining physical switches. The VLANs that need to pass upstream must be configured on adjoining network switch uplinks, and also on the ports on the upstream network devices.

One VLAN is assigned for external VxRail management access. Data center services (such as DNS and NTP) that are required by VxRail cluster must be able to connect to this VLAN. Routing services must be updated to enable connectivity to these services from this VxRail management network. Additional VLANs, such as those required for end-user access, must also be configured in routing services to connect end-users to the virtual machines running on the VxRail cluster.

2.5 VxRail node connectivity options

The following figures show the appliance connectivity options supported on the Network Daughter Cards (NDCs) for each VxRail node model, including the Dell 13th and 14th generation servers, and the connectivity requirements for the management port. These figures also show the available options supported for each VxRail node model for network connectivity not reserved for VxRail usage.
VxRail Node Connectivity Comparison

<table>
<thead>
<tr>
<th>VxRail Appliance Connectivity</th>
<th>E-Series</th>
<th>P-Series</th>
<th>S-Series</th>
<th>V-Series</th>
<th>G-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>2x10Gb or 4x10Gb RJ45 or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2x10Gb SFP+</td>
</tr>
<tr>
<td>2x10Gb or 4x10Gb SFP+ or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2x25Gb SFP28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*4x1Gb RJ45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management Port</th>
<th>1x1Gb RJ45 IDRAC 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Connectivity</td>
<td>8x10Gb RJ45</td>
</tr>
<tr>
<td></td>
<td>4x25Gb SFP28</td>
</tr>
<tr>
<td></td>
<td>16x10Gb RJ45</td>
</tr>
<tr>
<td></td>
<td>16x10Gb SFP+</td>
</tr>
<tr>
<td></td>
<td>12x10Gb RJ45</td>
</tr>
<tr>
<td></td>
<td>12x10Gb SFP+</td>
</tr>
<tr>
<td></td>
<td>16x10Gb RJ45</td>
</tr>
<tr>
<td></td>
<td>16x10Gb SFP+</td>
</tr>
<tr>
<td></td>
<td>4x10Gb RJ45</td>
</tr>
<tr>
<td></td>
<td>2x10Gb SFP+</td>
</tr>
</tbody>
</table>

*Maximum 8 nodes per cluster. 4 x 1Gb RJ45 ports on single CPU nodes only.

Figure 5  VxRail Node Connectivity Comparison

- E, P, S and V Series (14th Generation Dell EMC PowerEdge Servers) Appliance Connectivity Options
  - 2x10GbE in either SFP+ or RJ-45 NIC ports
  - 4x10GbE in either SFP+ or RJ-45 NIC ports
  - 2x25GbE SFP28 ports
- E, P, and S Series (14th Generation Dell EMC PowerEdge Servers)
  - 1 GbE connectivity is supported on single processor models only.
- G Series (14th Generation Dell EMC PowerEdge Servers) Appliance Connectivity Options
  - 2x10GbE SFP+ ports

VxRail Pre-14th Generation Node Connectivity Summary

<table>
<thead>
<tr>
<th>VxRail Appliance Connectivity</th>
<th>G-Series</th>
<th>E-Series</th>
<th>P-Series</th>
<th>S, V-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Connectivity</td>
<td></td>
<td>2x10Gb RJ45 or</td>
<td></td>
<td>*4x1Gb RJ45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2x10Gb SFP+ or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Port</td>
<td>1x1Gb RJ45 IDRAC 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional Connectivity</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6x10Gb RJ45 or</td>
<td></td>
<td></td>
<td>12x10Gb SFP+</td>
</tr>
<tr>
<td></td>
<td>6x10Gb SFP+</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Maximum 8 nodes per cluster. 4 x 1GbE RJ45 ports on single CPU nodes only.

Figure 6  VxRail Pre-14th Generation Node Connectivity Summary
- E, P, S and V Series (13th Generation Dell EMC PowerEdge Servers)
  - 2x10GbE + 2x1GbE in either SFP+ or RJ-45 NIC ports
- E, P, and S Series (13th Generation Dell EMC PowerEdge Servers)
  - 1 GbE connectivity is supported on single processor models only.
  - The 2x10GbE ports will auto-negotiate to 1 GbE when used with 1 GbE networking.

2.6 VxRail networking rules and restrictions
- The VxRail NICs on the Network Daughter Cards (NDCs) assigned to VxRail and selected for configuration during VxRail initialization process are reserved exclusively for VxRail usage and cannot be used for other purposes.
- VxRail initialization process will not touch any optional connectivity (PCIe NICs). You can use the ports for your own purposes such as VM networks, iSCSI, or NFS, etc.
- VxRail nodes supporting 10GbE can be configured with either two ports supporting VxRail cluster network traffic, or all four ports can be configured for the VxRail cluster network traffic.
- Four ports are required for each VxRail node when utilizing 1GbE networking on the supported single-processor models.
- All-flash VxRail models must use either 10GbE or 25GbE NICs. 1GbE is not supported for all-flash.
- The network hardware configuration in a VxRail appliance must have the same NDC across all VxRail nodes.
  - VxRail nodes with RJ45 and SFP+ ports cannot be mixed in the same VxRail appliance.
  - The port speed for each VxRail node (25 GbE, 10 GbE, 1 GbE) must be the same in the VxRail appliance.
  - These restrictions are not applicable to optional connectivity (PCI-e NICs).
- One additional port on the switch or one logical path on the VxRail external management VLAN is required for a workstation or laptop to access the VxRail user interface for the cluster.

2.7 Topology and connections
Various network topologies for switch(es) and VLANs are possible with VxRail Appliances. Complex production environments will have multiple core switches and VLANs. A site diagram showing the proposed network components and connectivity is highly recommended before cabling and powering on VxRail Appliances.

Be sure to follow your switch vendor’s best practices for performance and availability. For example, packet buffer banks may provide a way to optimize your network with your wiring layout.

Decide if you plan to use one or two switches for VxRail. One switch is acceptable and is often seen in test and development environments. To support high availability and failover in production environments, two or more switches are required. The VxRail appliance is a software-defined datacenter which is totally dependent on the physical top-of-rack switch for network communications. A lack of network redundancy places you at risk of losing availability to all of the virtual machines operating on the appliance.

The following figure shows the recommended physical network setup using a management switch (for iDRAC) and two ToR switches. Other network setup examples can be found in the Physical Network Switch Examples appendix.
Network topology of a 4-node VxRail cluster in a single rack connected to two 10 GbE switches using 2x10Gb connections per node, and a separate switch for out-of-band management.

**Note:** For 13th generation PowerEdge servers in the E, P, S and V series VxRail Appliances utilizing 1 GbE with two switches, the switches must be interconnected.

### 2.8 Out-of-band management (optional)

If the VxRail Appliances are located at a datacenter that you cannot access easily, we recommend setting up an out-of-band management switch to facilitate direct communication with each node.

To use out-of-band management, connect the internal Dell Remote Access Controller (iDRAC) port to a separate switch to provide physical network separation. Default values, capabilities, and recommendations for out-of-band management are provided with server hardware information.

You will need to reserve an IP address for each iDRAC in your VxRail cluster (one per node).
3 VxRail feature-driven decision points

Certain applications, software stacks and product features supported on VxRail can impact the architecture, deployment and operations of the cluster. If your plans for VxRail include any of the feature sets or software stacks listed in this section, make note of the requirements that each of these might have on your plans for VxRail.

3.1 Software-defined data center

If your plans include the transformation of your current data center with disparate technologies and processes towards a software-defined data center, consider that VxRail can be positioned as a building block towards that eventual outcome. The physical compute, network and storage resources from built VxRail clusters can be allocated to VMware’s cloud management and virtual desktop software solutions, and managed as a logical pool for end-user consumption. By using VxRail clusters as the underlying foundation, the software-defined data center can be designed and deployed to meet specific business and operational requirements.

Figure 8 VxRail as the foundation for the software-defined data center

The path starts with a structured discovery and planning process that focuses on business use cases and strategic goals, and that will drive the selection of software layers that will comprise the software-defined data center. Dell-EMC implements the desired software layers in a methodical, structured manner, where each phase involves incremental planning and preparation of the supporting network.

The next phase after the deployment of the VxRail cluster is to layer the VMware cloud foundation software on the cluster. This will enable assigning cluster resources as the underpinning for logical domains, whose policies align with use cases and requirements.

The information outlined in this guide covers networking considerations for VxRail. Go to the VMware Cloud on the Dell-EMC site to review the hyper-converged infrastructure options for software-defined data centers: VMware Cloud on Dell-EMC Infrastructure
3.2 Dell EMC SmartFabric network mode

Dell network switches support SmartFabric services, which enable the configuration and operation of the switches to be controlled outside of the standard management console through a REST API interface. Certain Dell switch models support initializing the switches with a VxRail personality profile at power-on, which then forms a unified network fabric, and enables VxRail to become the source for the automated configuration and administration of the Dell switches.

In this profile setting, VxRail uses the SmartFabric feature to discover VxRail nodes and Dell switches on the network, perform zero-touch configuration of the switch fabric to support VxRail deployment, and then create a unified hyper-converged infrastructure of the VxRail cluster and Dell switch network fabric.

![Diagram of Dell EMC SmartFabric](image)

Figure 9 Dell EMC SmartFabric

For ongoing VxRail cluster network management after initial deployment, the Dell EMC OMNI (Open Manage Network Interface) vCenter plug-in is provided free of charge. The Dell EMC OMNI plug-in will monitor state changes to the virtual network settings and properties on the vCenter instance and synchronize those changes to the Dell SmartFabric services using the REST API interface. In this scenario, there is no need to manually reconfigure the switches connected to the VxRail nodes when an update such as a new VLAN, port group, or virtual switch, is made in the vClient.

Planning for VxRail with the Dell EMC SmartFabric networking feature must be done in coordination with Dell-EMC representatives to ensure a successful deployment. The planned infrastructure must be a supported configuration as outlined in the VxRail Support Matrix.

Using the Dell EMC SmartFabric feature with VxRail requires an understanding of several key points:

- At the time of VxRail deployment, you must choose the method of network switch configuration. Enabling the VxRail personality profile on the switches resets the switches to the default state and passes switch configuration responsibility to VxRail. If you choose this method, all the switch configuration functionality except basic management functions are disabled at the console, and VxRail and the Dell EMC OMNI plug-in are the tools going forward for network switch configuration management.
- The Dell network switches enabled in VxRail personality profile mode cannot support any connected devices other than VxRail nodes.
- You must deploy a separate Ethernet switch to support out-of-band management for the iDRAC feature on the VxRail nodes.
• Configuring Dell switches using SmartFabric mode does not use standard OS10 commands on the console. The representation of the switch configuration from the console is not in sync with the SmartFabric configuration.
• Disabling the VxRail personality profile on the Dell network switches deletes the network configuration set up by SmartFabric services. If a VxRail cluster is operational on the Dell switch fabric, the cluster must be deployed.

3.3 vSAN stretched-cluster

vSAN stretched-cluster is a VMware solution that supports synchronous I/O on a vSAN datastore over distance and is supported on VxRail. A vSAN stretched-cluster enables site-level failure protection with no loss of service or loss of data.

If you plan to deploy a vSAN stretched-cluster on VxRail, note the following requirements:

• Three datacenter sites: two datacenter sites (Primary and Secondary) host the VxRail infrastructure, and the third site supports a witness to monitor the stretched-cluster
• A minimum of three VxRail nodes in the Primary site, and a minimum of three VxRail nodes in the Secondary site
• A minimum of one top-of-rack switch for the VxRail nodes in the Primary and Secondary sites
• An ESXi instance at the Witness site.

The vSAN stretched-cluster feature has strict networking guidelines, specifically for the WAN, that must be adhered to for the solution to work.

![vSAN Stretched-Cluster Topology](image)

Figure 10  vSAN Stretched-Cluster Topology
More detailed information on vSAN stretched-cluster and the networking requirements can be found in the Dell-EMC VxRail vSAN Stretched Cluster Planning Guide.

3.4 2-Node cluster

VxRail supports a solution specifically for small-scale deployments with reduced workload and availability requirements, such as those in a remote office setting. The solution is fixed to two VxRail nodes only, and like the stretched-cluster solution, requires a third site to act as a witness for monitoring purposes.

If you plan to deploy 2-node VxRail clusters, note of the following:

- The minimum VxRail software version for the 2-Node cluster is 4.7.1.
- The deployment is limited to a pair of VxRail E-Series nodes. Verify that your workload requirements do not exceed the resource capacity of this small-scale solution.
- Only one top-of-rack switch is required.
- The switch can support either 1 GbE or 10 GbE connectivity.
- Inter-cluster VxRail traffic between the nodes does not pass through the top-of-rack switch. Instead, the traffic utilizes a pair of network cables linked between the physical nodes.
- A customer-supplied external vCenter is required. The customer-supplied external vCenter cannot reside on the 2-Node cluster.
- The Witness is a small virtual appliance that monitors the health of the 2-Node cluster. A Witness is required for the 2-Node cluster.
  - An ESXi instance is required at the Witness site.
  - There is a 1:1 ratio of Witness per 2-Node cluster.
  - Witness can be deployed at the same site as the data nodes but not on the 2-Node cluster.
  - For instances where there are more than one 2-Node clusters deployed at the site, the Witness can reside on a 2-Node cluster it is not monitoring. This configuration requires a VMware RPQ.
  - The top-of-rack switch must be able to connect over the network with the Witness site.

![2-Node Cluster Topology](image)

**Figure 11  2-Node Cluster Topology**

Like the vSAN stretched-cluster feature, the small-scale solution has strict networking guidelines, specifically for the WAN, that must be adhered to for the solution to work.
4 VxRail hardware and switch selection decision points

Step 1. Assess your requirements and perform a sizing exercise to determine the quantity and characteristics of the VxRail nodes you need to meet planned workload and targeted use cases.

Step 2. Determine the number of physical racks needed to support the quantity and footprint of VxRail nodes required to meet workload requirements, including the top-of-rack switches. Verify the data center has sufficient floor space, power and cooling.

Step 3. Determine the optimal VxRail port speed to meet planned workload requirements, and to calculate the number of physical switch ports for connectivity.
   - VxRail supports 1 GbE, 10 GbE and 25 GbE connectivity options.
   - VxRail supports either two or four connections per node to the physical switch.

Step 4. Decide whether you want to attach the VxRail nodes to the switches with RJ45 connections or SFP+ connections.
   - VxRail nodes with RJ-45 ports require CAT5 or CAT6 cables. CAT6 cables are included with every VxRail.
   - VxRail nodes with SFP+ ports require optics modules (transceivers) and optical cables, or Twinax Direct-Attach Copper (DAC) cables. These cables and optics are not included; you must supply your own. The NIC and switch connectors and cables must be on the same wavelength.

Step 5. Determine the number of additional ports and port speed on the switch(es) for the uplinks to your core network infrastructure to meet VxRail workload requirements. Select a switch or switches that provide sufficient port capacity and characteristics.

Step 6. Reserve one additional port on the switch for a workstation/laptop to access the VxRail management interface for the cluster.
   - The additional port for access to the management interface is removed if connectivity is available elsewhere on the logical path on the VxRail management VLAN.

Step 7. Select a switch or switches that support the features and functionality required for VxRail.
   - IPV6 multicast is a requirement for VxRail device discovery.
   - If you want VxRail to be the source for the automated configuration of the top-of-rack switches using SmartFabric services, select a supported Dell switch model and OS10 Enterprise license.

Step 8. Determine whether a single switch will meet business objectives, as it is a potential single point of failure. Dual top-of-rack (ToR) switches provide protection from a switch failure.
   - If you are deploying dual top-of-rack switches, it is best practice to reserve ports on each switch for inter-switch links.

Step 9. Decide whether to deploy a separate switch to support connectivity to the VxRail management port on each node.
   - Dell iDRAC supports 1GbE connectivity. You can deploy a dedicated 1GbE switch for this purpose. You can also use open ports on the top-of-rack switches unless you elect to have VxRail to be the source for the automated configuration for the top-of-rack switches.
5 Planning the VxRail Implementation

VxRail is an entire software-defined datacenter in an appliance form factor. All administrative activities, including initial implementation and initialization, configuration, capacity expansion, online upgrades, as well as maintenance and support are handled within the VxRail management system. When the VxRail appliance is installed in your datacenter, connected to your network, and the physical components powered on, the VxRail management system automates the full implementation of the final software-defined datacenter based on your settings and input.

Before getting to this phase, several planning and preparation steps must be undertaken to ensure a seamless integration of the final product into your datacenter environment. These planning and preparation steps include:

1. Plan Data Center Routing Services.
2. Decide on VxRail Single Point of Management.
3. Plan the VxRail logical network.
4. Identify IP address range for VxRail logical networks.
5. Identify unique hostnames for VxRail management components.
6. Identify external applications and settings for VxRail.
7. Create DNS records for VxRail management components.
9. Reserve IP addresses for VxRail vMotion and vSAN networks.
10. Decide on VxRail Logging Solution
11. Decide on passwords for VxRail management.

Use the VxRail Setup Checklist and the VxRail Network Configuration Table to help create your network plan. References to rows in this document are to rows in the VxRail Network Configuration Table.

**Note:** Once you set up the VxRail cluster and complete the initial initialization phase to produce the final product, the configuration cannot easily be changed. Consequently, we strongly recommend that you take care during this planning and preparation phase to decide on the configurations that will work most effectively for your organization.

5.1 Plan Data Center Routing Services

Specific VxRail networks, including the VxRail external management network and any external-facing end-user networks configured for VxRail, must have routing services enabled to support connectivity to external services and applications, as well as end-users.

A VxRail cluster can be extended beyond a single physical rack, and can extend to as many as six racks. At initial implementation of the VxRail cluster, all of the network addresses applied to the VxRail nodes and management components must be within the same subnet. This same subnet rule applies to VxRail nodes and management components within a single physical rack.

You have two options if the VxRail cluster extends beyond a single rack:

- Use the same assigned subnet ranges for all VxRail nodes and management components
- Assign a new subnet range to the VxRail nodes and management components in the expansion racks. (Your VxRail cluster must be running a minimum version of 4.7.300 to use this option)
If the same subnets are extended to the expansion racks, then the VLANs representing those VxRail networks must be configured on the top-of-rack switches in each expansion rack and physical connectivity must be established. If new subnets are used for the VxRail nodes and management components in the expansion racks, then the VLANs will terminate at the router layer and routing services must be configured to enable connectivity between the racks.

**Figure 12** Multi-Rack VxRail sharing the same subnet

**Figure 13** Multi-Rack VxRail with different subnets

### 5.2 Decide on VxRail single point of management

The unified resources of a VxRail appliance create a virtual infrastructure that is defined and managed as a vSphere cluster under a single instance of vCenter. A decision must be made to use the VxRail vCenter Server, which is deployed in the cluster, or a customer-supplied vCenter server, which is external to the cluster. During the VxRail initialization process which creates the final product, you must select whether to deploy VxRail vCenter Server on the cluster or deploy the cluster on an external customer-supplied vCenter server. Once the initialization process is complete, migrating to a new vCenter single point of management requires professional services assistance, and is difficult to change.
Multiple VxRail clusters can be configured on a single customer-supplied vCenter server, while a deployment with VxRail vCenter server is limited to a single VxRail cluster. The customer-supplied vCenter server option is more scalable, provides more configuration options, and is the recommended choice. See the Dell EMC VxRail vCenter Server Planning Guide for details.

**Note:** Dell EMC strongly recommends that you take care during this planning and preparation phase and decide on the single point of management option that will work most effectively for your organization. Once VxRail initialization has configured the final product, the configuration cannot easily be changed.

### 5.3 Plan the VxRail logical network

The physical connections between the ports on your network switches and the NICs on the VxRail nodes enable communications for the virtual infrastructure within the VxRail cluster. The virtual infrastructure within the VxRail cluster uses the virtual distributed switch to enable communication within the cluster, and out to IT management and the application user community.

VxRail has pre-defined logical networks to manage and control traffic within the cluster and outside of the cluster. Certain VxRail logical networks must be made accessible to the outside community. For instance, connectivity to the VxRail management system is required by IT management. End-users and application owners will need to access their virtual machines running in the VxRail cluster. The network traffic supporting I/O to the vSAN datastore, or the vMotion network used to dynamically migrate virtual machines between VxRail nodes to balance workload, can stay within the VxRail cluster, or be configured with a routable network. The internal network used for device discovery is isolated and does not exit the top-of-rack switches.

Virtual LANs (VLANs) define the VxRail logical networks within the cluster, and the method used to control the paths a logical network can pass through. A VLAN, represented as a numeric ID, is assigned to a VxRail logical network. The same VLAN ID is also configured on the individual ports on your top-of-rack switches, and on the virtual ports in the virtual-distributed switch during the automated implementation process. When an application or service in the VxRail cluster sends a network packet on the virtual-distributed switch, the VLAN ID for the logical network is attached to the packet. The packet will only be able to pass through the ports on the top-of-rack switch and the virtual distributed switch where there is a match in VLAN IDs. Isolating the VxRail logical network traffic using separate VLANs is highly recommended, but not required. A ‘flat’ network is recommended only for test, non-production purposes.
As a first step, the network team and virtualization team should meet in advance to plan VxRail’s network architecture.

- The virtualization team must meet with the application owners to determine which specific applications and services planned for VxRail are to be made accessible to specific end-users. This will determine the number of logical networks required to support traffic from non-management virtual machines.
- The network team must define the pool of VLAN IDs needed to support the VxRail logical networks, and determine which VLANs will restrict traffic to the cluster, and which VLANs will be allowed to pass through the switch up to the core network.
- The network team must also plan to configure the VLANs on the upstream network, and on the switch(es) attached to the VxRail nodes.
- The network team must also configure routing services to ensure connectivity for external users and applications on VxRail network VLANs passed upstream.
- The virtualization team needs to assign the VLAN IDs to the individual VxRail logical networks.

VxRail groups the logical networks in the following categories: **External Management, Internal Management, vSAN, vSphere vMotion**, and **Virtual Machine**. VxRail assigns the settings you specify for each of these logical networks during the initialization process.

Before VxRail version 4.7, both external and internal management traffic shared the external management network. Starting with version 4.7 of VxRail, the external and internal management networks are broken out into separate networks.
**External Management** traffic includes all VxRail Manager, vCenter Server, ESXi communications, and vRealize Log Insight. All VxRail external management traffic is untagged by default and should be able to go over a Native VLAN on your top-of-rack switches. If this path is not accessible, you will not be able to build VxRail and configure the ESXi hosts without performing customizations first.

There are two methods that allow you to tag external management traffic:

1. Configure each port on your switch connected to a VxRail node to tag the management traffic and route it to the desired VLAN.
2. Alternately, you can configure a custom management VLAN to allow tagged management traffic after you power on each node, but before you run VxRail initialization. Your Dell EMC service representative will take care of this during installation.

The Internal Management network is used solely for device discovery by VxRail Manager during initial implementation and node expansion. This network traffic is non-routable and is isolated to the network switches connected to the VxRail nodes. Powered-on VxRail nodes advertise themselves on the Internal Management network using IPV6 multicast, which is required on this network, and discovered by VxRail Manager. The default VLAN of 3939 is configured on each VxRail node shipped from the factory. If a different VLAN value is used for this network, it must be applied to each VxRail node on-site, or device discovery will fail.

The vSphere vMotion and vSAN network traffic can be either routed or non-routed. Support for layer 3 networking is introduced with version 4.7.300 of VxRail for multi-rack clusters. If your requirements include expansion of the VxRail cluster beyond a single rack, then you can choose to extend either or both of these networks across the top-of-rack switches in each of the racks, or terminate the networks at the routing layer, and use routing services to enable connectivity between racks. This traffic will be tagged for the VLANs you specify in VxRail initialization.

The Virtual Machine network(s) are for the virtual machines running your applications and services. Dedicated VLANs are preferred to divide Virtual Machine traffic, based on business and operational objectives. VxRail creates one or more VM Networks for you, based on the name and VLAN ID pairs that you specify. Then, when you create VMs in vSphere Web Client to run your applications and services, you can easily assign the virtual machine to the VM Network(s) of your choice. For example, you could have one VLAN for Development, one for Production, and one for Staging.

<table>
<thead>
<tr>
<th>Network Configuration Table ✓</th>
<th>Enter the external management VLAN ID for VxRail management network (VxRail Manager, ESXi, vCenter Server/PSC, Log Insight). If you do not plan to have a dedicated management VLAN and will accept this traffic as untagged, enter “0” or “Native VLAN.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Configuration Table ✓</td>
<td>Enter the internal management VLAN ID for VxRail device discovery. The default is 3939. If you do not accept the default, the new VLAN must be applied to each VxRail node before cluster implementation.</td>
</tr>
<tr>
<td>Network Configuration Table ✓</td>
<td>Enter a VLAN ID for vSphere vMotion. (Enter 0 in the VLAN ID field for untagged traffic)</td>
</tr>
<tr>
<td>Network Configuration Table ✓</td>
<td>Enter a VLAN ID for vSAN. (Enter 0 in the VLAN ID field for untagged traffic)</td>
</tr>
<tr>
<td>Network Configuration Table ✓</td>
<td>Enter a Name and VLAN ID pair for each VM guest network you want to create. You must create at least one VM Network. (Enter 0 in the VLAN ID field for untagged traffic)</td>
</tr>
</tbody>
</table>
Note: If you plan to have multiple independent VxRail clusters, we recommend using different VLAN IDs for vSAN traffic and management traffic across multiple VxRail clusters to reduce network traffic congestion.

For a 2-Node cluster, the VxRail nodes must connect to the Witness over a separate Witness traffic separation network. The Witness traffic separation network is not required for stretched-cluster but is considered a best practice. For this network, a VLAN is required to enable Witness network on this VLAN must be able to pass through upstream to the Witness site.

![Diagram of logical network with Witness and Witness Traffic Separation](image)

**Figure 15** Logical network with Witness and Witness Traffic Separation

<table>
<thead>
<tr>
<th>ID</th>
<th>VLAN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXT DGMT</td>
<td>External Management</td>
</tr>
<tr>
<td>INT DGMT</td>
<td>Internal Management</td>
</tr>
<tr>
<td>VSAN</td>
<td>vSAN</td>
</tr>
<tr>
<td>vMotion</td>
<td>vMotion</td>
</tr>
<tr>
<td>Guest</td>
<td>Guest VM Networks</td>
</tr>
<tr>
<td>WTS</td>
<td>Witness Traffic Separation</td>
</tr>
</tbody>
</table>

**5.4 Plan network settings for VxRail management components**

During the initial build of the VxRail cluster, IP addresses entered are assigned to the VxRail components that are members of the External Management network and must follow certain rules:

- The IP address scheme must be a public IP address range.
- The IP address must be fixed (no DHCP).
- The IP addresses cannot be in use.
- The IP addresses assigned to the VxRail nodes must be contiguous (sequential order).
- The IP address range must all be in the same subnet (non-routable).

The decisions you make on the final VxRail configuration planned for your datacenter impacts the number of IP addresses you will need to reserve.
VxRail supports the Dell EMC ‘call home’ feature, where alerts from the appliance are routed to customer service. The Secure Remote Services gateway is required to enable alerts from VxRail to be sent to Dell EMC customer service.

- Decide whether to use an existing Secure Remote Services gateway in your datacenter for ‘call-home’, deploy a virtual instance of the Secure Remote Services gateway in the VxRail cluster for this purpose, or none.
- Reserve one IP address to deploy SRS-VE (Secure Remote Services Virtual Edition) in the VxRail cluster.

If you are planning to deploy a VxRail cluster that requires a Witness at a remote third site, such as VxRail stretched-cluster or 2-Node cluster, then two IP addresses are required to deploy the witness virtual appliance.

- One IP address is assigned to the witness management network.
- One IP address is assigned to the witness vSAN network.
- Both networks must be able to route to the VxRail cluster requiring the remote site witness.

For a 2-Node Cluster, the VxRail nodes must connect to the Witness over a separate Witness traffic separation network. For this network, an additional IP address is required for each of the two VxRail nodes.

- The VxRail nodes must be able to route to the remote site Witness.
- The traffic must be able to pass through the Witness traffic separation VLAN.

Use the following table to determine the number of public IP addresses required for the Management logical network:
<table>
<thead>
<tr>
<th>Component</th>
<th>Condition</th>
<th>Contiguous?</th>
<th>IP Address Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxRail Node</td>
<td>One per VxRail Node</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>VxRail Manager</td>
<td>One</td>
<td>No</td>
<td>1</td>
</tr>
<tr>
<td>vCenter</td>
<td>If you are supplying vCenter Server for VxRail: 0</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are using vCenter on VxRail: 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Insight</td>
<td>If you are supplying vCenter Server for VxRail: 0</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are supplying a syslog server for VxRail: 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you will not enable logging for VxRail: 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are using Log Insight on VxRail: 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRS-VE</td>
<td>If you are planning to deploy SRS Gateway on VxRail: 1</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you will not deploy SRS Gateway on VxRail: 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Request your networking team to provide you with a pool of unused IP addresses required for the VxRail External Management logical network. Record the IP address range for the ESXi hosts. These IP addresses are required.

Enter the starting and ending IP addresses for the ESXi hosts - a continuous IP range is required, with a minimum of 3 IPs.

Enter the subnet mask for the VxRail External Management network.

Enter the gateway for the VxRail External Management network.

Record the permanent IP address for VxRail Manager. This is required.

Enter the permanent IP address for VxRail Manager.

If you are going to deploy vCenter on the VxRail cluster, record the permanent IP address for vCenter and Platform Service Controller. Leave these entries blank if you will provide an external vCenter for VxRail.

Enter the IP address for VxRail vCenter.

Enter the IP address for VxRail Platform Service Controller.

Record the IP address for Log Insight. Leave this entry blank if you will not deploy Log Insight on VxRail.

Enter the IP address for vSphere Log Insight.

Record the two IP addresses for the witness virtual appliance. Leave blank if a witness is not required for your VxRail deployment.

Enter IP address for Witness Management Network.
5.5 Identify unique hostnames for VxRail management components

Each of the VxRail management components you deploy in the VxRail cluster will require you to assign an IP address, and assign a fully-qualified hostname. During initialization, each of these VxRail management components will be assigned a hostname and IP address.

Determine the naming format for the hostnames to be applied to the required VxRail management components: each ESXi host, and VxRail Manager. If you deploy the vCenter Server in the VxRail cluster, that also requires a hostname. In addition, if you decide to deploy Log Insight in the VxRail cluster, that needs a hostname as well.

**Note:** You cannot easily change the hostnames and IP addresses of the VxRail management components after initial implementation.

5.5.1 Select top-level domain

Begin the process by selecting the domain to use for VxRail and assign to the fully-qualified hostnames. Be aware that DNS is a requirement for VxRail, so select a domain where the naming services can support that domain.

5.5.2 Select ESXi hostnames

All ESXi hostnames in a VxRail cluster are defined by a naming scheme that comprises: an ESXi hostname prefix (an alphanumeric string), a separator ("None" or a dash ":-"), an iterator (Alpha, Num X, or Num 0X), an offset\(^1\) (empty or numeric), a suffix\(^2\) (empty or alphanumeric string with no .) and a domain. The Preview field shown during VxRail initialization is an example of the hostname of the first ESXi host. For example, if the prefix is "host," the separator is "None," the iterator is "Num 0X," the offset is empty, and the suffix is "lab," and the domain is "local," the first ESXi hostname would be "host01lab.local". The domain is also automatically applied to the VxRail management components. (Example: my-vcenter.local).

---

\(^1\) Offset is available starting in VxRail Release 4.0.200. It is only applicable when the iterator is numeric.

\(^2\) Suffix is available starting in VxRail Release 4.0.200.
5.5.3 **Select VxRail Manager hostname**

A hostname must be assigned to VxRail Manager. The domain is also automatically applied to the chosen hostname. Dell EMC recommends following the naming format selected for the ESXi hosts to simplify cluster management.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter an example of your desired ESXi host-naming scheme. Be sure to show your desired prefix, separator, iterator, offset, suffix and domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Rows 6-11</td>
<td></td>
</tr>
</tbody>
</table>

5.5.4 **Select VxRail vCenter Server hostname**

**Note**: You can skip this section if you plan to use an external vCenter Server in your datacenter for VxRail. These action items are only applicable if you plan to use the VxRail vCenter Server.

If you want to deploy a new vCenter Server on the VxRail cluster, you will need to specify a hostname for the VxRail vCenter Server and Platform Services Controller (PSC) virtual machines. Again, the domain is also automatically applied to the chosen hostname. Dell EMC recommends following the naming format selected for the ESXi hosts to simplify cluster management.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter an alphanumeric string for the new vCenter Server hostname. The domain specified will be appended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 14</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter an alphanumeric string for the new Platform Services Controller hostname. The domain specified will be appended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 16</td>
<td></td>
</tr>
</tbody>
</table>

5.5.5 **Select Log Insight hostname**

**Note**: You can skip this section if you plan to use an external syslog server instead of Log Insight, if you plan to use an external vCenter Server in your datacenter for VxRail or will not enable logging.

To deploy Log Insight to the VxRail cluster, the management component must be assigned a hostname. You can use your own third-party syslog server, use the vRealize Log Insight solution included with VxRail, or no logging. You can only select the vRealize Log Insight option if you also use the VxRail vCenter Server.
The domain is automatically applied to the chosen hostname. Dell EMC recommends following the naming format selected for the ESXi hosts to simplify cluster management.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the hostname for Log Insight.</th>
</tr>
</thead>
</table>

5.6 Identify external applications and settings for VxRail

VxRail is dependent on specific applications in your datacenter to be available over your datacenter network. These datacenter applications must be accessible to the VxRail management network.

5.6.1 Set time zone and NTP server

A time zone is required. It is configured on vCenter server and each ESXi host during VxRail initial configuration.

An NTP server is not required, but is recommended. If you provide an NTP server, vCenter server will be configured to use it. If you do not provide at least one NTP server, VxRail uses the time that is set on ESXi host #1 (regardless of whether the time is correct or not).

Note: Make sure the NTP IP address is accessible from the VxRail External Management Network which the VxRail nodes will be connected to and is functioning properly.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter your time zone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the hostname(s) or IP address(es) of your NTP server(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 4</td>
<td></td>
</tr>
</tbody>
</table>

5.6.2 Create DNS Records for VxRail Management Components

One or more external, customer-supplied DNS servers are required for VxRail. The DNS server you select for VxRail must be able to support naming services for all the VxRail management components (VxRail Manager, vCenter, etc.).

Note: Make sure that the DNS IP address is accessible from the network to which VxRail is connected and functioning properly.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the IP address(es) for your DNS server(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 5</td>
<td></td>
</tr>
</tbody>
</table>
Lookup records must be created in your selected DNS for every VxRail management component you are deploying in the cluster and are assigning a hostname and IP address. These components can include VxRail Manager, VxRail vCenter Server, VxRail Platform Service Controller, Log Insight, and each ESXi host in the VxRail cluster. The DNS entries must support both forward and reverse lookups.

### Sample DNS Forward Lookup Entries

<table>
<thead>
<tr>
<th>Host (A)</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>26P-APP01-ESX-01</td>
<td>10.244.12.141</td>
</tr>
<tr>
<td>26P-APP01-ESX-02</td>
<td>10.244.12.142</td>
</tr>
<tr>
<td>26P-APP01-ESX-03</td>
<td>10.244.12.143</td>
</tr>
<tr>
<td>26P-APP01-ESX-04</td>
<td>10.244.12.144</td>
</tr>
<tr>
<td>26P-APP01-LOG-01</td>
<td>10.244.12.148</td>
</tr>
<tr>
<td>26P-APP01-PSC-01</td>
<td>10.244.12.147</td>
</tr>
<tr>
<td>26P-APP01-VCC-01</td>
<td>10.244.12.145</td>
</tr>
<tr>
<td>26P-APP01-VXM-01</td>
<td>10.244.12.146</td>
</tr>
</tbody>
</table>

### Sample DNS Reverse Lookup Entries

<table>
<thead>
<tr>
<th>Pointer (PTR)</th>
<th>Fully Qualified Domain Name (FQDN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.244.12.143</td>
<td>25p-app01-esx-03.row26.local.</td>
</tr>
<tr>
<td>10.244.12.147</td>
<td>25p-app01-psc-01.row26.local.</td>
</tr>
</tbody>
</table>

Use the VxRail Network Configuration table to determine which VxRail management components to include in your planned VxRail cluster, and have assigned a hostname and IP address. vMotion and vSAN IP addresses are not configured for routing by VxRail, so there are no entries required in the DNS server.

### 5.7 Prepare customer-supplied vCenter server

**Note:** You can skip this section if you plan to use the VxRail vCenter server. These action items are only applicable if you plan to use a customer-supplied vCenter server in your datacenter for VxRail.

Certain pre-requisites must be completed, and settings provided before VxRail initialization if you use a customer-supplied vCenter as the VxRail cluster management platform. During the VxRail initialization process, it will connect to your customer-supplied vCenter to perform the necessary validation and configuration steps to deploy the VxRail cluster on your vCenter instance.

- Determine if your customer-supplied vCenter server is compatible with your VxRail version.
  - Refer to the Knowledge Base article VxRail: VxRail and External vCenter Interoperability Matrix on the Dell EMC product support site for the latest support matrix.
- Enter the FQDN of your selected, compatible customer-supplied vCenter server in the VxRail Network Configuration table.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the FQDN of the customer-supplied vCenter Server</th>
</tr>
</thead>
</table>
- Determine whether your customer-supplied vCenter server has an embedded or external platform services controller. If the platform services controller is external to your customer-supplied vCenter, enter the platform services controller FQDN in the VxRail Network Configuration table.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the FQDN of the customer-supplied platform services controller (PSC) Leave this row blank if the PSC is embedded in the customer-supplied vCenter server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 18</td>
<td></td>
</tr>
</tbody>
</table>

- Decide on the single sign-on (SSO) domain configured on the customer-supplied vCenter you want to use to enable connectivity for VxRail, and enter the domain in the VxRail Network Configuration Table.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the single sign-on (SSO) domain for the customer-supplied vCenter server. (For example, vsphere.local)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 20</td>
<td></td>
</tr>
</tbody>
</table>

- The VxRail initialization process requires login credentials to your customer-supplied vCenter. The credentials must have the privileges to perform the necessary configuration work for VxRail. You have two choices:
  - Provide vCenter login credentials with administrator privileges
  - Create a new set of credentials in your vCenter for this purpose. Two new roles will be created and assigned to this user by your Dell EMC representative.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the administrative username/password for the customer-supplied vCenter server, or the VxRail non-admin username/password you will create on the customer-supplied vCenter server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 21</td>
<td></td>
</tr>
</tbody>
</table>

- A set of credentials must be created in the customer-supplied vCenter for VxRail management with no permissions and no assigned roles. These credentials are assigned a role with limited privileges during the VxRail initialization process, and then assigned to VxRail to enable connectivity to the customer-supplied vCenter after initialization completes.
  - If this is the first VxRail cluster on the customer-supplied vCenter, enter the credentials you will create in the customer-supplied vCenter.
  - If you already have an account for a previous VxRail cluster in the customer-supplied vCenter, enter those credentials.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the full VxRail management username/password. (For example, <a href="mailto:cluster1-manager@vsphere.local">cluster1-manager@vsphere.local</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 22</td>
<td></td>
</tr>
</tbody>
</table>

- The VxRail initialization process will deploy the VxRail cluster under an existing datacenter in the customer-supplied vCenter. Create a new datacenter or select an existing Datacenter on the customer-supplied vCenter.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the name of a datacenter on the customer-supplied vCenter server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Row 23</td>
<td></td>
</tr>
</tbody>
</table>
- Specify the name of the cluster that will be created by the VxRail initialization process in the selected datacenter. This name must be unique, and not used anywhere in the datacenter on the customer-supplied vCenter.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the name of the cluster that will be used for VxRail.</th>
</tr>
</thead>
</table>

### 5.8 Reserve IP addresses for VxRail vMotion and vSAN networks

An IP address is required for the vMotion and vSAN networks for each ESXi host in the VxRail cluster. A private address range is acceptable if you decide the vMotion and vSAN networks will not be routable. The IP addresses must be contiguous, with the specified range in a sequential order. The IP address range must be large enough to cover the number of ESXi hosts planned for the VxRail cluster. A larger IP address range can be specified to cover for planned expansion.

If your plans include expanding the VxRail cluster to deploy nodes in more than one physical rack, then you have the option of whether to stretch the IP subnet for vSAN and vMotion between the racks, or to use routing services in your data center instead. If you plan to enable routing services, a routable address range is required for the vSAN and vMotion networks.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the starting and ending IP addresses for vSphere vMotion.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Configuration Table</td>
<td>Enter the subnet mask for vMotion.</td>
</tr>
<tr>
<td>Network Configuration Table</td>
<td>Use the default TCP-IP gateway for the VxRail external management network, or enter a new gateway for the vMotion network</td>
</tr>
<tr>
<td>Network Configuration Table</td>
<td>Enter the starting and ending IP addresses for vSAN. Routing is not configured for vSAN.</td>
</tr>
<tr>
<td>Network Configuration Table</td>
<td>Enter the subnet mask for vSAN.</td>
</tr>
</tbody>
</table>

### 5.9 Decide on VxRail logging solution

Decide whether to use your own third-party syslog server, use the vRealize Log Insight solution included with VxRail, or no logging. You can only select the vRealize Log Insight option if you use the VxRail vCenter server. If you use a customer-supplied vCenter server, you can either use your own third-part syslog server, or no logging. If you choose the vRealize Log Insight option, the IP address assigned to Log Insight must be on the same subnet as the VxRail management network.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the IP address for vRealize Log Insight or the hostname(s) of your existing third-party syslog server(s). Leave blank for no logging.</th>
</tr>
</thead>
</table>
5.10 Assign passwords for VxRail management

You will need to assign a password to the accounts that are members of the VxRail management ecosystem. Refer to the VxRail Passwords table to use as worksheets for your passwords.

**Note:** The Dell EMC service representative will need passwords for the VxRail accounts in this table. For security purposes, you can enter the passwords during the VxRail initialization process, as opposed to providing them visibly in a document.

- For ESXi hosts, passwords must be assigned to the ‘root’ account. You can use one password for each ESXi host or apply the same password to each host.
- For VxRail Manager, a password must be assigned to the ‘root’ account [Row 1]. This credential is for access to the console.
- Access to the VxRail Manager web interface will use the ‘administrator@<SSO Domain>’ credentials
  - If you deploy the VxRail vCenter Server, VxRail Manager and vCenter share the same default administrator login, ‘administrator@vsphere.local’. Enter the password you want to use [Row 2].
  - If you use a customer-supplied vCenter server, VxRail Manager will use the same ‘administrator@<SSO Domain>’ login credentials you use for access to the customer-supplied vCenter server.
- If you deploy the VxRail vCenter Server:
  - Enter the ‘root’ password for the VxRail vCenter Server [Row 3].
  - Enter a password for ‘management’ for the VxRail vCenter Server [Row 4].
  - A Platform Services controller will be deployed. Enter the ‘root’ password for the Platform Services controller [Row 5].
- If you deploy vRealize Log Insight:
  - Enter a password for ‘root’ [Row 6].
  - Enter a password for ‘admin’ [Row 7].

Passwords must adhere to VMware vSphere complexity rules. Passwords must contain between eight and 20 characters with at least one lowercase letter, one uppercase letter, one numeric character, and one special character. For more information about password requirements, see the vSphere password and vCenter Server password documentation.
5.11 Prepare for Dell EMC SmartFabric services enablement

Note: Skip this section if you do not plan to enable Dell EMC SmartFabric services to pass control of switch configuration to VxRail.

Figure 19 Logical Network with VxRail Cluster Build VLAN

To enable the Dell EMC SmartFabric feature, and pass control of switch configuration management to VxRail and the Dell EMC OMNI vCenter plug-in, a VLAN for the **VxRail Cluster Build Network** must be defined.

When the VxRail personality profile is enabled on a pair of Dell switches running in SmartFabric mode, a VLAN must be entered as part of the configuration process. This VLAN is assigned to every switch data port as ‘untagged’. This establishes an access network across the entire switch fabric for enabling connectivity to VxRail Manager for initial configuration.

At the time of VxRail personality profile enablement on the Dell switch fabric, the VxRail Cluster Build network and the Internal Management network are both established on every data port on the switch pair. The switches and VxRail nodes advertise themselves at power-on on the Internal Management network and are discovered by VxRail Manager on the same network. VxRail Manager then connects itself to the VxRail Cluster Build network to enable access on the ‘untagged’ network for cluster implementation. During the cluster implementation process, VxRail Manager will connect itself to the External Management network and transition off the VxRail Cluster Build network.

When the cluster implementation process completes, all VxRail Manager, vCenter Server, and ESXi management communications occurs over the External Management network, freeing the VxRail Cluster Build network for additional clusters to be added to the switch fabric.
**Note:** Be aware that the VLAN assigned to the VxRail Cluster Build Network is permanent and can only be changed by resetting the Dell EMC switch fabric back to the factory default state.

The Dell EMC Open Management Network Interface (OMNI) plug-in must be deployed on the vCenter instance to support automated switch management after the VxRail cluster is built. The Dell EMC OMNI vCenter plug-in is required for each Dell EMC switch fabric pair, and requires network properties to be set during the deployment process.

Record the VxRail Cluster Build network VLAN and the network settings for Dell EMC OMNI vCenter plug-in.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Row 44</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable Dell EMC SmartFabric services on your switches and enable the VxRail personality profile, enter a VLAN ID for the VxRail Cluster Build Network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Row 45</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address for Dell EMC OMNI vCenter plug-in.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Row 46</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the subnet mask for Dell EMC OMNI vCenter plug-in.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Row 47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the gateway for Dell EMC OMNI vCenter plug-in.</td>
<td></td>
</tr>
</tbody>
</table>
6 Configure the upstream network for VxRail

The upstream network from the VxRail cluster must be configured to allow passage for VxRail networks that require external access. The switches supporting direct connectivity to the VxRail cluster (TOR switch) should pass the external-facing VxRail network traffic through a pair of switch ports upstream to a pair of switch ports on the next network layer (spine switch). The switch at the next layer needs to direct this network traffic to the appropriate end-user community.

The **VxRail External Management Network** should be accessible to your location’s IT infrastructure and personnel only. IT administrators require access to this network for day-to-day management of the VxRail cluster, and the VxRail cluster is dependent on outside applications such as DNS and NTP to operate correctly.

![Logical Network including Upstream Elements](image)

**Figure 20** Logical Network including Upstream Elements

**VxRail Virtual Machine Networks** support access to applications and software deployed on the virtual machines on the VxRail cluster. While you must create at least one VxRail Virtual Machine network at VxRail initial implementation, additional VxRail Virtual Machine networks can be added to support the end-user community. The spine switch must be configured to direct the traffic from these VxRail Virtual Machine networks to the appropriate end-users.

The **VxRail Cluster Build Network** is required only if you plan to enable Dell EMC SmartFabric services and extend VxRail automation to the switch layer. The VxRail Cluster Build network enables access to VxRail Manager during initial implementation using a jump host.

The **VxRail Witness Traffic Separation Network** is optional if you plan to deploy a stretched-cluster. The VxRail Witness traffic separation network enables connectivity between the VxRail nodes with the witness at an offsite location. The remote-site witness monitors the health of the vSAN datastore on the VxRail cluster over this network.

Using the VxRail Network Configuration table, perform the following steps:

**Step 1.** Configure the **External Management Network VLAN (Row 1)** on the spine switch.

**Step 2.** Configure all of the VxRail Virtual Machine Network VLANs (Rows 39,40) on the spine switch.

**Step 3.** If applicable, configure the VxRail Cluster Build Network VLAN (Row 44) on the spine switch.
Step 4. If applicable, configure the VxRail Witness Traffic Separation Network VLAN (Row 50) on the spine switch.

Step 5. Create a logical pair (port channel) on the spine switch ports that will connect downstream to the uplinks on the TOR switch.
- Make sure the port channel settings (active/passive) on the spine switch matches the setting on the TOR switch.
- Configure all the external VLANs on this port channel.

Step 6. Enable routing services or configure additional logical pairs as necessary to direct VxRail network traffic to the appropriate end destination.

6.1 Setting up the network switch for VxRail connectivity

**Note:** You can skip this section if you plan to enable Dell EMC SmartFabric services and extend VxRail automation to the TOR switch layer.

For the VxRail initialization process to pass validation and build the cluster, you must configure the ports that VxRail will connect to on your switch **before you plug in VxRail nodes and powering them on.**

Follow these steps to set up your switch:

1. Plan switch configuration.
2. Plan switch port configuration.
3. Configure ports and VLANs on your switch(es).

**Note:** This section provides guidance for preparing and setting up your switch for VxRail. Be sure to follow your vendor’s documentation for specific switch configuration activities and for best practices for performance and availability.

6.1.1 Plan switch configuration

6.1.1.1 Enable multicast for VxRail Internal Management network

VxRail Appliances have no backplane, so communication between its nodes is facilitated through the network switch. This communication between the nodes uses VMware’s Loudmouth auto-discovery capabilities, based on the RFC-recognized “Zero Network Configuration” protocol. New VxRail nodes advertise themselves on the network using the VMware Loudmouth service, and are discovered by VxRail Manager with the Loudmouth service. VMware’s Loudmouth service depends on IPv6 multicast, which is required for the VxRail internal management network.

The network switch ports that connect to VxRail nodes must allow for pass-through of multicast traffic on the VxRail Internal Management VLAN. Multicast is **not** required on your entire network, just on the ports connected to VxRail nodes.

VxRail creates very little traffic through IPv6 multicast for auto-discovery and device management. We recommend that you limit traffic further on your switch by enabling **MLD Snooping** and **MLD Querier**.

If MLD Snooping is enabled, MLD Querier **must be** enabled. If MLD Snooping is disabled, MLD Querier **must be** disabled.
For VxRail clusters running at version 4.7 or later, VxRail management traffic is segmented into two separate logical networks: one which is external to service administrators and end-users, and a second internal network used solely for auto-discovery and device management and is isolated from the upstream network. Multicast must be enabled on the second internal management network only.

6.1.1.2 Enable Unicast or Multicast for VxRail vSAN Network

Starting in VxRail v4.5.0, all vSAN traffic replaces multicast with unicast. This change helps reduce network configuration complexity and simplifies switch configuration.

For VxRail v4.5.0 and earlier, IPv4 multicast is required for the vSAN VLAN. The network switch(es) that connect to VxRail must allow for pass-through of multicast traffic on the vSAN VLAN. Multicast is not required on your entire network, just on the ports connected to VxRail.

There are two options to handle vSAN IPv4 multicast traffic. Either limit multicast traffic by enabling or disabling IGMP Snooping and IGMP Querier. We recommend enabling both IGMP Snooping and IGMP Querier if your switch supports them.

IGMP Snooping software examines IGMP protocol messages within a VLAN to discover which interfaces are connected to hosts or other devices interested in receiving this traffic. Using the interface information, IGMP Snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding an entire VLAN. IGMP Snooping tracks ports that are attached to multicast-capable routers to help manage IGMP membership report forwarding. It also responds to topology change notifications. Disabling IGMP Snooping might lead to additional multicast traffic on your network.

IGMP Querier sends out IGMP group membership queries on a timed interval, retrieves IGMP membership reports from active members, and allows updates to group membership tables. By default, most switches enable IGMP Snooping but disable IGMP Querier. You will need to change the settings if this is the case.

If IGMP Snooping is enabled, IGMP Querier must be enabled. If IGMP Snooping is disabled, IGMP Querier must be disabled.

If your switch does not support IGMP nor MLD Snooping, VxRail multicast traffic will be broadcasted in one broadcast domain per VLAN. There is minimal impact on network overhead as management traffic is nominal.

For questions about how your switch handles multicast traffic, contact your switch vendor.

6.1.1.3 Enable uplinks to pass inbound and outbound VxRail network traffic

The uplinks on the switches must be configured to allow passage for external network traffic to administrators and end-users. This includes the VxRail external management network (or combined VxRail management network prior to version 4.7) and Virtual Machine network traffic. The VLANs representing these networks need to be passed upstream through the uplinks. For VxRail clusters running at version 4.7 or later, the VxRail internal management network must be blocked from outbound passage.

If the VxRail vMotion network is going to be configured to be routable outside of the top-of-rack switches, include the VLAN for this network in the uplink configuration. This is usually the case for a multi-rack VxRail configuration where a new subnet will be assigned to the expansion racks. In addition, the VxRail vSAN network will follow this same rule for a multi-rack VxRail cluster.
6.1.4 Enable Inter-Switch communication

In a dual-switch environment, configure the ports used for inter-switch communication to allow passage for all of the VxRail virtual networks. Both switches must be configured to allow passage of IPv6 multicast traffic used for device discovery, and IPv4 traffic (unicast starting in VxRail v4.5.0 and multicast in earlier versions).

If a multi-rack VxRail cluster is planned, and you plan to extend the VxRail External Management, vMotion, vSAN and guest networks to the expansion racks, configure the ports on the switch to pass these VLANs to the switches in the expansion racks.

6.1.5 Enable Inter-Switch links

If you are using multiple switches, connect them using trunked interfaces on each switch and ensure that all VLANs used for VxRail are carried across the trunk following the requirements in this document.

6.1.2 Plan switch port configuration

6.1.2.1 Determine Switch Port Mode

Configure the port mode on your switch based on the plan for the VxRail logical networks, and whether VLANs will be used to segment VxRail network traffic. Ports on a switch operate in one of the following modes:

- **Access mode** – The port accepts untagged packets only and distributes the untagged packets to all VLANs on that port. This is typically the default mode for all ports.
- **Trunk mode** – When this port receives a tagged packet, it passes the packet to the VLAN specified in the tag. To configure the acceptance of untagged packets on a trunk port, you must first configure a single VLAN as a “Native VLAN.” A “Native VLAN” is when you configure one VLAN to use as the VLAN for all untagged traffic.
- **Tagged-access mode** – The port accepts tagged packets only.

Note: Do not enable Link Aggregation on VxRail switch ports.

Do not use link aggregation, including protocols such as LACP and EtherChannel, on any ports directly connected to VxRail nodes. VxRail Appliances use the vSphere active/standby configuration (NIC teaming) for network redundancy. However, LACP can be enabled on non-system ports, such as additional NIC ports or 1G ports, for user traffic.

VxRail uses vSphere Network I/O Control (NIOC) to allocate and control network resources for the four predefined network traffic types required for operation: Management, vSphere vMotion, vSAN, and Virtual Machine. The respective NIOC settings for the predefined network traffic types are listed in the following tables for the various VxRail Models.  

---

[3] For a general overview on NIOC shares refer to [http://frankdenneman.nl/2013/01/17/a-primer-on-network-i-o-control/].
### 4x10GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Multicast Requirements</th>
<th>UPLINK1 (10Gb) VMNIC0</th>
<th>UPLINK2 (10Gb) VMNIC1</th>
<th>UPLINK3 (10Gb) VMNIC2</th>
<th>UPLINK4 (10Gb) VMNIC3</th>
<th>NIOC Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>IPv6 multicast</td>
<td>Standby</td>
<td>Active</td>
<td>Unused</td>
<td>Unused</td>
<td>40</td>
</tr>
<tr>
<td>vSphere vMotion</td>
<td>None</td>
<td>Unused</td>
<td>Unused</td>
<td>Standby</td>
<td>Active</td>
<td>50</td>
</tr>
<tr>
<td>vSAN</td>
<td>None</td>
<td>Unused</td>
<td>Unused</td>
<td>Active</td>
<td>Standby</td>
<td>100</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>None</td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>60</td>
</tr>
</tbody>
</table>

### 2x10GbE or 2x25GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Multicast Requirements</th>
<th>UPLINK1 (10Gb or 25Gb) VMNIC0</th>
<th>UPLINK2 (10Gb or 25Gb) VMNIC1</th>
<th>UPLINK3 (No VMNIC)</th>
<th>UPLINK4 (No VMNIC)</th>
<th>NIOC Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>IPv6 multicast</td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>20</td>
</tr>
<tr>
<td>vSphere vMotion</td>
<td>None</td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>50</td>
</tr>
<tr>
<td>vSAN</td>
<td>None</td>
<td>Standby</td>
<td>Active</td>
<td>Unused</td>
<td>Unused</td>
<td>100</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>None</td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>30</td>
</tr>
</tbody>
</table>

### 1GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Multicast Requirements</th>
<th>UPLINK1 (1Gb) VMNIC0</th>
<th>UPLINK2 (1Gb) VMNIC1</th>
<th>UPLINK3 (1Gb) VMNIC2</th>
<th>UPLINK4 (1Gb) VMNIC3</th>
<th>NIOC Shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>IPv6 multicast</td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>40</td>
</tr>
<tr>
<td>vSphere vMotion</td>
<td>None</td>
<td>Unused</td>
<td>Unused</td>
<td>Standby</td>
<td>Active</td>
<td>50</td>
</tr>
<tr>
<td>vSAN</td>
<td>None</td>
<td>Unused</td>
<td>Unused</td>
<td>Active</td>
<td>Standby</td>
<td>100</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>None</td>
<td>Standby</td>
<td>Active</td>
<td>Unused</td>
<td>Unused</td>
<td>60</td>
</tr>
</tbody>
</table>

#### 6.1.2.2 Limited spanning tree protocol on VxRail switch ports

Network traffic must be allowed uninterrupted passage between the physical switch ports and the VxRail nodes. Certain Spanning Tree states can place restrictions on network traffic and can force the port into an unexpected timeout mode. These conditions caused by Spanning Tree can disrupt VxRail normal operations and impact performance.
If Spanning Tree is enabled in your network, ensure that the physical switch ports connected to VxRail nodes are configured with a setting such as 'Portfast', or set as an edge port. These settings set the port to forwarding state, so no disruption occurs. Because vSphere virtual switches do not support STP, physical switch ports connected to an ESXi host must have a setting such as 'Portfast' configured if spanning tree is enabled to avoid loops within the physical switch network.

6.1.3 Configure ports and VLANs on your switch(es)

Now that you understand the switch requirements, it is time to configure your switch(es). The VxRail network can be configured with or without VLANs. For performance and scalability, we highly recommend configuring VxRail with VLANs. As listed in the VxRail Setup Checklist, you will be configuring the following VLANs:

For VxRail clusters using version 4.7 or later:
- VxRail External Management VLAN (default is untagged/native)
- VxRail Internal Management VLAN - Make sure that IPv6 multicast is configured/enabled on this VLAN.

For VxRail clusters using versions earlier than 4.7:
- VxRail Management VLAN (default is untagged/native) – Make sure that IPv6 multicast is configured/enabled on this VLAN.

For VxRail clusters using version 4.5 or later:
- vSAN VLAN – Make sure that IPv4 unicast mode is configured/enabled.

For VxRail clusters using versions earlier than 4.5:
- vSAN VLAN – Make sure that IPv4 multicast is configured/enabled. Enabling IGMP snooping and querier is highly recommended.
- vSphere vMotion VLAN

VM Networks VLAN

Figure 21 VxRail Logical Networks: Version earlier than 4.7 and 4.7 or later
VxRail Logical Networks: 2-Node Cluster with Witness

- The additional VxRail Witness traffic separation VLAN to manage traffic between the VxRail cluster and the witness. This is only needed if deploying VxRail stretched-cluster or 2-Node cluster.

Using the VxRail Network Configuration table, perform the following steps:

1. Configure a VLAN on the switch(es) for each VxRail logical network.
2. Configure each switch port that will be connected to a VxRail node.
   - Set the switch port mode to the appropriate setting.
   - Set the port to the appropriate speed or to auto-negotiate speed.
3. Configure the External Management VLAN (Row 1) on the switch ports. If you entered “Native VLAN,” set the ports on the switch to accept untagged traffic and tag it to the native management VLAN ID. Untagged management traffic is the default management VLAN setting on VxRail.
4. For VxRail version 4.7 and later, configure the Internal Management VLAN (Row 2) on the switch ports.
5. You must set the management VLAN (prior to version 4.7) or internal management VLAN (version 4.7 or later) to allow IPv6 multicast traffic to pass through the VxRail switch ports. Depending on the type of switch you have, you may need to turn on IPv6 and multicast directly on the port or on the VLAN. If necessary, consult the switch manufacturer for further instructions on how to configure these settings.
6. Configure a vSphere vMotion VLAN (Row 34) on the switch ports.
7. Configure a vSAN VLAN (Row 38) on the switch ports. For release prior to VxRail v4.5.0, set the switch to allow IPv4 multicast traffic to pass through. For VxRail v4.5.0 and later, set the switch to allow IPv4 unicast traffic to pass through.
8. Configure the VLANs for your VM Networks (Rows 39-41) on the switch ports.
9. Configure the optional **VxRail Witness Traffic Separation VLAN (Row 50)** on the switch ports if required.

10. Configure the switch uplinks to allow the **External Management VLAN (Row 1)** and VM Network VLANS (Rows 39-40) to pass through, and optionally the **vSphere vMotion VLAN** and **vSAN VLAN**. If a vSAN witness is required for the VxRail cluster, include the **VxRail Witness Traffic Separation VLAN (Row 50)** on the uplinks.

11. Configure the inter-switch links to allow the **all VLANS** to pass through if deploying dual switches.

### 6.2 Confirm your datacenter network

Upon completion of the switch configuration, there should be unobstructed network paths between the switch ports and the ports on the VxRail nodes. The VxRail management network and VM network should have unobstructed passage to your datacenter network. Before forming the VxRail cluster, the VxRail initialization process will perform several verification steps, including:

- Verifying switch and datacenter environment supportability
- Verifying passage of VxRail logical networks
- Verifying accessibility of required datacenter applications
- Verifying compatibility with the planned VxRail implementation

Certain datacenter environment and network configuration errors will cause the validation to fail, and the VxRail cluster will not be formed. When validation fails, the datacenter settings and switch configurations must undergo troubleshooting to resolve the problems reported.

Confirm the settings on the switch, using the switch vendor instructions for guidance:

1. Confirm that IPv4 multicast (VxRail release earlier than v4.5.0) or unicast (VxRail v4.5.0 and later) and IPv6 multicast are enabled for the VLANS described in this document.
2. If you have two or more switches, confirm that IPv4 multicast/unicast and IPv6 multicast traffic is transported between them.
3. External management traffic will be untagged on the **native VLAN** on your switch by default. If this has changed, the switches and/or ESXi hosts must be customized with the new VLAN.
4. Internal device discovery network traffic will use the default VLAN of 3939. If this has changed, all ESXi hosts must be customized with the new VLAN, or device discovery will not work.
5. Confirm that the switch ports that will attach to VxRail nodes allow passage of all VxRail network VLANS.
6. Confirm that the switch uplinks allow passage of external VxRail networks.

If you have positioned a firewall between the switch(es) planned for VxRail and the rest of your datacenter network, be sure the required firewall ports are open for VxRail network traffic.

### 6.3 Confirm your firewall settings

1. Verify that VxRail will be able to communicate with your DNS server.
2. Verify that VxRail will be able to communicate with your NTP server.
3. Verify that your IT administrators will be able to communicate with the VxRail management system.
4. If you plan to use a customer-supplied vCenter, verify open communication between the vCenter instance and the VxRail managed hosts.
5. If you plan to use a third-party syslog server instead of Log Insight, verify that open communication between the syslog server and the VxRail management components.

6. If you plan to deploy a separate network for ESXi host management (iDRAC), verify that your IT administrators will be able to communicate with the iDRAC network.

7. If you plan to use an external Secure Remote Services (SRS) gateway in your datacenter instead of SRS-VE deployed in the VxRail cluster, verify the open communications between VxRail management and the SRS gateway.

Refer to VxRail Open Ports Requirements for information of VxRail port requirements.

6.4 Confirm your datacenter environment

1. Confirm that you cannot ping any IP address reserved for VxRail management components.
2. Confirm that your DNS server(s) are reachable from the VxRail external management network.
3. Confirm the forward and reverse DNS entries for the VxRail management components.
4. Confirm that your management gateway IP address is accessible.
5. If you decide to use the TCP-IP stack for vMotion instead of the default TCP-IP stack, confirm that your vMotion gateway IP address is accessible.
6. If you have configured NTP servers, or a third-party syslog server, confirm that you can reach them from your configured VxRail external management network.
7. If you plan to use a customer-supplied vCenter, confirm that it is accessible from the VxRail external management network.
8. If you plan to deploy a witness at a remote site to monitor vSAN, and plan to enable Witness Traffic Separation, confirm that there is a routable path between the witness and this network.
9. If you plan to install the VxRail nodes in more than one rack, and you plan to terminate the VxRail networks at the ToR switches, verify that routing services have been configured upstream for the VxRail networks.
7 Preparing to build the VxRail cluster

The steps outlined in this section will be performed by Dell-EMC professional services. They are described here to provide insight into the activities to be performed during the delivery engagement.

7.1 Configuring a workstation/laptop for VxRail initialization

A workstation/laptop with a web browser for the VxRail user interface is required to perform the initialization process. It must be plugged into the top-of-rack switch, or be able to logically reach the VxRail external management VLAN from elsewhere on your network; for example, a jump server (Jump Server Description). If you are planning to enable Dell EMC SmartFabric services, and extend VxRail automation to the switch layer, the jump host must be able to also reach the VxRail Cluster Build Network VLAN as well as the VxRail external management VLAN. Once the VxRail initialization process is complete, the switch port or jump host is no longer required to manage VxRail.

Note: Don’t try to plug your workstation/laptop directly into a VxRail server node to connect to the VxRail management interface for initialization. It must be plugged into your network or switch, and the workstation/laptop must be logically configured to reach the necessary networks.

A supported web browser is required to access VxRail management interface. The latest versions of Firefox, Chrome, and Internet Explorer 10+ are all supported. If you are using Internet Explorer 10+ and an administrator has set your browser to “compatibility mode” for all internal websites (local web addresses), you will get a warning message from VxRail. Contact your administrator to whitelist URLs mapping to the VxRail user interface.

To access the VxRail management interface to perform initialization, you must use the temporary, pre-configured VxRail initial IP address: 192.168.10.200/24. This IP address will automatically change during VxRail initialization to your desired permanent address, and assigned to VxRail Manager during cluster formation.

<table>
<thead>
<tr>
<th>Example Configuration</th>
<th>VxRail IP address/netmask</th>
<th>Workstation/laptop</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial (temporary)</td>
<td>192.168.10.200/24</td>
<td>192.168.10.150</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Post-configuration (permanent)</td>
<td>10.10.10.100/24</td>
<td>10.10.10.150</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Your workstation/laptop will need to be able to reach both the temporary VxRail initial IP address and the permanent VxRail Manager IP address (Row 26 from VxRail Network Configuration table). VxRail initialization will remind you that you might need to reconfigure your workstation/laptop network settings to access the new IP address.

It is best practice to give your workstation/laptop or your jump server two IP addresses on the same network port, which allows for a smoother experience. Depending on your workstation/laptop, this can be implemented in several ways (such as dual-homing or multi-homing). Otherwise, change the IP address on your workstation/laptop when instructed to and then return to VxRail Manager to continue with the initialization process.

If you cannot reach the VxRail initial IP address, Dell EMC support team can configure a custom IP address, subnet mask, and gateway on VxRail Manager before initialization.
Note: If a custom VLAN ID will be used for the VxRail management network other than the default "Native VLAN", make sure the workstation/laptop can also access this VLAN.

7.2 Perform initialization to create a VxRail cluster

If you have successfully followed all of the steps listed in this document, you are ready to move to the final phase: connect the laptop/workstation to a switch port, and perform VxRail initialization. These steps are done by Dell EMC service representatives and are included here to help you understand the complete process.

**Step 1.** Before coming on-site, the Dell EMC service representative will have contacted you to capture and record the information described in the VxRail Network Configuration Table and walk through the VxRail Setup Checklist.

**Step 2.** If your planned VxRail deployment requires a Witness at a remote datacenter location, the Witness virtual appliance is deployed.

**Step 3.** Install the VxRail nodes in a rack or multiple racks in the datacenter. For ease of manageability, install the network switches supporting the VxRail cluster into the same racks.

**Step 4.** Attach Ethernet cables between the ports on the VxRail nodes and switch ports configured to support VxRail network traffic.

**Step 5.** Power on three or four initial nodes to form the initial VxRail cluster. Do not turn on any other VxRail nodes until you have completed the formation of the VxRail cluster with the first three or four nodes.

**Step 6.** Connect a workstation/laptop configured for VxRail initialization to access the VxRail external management network on your selected VLAN. It must be either plugged into the switch or able to logically reach the VxRail external management VLAN from elsewhere on your network.

**Step 7.** Open a browser to the VxRail initial IP address to begin the VxRail initialization process.

**Step 8.** The Dell EMC service representative will populate the input screens on the menu with the data collected and recorded in the VxRail Network Configuration Table.

**Step 9.** If you have enabled Dell EMC SmartFabric services, VxRail will automatically configure the switches connected to VxRail nodes.

**Step 10.** VxRail performs the verification process, using the information input into the menus.

**Step 11.** After validation is successful, the initialization process will begin to build a new VxRail cluster.

**Step 12.** The new permanent IP address for VxRail Manager will be displayed.

- If you configured the workstation/laptop to enable connectivity to both the temporary VxRail IP address and the new permanent IP address, the browser session will make the switch automatically. If not, you must manually change the IP settings on your workstation/laptop to be on the same subnet as the new VxRail IP address.

- If your workstation/laptop cannot connect to the new IP address that you configured, you will get a message to fix your network and try again. If you are unable to connect to the new IP address after 20 minutes, VxRail will revert to its un-configured state and you will need to re-enter your configuration at the temporary VxRail IP address.

- After the build process starts, if you close your browser, you will need to browse to the new, permanent VxRail IP address.

**Step 13.** Progress is shown as the VxRail cluster is built.
Step 14. When you see the **Hooray!** page, VxRail initialization is complete and a new VxRail cluster is built. Click the **Manage VxRail** button to continue to VxRail management. You should also bookmark this IP address in your browser for future use.

Step 15. Connect to VxRail Manager using either the VxRail Manager IP address (**Row 26**) or the fully-qualified domain name (FQDN) (**Row 25**) that you configured on your DNS server.

Step 16. If the Dell EMC SmartFabric services was enabled to pass control of switch configuration to VxRail, the Dell EMC OMNI plug-in is deployed on the vCenter instance.
8 After VxRail initialization network considerations

8.1 Support for NSX
VxRail is fully compatible with other software in the VMware ecosystem, including VMware NSX. A primer on deploying NSX on VxRail can be found in NSX Support on VxRail. Refer to the VMware Product Interoperability Matrices for specific versions of NSX supported on vSphere.

8.2 Using unassigned VxRail physical ports
For VxRail nodes ordered with extra physical network ports, VxRail Manager will not manage the optional PCI-e NICs. You can configure the additional ports in vCenter for non-VxRail system traffic, such as VM networks, iSCSI, NFS, etc.

The supported operations include:

- Create a new vSphere Standard Switch (VSS), and connect unused ports to the VSS.
- Connect unused ports to new port groups on the default vSphere Distributed Switch.
- Create a new vSphere Distributed Switch (VDS), add VxRail nodes to the new VDS, and connect their unused network ports to the VDS.
- Create new VMKernel adapters and enable services of IP Storage and vSphere Replication.
- Create new VM Networks and assign them to new port groups.

Note: You must follow the official instructions/procedures from VMware and Dell EMC for these operations.

The following operations are not supported:

- Migrating or moving VxRail system traffic to the optional ports. VxRail system traffic includes the management, vSAN, vCenter Server and vMotion Networks.
- Migrating VxRail system traffic to other port groups.
- Migrating VxRail system traffic to another VDS.

Note: Performing any of these unsupported operations will impact the stability and operations of the VxRail cluster, and likely cause a failure in the VxRail cluster.
## A VxRail Network Configuration Table

The Dell EMC service representative will use a data collection workbook to capture the settings needed to build the VxRail cluster. The workbook will include the following information:

<table>
<thead>
<tr>
<th>Row</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VxRail</td>
<td>External Management VLAN ID</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Internal Management VLAN ID</td>
</tr>
<tr>
<td>3</td>
<td>System</td>
<td>Global settings</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>NTP server(s)</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>DNS server(s)</td>
</tr>
<tr>
<td>6</td>
<td>Management</td>
<td>ESXi hostnames and IP addresses</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Separator</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Iterator</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Offset</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Suffix</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Domain</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>ESXi starting address for IP pool</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>ESXi ending address for IP pool</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>vCenter Server hostname</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>vCenter Server IP address</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>Platform Services Controller hostname</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Platform Services Controller IP address</td>
</tr>
<tr>
<td>18</td>
<td>Customer-supplied vCenter Server Leave blank if VxRail VC</td>
<td>Customer-supplied Platform Services Controller (PSC) Hostname (FQDN) Leave blank if PSC is embedded in customer-supplied vCenter Server</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>Customer-supplied vCenter Server hostname (FQDN)</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>Customer-supplied vCenter Server SSO domain</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>Admin username/password or the newly created VxRail non-admin username and password</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>New VxRail management username and password</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>Customer-supplied datacenter name</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>New cluster name</td>
</tr>
<tr>
<td>25</td>
<td>VxRail Manager</td>
<td>VxRail hostname</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>VxRail IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networking</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>------------</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td>Default Gateway</td>
</tr>
<tr>
<td>31</td>
<td>vMotion</td>
<td>Starting address for IP pool</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>Ending address for IP pool</td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>VLAN ID</td>
</tr>
<tr>
<td>35</td>
<td></td>
<td>Default/vMotion Gateway</td>
</tr>
<tr>
<td>36</td>
<td>vSAN</td>
<td>Starting address for IP pool</td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>Ending address for IP pool</td>
</tr>
<tr>
<td>38</td>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td>39</td>
<td></td>
<td>VLAN ID</td>
</tr>
<tr>
<td>40</td>
<td>VM Networks</td>
<td>... (unlimited number)</td>
</tr>
<tr>
<td>41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Solutions</td>
<td>Logging</td>
</tr>
<tr>
<td>43</td>
<td></td>
<td>vRealize Log Insight IP address</td>
</tr>
<tr>
<td>44</td>
<td></td>
<td>Syslog Server (instead of Log Insight)</td>
</tr>
</tbody>
</table>

**Optional Feature-Driven Settings**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>SmartFabric</td>
<td>VxRail Cluster Build Network VLAN ID</td>
</tr>
<tr>
<td>45</td>
<td>Dell EMC OMNI plug-in</td>
<td>IP address</td>
</tr>
<tr>
<td>46</td>
<td></td>
<td>Subnet Mask</td>
</tr>
<tr>
<td>47</td>
<td></td>
<td>Gateway</td>
</tr>
<tr>
<td>48</td>
<td>Witness Site</td>
<td>Management IP Address</td>
</tr>
<tr>
<td>49</td>
<td></td>
<td>Witness management network IP address</td>
</tr>
<tr>
<td>50</td>
<td>Witness Traffic Separation</td>
<td>Witness Traffic Separation VLAN ID</td>
</tr>
<tr>
<td>51</td>
<td>2-Node Cluster</td>
<td>Node 1 WTS IP address</td>
</tr>
<tr>
<td>52</td>
<td></td>
<td>Must be routable to Witness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Node 2 WTS IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be routable to Witness</td>
</tr>
</tbody>
</table>
## VxRail Passwords

<table>
<thead>
<tr>
<th>Item</th>
<th>Account</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxRail Manager</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>VxRail vCenter Server</td>
<td>administrator@&lt;SSO Domain&gt;</td>
<td>root</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management</td>
</tr>
<tr>
<td>VxRail Platform Service Controller</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>vRealize Log Insight</td>
<td>root</td>
<td>admin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Account</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Host #1</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>ESXi Host #2</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>ESXi Host #3</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>ESXi Host #4</td>
<td>root</td>
<td></td>
</tr>
</tbody>
</table>
# VxRail Setup Checklist

## Physical Network

- **VxRail cluster**: Decide if you want to plan for additional nodes beyond the initial three (or four)-node cluster. You can have up to 64 nodes in a VxRail cluster.
- **VxRail ports**: Decide how many ports to configure per VxRail node, what port type, and what network speed.
- **Network switch**: Ensure your switch supports VxRail requirements and provides the connectivity option you chose for your VxRail nodes. Verify cable requirements.
- **Datacenter**: Verify that the required external applications for VxRail are accessible over the network and correctly configured. If you are deploying VxRail over more than one rack, be sure network connectivity is set up between the racks.
- **Topology**: Decide if you will have a single or multiple switch setup for redundancy.
- **Workstation/laptop**: Any operating system with a browser to access the VxRail user interface. The latest versions of Firefox, Chrome, and Internet Explorer 10+ are all supported.
- **Out-of-band Management** (optional): One available port that supports 1Gb for each VxRail node.

## Logical Network

- **Reserve VLANs**
  - ✓ One external management VLAN with IPv6 multicast for traffic from VxRail, vCenter Server, ESXi (recommendation is untagged/native).
  - ✓ One internal management VLAN for auto-discovery and device management. The default is 3939.
  - ✓ One VLAN with IPv4 unicast (starting with VxRail v4.5.0) or IPv4 multicast (prior to v4.5.0) for vSAN traffic
  - ✓ One VLAN for vSphere vMotion
  - ✓ One or more VLANs for your VM Guest Network(s)
  - ✓ If you are planning to enable Dell EMC SmartFabric services, one VLAN for the VxRail cluster build network.
  - ✓ If you are enabling witness traffic separation, one VLAN for the VxRail witness traffic separation network.

- **System**
  - ✓ Time zone
  - ✓ Hostname or IP address of the NTP server(s) on your network (recommended)
  - ✓ IP address of the DNS server(s) on your network (required)
  - ✓ Forward and reverse DNS records for VxRail management components

- **Management**
  - ✓ Decide on your VxRail host naming scheme. The naming scheme will be applied to all VxRail management components.
  - ✓ Reserve three or more contiguous IP addresses for ESXi hosts.
  - ✓ Determine whether you will use a vCenter Server that is customer-supplied or new to your VxRail cluster.
  - ✓ VxRail vCenter Server: Reserve two IP addresses for vCenter Server and PSC.
  - ✓ Customer-supplied vCenter Server: Determine hostname and IP address for vCenter and PSC, administration user, and name of vSphere datacenter. Create a VxRail management user in vCenter. Select a unique VxRail cluster name. (Optional) Create a VxRail non-admin user.
  - ✓ Reserve one IP address for VxRail Manager.
  - ✓ Determine default gateway and subnet mask.
  - ✓ Select passwords for VxRail management components.
| vMotion | ✓ Decide whether you want to use the default TCP-IP stack for vMotion, or a separate IP addressing scheme for the dedicated vMotion TCP-IP stack  
✓ Reserve three or more contiguous IP addresses and a subnet mask for vSphere vMotion.  
✓ Select the gateway for either the default TCP-IP stack, or the dedicated vMotion TCP-IP stack |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN</td>
<td>✓ Reserve three or more contiguous IP addresses and a subnet mask for vSAN</td>
</tr>
</tbody>
</table>
| Solutions | ✓ To use vRealize Log Insight: Reserve one IP address.  
✓ To use an existing syslog server: Get the hostname or IP address of your third-party syslog server. |
| Witness Site | ✓ If Witness is required, reserve one IP address for the management network and one IP address for the vSAN network. |
| Workstation | ✓ Configure your workstation/laptop to reach the VxRail initial IP address.  
✓ Make sure you know how to configure the laptop to reach the VxRail Manager IP address after configuration. |
| Set up Switch | ✓ Configure your selected external management VLAN (default is untagged/native).  
✓ Configure your internal management VLAN.  
✓ Confirm that IPv6 multicast is configured/enabled on either the external management VLAN (prior to version 4.7) or internal management VLAN (version 4.7 and later).  
✓ Configure your selected VLANs for vSAN, vSphere vMotion, and VM Networks.  
✓ If applicable, configure your Witness traffic separation VLAN.  
✓ In dual-switch environments, configure the management and vSAN VLANs to carry the multicast and unicast traffic respectively between switches.  
✓ Configure uplinks to carry upstream network VLANs.  
✓ Configure one port as an access port for laptop/workstation to connect to VxRail Manager for initial configuration.  
✓ Confirm configuration and network access. |
| Workstation/Laptop | ✓ Configure your workstation/laptop to reach the VxRail Manager initial IP address.  
✓ Configure the laptop to reach the VxRail Manager IP address after permanent IP address assignment. |
NSX Support on VxRail

VxRail supports VMware NSX software-defined networking (SDN) through vCenter Server. vCenter Server offers a fully integrated option for SDN and network-layer abstraction with NSX. The NSX network-virtualization platform delivers for networking what VMware delivers for compute and storage. In much the same way that server virtualization allows operators to programmatically create, snapshot, delete, and restore software-based virtual machines (VMs) on demand, NSX enables virtual networks to be created, saved, deleted, and restored on demand without requiring reconfiguration of the physical network. The result fundamentally transforms the datacenter network-operational model, reduces network-provisioning time from days or weeks to minutes, and dramatically simplifies network operations. NSX is a non-disruptive solution that is deployed on any IP network, including existing datacenter network designs or next-generation fabric architectures from any networking vendor.

With network virtualization, the functional equivalent of a “network hypervisor” reproduces the complete set of Layer 2 to Layer 7 networking services (e.g., switching, routing, access control, firewalls, QoS, and load balancing) in software. Just as VMs are independent of the underlying x86 hardware platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand.

NSX coordinates ESXi’s vSwitches and the network services pushed to them for connected VMs to effectively deliver a platform—or “network hypervisor”—for the creation of virtual networks. Similar to the way that a virtual machine is a software container that presents logical compute services to an application, a virtual network is a software container that presents logical network services—logical switches, logical routers, logical firewalls, logical load balancers, logical VPNs and more—to connected workloads. These network and security services are delivered in software and require only IP packet forwarding from the underlying physical network.

To connected workloads, a virtual network looks and operates like a traditional physical network. Workloads “see” the same Layer 2, Layer 3, and Layers 4-7 network services that they would in a traditional physical configuration. It’s just that these network services are now logical instances of distributed software modules running in the hypervisor on the local host and applied at the vSwitch virtual interface.

The following NSX components are illustrated in Figure 23:

- **NSX vSwitch** operates in ESXi server hypervisors to form a software abstraction layer between servers and the physical network.
- **NSX Controller** is an advanced, distributed state management system that controls virtual networks and overlays transport tunnels. It is the central control point for all logical switches within a network and maintains information of all virtual machines, hosts, logical switches, and VXLANs.
- **NSX Edge** provides network-edge security and gateway services to isolate a virtualized network. You can install NSX Edge either as a logical (distributed) router or as a services gateway.
- **NSX Manager** is the centralized network management component of NSX, installed as a virtual appliance on an ESXi host.
One NSX Manager maps to a single vCenter Server and multiple NSX Edge, vShield Endpoint, and NSX Data Security instances. Before you install NSX in your vCenter Server environment, consider your network configuration and resources using the following chart.

Figure 23  NSX component information flow: NSX Manager, NSX Controller, NSX Edge, NSX vSwitch

Legend:
1. Controller Configuration (Logical Switches and Logical Routers)
2. Logical Router
3. Load Balancer, Firewall, VPN Configuration
4. Routing Information
NSX Resource Requirements:

<table>
<thead>
<tr>
<th></th>
<th>Memory</th>
<th>Disk Space</th>
<th>vCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>12GB</td>
<td>60GB</td>
<td>4</td>
</tr>
<tr>
<td>NSX Edge:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compact</td>
<td>512MB</td>
<td>512MB</td>
<td>1</td>
</tr>
<tr>
<td>Large</td>
<td>1GB</td>
<td>512MB</td>
<td>2</td>
</tr>
<tr>
<td>Extra Large</td>
<td>8GB</td>
<td>4.5GB (with 4GB swap)</td>
<td>6</td>
</tr>
<tr>
<td>Quad Large</td>
<td>1GB</td>
<td>512MB</td>
<td>4</td>
</tr>
<tr>
<td>vShield Endpoint</td>
<td>1GB</td>
<td>4GB</td>
<td>2</td>
</tr>
<tr>
<td>NSX Data Security</td>
<td>512MB</td>
<td>6GB per ESXi host</td>
<td>1</td>
</tr>
</tbody>
</table>

In a VxRail cluster, the key benefits of NSX are consistent, simplified network management and operations, plus the ability to leverage connected workload mobility and placement. With NSX, connected workloads can freely move across subnets and availability zones. Their placement is not dependent on the physical topology and availability of physical network services in a given location. Everything a VM needs from a networking perspective is provided by NSX, wherever it resides physically. It is not necessary to over-provision server capacity within each application/network pod. Instead, organizations can take advantage of available resources wherever they’re located, thereby allowing greater optimization and consolidation of resources. VxRail easily inserts into existing NSX environments and provide NSX awareness so network administrators can leverage simplified network administration. See the VMware NSX Design Guide for NSX best practices and design considerations.

For additional information related to NSX, refer to the following materials:

VxRail Open Ports Requirements

Use the tables in this Appendix for guidance on firewall settings specific for the VxRail cluster.

The VxRail cluster needs to be able to connect to specific applications in your datacenter. DNS is required, and NTP is optional. Open the necessary ports to enable connectivity to the external syslog server, and for LDAP and SMTP.

<table>
<thead>
<tr>
<th>Description</th>
<th>Source Device(s)</th>
<th>Destination Device(s)</th>
<th>Protocol</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>VxRail Manager, Dell iDRAC</td>
<td>DNS Server(s)</td>
<td>UDP</td>
<td>53</td>
</tr>
<tr>
<td>NTP Client</td>
<td>Host ESXi Management Interface, Dell iDRAC, VMware vCenter Servers, VxRail Manager</td>
<td>NTP Server(s)</td>
<td>UDP</td>
<td>123</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>Host ESXi Management Interface, vRealize Log Insight</td>
<td>Syslog Server</td>
<td>TCP</td>
<td>514</td>
</tr>
<tr>
<td>LDAP</td>
<td>VMware vCenter Servers, PSC</td>
<td>LDAP Server</td>
<td>TCP</td>
<td>389, 636</td>
</tr>
<tr>
<td>SMTP</td>
<td>ESRS Gateway VMs, vRealize Log Insight</td>
<td>SMTP Server (s)</td>
<td>TCP</td>
<td>25</td>
</tr>
</tbody>
</table>

Open the necessary firewall ports to enable IT administrators to manage the VxRail cluster.

<table>
<thead>
<tr>
<th>Description</th>
<th>Source Device(s)</th>
<th>Destination Device(s)</th>
<th>Protocol</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Management</td>
<td>Administrators</td>
<td>Host ESXi Management Interface</td>
<td>TCP, UDP</td>
<td>902</td>
</tr>
<tr>
<td>VxRail Management GUI/Web Interfaces</td>
<td>Administrators</td>
<td>VMware vCenter Server, VxRail Manager, Host ESXi Management, Dell iDRAC port, vRealize Log Insight, PSC</td>
<td>TCP</td>
<td>80, 443</td>
</tr>
<tr>
<td>Dell server management</td>
<td>Administrators</td>
<td>Dell iDRAC</td>
<td>TCP</td>
<td>623, 5900, 5901</td>
</tr>
<tr>
<td>SSH &amp; SCP</td>
<td>Administrators</td>
<td>Host ESXi Management, vCenter Server Appliance, Dell iDRAC port, VxRail Manager Console</td>
<td>TCP</td>
<td>22</td>
</tr>
</tbody>
</table>

If you plan to use a customer-supplied vCenter server instead of deploying a vCenter server in the VxRail cluster, open the necessary ports so that the vCenter instance can manage the ESXi hosts.
### vCenter and vSphere

<table>
<thead>
<tr>
<th>Description</th>
<th>Source Device(s)</th>
<th>Destination Device(s)</th>
<th>Protocol</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Clients to vCenter Server</td>
<td>vSphere Clients</td>
<td>vCenter Server</td>
<td>TCP</td>
<td>5480, 8443, 9443, 10080, 10443</td>
</tr>
<tr>
<td>Managed Hosts to vCenter</td>
<td>Host ESXi Management</td>
<td>vCenter Server</td>
<td>TCP</td>
<td>443, 902, 5988, 5989, 6500, 8000, 8001</td>
</tr>
<tr>
<td>Managed Hosts to vCenter Heartbeat</td>
<td>Host ESXi Management</td>
<td>vCenter Server</td>
<td>UDP</td>
<td>902</td>
</tr>
</tbody>
</table>

If you plan to enable Dell EMC ‘call-home’ with an external SRS gateway already deployed in your datacenter, open the necessary ports to enable communications between the SRS gateway and VxRail Manager.

### VxRail Manager and External SRS Gateway

<table>
<thead>
<tr>
<th>Description</th>
<th>Source Device(s)</th>
<th>Destination Device(s)</th>
<th>Protocol</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRS Connect Home</td>
<td>VxRail Manager</td>
<td>SRS Gateway</td>
<td>TCP</td>
<td>21,5400-5413</td>
</tr>
<tr>
<td>SRS Remote Support</td>
<td>SRS Gateway</td>
<td>VxRail Manager</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td>SRS Process Connect Home Files</td>
<td>VxRail Manager</td>
<td>SRS Gateway</td>
<td>TCP</td>
<td>25</td>
</tr>
<tr>
<td>SRS Device Notification</td>
<td>VxRail Manager</td>
<td>SRS Gateway</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>SRS Management</td>
<td>VxRail Manager</td>
<td>SRS Gateway</td>
<td>TCP</td>
<td>9443</td>
</tr>
</tbody>
</table>

Additional firewall port settings may be necessary depending on your datacenter environment. The list of documents in this table is provided for reference purposes.

<table>
<thead>
<tr>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Incoming and Outgoing Firewall Ports for ESXi 6.5 Hosts</td>
<td>List of Incoming and Outgoing Firewall Ports for ESXi 6.5 Hosts</td>
</tr>
<tr>
<td>List of Incoming and Outgoing Firewall Ports for ESXi 6.0 Hosts</td>
<td>List of Incoming and Outgoing Firewall Ports for ESXi 6.0 Hosts</td>
</tr>
<tr>
<td>Required port to access VMware vCenter Server and VMware ESXi hosts</td>
<td>TCP and UDP Ports required to access VMware vCenter Server and VMware ESXi hosts</td>
</tr>
<tr>
<td>Secure Remote Services Port Requirements</td>
<td>Dell EMC Secure Remote Services Documentation</td>
</tr>
</tbody>
</table>
Physical Network Switch Examples

These diagrams show different physical network switch wiring examples. They are provided as illustrative examples.

Figure 24  VxRail nodes with two ports connected to 2x TOR switches, 1x Optional Management Switch with iDRAC
Figure 25  VxRail nodes with 4 ports connected to 2x TOR switches, 1 x Optional Management Switch with iDRAC
Figure 26  VxRail nodes with 4 ports connected to 4x TOR switches, 1x optional Management Switch with iDRAC.

TOR 3 and 4’s Upstream switches are optional because those TORs only carry vSAN and vMotion which might not need access to the rest of the network.
VxRail 2-Node Cluster with ports 1 and 2 connected to 2x TOR switches for external network traffic, and a direct connection between ports 3 and 4 on each node for internal network traffic. 1/10/25GbE TOR switches are supported. Witness runs on host separate from 2-Node cluster and routable from 2xTOR switches.