ABSTRACT

This is a planning and consideration guide for VxRail Appliances. It can be used to understand better the networking required for VxRail implementation. This whitepaper does not replace the requirement for implementation services with VxRail Appliances and should not be used in an attempt to implement the required networking for VxRail Appliances.

October 2018
## Table of contents

- Intended Use and Audience ........................................................................................................ 4
- Introduction to VxRail ............................................................................................................... 4
- Planning Your Data Center Network for VxRail ........................................................................ 5
  - VxRail Hardware and the Physical Network Infrastructure ...................................................... 5
  - VxRail Clusters, Appliances and Nodes .................................................................................. 5
  - Network Switch ......................................................................................................................... 8
  - Topology and Connections ....................................................................................................... 10
  - Out-of-Band Management (optional) ...................................................................................... 11
- VxRail Feature-Driven Decision Points ....................................................................................... 12
  - VMware Validated Design on VxRail .................................................................................... 12
  - vSAN Stretched Cluster .......................................................................................................... 12
- VxRail Hardware and Switch Selection Decision Points ............................................................. 13
- Planning the VxRail Implementation ........................................................................................... 13
  - Step 1: Decide on VxRail Single Point of Management ............................................................ 14
  - Step 2: Plan the VxRail Logical Network ............................................................................... 14
  - Step 4: Identify unique hostnames for VxRail management components ............................. 19
  - Step 5: Identify external applications and settings for VxRail .............................................. 20
  - Step 6: Create DNS records for VxRail management components ....................................... 21
  - Step 7: Prepare Customer-Supplied vCenter Server .............................................................. 22
  - Step 8. Reserve IP addresses for VxRail vMotion and vSAN networks .................................. 23
  - Step 9. Decide on VxRail Logging Solution ............................................................................ 24
  - Step 10: Decide on Passwords for VxRail Management .......................................................... 24
- Setting up the network switch for VxRail .................................................................................... 25
  - Enable Multicast for VxRail Management Network ............................................................... 25
  - Enable Unicast or Multicast for VxRail vSAN Network ......................................................... 26
  - Enable Uplinks to pass inbound and outbound VxRail network traffic ................................ 26
  - Enable Inter-switch Communication ...................................................................................... 26
  - Enable Inter-switch Links ........................................................................................................ 26
  - Step 2. Plan Switch Port Configuration .................................................................................... 26
    - Determine switch port mode ................................................................................................. 26
    - Do not enable Link Aggregation on VxRail Switch Ports .................................................... 27
    - Limit Spanning Tree Protocol on VxRail Switch Ports .......................................................... 28
  - Step 3. Configure Ports and VLANs on Your Switch(es) .......................................................... 28
- Confirm Your Data Center Network ............................................................................................. 30
- Configuring a Workstation/Laptop for VxRail Initialization ....................................................... 31
- Perform Initialization to create VxRail cluster .......................................................................... 32
After VxRail Initialization Network Considerations ................................................................. 33
Support for NSX .......................................................................................................................... 33
Using Unassigned VxRail Physical Ports ................................................................................ 33
VxRail Network Configuration Table ....................................................................................... 34
VxRail Password Tables ............................................................................................................. 35
VxRail Setup Checklist .............................................................................................................. 36
Appendix A: NSX Support on VxRail ....................................................................................... 37
Appendix B: VxRail Open Ports Requirement ......................................................................... 40
Appendix C: Physical Network Switch Examples ..................................................................... 42
Intended Use and Audience

This guide discusses the essential network details for VxRail deployment planning purposes only. It also introduces best practices, recommendations, and requirements for both physical and virtual network environments. The guide 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. Please work with your Dell EMC service representative to perform the actual installation.

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 data center 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 based on a single node. A 10Gb Ethernet switch (or a 1Gb Ethernet switch for certain models of VxRail) is required. 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 included for all components except VMware vSphere. The vSphere licenses can be purchased through Dell EMC, VMware or your preferred VMware reseller partner.

The VxRail Appliances also includes 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 Data Center Network for VxRail

The network considerations for VxRail are no different from those of any enterprise IT infrastructure: availability, performance, and extensibility. VxRail Appliances are delivered to your data center ready for deployment. The nodes in the appliance can attach to any compatible 10GbE network infrastructure with either RJ45 or SFP+ ports. Some models with single processors can attach to compatible 1GbE 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 will guide 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 data center before product delivery

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

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

*NOTE:* Follow all of 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 data center, 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 data center 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 to 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 enable 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 a VxRail cluster:

- VxRail clusters, appliances and nodes
- Network switch
- 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 customer shipment. A set of prepared VxRail nodes are prepared and delivered to the customer site based on a purchase order. The set of VxRail nodes are delivered ready for data center installation and connectivity into the data center network infrastructure. Once the data center installation and network connectivity is 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 VxRail cluster starts with a minimum of 3 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:
### VxRail Series

<table>
<thead>
<tr>
<th>VxRail Series</th>
<th>Target Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Series</td>
<td>Entry Level</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 and Space Optimized (2U4N chassis)</td>
</tr>
</tbody>
</table>

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

**Figure 1. VxRail P and V Series on Dell 14th Generation PowerEdge Servers**

- **1G RJ45 iDRAC**
- **4 x 10G SFP+**

- **1G RJ45 iDRAC**
- **4 x 10G SFP+**

- **1G RJ45 iDRAC**
- **4 x 10G RJ45**
Figure 2. VxRail E Series on Dell 14th Generation PowerEdge Servers

1G RJ45 iDRAC  4 x 10G RJ45

Figure 3. VxRail S-Series on Dell 14th Generation PowerEdge Servers

2 x 10G SFP+  1G RJ45 iDRAC  2 x 10G SFP+  1G RJ45 iDRAC

Figure 4. VxRail G-Series node on Dell 14th Generation PowerEdge Servers

1G RJ45 iDRAC  2 x 10G RJ45  2 x 1G RJ45

Figure 5. VxRail E, P, S and V Series on Dell 13th generation PowerEdge Servers

NOTE: 2x10GbE ports will auto-negotiate to 1GbE when used with 1GbE networking
In addition to network connectivity, review the physical power, space and cooling requirements for your planned infrastructure to ensure data center compatibility.

Network Switch

VxRail is broadly compatible with most customer networks and Ethernet switches. One example is the Dell EMC Switch S4048 (more details on planning configuration specific to that switch can be found in DELL EMC Switch Configuration Guide for VxRail.)

Switch requirements

- The switch(es) must support both IPv4 and IPv6 network protocols
- The switch(es) connected directly to VxRail Appliances must support multicast on 10GbE ports for all models of VxRail except for the models that utilize 1GbE for their primary networking as specified:
  - VxRail Releases prior to Release 4.5.0: both IPv4 and IPv6 multicast pass-through must be supported. Layer 3 multicast is not required.
  - VxRail Releases starting with Release 4.5.0: IPv6 multicast pass-through and IPv4 unicast must be supported.¹

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

VxRail Node Connectivity Options

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

¹ vSAN no longer requires multicast, but is using unicast instead.
Figure 6.  VxRail 14th Generation Node Connectivity Summary

- 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 (Starting with VxRail 4.5.200)
- E, P, and S Series (14th Generation Dell EMC PowerEdge Servers)
  - 1GbE connectivity is supported on single processor models only
- G Series (14th Generation Dell EMC PowerEdge Servers) Appliance Connectivity Options
  - 2x10GbE SFP+ ports

```plaintext
VxRail Node Connectivity Comparison

<table>
<thead>
<tr>
<th>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></td>
<td></td>
<td>2 x 10Gb RJ45 or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 x 10Gb SFP+ or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*4 x 1Gb RJ45</td>
<td></td>
<td>No 1Gb option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Port</td>
<td>1 x 100Mb</td>
<td>1 x 1Gb RJ45 iDRAC 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RJ45 BMC</td>
<td></td>
<td>6 x 10Gb RJ45 or</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional Connectivity</td>
<td>N/A</td>
<td>6 x 10Gb SFP+</td>
<td></td>
<td>12 x 10GbE SFP+</td>
</tr>
</tbody>
</table>

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

Figure 7.  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)
  - 1GbE connectivity is supported on single processor models only
  - The 2x10GbE ports will auto-negotiate to 1GbE when used with 1GbE networking.
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 purpose.
- VxRail initialization process will not touch any optional connectivity (PCIe NICs). Customers can use the ports for their own purposes such as VM networks, iSCSI, or NFS, etc.
- VxRail nodes supporting 10GbE can be configured with either 2 ports supporting VxRail cluster network traffic, or all 4 ports can be configured for the VxRail cluster network traffic.
- 4 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 same NDC across all VxRail nodes.
  - VxRail nodes with RJ45 ports and SFP+ ports cannot be mixed in the same VxRail appliance
  - The port speed for each VxRail node (25GbE, 10GbE, 1GbE) must be the same in the VxRail appliance
  - These restrictions are not applicable to optional connectivity (PCI-e NICs)
- One (1) additional port on the switch or one logical path on the VxRail management VLAN is required for a workstation/laptop to access the VxRail user interface for the cluster.

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/development or remote/branch office (ROBO) environments. To support high availability and failover in production environments, two or more switches are required. The VxRail appliance is an entire software-defined data center 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 figure shows the recommended physical network setup using a management switch (for iDRAC) and two ToR switches. Other network setups can be found in Appendix \( C \).

![Network Diagram](image)

**Figure 8.** Rear view of one deployment of a 4-node VxRail appliance connected to two 10GbE switches and a separate switch for out-of-band management. These are 14G E series servers.

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

**Out-of-Band Management (optional)**

If the VxRail Appliances are located at a data center 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. The default credentials are:

- **Username:** root  
- **Password:** calvin

You will need to reserve an IP address for each iDRAC in your VxRail cluster (one per node).
VxRail Feature-Driven Decision Points

Certain applications, software stacks and product features supported on VxRail can have an 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 each of these may have on your plans for VxRail.

VMware Validated Design on VxRail

VMware Validated Design (VVD) on VxRail enables VMware’s vRealize and NSX capabilities to be deployed on VxRail. The integrated solution involves a complete end-to-end validation of the hardware and software stack for interoperability and scalability. VMware Validated Design on VxRail includes the following software stack:

- vRealize Automation
- vRealize Operations
- vRealize Log Insight
- vRealize Business
- vRealize Network Insight
- NSX
- vSphere Enterprise Plus
- vSAN

If your plans include the deployment of VVD on VxRail, make note of the following requirements:

- A minimum of 8 VxRail nodes are required.
  - A minimum of 4 VxRail nodes are for the Management pod,
  - A minimum of 4 nodes are required for the Edge and Compute pod
- The nodes in the Management pod require a minimum of 192GB of RAM
- The nodes in the Management pod require a minimum of 2 sockets with a total of at least 8 CPU cores
- The VxRail nodes in both the Management pod and Edge and Compute pod must be configured with 2x10Gb Ethernet ports

More detailed information on VMware Validated Design on VxRail is located here: [https://community.emc.com/docs/DOC-66332](https://community.emc.com/docs/DOC-66332)

vSAN Stretched Cluster

vSAN stretched cluster is a VMware solution to support 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 your plans include the deployment of vSAN stretched cluster on VxRail, make note of the following requirements:
• Three data center sites required: two data center sites (Primary and Secondary) host the VxRail infrastructure, and the third site is required to support a witness to monitor the stretched cluster
• A minimum of 3 VxRail nodes is required in the Primary site, and a minimum of 3 VxRail nodes is required in the Secondary site
• A minimum of 1 top-of-rack switch for the VxRail nodes is required in the Primary and Secondary sites
• An ESXi instance is required 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. More detailed information on vSAN stretched cluster and the networking requirements is located here: https://www.dell.com/resources/en-us/asset/white-papers/products/converged-infrastructure/h15275-vxrail-planning-guide-virtual-san-stretched-cluster.pdf

VxRail Hardware and Switch Selection Decision Points

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

Step 2. Determine the optimal VxRail port speed to meet planned workload requirements, and to calculate the number of physical switch ports for connectivity
  o VxRail supports 1GbE, 10GbE and 25GbE connectivity options
  o VxRail supports either 2 or 4 connections per node to the physical switch

Step 3. Decide whether you want to attach the VxRail nodes to the switches with RJ45 connections or SFP+ connections
  o VxRail nodes with RJ-45 ports require CAT5 or CAT6 cables. CAT6 cables are included with every VxRail
  o 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 4. 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

Step 5. Reserve one additional port on the switch for a workstation/laptop to access the VxRail management interface for the cluster
  o 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 6. Select a switch or switches that provide sufficient port capacity and characteristics, and support the features and functionality required for VxRail

Step 7. 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.
  o If you are deploying dual top-of-rack switches, it is best practice to reserve ports on each switch for inter-switch links

Step 8. Decide whether to deploy a separate switch to support connectivity to the VxRail management port on each node

Planning the VxRail Implementation

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

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

1. Decide on VxRail Single Point of Management
2. Plan the VxRail logical network
3. Identify IP address range for VxRail logical networks
4. Identify unique hostnames for VxRail management components
5. Identify external applications and settings for VxRail
6. Create DNS records for VxRail management components
7. Prepare Customer-Supplied vCenter Server
8. Reserve IP addresses for VxRail vMotion and vSAN networks
9. Decide on VxRail Logging Solution
10. 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.

Once you set up VxRail Appliances, and complete the initial initialization phase to produce the final product, the configuration cannot be changed easily. 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.

**Step 1: 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. Refer to the Dell EMC VxRail vCenter Server Planning Guide for details.

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 be changed easily.

**Step 2: 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. Other types of VxRail-generated network traffic, such as the network traffic supporting I/O to the vSAN datastore, or the network used to dynamically migrate virtual machines between VxRail nodes to balance workload, needs to stay within the VxRail cluster.

Virtual LANs (VLANs) are the method used to define the VxRail logical networks within the cluster, and the method used to control the paths a logical network is allowed to 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 also 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).

As a first step, the network team and virtualization team should to meet in advance to plan VxRail’s network architecture.

- The virtualization team needs to 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 that are needed to support traffic from non-management virtual machines.
- The network team needs to 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 needs to plan to configure the VLANs on the network switch(es) attached to the VxRail nodes.
- The virtualization team needs to assign the VLAN IDs to the individual VxRail logical networks.

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

**Management traffic** includes all VxRail Manager, vCenter Server, and ESXi communication. The management VLAN also carries traffic for vRealize Log Insight. All management traffic should be untagged and must be able to go over a Native VLAN on your switch, or you will not be able to build VxRail and configure the ESXi hosts.

Special cases can allow you to tag management traffic in one of two ways:

1. Configure each VxRail port on your switch 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.

In VxRail Appliances, **vSphere vMotion** and **vSAN** traffic cannot be routed, and is isolated with the VxRail cluster. 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 will create 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></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>✓ Row 1</strong></td>
<td>Enter the 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 &quot;0&quot; or &quot;Native VLAN.&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>✓ Row 34</strong></td>
<td>Enter a VLAN ID for vSphere vMotion. (Enter a 0 in the VLAN ID field for untagged traffic)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>✓ Row 38</strong></td>
<td>Enter a VLAN ID for vSAN. (Enter a 0 in the VLAN ID field for untagged traffic)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>✓ Rows 39-40</strong></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 a 0 in the VLAN ID field for untagged traffic)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** If you 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.

During the VxRail automated implementation process, IP addresses entered are assigned to the components within the VxRail cluster that are part of the Management virtual network. The IP addresses assigned to the components within the Management virtual network must follow certain rules:

- The IP address scheme be a public IP address range
- The IP address must be free, and 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 data center impacts the number of IP addresses you will need to reserve.
• Decide if you want to reserve additional IP addresses in the VxRail management system to assign to VxRail nodes in the future for expansion purposes. When a new node is added to an existing VxRail cluster, it will assign an IP address from the unused reserve pool, or prompt you to enter an IP address manually.

• Decide whether you will use the vCenter instance that is deployed in the VxRail cluster, or if you will use an external vCenter already operational in your data center. If you choose to use the vCenter instance deployed on the VxRail cluster, you will need to reserve an IP address for vCenter and an IP address for the Platform Service Controller.

• Decide if you will use vSphere Log Insight that can be deployed in the VxRail cluster.
  o If you choose to use the vCenter instance deployed in the VxRail cluster, then you have the option to deploy vSphere Log Insight, use an existing syslog server in your data center, or no logging at all. Reserve one IP address if you choose to deploy vSphere Log Insight in the VxRail cluster.
  o If you choose to use an external vCenter already operational in your data center for VxRail, then vSphere Log Insight will not be deployed.

• VxRail supports the Dell-EMC ‘call home’ feature, where alerts from the appliance are routed to customer service. The Secure Remote Gateway is required to enable alerts from VxRail to be sent to Dell-EMC customer service.
  o Decide whether to use an existing Secure Remote Services gateway in your data center for ‘call-home’, deploy a virtual instance of the Secure Remote Services gateway in the VxRail cluster for this purpose, or none at all.
  o Reserve 1 IP address if you choose to deploy SRS-VE (Secure Remote Services Virtual Edition) in the VxRail cluster.
Use the table below 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 using 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><strong>TOTAL</strong></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 Management logical network.

Record the IP address range for the ESXi hosts. These IP addresses are required.

Network Configuration Table
✓ Rows 12 and 13
Enter the starting and ending IP addresses for the ESXi hosts - a continuous IP range is required, with a minimum of 4 IPs.

Network Configuration Table
✓ Row 27
Enter the subnet mask for the VxRail Management network

Network Configuration Table
✓ Rows 28
Enter the gateway for the VxRail Management network

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

Network Configuration Table
✓ Row 25
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

Network Configuration Table
✓ Row 15
Enter the IP address for VxRail vCenter

Network Configuration Table
✓ Row 17
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.

<table>
<thead>
<tr>
<th>Network Configuration Table</th>
<th>Enter the IP address for vSphere Log Insight</th>
</tr>
</thead>
</table>

**Step 4: Identify unique hostnames for VxRail management components**

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

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

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

**Domain**

Begin the process by selecting the domain you want to use for VxRail, and want to 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.

**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 offset2 (empty or numeric), a suffix3 (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).

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Example 1</th>
<th>Example 2</th>
<th>Example 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separator</td>
<td>None</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Iterator</td>
<td>Num 0X</td>
<td>Num X</td>
<td>Alpha</td>
</tr>
<tr>
<td>Offset</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suffix</td>
<td>lab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>local</td>
<td>college.edu</td>
<td>company.com</td>
</tr>
</tbody>
</table>

| Resulting hostname | host01.local | myname-4lab.college.edu | esxi-host-a.company.com |

Network Configuration Table

✓ Rows 6-11

Enter an example of your desired ESXi host-naming scheme. Be sure to show your desired prefix, separator, iterator, offset, suffix and domain.

-Saharan Ali H. - Murtaza

2 Offset is available starting in VxRail Release 4.0.200. It is only applicable when the iterator is numeric.

3 Suffix is available starting in VxRail Release 4.0.200.
**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 the hostname for VxRail Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Row 25</td>
<td></td>
</tr>
</tbody>
</table>

**VxRail vCenter Server Hostname**

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

If you want 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, and 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>

**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 data center for VxRail, or will not enable logging.

If you decide to deploy Log Insight to the VxRail cluster, then the management component must be assigned a hostname. You can choose 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 also choose to use the VxRail vCenter Server.

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 the hostname for Log Insight.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Row 41</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5: Identify external applications and settings for VxRail**

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

**Time Zone, 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 it 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).
Make sure the NTP IP address is accessible from the network to which VxRail 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>

**DNS Server**

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 of the VxRail management components (VxRail Manager, vCenter, etc.).

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>

**Step 6: Create DNS records for VxRail management components**

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.

- 26P-APP01-ESX-01 Host (A) 10.244.12.141
- 26P-APP01-ESX-02 Host (A) 10.244.12.142
- 26P-APP01-ESX-03 Host (A) 10.244.12.143
- 26P-APP01-ESX-04 Host (A) 10.244.12.144
- 26P-APP01-LOG-01 Host (A) 10.244.12.148
- 26P-APP01-PSC-01 Host (A) 10.244.12.147
- 26P-APP01-VCC-01 Host (A) 10.244.12.145
- 26P-APP01-VXM-01 Host (A) 10.244.12.146
Step 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 data center for VxRail.

Certain pre-requisites must be completed and settings provided before VxRail initialization if you decide to use a Customer-Supplied vCenter as the VxRail cluster management platform. During the VxRail initialization process, it will connect to your Customer-Supplied vCenter in order 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 most current support matrix.

- Enter the FQDN of your selected, compatible Customer Supplied vCenter Server in the **VxRail Network Configuration 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**.

- Decide on the Single Sign-on (SSO) domain configured on your Customer-Supplied vCenter you want to use to enable connectivity for VxRail, and enter the domain in the **VxRail Network Configuration Table**.

---

**Figure 9. Sample DNS Forward Lookup Entries**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Type</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.244.12.141</td>
<td>Pointer</td>
<td>26p-app01-esx-01.row26.local.</td>
</tr>
<tr>
<td>10.244.12.142</td>
<td>Pointer</td>
<td>26p-app01-esx-02.row26.local.</td>
</tr>
<tr>
<td>10.244.12.143</td>
<td>Pointer</td>
<td>26p-app01-esx-03.row26.local.</td>
</tr>
<tr>
<td>10.244.12.146</td>
<td>Pointer</td>
<td>26p-app01-vxm-01.row26.local.</td>
</tr>
<tr>
<td>10.244.12.147</td>
<td>Pointer</td>
<td>26p-app01-psc-01.row26.local.</td>
</tr>
</tbody>
</table>

**Figure 10. Sample DNS Reverse Entries**

Use the **VxRail Network Configuration Table** to determine which VxRail management components you will be including 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.
Network Configuration Table

Row 20

Enter the Single Sign-on (SSO) domain for the Customer Supplied vCenter Server. (For example vsphere.local)

- The VxRail initialization process will require 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.

Network Configuration Table

Row 21

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.

- A set of credentials need to 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 have already an account for a previous VxRail cluster in the Customer-Supplied vCenter, enter those credentials

Network Configuration Table

Row 22

Enter the full VxRail management username/password. (For example, cluster1-manager@vsphere.local)

- The VxRail initialization process will deploy the VxRail cluster under an existing Data Center in the Customer-Supplied vCenter. Create a new Data Center, or select an existing Data Center on the Customer Supplied vCenter.

Network Configuration Table

Row 23

Enter the name of a datacenter on the Customer Supplied vCenter Server.

- Specify the name of the Cluster that will be created by the VxRail initialization process in the selected Data Center. This name must be unique, and not used anywhere in the Data Center on the Customer-Supplied vCenter.

Network Configuration Table

Row 24

Enter the name of the cluster that will be used for VxRail.

**Step 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. The vMotion and vSAN networks are not routable by default, so a private address range is acceptable. 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, but a larger IP address range can be specified to cover for planned expansion.
Step 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 also choose to use the VxRail vCenter Server. If you choose instead to use a Customer-Supplied vCenter Server, then the choices are to 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>
<tbody>
<tr>
<td>✓ Rows 42 or ✓ Row 43</td>
<td></td>
</tr>
</tbody>
</table>

Step 10: Decide on 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 tables in VxRail Password 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 choose to 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 choose to 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 choose to deploy the VxRail vCenter Server, then VxRail Manager and vCenter share the same default administrator login, ‘administrator@vsphere.local’. Enter the password you want to use [Row 2]
  - If you choose to use a Customer-Supplied vCenter Server, then VxRail Manager will use the same ‘administrator@<SSO Domain>’ login credentials you use for access to the Customer-Supplied vCenter Server
- If you choose to deploy the VxRail vCenter Server:
  - Enter the ‘root’ password for the VxRail vCenter Server [Row 3]
Setting up the network switch for VxRail

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

Set up your switch by following these steps:

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.

**Step 1. Plan Switch Configuration**

Enable Multicast for VxRail Management Network

VxRail Appliances have no backplane, so communication between its nodes is facilitated via 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 to be configured in the switch. IPv6 multicast is required for the VxRail management network.

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

VxRail creates very little traffic via IPv6 multicast for auto-discovery and management. It is recommended to limit traffic further on your switch by enabling MLD Snooping and MLD Querier.

IPv6 multicast is required for the VxRail management network. The network switch(es) that connect to VxRail must allow for pass-through of multicast traffic on the VxRail Management VLAN. Multicast is not required on your entire network, just on the ports connected to VxRail.

If MLD Snooping is enabled, then MLD Querier must be enabled. If MLD Snooping is disabled, then MLD Querier must be disabled.
Enable Unicast or Multicast for VxRail vSAN Network

Starting in VxRail Release 4.5.0, all vSAN traffic replaces multicast with unicast. This change helps to reduce network configuration complexity and simplifies switch configuration.

Prior to VxRail 4.5.0, 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 both IGMP Snooping and IGMP Querier or disable both of these features. 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 may 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, then IGMP Querier must be enabled. If IGMP Snooping is disabled, then IGMP Querier must be disabled.

If your switch does not support IGMP Snooping or MLD Snooping, VxRail multicast traffic will be broadcast in one broadcast domain per VLAN. There is minimal impact on network overhead as management traffic is nominal.

For questions on your switch handles multicast traffic, contact your switch vendor.

Enable Uplinks to pass inbound and outbound VxRail network traffic

The uplinks on the switches must be configured to allow the traffic from the VxRail management network to pass through the uplinks. In addition, the uplinks must be configured to allow passage of Virtual Machine network traffic. Conversely, the uplinks need to be configured to block traffic from the VxRail vMotion and vSAN networks from outbound passage.

Enable Inter-switch Communication

In a multi-switch environment, configure the ports used for inter-switch communication to carry IPv6 multicast traffic for the VxRail management VLAN. Likewise, configure the ports to carry IPv4 traffic (unicast starting in VxRail Release 4.5.0 and multicast in prior releases) between switches for the vSAN VLAN.

Enable Inter-switch Links

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

Step 2. Plan Switch Port Configuration

Determine switch port mode

The decision on which port mode to configure on your switch is 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 only untagged packets 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 only tagged packets.

**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 could 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 tables below for the various VxRail Models.

4x10GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Requirement</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>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>40</td>
</tr>
<tr>
<td>vSphere vMotion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vSAN</td>
<td>IPv4 unicast</td>
<td>Unused</td>
<td>Unused</td>
<td>Standby</td>
<td>Active</td>
<td>50</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
<td>Standby</td>
<td>Active</td>
<td>Unused</td>
<td>Unused</td>
<td>100</td>
</tr>
</tbody>
</table>

2x10GbE or 2x25GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>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></td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>50</td>
</tr>
<tr>
<td>vSAN</td>
<td>VxRail starting with 4.5 (IPv4 unicast) VxRail prior to 4.5 (IPv4 multicast)</td>
<td>Standby</td>
<td>Active</td>
<td>Unused</td>
<td>Unused</td>
<td>100</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
<td>Active</td>
<td>Standby</td>
<td>Unused</td>
<td>Unused</td>
<td>30</td>
</tr>
</tbody>
</table>

*For a general overview on NIOC shares refer to [http://frankdenneman.nl/2013/01/17/a-primer-on-network-io-control/](http://frankdenneman.nl/2013/01/17/a-primer-on-network-io-control/).*
### 1GbE Traffic Configuration

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Management</th>
<th>vSphere vMotion</th>
<th>vSAN</th>
<th>Virtual Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPLINK1 (1Gb) VMNIC0</td>
<td>IPv6 multicast</td>
<td>Unused</td>
<td>Unused</td>
<td>Standby</td>
</tr>
<tr>
<td>UPLINK2 (1Gb) VMNIC1</td>
<td>IPv6 multicast</td>
<td>Unused</td>
<td>Unused</td>
<td>Active</td>
</tr>
<tr>
<td>UPLINK3 (1Gb) VMNIC2</td>
<td>Unused</td>
<td>Unused</td>
<td>Active</td>
<td>Standby</td>
</tr>
<tr>
<td>UPLINK4 (1Gb) VMNIC3</td>
<td>Unused</td>
<td>Unused</td>
<td>Unused</td>
<td>Unused</td>
</tr>
</tbody>
</table>

#### Limit 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.

#### Step 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, it is highly recommended to configure VxRail with VLANs. As listed in the [VxRail Setup Checklist](#), you will be configuring the following VLANs:

- **Management VLAN** (recommended is untagged/native): make sure that IPv6 multicast is configured/enabled on the management VLAN.
- **vSAN VLAN**: starting in VxRail 4.5.0, make sure that IPv4 unicast mode is used for vSAN traffic. For earlier releases, make sure that IPv4 multicast is configured/enabled on the vSAN VLAN (enabling IGMP snooping and querier is highly recommended).
- **vSphere vMotion VLAN**
- **VM Networks VLANs**
**Figure 11. VxRail VLAN configuration, G Series.**

**Step 1.** Using the VxRail Network Configuration Table, configure a VLAN on the switch(es) for each VxRail logical network.

**Step 2.** Using the VxRail Network Configuration Table, 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.

**Step 3.** Configure the Management VLAN (Row 1) on the switch ports. If you entered “Native VLAN,” then set the ports on the switch to accept untagged traffic and tag it to the custom management VLAN ID. Untagged management traffic is the recommended management VLAN setting on VxRail.

**Step 4.** You must set the management VLAN to allow IPv6 multicast traffic to pass through on 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. Be sure to review the previous section, and consult the switch manufacturer for further instructions on how to configure these settings.

**Step 5.** Configure a vsphere vMotion VLAN (Row 34) on the switch ports.

**Step 6.** Configure a vsAN VLAN (Row 38) on the switch ports for release prior to VxRail Release 4.5.0, set to allow IPv4 multicast traffic to pass through. Starting in VxRail Release 4.5.0, set to allow IPv4 unicast traffic to pass through.
Step 7. Configure the VLANs for your VM Networks (Rows 39-41) on the switch ports.

Step 8. Configure the switch uplinks to allow the Management VLAN (Row 1) and VM Networks (Rows 39-40) to pass through.

Step 9. Configure the inter-switch links to allow all VLANs to pass through if deploying dual switches.

Confirm Your Data Center Network

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

- Verify switch and data center environment supportability
- Verify passage of VxRail logical networks
- Verify accessibility of required data center applications
- Verify compatibility with the planned VxRail implementation

Certain data center environment and network configuration errors will cause validation to fail, and the VxRail cluster will not be formed. When validation fails, the data center 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 prior to 4.5.0) or unicast (VxRail Release 4.5.0 and beyond) 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. Remember that management traffic will be untagged on the native VLAN on your switch unless all ESXi hosts have been customized for a specific management VLAN.
4. Confirm the switch ports that will attach to VxRail nodes allow passage of all VxRail network VLANs.
5. Confirm the switch uplinks allow passage of VxRail networks for external users.

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

Confirm your firewall settings:

1. Verify VxRail will be able to communicate with your DNS server.
2. Verify VxRail will be able to communicate with your NTP server.
3. Verify 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 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 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 data center instead of SRS-VE deployed in the VxRail cluster, verify open communications between VxRail management and the SRS gateway.

Refer to Appendix B for information of VxRail port requirements.

Confirm your data center 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 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 have configured NTP servers, or a third-party syslog server, confirm that you can reach them from your configured VxRail management network
6. If you plan to use a Customer-Supplied vCenter, confirm it is accessible from the VxRail management network

**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 either plugged into the top-of-rack switch, or able to logically reach the VxRail management VLAN from elsewhere on your network; for example, a jump server (https://en.wikipedia.org/wiki/Jump_server). Once the VxRail initialization process is complete, the switch port or jump host is no longer required to manage VxRail.

Don’t try to plug your workstation/laptop directly into a server node on a VxRail Appliance 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 VxRail management interface.

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</th>
<th>Workstation/laptop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address/netmask</td>
<td>IP address</td>
</tr>
<tr>
<td>Initial (temporary)</td>
<td>192.168.10.200/24</td>
<td>192.168.10.150</td>
</tr>
<tr>
<td>Post-configuration</td>
<td>10.10.10.100/24</td>
<td>10.10.10.150</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 may 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.

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 management VLAN.
Perform Initialization to create 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 beforehand to capture and record the information described in the VxRail Network Configuration Table and walk through the VxRail Setup Checklist.

**Step 2.** Install the VxRail nodes into a rack in the data center. For ease of manageability, install the network switches supporting the VxRail cluster into the same rack

**Step 3.** Attach Ethernet cables between the ports on the VxRail nodes and switch ports configured to support VxRail network traffic

**Step 4.** Power on all 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 5.** Connect a workstation/laptop configured for VxRail initialization to access the VxRail management network on your selected management VLAN. It must be either plugged into the switch or able to logically reach the VxRail management VLAN from elsewhere on your network.

**Step 6.** Open a browser to the VxRail initial IP address to begin the VxRail initialization process

**Step 7.** 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.** VxRail performs the verification process, using the information input into the menus

**Step 10.** After validation is successful, the initialization process will begin to build a new VxRail cluster

**Step 11.** 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, then the browser session will make the switch automatically
- If not, you need to 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 12.** Progress is shown as the VxRail cluster is built.

**Step 13.** 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 14.** 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
After VxRail Initialization Network Considerations

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 Appendix A. Refer to the VMware Product Interoperability Matrixes for specific versions of NSX supported on vSphere specific versions.

Using Unassigned VxRail Physical Ports

For VxRail nodes order with extra physical network ports, VxRail Manager will not manage the optional PCI-e NiCs. Customers 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: Customers need to follow the official instructions/procedures from VMware and Dell-EMC for any of these operations.

Unsupported Operations:

- Migrating or moving VxRail system traffic to these 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 vSphere Distributed Switch (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.
## VxRail Network Configuration Table

The Dell EMC service representative will use a VxRail Pre-Site Installation tool with 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>Management VLAN ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The recommended is untagged traffic on the Native VLAN. If you want the host to send only tagged frames, manually configure the VLAN on each ESXi™ host using DCUI, and set tagging for your management VLAN on your switch before you deploy VxRail.</td>
</tr>
<tr>
<td>3</td>
<td>System</td>
<td>Global settings</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Time zone</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>NTP 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>vCenter Server Leave blank if Customer Supplied VC</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 host name (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>27</td>
<td>Networking</td>
<td>Subnet mask</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td>Gateway</td>
</tr>
<tr>
<td>31</td>
<td>vMotion</td>
<td>vMotion Starting address for IP pool</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>vMotion Ending address for IP pool</td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>vMotion Subnet mask</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>vMotion VLAN ID</td>
</tr>
<tr>
<td>35</td>
<td>vSAN</td>
<td>vSAN Starting address for IP pool</td>
</tr>
<tr>
<td>36</td>
<td></td>
<td>vSAN Ending address for IP pool</td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>vSAN Subnet mask</td>
</tr>
<tr>
<td>38</td>
<td></td>
<td>vSAN VLAN ID</td>
</tr>
<tr>
<td>39</td>
<td>VM Networks</td>
<td>VM Networks … (unlimited number)</td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>VM Network name and VLAN ID</td>
</tr>
<tr>
<td>41</td>
<td>Solutions</td>
<td>Logging vRealize Log Insight™ hostname</td>
</tr>
<tr>
<td>42</td>
<td></td>
<td>vRealize Log Insight IP address</td>
</tr>
<tr>
<td>43</td>
<td></td>
<td>Syslog Server (instead of Log Insight)</td>
</tr>
</tbody>
</table>
### VxRail Password Tables

<table>
<thead>
<tr>
<th>Row</th>
<th>Item</th>
<th>Account</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VxRail Manager</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>VxRail vCenter Server</td>
<td>administrator@&lt;SSO Domain&gt;</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>management</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>VxRail Platform Service Controller</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>vRealize Log Insight</td>
<td>root</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>admin</td>
<td></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.
- **Data Center**: Verify the required external applications for VxRail are accessible over the network and correctly configured.
- **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

<table>
<thead>
<tr>
<th>Reserve VLANs</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ One management VLAN with IPv6 multicast for traffic from VxRail, vCenter Server, ESXi (recommended is untagged/native).</td>
<td>✓ Time zone.</td>
</tr>
<tr>
<td>✓ One VLAN with IPv4 unicast (starting with VxRail 4.5.0) or IPv4 multicast (prior to Release 4.5.0) for vSAN traffic.</td>
<td>✓ Hostname or IP address of the NTP server(s) on your network (recommended).</td>
</tr>
<tr>
<td>✓ One VLAN for vSphere vMotion.</td>
<td>✓ IP address of the DNS server(s) on your network (required).</td>
</tr>
<tr>
<td>✓ One or more VLANs for your VM Network(s).</td>
<td>✓ Forward and reverse DNS records for VxRail management components</td>
</tr>
</tbody>
</table>

### 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.
- Decide if 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 data center. Create a VxRail management user in vCenter. Decide on a unique VxRail cluster name. (Optional) Create a VxRail non-admin user.
- Reserve one IP address for VxRail Manager.
- Determine IP address of the default gateway and subnet mask.
- Select passwords for VxRail management components.

### vMotion and vSAN

- Reserve three or more contiguous IP addresses and a subnet mask for vSphere vMotion.
- Reserve three or more contiguous IP addresses and a subnet mask for vSAN.

### 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.

### Workstation

- Configure your workstation/laptop to reach the VxRail initial IP address.
- Make sure you also know how to configure the laptop to reach the VxRail Manager IP address after configuration.

### Set up Switch

- Configure your selected management VLAN (recommended is untagged/native).
- Confirm that IPv6 multicast is configured/enabled on the management VLAN.
- Configure your selected VLANs for vSAN, vSphere vMotion, and VM Networks.
- In multi-switch environments, configure the management and vSAN VLANs to carry the multicast and unicast traffic respectively between switches.
- Configure uplinks to carry management VLAN and VM Networks VLANs.
- Confirm configuration and network access.
Appendix A: 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 programatically 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 11:

- 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 chart below.
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 no longer necessary to over-provision server capacity within each application/network pod. Instead, organizations can take advantage of available resources wherever they are 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:

Appendix B: VxRail Open Ports Requirement

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 data center. DNS is required and NTP is optional. Open the necessary ports to enable connectivity to the external syslog server, and for LDAP and SMTP.

### Data Center Application Access

<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

### Administration Access

<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>
</table>
If you plan to enable Dell-EMC ‘call-home’ with an external SRS gateway already deployed in your data center, 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 data center 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><a href="#">List of Incoming and Outgoing Firewall Ports for ESXi 6.5 Hosts</a></td>
</tr>
<tr>
<td>List of Incoming and Outgoing Firewall Ports for ESXi 6.0 Hosts</td>
<td><a href="#">List of Incoming and Outgoing Firewall Ports for ESXi 6.0 Hosts</a></td>
</tr>
<tr>
<td>Required port to access VMware vCenter Server and VMware ESXi hosts</td>
<td><a href="#">TCP and UDP Ports required to access VMware vCenter Server and VMware ESXi hosts</a></td>
</tr>
<tr>
<td>Secure Remote Services Port Requirements</td>
<td><a href="#">Dell EMC Secure Remote Services Documentation</a></td>
</tr>
</tbody>
</table>
Appendix C: Physical Network Switch Examples

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

Figure 13. Rear view of VxRail Appliance connected to 2x10GbE SFP+ ToR switch, 1 x Management Switch with iDRAC
Figure 14. Rear view of VxRail Appliance connected to 1x10GbE SFP+ ToR switch with no iDRAC
Figure 15. Rear view of VxRail Appliance connected to 1x(1GbeE + 10 GbE) SPF+ ToR switch with iDRAC
Figure 16. Rear view of VxRail Appliance connected to 2x10GbE SPF+ ToR switches with no iDRAC
Figure 17. Rear view of VxRail Appliance connected to 2x(1Gbe + 10GbE) SPF+ ToR switches with iDRAC