Abstract
This guide is for customers interested in deploying VMware Cloud Foundation on VxRail. This guide covers version 4.2 of Cloud Foundation on VxRail. It outlines the planning and preparation that needs to be undertaken before commencing with the product deployment.
## Contents

**Chapter 1**  Executive Summary 6
- Solution description ................................................................. 7
- Solution version reference ....................................................... 7
- Document purpose ..................................................................... 7
- Intended audience ................................................................. 7
- Revisions ................................................................................. 7

**Chapter 2**  VMware Cloud Foundation on VxRail 9
- Product overview ................................................................. 10

**Chapter 3**  VMware Cloud Foundation on VxRail Deployment 14
- Introduction ........................................................................... 15
- VMware Cloud Foundation on VxRail network and workload planning ........ 16
- VMware Cloud Foundation on VxRail initial deployment ....................... 17

**Chapter 4**  VMware Cloud Foundation on VxRail Workload Domains 19
- Introduction ........................................................................... 20
- NSX-T Management options for VI workload domain ............................ 21
- vRealize software option for VI workload domains ................................ 22
- vSphere with Kubernetes workload domains ....................................... 22

**Chapter 5**  Data Center and Network Requirements 24
- Introduction ........................................................................... 25
- Data center rack space requirements ................................................ 25
- Data center networking ................................................................ 25
- Network switch selection ............................................................ 25
- Switch port capacity ................................................................... 26
- Switch port type ........................................................................ 26
- Jumbo Frames ............................................................................ 27
- Multicast .................................................................................... 27
- Border Gateway Protocol ............................................................ 27
- Hardware VTEP for multi-rack deployments ....................................... 28
- Network services ....................................................................... 28

**Chapter 6**  Cloud Foundation on VxRail High-Level Design 30
- Introduction ........................................................................... 31
- Consolidated vs. standard architecture ........................................... 31
- Site locations .......................................................................... 32
Select the settings for NSX-T host overlay network ............................................. 74
Create Forward and Reverse DNS Entries for the management VI workload domain ................................................................................................................. 74
Select the NSX-T host overlay VLAN .................................................................. 74
Select names for resource pools in VI Management workload domain .............. 75
Select names for portgroups in VI Management workload domain ..................... 75
Prepare passwords ............................................................................................. 75
Obtain VMware license keys ............................................................................... 75

Chapter 13 Prepare for Cloud Foundation Application Virtual Network 76
Introduction ......................................................................................................... 77
Select the Application Virtual Network region settings ......................................... 77
Select settings for NSX-T edge nodes .................................................................. 78
Select external router settings for eBGP peering ................................................. 79
Select NSX-T Edge overlay network settings ...................................................... 80
Select second site settings for stretched cluster .................................................. 80

Chapter 14 Prepare for Cloud Foundation VI Workload Domain 82
Introduction ......................................................................................................... 83
Prepare NSX-T host overlay network .................................................................. 83
Capture settings for VI workload domain ............................................................. 84
Prepare for vSphere for Tanzu Workload Domain ............................................... 84
Prepare for Multi-Region with NSX-T Federation ................................................ 86

Appendixes 87
Appendix A: Cloud Foundation on VxRail checklist ............................................. 88
Appendix B: Cloud Foundation on VxRail footprints for sizing ............................ 92
Appendix C: Cloud Foundation on VxRail VLANs ............................................. 94
Appendix D: VxRail network configuration ........................................................... 95
Appendix E: Cloud Builder and management VI workload configuration .......... 97
Appendix F: Application Virtual Network configuration ...................................... 99
Appendix G: VI workload domain configuration settings .................................... 100
Appendix H: Sample switch configuration settings ............................................ 102
This chapter presents the following topics:

Solution description ........................................................................................................7
Solution version reference .........................................................................................7
Document purpose ....................................................................................................7
Intended audience .....................................................................................................7
Revisions .....................................................................................................................7
Solution description

VMware Cloud Foundation (VCF) on VxRail™ is a Dell Technologies and VMware jointly engineered integrated solution. It contains features that simplify, streamline, and automate the operations of your entire Software-Defined Datacenter (SDDC) from Day 0 through Day 2. The new platform delivers a set of software-defined services for compute (with vSphere and vCenter), storage (with vSAN), networking (with NSX), security, and cloud management (with vRealize Suite) in both private and public environments, making it the operational hub for your hybrid cloud.

VCF on VxRail provides the simplest path to the hybrid cloud through a fully integrated hybrid cloud platform that leverages native VxRail hardware and software capabilities and other VxRail-unique integrations (such as vCenter plugins and Dell EMC networking). These components work together to deliver a new turnkey hybrid cloud user experience with full-stack integration. Full-stack integration means you get both HCI infrastructure layer and cloud software stack in one complete automated life-cycle turnkey experience.

Solution version reference

This guide supports the major software release 4.2 of VMware Cloud Foundation, and major software release 7.0 of VxRail. The specific versions of the software stack supported for the major versions of VMware Cloud Foundation on VxRail covered in this guide can be found in the support matrix at VMware Cloud Foundation 4.x on VxRail Support Matrix.

Document purpose

This guide provides detailed guidance for the initial deployment of a VCF on VxRail solution in a data center. It outlines the tasks and processes that you should expect and prepare for from the planning and design phase through deployment of the solution. The guide also serves as an aid in helping determine a configuration that meets your business and operational objectives.

Intended audience

This planning and preparation guide is intended for cloud architects, network architects, and technical sales engineers who are interested in the planning, designing, and deployment of the VMware Cloud Foundation on VxRail solution to meet business and operational requirements. Readers should be familiar with VMware vSphere, NSX, vSAN, and vRealize product suites in addition to general network architecture concepts.

Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>Initial release</td>
</tr>
<tr>
<td>May 2019</td>
<td>Minor edits to provide more clarity and detail</td>
</tr>
</tbody>
</table>
## Executive Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2019</td>
<td>Updated to support VMware Cloud Foundation 3.8</td>
</tr>
<tr>
<td>February 2020</td>
<td>Updated to support VMware Cloud Foundation 3.9.1</td>
</tr>
<tr>
<td>May 2020</td>
<td>Updated to support VMware Cloud Foundation 4.0</td>
</tr>
<tr>
<td>July 2020</td>
<td>Updated for VxRail stretched cluster requirements post-deployment</td>
</tr>
<tr>
<td>August 2020</td>
<td>Updated to support VMware Cloud Foundation 4.0.1</td>
</tr>
<tr>
<td>September 2020</td>
<td>Updated to support VMware Cloud Foundation 4.1 on VxRail 7.0.010</td>
</tr>
<tr>
<td>October 2020</td>
<td>Removed references to Witness Traffic Separation</td>
</tr>
<tr>
<td>November 2020</td>
<td>Updated to support VMware Cloud Foundation 4.1 on VxRail 7.0.100</td>
</tr>
<tr>
<td>March 2021</td>
<td>Updated to support VMware Cloud Foundation 4.2 on VxRail 7.0.131</td>
</tr>
</tbody>
</table>
Chapter 2  VMware Cloud Foundation on VxRail

This chapter presents the following topic:

Product overview .............................................................................................................. 10
### Product overview

The VMware Cloud Foundation on VxRail solution is integrated end-to-end to fully enable a software-defined cloud platform that is designed for the rapid deployment of physical resources into managed consumption pools, and for the provisioning of these resource pools on-demand to meet flexible and resilient workload requirements.

VxRail provides the physical resource foundation for the cloud delivery platform. VxRail is a set of specially engineered and manufactured compute nodes that when logically bound together after initial configuration, represent a single managed cluster for virtual workloads.

![VxRail cluster representing a pool of virtual resources](image)

VxRail integrates software products from VMware with custom software engineered from Dell Technologies so that the physical compute, memory, network, and storage resources are placed under a virtualization layer to be managed and controlled as an adaptable pool of resources. The physical disk devices on each VxRail node are encapsulated under the virtualization layer to create a single consumable data store for the virtual workloads. In addition, a virtual switch is created during initial configuration and distributed across the entire VxRail cluster. The Ethernet ports on each node are placed under the virtualization layer to enable connectivity between virtual machines on the VxRail cluster, and to enable connectivity to end-users.

When integrated with VMware Cloud Foundation, the VxRail cluster is positioned as an individual building block to supply compute resources for consumption in Cloud Foundation virtual workloads. Cloud Foundation allows users to dynamically allocate and assign VxRail clusters into individual consumption pools, known as Virtual Infrastructure (VI) workload domains. A VI workload domain represents the logical boundary of consumable resources, and all functionality within these boundaries is managed through a single vCenter instance. Under this model, VI workload domains can be planned and deployed to support the distinct requirements of individual organizations or a set of applications.
The resources of individual VI workload domains can be expanded through the addition of individual nodes into a VxRail cluster, or through the addition of an entire new VxRail cluster into a VI workload domain. The physical resources are automatically added to the VI workload domain pool upon completion of this event.

The networking resources for each VI workload domain are also logically segmented, so that the distinct requirements for a set of applications can be individually managed. With the layering of the VMware’s Cloud Foundation software stack on VxRail virtual switches, enterprise networking features such as routing, VPN, and security from NSX-T are embedded and enabled into each VI workload domain.
With support for NSX-T logical routing, virtual machine traffic that previously had to pass through to the physical network can now traverse the virtual network when established on a Cloud Foundation on VxRail VI workload domain.

Virtual machines running will connect to the network using a logical switch in a Cloud Foundation domain. Cloud Foundation on VxRail supports the linking of these virtual switches into an extended logical network, known as a segment. This allows virtual machines in different VI workload domains to connect to each other through this extended switch fabric.
Figure 4. Virtual machines connected to an extended logical network with routing services

If a virtual machine requires routing services, the extended logical switch, or segment, can use routing services within the virtual network. To support connectivity outside of the virtual network, the virtual routing services form a peer relationship with existing upstream physical routers in the data center to form a seamless connection between the physical and logical networks.
This chapter presents the following topics:

**Introduction** ................................................................. 15

**VMware Cloud Foundation on VxRail network and workload planning** ......... 16

**VMware Cloud Foundation on VxRail initial deployment** ............................. 17
Introduction

The Cloud Foundation on VxRail cloud platform in a data center has a transformational effect on the way IT resources are delivered to support applications and users. The deployment of a Cloud Foundation on VxRail cloud platform in your environment involves careful and deliberate planning and preparation to ensure an efficient and seamless deployment experience.

The Cloud Foundation on VxRail deployment life cycle starts before a purchase order is issued. In the initial phase, the business and operational requirements are captured and applied toward the overall solution. The requirements process captures the use cases for the planned Cloud Foundation on VxRail deployment. At this stage, decisions can be made about requirements such as site locations and availability. In addition, various organizations and business units are aligned with their application requirements to propose a high-level design. Dell Technologies specialists work jointly with the account team at this stage of the effort.

After acceptance of a high-level design and proposal, technologists and subject matter experts will join the effort. The applications and virtual machines targeted for the Cloud Foundation on VxRail platform are used in a sizing exercise to produce a detailed VxRail infrastructure bill-of-materials needed to support the planned workload.

Figure 5. Anatomy of a Cloud Foundation on VxRail deployment experience

Also, during this phase, the dependencies between the planned sets of applications for Cloud Foundation are analyzed and used to produce a high-level network design. These
requirements are then used as the baseline in the planning efforts for the upstream external network and for the virtual networks in the management workload domain and the VI workload domains.

VMware Cloud Foundation on VxRail network and workload planning

At this point in time, decisions are made on the overall Cloud Foundation architecture based on best practices and use case requirements:

- Resource consumption on the management workload domain depends on decisions made regarding network connectivity for the workload domains. A new workload domain can either leverage existing NSX-T management virtual appliances deployed in the management workload domain, or new NSX-T management virtual appliances must be deployed to support networking requirements. Capacity must be reserved in instances where additional NSX-T virtual appliances will be deployed.

- The default size of the NSX-T management virtual appliances deployed during Cloud Foundation initial deployment is adequate for most workloads. An expansion of virtual machine workload or the enablement of additional networking services can impact NSX-T management resources, and impose constraints on the management workload domain if there is a lack of resource capacity.

- For smaller, less impactful workload requirements, a consolidated architecture can be considered. A consolidated architecture does not support additional domains beyond the management workload domain, which means the resources for Cloud Foundation management and all application workloads are shared in a single management workload domain. This option should be considered only if the sizing exercises show a consolidated architecture can be supported, including plans for future growth.

Once the decisions have been made on workload and network planning, the work effort transitions to a professional services engagement. This planning and design phase will commence while awaiting equipment delivery from Dell Technologies manufacturing to your site locations. The solutions architect will walk through the deployment process using information gathered in the initial planning phase, and capture the detailed design and configuration settings for the initial deployment of Cloud Foundation on VxRail.

The design and configuration settings include the properties for the planned VxRail clusters and the Cloud Foundation Cloud Builder virtual appliance, a tool that is used in initial deployment of Cloud Foundation on VxRail. The solutions architect will also perform a validation of the data center environment based on the captured configuration settings to ensure that all the prerequisites have been met.

If a requirement is the future deployment of the vRealize management software to support workload and application requirements, the solutions architect needs to capture additional configuration settings for the Application Virtual Network. The Application Virtual Network (AVN) provides connectivity to the external network for Cloud Foundation on VxRail during initial deployment. The deployment of vRealize Suite Lifecycle Manager on the management workload domain, the tool which downloads and deploys the vRealize management software, depends on the Application Virtual Network.
If Dell Technologies is responsible for the configuration of the switches enabling network connectivity for the Cloud Foundation on VxRail infrastructure, those services will be performed after the networking hardware is installed and cabled in the data center. This work effort includes configuring uplinks to the data center network. The VxRail clusters and VMware Cloud Foundation depend on the supporting network infrastructure to be properly configured, and for all required data center and network services to be properly configured, before actual deployment.

**VMware Cloud Foundation on VxRail initial deployment**

The next phase is the deployment process of the VxRail cluster targeted for the Cloud Foundation management workload domain. It is built using the information captured during the planning and design phase.

The next step is to deploy the Cloud Foundation Cloud Builder virtual appliance on the VxRail cluster. The configuration settings captured from the planning and design phase are fed into the Cloud Builder virtual appliance, which automates the deployment of the Cloud Foundation software onto the VxRail cluster. This creates the Cloud Foundation management workload domain, and deploys the virtual machines required to support the management workload domain. If a use case requirement is for the future deployment of the vRealize software suite, Cloud Builder deploys two NSX-T Edge virtual appliances into the management workload domain to support upstream connectivity for the Application Virtual Network.
Figure 7. Overview of Cloud Builder automatic deployment of virtual appliances for a basic Cloud Foundation management workload domain

Figure 8. Overview of Cloud Builder automatic deployment of virtual appliances for a Cloud Foundation management workload domain to support the Application Virtual Network
Chapter 4  VMware Cloud Foundation on VxRail Workload Domains

This chapter presents the following topics:

Introduction ....................................................................................................... 20
NSX-T Management options for VI workload domain ..................................... 21
vRealize software option for VI workload domains ........................................ 22
vSphere with Kubernetes workload domains ................................................. 22
Introduction

Once Cloud Builder has completed the initial phase of deploying the Cloud Foundation management workload domain, the next phase is the deployment of the Cloud Foundation VI workload domains to support use cases and workload requirements, with the exception being the single-domain consolidated architectures. For this phase, a VI workload domain is initialized using SDDC Manager with initial configuration settings. Next, the underlying VxRail cluster or clusters to support the workload domain are deployed. Then as a final step, the VxRail cluster or clusters are assigned to the VI workload domain.

The initialization of a VI workload domain lays down the basic foundation for the future deployment of virtual machines and their network interconnections. SDDC Manager can also deploy a workload domain to address a specific use case. This action, depending on the option, can alter the pre-requisites and requirements that must be addressed before configuring the workload domain.

This section provides an overview of the workload domains that can be created with Cloud Foundation on VxRail to address specific use cases, and raise awareness of the impact these choices have on the planning and preparation phase. The specific details on how to implement a VI workload domain for a specific use can be found in the Cloud Foundation documentation on the VMware support site: VMware Cloud Foundation Documentation.

Figure 9. Solutions layers on Cloud Foundation for VxRail
NSX-T Management options for VI workload domain

With each new VI workload domain, there is the option to deploy three new NSX-T management virtual appliances to manage network requirements, or to reuse existing NSX-T managers. The use cases that trigger this decision include:

- Test/Development or pre-production workloads that do not use the production network
- Applications in the workload domain have an NSX-T version dependency.
- Applications that require more isolation and security
- Cloud Foundation deployments that have a multi-tenant workload requirement
- A new VLAN-backed transport zone is required.

If a new set of NSX-T management virtual appliances is planned for the management workload domain, the following points must be considered:

- Each NSX-T manager has a resource reservation of 48 GB of memory.
- NSX-T managers are subject to vSphere HA admission control.
- NSX-T manager virtual appliances can be CPU intensive depending on workload activity.

Figure 10. VI workload domain deployment using existing NSX-T managers

Figure 11. Overview of initial deployment of NSX-T based VI workload by SDDC Manager
**vRealize software option for VI workload domains**

If the use case requirements for any Cloud Foundation VI workload domains include the vRealize software suite, plan for the vRealize management virtual appliances to require resources in the management workload domain.

![vRealize management virtual appliances in management workload domain](image)

**vSphere with Kubernetes workload domains**

SDDC Manager supports VI workload domain configurations that provide the infrastructure foundation required by vSphere with Kubernetes. A VI workload domain configured for Kubernetes transforms the vSphere platform into a platform for running Kubernetes workloads natively on the hypervisor layer. If there is a use case requirement for vSphere with Kubernetes, the following items must be considered:

- All the nodes in the VxRail cluster supporting the VI workload domain must have a vSphere with Kubernetes license.
- An NSX-T edge cluster must be deployed on the VI workload domain that is targeted for vSphere with Kubernetes.

![Edge appliances deployed for VI workload domain for vSphere with Kubernetes](image)
• The NSX-T edge cluster requires connectivity upstream using eBGP. Plan on preparing the upstream network for BGP peering and route distribution.

• Additional IP addresses specific for vSphere with Kubernetes will be required when the VI workload domain is configured.
  ▪ Non-routable subnet for pod networking (minimum /22)
  ▪ Non-routable subnet for service IP addresses (minimum /24)
  ▪ Routable subnets for ingress and egress for the NSX-T edge cluster (minimum /27).
This chapter presents the following topics:

- Introduction................................................................. 25
- Data center rack space requirements................................. 25
- Data center networking.......................................................... 25
- Network switch selection.................................................... 25
- Switch port capacity.......................................................... 26
- Switch port type................................................................. 26
- Jumbo Frames................................................................. 27
- Multicast.......................................................................... 27
- Border Gateway Protocol................................................. 27
- Hardware VTEP for multi-rack deployments.......................... 28
- Network services............................................................. 28
Introduction

Your data center environment must meet certain requirements to support the deployment of Cloud Foundation on VxRail. Before the product is delivered, Dell Technologies will review these prerequisites with you to ensure compliance.

Data center rack space requirements

The Cloud Foundation on VxRail platform is a consolidated, self-contained architecture, as there is no requirement for external storage to support workload. Furthermore, there is the expectation that network traffic will migrate onto the virtual network within the VI workload domains, which might free up physical space occupied by excess physical network equipment.

The amount of rack space required for the VxRail nodes depends on the models you select to support your Cloud Foundation on VxRail platform. Dell Technologies will go through a sizing exercise to produce a bill of materials of the VxRail nodes needed to support your requirements.

Table 1. VxRail Node Rack Space

<table>
<thead>
<tr>
<th>VxRail Model</th>
<th>Rack Units</th>
<th>Power Supply</th>
<th>Plug Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Series</td>
<td>1</td>
<td>750 W, 1100 W</td>
<td>C14</td>
</tr>
<tr>
<td>D-Series</td>
<td>1</td>
<td>550 W, 600 W</td>
<td>C14</td>
</tr>
<tr>
<td>P-Series</td>
<td>2</td>
<td>1100 W, 1600 W</td>
<td>C14</td>
</tr>
<tr>
<td>S-Series</td>
<td>2</td>
<td>1100 W, 1600 W</td>
<td>C14</td>
</tr>
<tr>
<td>V-Series</td>
<td>2</td>
<td>2000 W</td>
<td>C20</td>
</tr>
<tr>
<td>G-Series</td>
<td>2</td>
<td>2000 W, 2400 W</td>
<td>C20</td>
</tr>
</tbody>
</table>

The amount of rack space required for the supporting physical network depends on the network topology selected for the Cloud Foundation on VxRail deployment. The most common network topology is leaf-spine, so plan on additional rack space for the switches.

Data center networking

You can either bundle a Dell network infrastructure with your Cloud Foundation on VxRail for a single source solution, or acquire, implement, and configure your own supporting network.

If you choose a network infrastructure based on Dell network switches, your Dell Technologies specialist will work with you to design the network that meets the requirements for your specific Cloud Foundation on VxRail deployment. Regardless of which option you choose, your network infrastructure must support certain requirements for Cloud Foundation on VxRail.

Network switch selection
Cloud Foundation on VxRail is supported with either Dell-branded switches or most major enterprise switching products. You should plan on a pair of switches in the top of each data center rack used for Cloud Foundation on VxRail for redundancy purposes. Each VxRail node deployed to support Cloud Foundation on VxRail needs at least one connection into each switch, and possibly more depending on use cases and workload requirements. The first rack which supports the Cloud Foundation on VxRail management domain must integrate with your existing data center infrastructure using Layer 3 network services with a pair of uplinks. If your requirements will expand beyond a single rack, plan on expanding to a leaf-spine network topology. A multi-rack deployment requires additional switch ports be reserved on the top-of-rack switches to connect to the spine layer.

![Diagram of a single site Cloud Foundation on VxRail deployment across two racks]

**Switch port capacity**

If deployed into a 25Gb network, Cloud Foundation for VxRail supports either two or four Ethernet ports per node to be reserved for Cloud Foundation on VxRail networking purposes. Instead, if the nodes are plugged into a 10Gb network, either two, four, or six Ethernet ports per node can be reserved for Cloud Foundation on VxRail networking. The total number of ports required on the adjacent switches is depending on the number of VxRail nodes to be deployed to support the Cloud Foundation working, and the number of ports selected per node to reserve for this purpose.

**Switch port type**

VxRail nodes can support either SFP+ or RJ45 for 10 Gb Ethernet network connections, or SFP28 for 25 Gb Ethernet connections. The ports on the physical switch supporting your Cloud Foundation on VxRail cloud platform must match the network type on the VxRail nodes.
### Jumbo Frames

NSX-T depends on extending the standard Ethernet frame beyond the default 1500 bytes to support the tunneling of virtual machine traffic over the physical network in Cloud Foundation on VxRail. NSX-T depends on the GENEVE (GEneric NEtwork Virtualization) standard, which requires an MTU size of 1600 or higher to support the encapsulation of virtual machine traffic and provide the additional required header space. The physical network supporting Cloud Foundation on VxRail must support the ability to increase the MTU size to support tunneling.

![NSX-T extended frames](image)

**Figure 15. NSX-T extended frames**

### Multicast

VxRail depends on IPV6 multicasting to support device discovery during the cluster build operation and node expansion. The IPV6 is a private network that is isolated within the switches supporting the VxRail cluster in order to limit the impact on the data center network. Enabling MLD snooping and snooping querier is recommended on the physical switch to optimize multicast traffic.

If your network infrastructure does not support IPV6 multicast, or if your network policy does not allow IPV6 multicast, you can choose to have the nodes ingested manually during the cluster build operation and during node expansion. This option is supported with VMware Cloud Foundation 4.2 or later, as this option depends on VxRail version 7.0.130 or later.

### Border Gateway Protocol

Cloud Foundation on VxRail leverages NSX-T edge gateways to serve as the boundary point between the physical and virtual networks. This gateway is the passageway for traffic external to the data center to communicate with the virtual workload running on Cloud Foundation on VxRail. To enable routing between the physical and virtual networks, the upstream physical network must support Border Gateway Protocol. The NSX-T edge gateways require BGP adjacency to peer with upstream routing services.
Hardware VTEP for multi-rack deployments

Dell Technologies recommends selecting network switches that support hardware-based Virtual Tunnel Endpoints (VTEP) for multi-rack deployments. This feature is beneficial for customers expecting to deploy VxRail clusters over multiple racks, and do not want to extend the Layer 2 networks across racks. This feature is also beneficial in avoiding a rack being single point of failure, as the virtual machines in the management workload domain can migrate between racks without the need to change the IP address.

The feature supports the bridging of Layer 2 network traffic VxRail nodes in different racks through packet encapsulation and decapsulation on a Layer 3 overlay network. This feature optimizes VxRail network traffic across racks in a multi-rack cluster by eliminating the need to route through upstream routing services.

Network services

The network services listed in this section are required in the host data center for your Cloud Foundation on VxRail deployment. These services must be enabled in the data center planned for the Cloud Foundation on VxRail deployment, and configured with the settings required for your specific deployment.

- Domain Name Service (DNS) – You must enter forward and reverse DNS entries for every VxRail node. In addition, the virtual components used for the management
of the VxRail clusters and the Cloud Foundation domains also require forward and reverse DNS entries.

- **Network Time Protocol (NTP)**
- **Dynamic Host Configuration Protocol (DHCP)** – IP addresses are assigned to each host in the VxRail cluster to serve as the endpoints for NSX-T inbound/outbound traffic at the edge. The IP addresses can either be assigned manually or dynamically using DHCP. A DHCP server must be deployed in the host data center, and be pre-populated with the IP addresses to be assigned to the host endpoints.

- **SFTP Server** – The SFTP server supports backups of NSX-T Data Center instances and SDDC Manager.

The following network services are optional, but recommended:

- **Simple Message Transfer Protocol (SMTP)**
- **Certificate Authority (CA)** – The Certificate Authority must be able to ingest a Certificate Signing Request from the SDDC components, and issue a signed certificate. Cloud Foundation on VxRail supports Microsoft Windows Enterprise Certificate Authority. The domain controller must be configured with the Certificate Authority Service and the Certificate Authority Web Enrollment roles.

The following network services may be required, depending on the use cases targeted for Cloud Foundation on VxRail VI workload domains:

- **Active Directory** - Cloud Foundation on VxRail uses Active Directory service accounts for application-to-application communications.
Chapter 6  Cloud Foundation on VxRail
High-Level Design

This chapter presents the following topics:

Introduction ....................................................................................................... 31
Consolidated vs. standard architecture .......................................................... 31
Site locations ..................................................................................................... 32
Application availability ..................................................................................... 32
VxRail Cluster Network Planning ..................................................................... 33
Introduction

There are many factors to consider when deciding on the use cases for a Cloud Foundation on the VxRail platform. Because of the adaptive architecture designed into Cloud Foundation on VxRail, the business and operational requirements vary from one situation to another.

Consolidated vs. standard architecture

In a standard deployment, the Cloud Foundation management workload domain consists of workloads supporting the virtual infrastructure, cloud operations, cloud automation, business continuity, and security and compliance components for the SDDC. Using SDDC Manager, separate workload domains are allocated to tenant or containerized workloads. In a consolidated architecture, the Cloud Foundation management workload domain runs both the management workloads and tenant workloads.

There are limitations to the consolidated architecture model that must be considered that will impact this decision-making process.

- The decision to deploy a consolidated architecture must be made at the time of deployment, as a consolidated architecture cannot be converted to a standard architecture.
- Use cases that require a VI workload domain to be configured to meet specific application requirements cannot run on a consolidated architecture. The singular management workload domain cannot be tailored to support management functionality and these use cases. If your plans include applications that require a specialized VI workload domain, plan to deploy a standard architecture.
- Life-cycle management can be applied to individual VI workload domains in a standard architecture. If the applications targeted for Cloud Foundation on VxRail have strict dependencies on the underlying platform, consolidated architecture is not an option.
- Autonomous licensing can be used in a standard architecture, where licensing can be applied to individual VI workload domains. In a consolidated architecture, this is not an option.
- Scalability in a consolidated architecture has less flexibility than a standard architecture. Expansion is limited to the underlying VxRail cluster or clusters supporting the single management workload domain in a consolidated architecture, as all resources are shared. The minimum node count is eight for a standard architecture. Dell-Technologies recommends that any workload requirements that will require eight or more nodes should plan for a deployment using a standard architecture.
- If a VxRail cluster was built using two Ethernet ports, consolidating VxRail traffic and NSX-T traffic, additional nodes added to a cluster are limited to two Ethernet ports being used for Cloud Foundation for VxRail.
- VxRail nodes of differing network port speeds cannot be mixed in a VxRail cluster. If the workload is constrained due to network bandwidth and/or throughput, expanding the cluster with nodes that support higher port speeds is not an option.
Site locations

The requirement for multiple site locations for Cloud Foundation on VxRail deployments affect the overall high-level design. Factors such as distance and the quality of the network between sites must be considered.

- The management of multiple sites from a single management instance has network guidelines that must be met for supportability.
- The migration of virtual machines between sites using vMotion has network guidelines that must be considered for supportability.
- Both private and public WAN connectivity are supported for Cloud Foundation on VxRail provided compatibility requirements are met.
- Considerations for SD-WAN are merited for deployments spanning across multiple remote sites.

![Figure 18. Support for remote sites over Internet and private networks](image)

Primary and secondary active WAN links are strongly recommended. Without network redundancy, you might encounter conditions that can lead to failure states such as a two-failure state condition, which can result in unrecoverable virtual machines and application failure.

Application availability

Assess and categorize the availability requirements for the sets of application planned for deployment on Cloud Foundation on VxRail.

- If a primary objective is protection from a site-level failure with no loss of service, stretching the vSAN datastore in the VxRail cluster between sites is an option. In this configuration, synchronous I/O is supported for the virtual machines operating in the Cloud Foundation domains where a VxRail vSAN stretched cluster is present. However, there are strict latency requirements for the network between the sites, and this option requires a third site for a ‘witness’ to monitor the stretched vSAN datastore.
- Determine the operational recovery and disaster recovery objectives of the application sets planned for Cloud Foundation on VxRail. Certain application sets can then be placed in VI workload domains configured to support these objectives.
VxRail Cluster Network Planning

There are options and design decisions to be considered on the integration of the VxRail cluster physical and virtual networks with your data center networks. The decisions made regarding VxRail networking cannot be easily modified after the cluster is deployed and supporting Cloud Foundation, and should be decided before actual VxRail cluster deployment.

Each VxRail node has an integrated network daughter card (NDC). The NDC can support either 2x10Gb or 2x25Gb Ethernet ports, or 4x10Gb Ethernet ports. You can choose to support your Cloud Foundation on VxRail workload using only the ports on the Network Daughter Card. If NIC-level redundancy is a business requirement, a decision can be made to install optional PCIe cards into each VxRail node. The PCIe adapter cards support both 10 Gb and 25 Gb expansion ports.

VxRail supports both predefined network profiles and custom network profiles when deploying the cluster to support Cloud Foundation VI workload domains. The best practice is to select the network profile that supports the number of NDC-based ports and PCIe-based ports being selected per node to support Cloud Foundation on VxRail networking. This ensures that VxRail and CloudBuilder will configure the supporting virtual networks by following the guidance designed into these network profiles.

If VCF on VxRail networking will be configured on two node ports, a decision must be made whether to add a PCIe expansion card into each VxRail node to eliminate the NDC as a single point of failure. If only the NDC is present, the first two ports on each VxRail node will be reserved to support VCF on VxRail networking using a predefined network profile. If both NDC and PCIe ports are present, a custom network profile can be configured, with the option to select a port on the NDC and a port on the PCIe adapter card to reserve for VCF on VxRail networking.

In both two-port instances, the NSX and VxRail networks are configured to share the bandwidth capacity of the two Ethernet ports.
If VCF on VxRail networking will be configured with four ports, either all four ports on the NDC can be used (provided it is based on 10gb connectivity), or the workload can be spread across ports on the NDC and PCIe adapter cards. The latter option is preferred because it enables resiliency across the node devices, and also across the pair of switches.

The option to use only NDC ports uses a predefined network profile, with automatic assignment of the VMnics to the uplinks. If deploying the VxRail cluster using two NDC-based ports and two PCIe-based ports, the best practice is to use a profile that maps the uplinks from the virtual distributed switch to the VMnics as shown in the following graphic. Then, to enable network resiliency, plug the NDC-based ports into separate switches, and then plug the PCIe-based ports into separate switches. This profile permits the NSX and VxRail networks to optimize the sharing of bandwidth capacity across the four Ethernet ports, and best support the default teaming and failover policies configured for each Cloud Foundation on VxRail network.
Cloud Foundation on VxRail High-Level Design

Figure 20. Four ports reserved for VCF on VxRail networking

Cloud Foundation on VxRail supports the physical segmentation of VxRail and Cloud Foundation network traffic onto dedicated network ports, and onto separate, dedicated virtual distributed switches.

Note: Support of more than a single virtual distributed switch requires a minimum version of VMware Cloud Foundation 4.0.1.

If two node ports are selected for Cloud Foundation on VxRail networking, all the VxRail network traffic and Cloud Foundation/NSX traffic is consolidated onto the two ports. A second virtual distributed switch is not support for the two-port connectivity option, so all VxRail and Cloud Foundation/NSX traffic flows through a single virtual distributed switch.
With the four-port node option without the optional PCIe card, the vMotion and vSAN network traffic supporting VxRail are positioned on the second port on the network daughter card, and the Cloud Foundation/NSX traffic is assigned to the last two ports. With this network profile, a second virtual distributed switch can be deployed to isolate the VxRail network traffic on the first virtual distributed switch, and the Cloud Foundation/NSX traffic on the second virtual distributed switch.

For the four-port option using both NDC-based ports and PCIe-based ports from each VxRail node, a decision can be made to direct all Cloud Foundation on VxRail traffic onto a single virtual distributed switch. The uplinks can be assigned to a single virtual distributed switch to support all network traffic, or a second virtual distributed switch can be deployed to segment VxRail network traffic and Cloud Foundation/NSX network traffic.
For planned workloads that have very high bandwidth requirements, up to eight Ethernet ports can be used across the NDC and PCIe cards. The VxRail network traffic is spread across four ports, and Cloud Foundation/NSX network traffic is spread across the other four ports.

The reservation and assignment of the physical ports on the VxRail nodes to support Cloud Foundation on VxRail networking is performed during the initial deployment of the VxRail cluster. Dell-EMC recommends that careful consideration be taken to ensure that sufficient network capacity is built into the overall design to support planned workloads. If possible, Dell Technologies recommends an overcapacity of physical networking resources to support future workload growth.
Chapter 7  Cloud Foundation on VxRail
Workload Planning

This chapter presents the following topics:

Introduction ...............................................................................................................39
Determine use cases for Cloud Foundation VI workload domain ...................39
Deciding on single-site VxRail cluster or stretched cluster .........................39
Planning the Management workload domain resources ..........................41
Planning the VI workload domain resources ..................................................42
Sizing the Cloud Foundation domains ..............................................................42
Introduction

The primary building block for compute resources for Cloud Foundation on VxRail is the server node. VxRail leverages the Dell PowerEdge server products as the foundation for a cluster. A VxRail cluster can scale to a maximum of 64 nodes. The first VxRail cluster deployed is always used to support the management workload domain, which requires a minimum of four nodes. VxRail supports a wide variety of server physical configurations, with flexibility on CPU model, CPU quantity and speed, RAM capacity, physical storage capacity, and network port quantity and speed.

For more details, see the VxRail 14G Series Specification Sheet.

The mixing of different server models in a single cluster is supported because VxRail views the individual server node as a static pool of compute resources. This offers additional flexibility to start the initial configuration to meet a predefined baseline, and adapt and expand as necessary for changing workload requirements.

Determine use cases for Cloud Foundation VI workload domain

Before performing an overall sizing effort for Cloud Foundation on VxRail, decisions must be made on the rules and criteria for the creation of VI workload domains within your business. The criteria can be for a range of reasons, for instance:

- Logical grouping of applications or application sets for streamlined interconnectivity
- Ease of assigning and controlling a pool of IT resources to internal organizations
- Managing multiple sites from a single management entity

Each of these criteria will impact the resources required to support the workload planned for each domain. If plans include special use cases, such as the deployment of the vRealize suite, the overhead required to support these product suites must be considered with the sizing effort.

Deciding on single-site VxRail cluster or stretched cluster

If you deploy VxRail stretched clusters instead of a single-site cluster in order to meet availability requirements, be aware of the impact this decision has in planning the workload. A VxRail stretched cluster requires double the number of VxRail nodes to support any planned workload, as each site must be able to support that workload in the event of a site failure.
The reason for this is because every write operation by a virtual machine is performed on the vSAN datastore at both sites. Therefore, the size of the physical storage positioned to support any planned workload must be doubled.

In addition, there are a couple of other items of importance to consider with using stretched cluster to support your Cloud Foundation workloads:

- You must use DHCP to assign IP addresses to each VxRail node to support the overlay network required by NSX-T if your plans include VxRail stretched clusters to support the Cloud Foundation workload domains. Assigning static IP addresses to support the overlay network is not supported with stretched clusters.
- A feature in vSAN called ‘HCI Mesh’ support the sharing of vSAN datastore resources between VxRail clusters. This is accomplished by a VxRail cluster mounting a remote vSAN datastore and allocating those resources to local virtual machines. The ‘HCI Mesh’ feature is not supported with stretched clusters.

If you require support for workloads at multiple locations, you can choose a single-site deployment with a single point of management at each location, or have a centralized site designated to manage workloads at the local site and at remote sites.
The decision whether to pursue a centralized site model must meet the following considerations:

- The number of nodes at the remote site to support the VI workload domain is limited to four nodes.
- The minimum network bandwidth between sites is 10 Mb per second.
- The maximum latency between sites is 50-millisecond round-trip time.
- Redundant WAN links between sites are strongly recommended to eliminate the WAN as a single point of failure.

If your plans include expansion of Cloud Foundation on VxRail instances across regions using NSX-T Federation, consider both the latency and bandwidth of the physical network between regions. You can begin by deploying Cloud Foundation on VxRail in a single region, and decide to scale out into a multi-region architecture as a future expansion.

The maximum round-trip latency supported for NSX-T Federation is 150 milliseconds. Ideally, your latency between regions should fall within the performance threshold requirements set for the applications that are interconnected across regions. In addition, the network between sites must be configured to support NSX-T. The MTU size of the connecting network must be 1600 or larger.

![Figure 27. RTT latency for NSX-T Federation with Cloud Foundation on VxRail](image)

### Planning the Management workload domain resources

Guest virtual machines cannot be deployed in the Cloud Foundation management workload domain except under a consolidated architecture. At initial deployment of Cloud Foundation on VxRail, after the first VxRail cluster is built, Dell Technologies will deploy a temporary virtual appliance named ‘Cloud Foundation Cloud Builder’ on the cluster. This tool uses the deployment parameters captured during the planning and design phase, and layers the Cloud Foundation management workload domain on the VxRail cluster. In the same process, Cloud Builder deploys an initial core set of virtual machines to support Cloud Foundation on VxRail management.

This initial set of core virtual machines from Cloud Builder provides a baseline on the resources required to bring up the management workload domain and to begin deploying
VI workload domains on a standard architecture. However, for each VI workload domain that is created, additional virtual machines for management purposes are deployed. Therefore, in order to get more accurate sizing guidelines for the management workload domain and VI workload domains, the planned use cases for the VI workload domains must be understood and captured. Then, a resource consumption assessment is completed for both the management workload domain and the VI workload domains, which are used to determine the required size of the underlying VxRail platform for all the planned domains.

The tables in Appendix A: Cloud Foundation on VxRail checklist can be used to provide estimates of the minimum sizing requirements for the management components, based on planned use cases.

**Planning the VI workload domain resources**

At least one VI workload domain must be created to support guest virtual machines for a standard architecture, and at least one VxRail cluster of any supported size and configuration must be used as the resource foundation for a VI workload domain. A VxRail cluster that is assigned to support the workload of a Cloud Foundation domain is dedicated to that domain, and its resources cannot be shared with other Cloud Foundation domains.

For each VI workload domain that is created, SDDC Manager will deploy a vCenter virtual machine in the management workload domain. For VI workload domains that are not sharing existing NSX-T management resources, a new set of NSX-T management virtual appliances are deployed in the management workload domain. Depending on the use case, additional virtual machines might need to be deployed to support those specific applications.

Use the tables in Appendix B: Cloud Foundation on VxRail footprints for sizing for an understanding of the baseline sizing at the creation of the management workload domain, and for estimating the sizing requirements for additional components based on planned use cases.

**Sizing the Cloud Foundation domains**

The best practice for the resource sizing effort of the Cloud Foundation domains is to consider initial baseline of resources required for overall management based on use cases, and then calculate the additional resources needed for guest virtual machines.

Dell Technologies uses a sizing tool to calculate the workload resource requirements for the Cloud Foundation domains. Dell Technologies will conduct a sizing exercise to determine the pools of resources required to satisfy VI workload domain demands and their service level objectives at an optimal cost.
Figure 28. VxRail online sizing tool

The VxRail sizing tool performs calculations on one Cloud Foundation domain at a time. Therefore, the resources overhead required for management of each of the VI workload domains can be factored into the sizing effort for the management workload domain.

Figure 29. Selecting options for architecture in VxRail sizing tool

At least one workload domain is also included in the sizing effort. It is important to understand the applications planned for each respective workload domain to ensure accurate sizing.
For calculating resource requirements for guest virtual machines, the VxRail sizing tool accepts sizing data either through manual entry or by downloading metrics from a collector tool. For the most accurate sizing calculations, Dell Technologies’ best practice is to use a collector tool for guest virtual machine resource requirements. Dell Technologies uses LiveOptics data collection for this purpose. The capture from the data collector can then be input directly into the VxRail sizing tool to produce the sizing report for each VxRail cluster.

The VxRail sizing tool also supports reference workloads. A reference workload is a synthetic workload that attempts to represent real-life workloads. Select the reference workloads that best represent what is planned for a given VI workload domain to enable proper sizing.

The VxRail sizing tool performs its calculations using virtual machine profiles, and number of virtual machines that fit for each profile. Note that more than one profile can be defined for the same sizing exercise.

For best results, define the following metrics for each virtual machine profile:

- A reference workload
- The expected I/O activity per VM
- The usable storage capacity per VM
- The number of vCPUs or the amount of CPU in MHz per VM
- The amount of memory per VM

Dell Technologies will include the sizing metrics entered for each virtual infrastructure domain, and then perform the sizing analysis. When the settings are finalized, the resulting report from the VxRail sizing tool will show the required node count for a VxRail model and the HW characteristics for each node to meet the overall workload requirements.
This chapter presents the following topic:

Understanding connection dependencies ......................................................47
Understanding connection dependencies

Understanding the connection dependencies between the applications planned for Cloud Foundation on VxRail will streamline the high-level network design process and improve its effectiveness. It will also simplify the final decisions to be made on the placement of application sets on specific VI workload domains. To reduce the routing workload at the physical network layer and optimize the efficiency of the virtual networks, an assessment of the routing maps and dependencies for the sets of applications targeted for Cloud Foundation on VxRail is recommended.

When applications running on different subnets need to connect with each other, the network traffic is directed to a router, which then decides the path the network traffic takes to communicate. For environments that do not use VMware NSX-T, this means that the virtual machine network traffic must travel upstream out of the virtual network layer, where the routing decisions are made at the physical network layer.

Cloud Foundation on VxRail leverages NSX-T to enable support for routing in the virtual networks on the VI workload domains. This means that the defined network paths can be in different locations:

- Between applications within a Cloud Foundation VI workload domain
- Between applications in different Cloud Foundation VI workload domains
- Connected to external applications outside of a Cloud Foundation VI workload domain

Your sets of applications are likely separated by factors such as function or end-user accessibility (such as web tiers and database tiers). Within Cloud Foundation on VxRail VI workload domains, you might want to segment those application sets for network isolation, so that end-users can only access, for instance, the web tier network. You might also want flexibility so that the applications in each isolated network are not tied to a static pool of resources, or a static location.

![Three-tier application on separate virtual networks connected with virtual routers](image)

*Figure 32. Three-tier application on separate virtual networks connected with virtual routers*
Virtual machines deployed in a Cloud Foundation VI workload domain connect to port groups on a virtual switch in their Cloud Foundation VI workload domain. Each port group on a virtual switch is assigned a unique ‘virtual LAN’ (VLAN) identifier, and the traffic on a VLAN is logically isolated from the network traffic on another VLAN. If a virtual machine needs to connect with another virtual machine on the same VLAN but not on the same virtual switch, an extended network is deployed. Using GENEVE for NSX-T supports extending the non-routable VLAN-based network over a routable network. The traffic from one virtual machine flows through the virtual switch on a host and up a Tunnel Endpoint, over the physical network, and down through the Tunnel Endpoint on the second host, and is delivered to the second virtual machine.

An extended physical network supports accessibility between the virtual networks in the VI workload domains. This configuration forms an extended logical switch, or segment within NSX-T, across the individual virtual switches in the VxRail clusters. A virtual router, known as a Tier-1 gateway, is deployed within NSX-T for the applications on one segment that need to access an application on another segment, such as connecting from the web tier application to the app tier.

The Tier-1 gateways are positioned in the NSX-T network adjacent to edge devices, or Tier-0 gateways, which serve as the ingress and egress point with the external network. The Tier-1 gateways peer with the Tier-0 gateways in the NSX-T network using BGP for sharing routing information. The Tier-0 gateway, represented by NSX-T edge virtual devices, peer with upstream external routers for the purposes of sharing routing information. This enables a pathway for traffic from a virtual machine to connect to an application on an external host, or connect to external networking services. These peering relationships form a seamless barrier between the physical network and the NSX-T virtual networks.
Figure 33. Overview of Physical and Logical Network Routing Relationships

Documenting the interdependencies between the applications will guide the high-level network design to support the application connectivity dependencies, and serve as the basis for the planning process of the placement of the virtual machines into VI workload domains.
Chapter 9  Cloud Foundation on VxRail Physical Network Planning

This chapter presents the following topics:

Introduction .........................................................................................................................51
Select a physical network architecture and topology .........................................................51
VxRail stretched cluster physical network planning .........................................................53
Introduction

A complete planning phase of the physical and logical networking is critical for a successful deployment of Cloud Foundation on VxRail and the ongoing operations of the Cloud Foundation management and VI workload domains. VxRail clusters are dependent on a set of physical Ethernet switches to serve as the backplane for all networking communications. The Cloud Foundation management and VI workload domains are also dependent on the supporting physical network layer to enable virtual machine connectivity within a domain, between domains, and to the external network. The supporting physical network for VxRail must be properly configured before building the cluster, and the same interconnected network must also meet the requirements for VMware Cloud Foundation before attempting initial deployment. Before moving to a planning and design phase, ensure the key requirements for Cloud Foundation on VxRail are understood. As a starting point, have a good understanding of the interdependencies between the applications targeted for the Cloud Foundation VI workload domains.

Select a physical network architecture and topology

Cloud Foundation on VxRail offers flexibility regarding the selection of a physical network architecture to support the planned deployment. A spine-leaf topology is the most common network topology for Cloud Foundation on VxRail and is considered a best practice. In this model, the VxRail nodes connect directly to the leaf-layer switches, and multiple VxRail clusters can be supported on a single pair of leaf-layer switches. The spine layer is positioned primarily for aggregating upstream traffic, providing connectivity to external resources and enabling VTEP tunneling between racks.

Decisions must be made regarding the location of the Layer 2 and Layer 3 boundaries to support Cloud Foundation on VxRail networking. The NSX-T Tier-0 gateways depend on peering with a router upstream in the physical network using External Border Gateway Protocol (eBGP) to update routing tables in the virtual network.

The VLANs used in Cloud Foundation on VxRail to support the guest virtual machine networks terminate at these upstream routers in the physical network. Therefore, using the route mapping for the applications planned for the VI workload domains drives the decisions for the peering of the NSX-T edge virtual devices in Cloud Foundation, and guides the process for enabling and configuring the adjacent routers in the physical network.

In most cases, routing outside of the virtual network is positioned in either the spine layer or leaf layer. If you deploy a spine-leaf network topology, enabling Layer 3 at either the spine layer or the leaf layer is not required. However, this means Layer 2 traffic must pass through both the leaf and the spine layers to reach the routers. This option is more suitable for small-scale deployments, and it is easy to deploy and configure. It is appealing for sites that have low routing requirements, or the plan is for a small workload.
Establishing the router layer at the spine layer means the uplinks on the leaf layer are trunked ports, and pass through all the required VLANs to the routing services on the spine layer. This topology has the advantage of enabling the Layer 2 networks to span across all the switches at the leaf layer. This topology can simplify VxRail networks that extend beyond one rack because the switches at the leaf layer do not need to support Layer 3 services, and enabling VTEP tunneling between the switches in different racks is not necessary.

A major drawback to this topology is scalability. Ethernet standards enforce a limitation of addressable VLANs to 4094, which can be a constraint in a shared switch layer fabric. Do not select this topology option if your deployment might breach this threshold.

Enabling routing services at the leaf layer is preferred for Cloud Foundation on VxRail deployments. This option overcomes the VLAN limitation imposed by establishing the routing at the spine layer. This option optimizes routing traffic, as it requires the least number of hops for the NSX-T edge virtual devices to peer with an adjacent upstream router. A caveat is that this option does require Layer 3 services to be licensed and configured at the leaf layer. In addition, since Layer 2 networks now terminate at the leaf layer, they cannot span leaf switches. If there is a requirement to extend Layer 2 networks across switches in multiple racks, the best practice is to enable hardware-based (VTEP) tunneling.

The key points to consider for the decisions regarding the network architecture and topology are:

1. Select Ethernet switches that support the features required for Cloud Foundation on VxRail:
   - Border Gateway Protocol: Required for peering with NSX-T edge gateways
   - Unicast: Required for VxRail traffic
   - Multicast: Required for device discovery. Not required if selecting manual device discovery option instead.
Cloud Foundation on VxRail Physical Network Planning

- Jumbo Frames: Required for GENEVE
- Hardware-based tunneling (VTEP): Required to extend Layer 2 traffic over a Layer 3 network at the physical switch layer
- DHCP ‘helper’: Switches that support the DHCP ‘helper’ functionality will ease connecting DHCP services in the data center to the Cloud Foundation on VxRail environment.

2. Decide which physical network layer will support Layer 3 routing services.

VxRail stretched cluster physical network planning

Cloud Foundation on VxRail supports two types of VxRail clusters: one where all nodes are in a single site and a stretched cluster where the nodes are equally distributed between two sites. VxRail stretched cluster is targeted specifically for situations with very high RPO and RTO requirements, and as such includes additional requirements to those for a cluster in a single location.

Note: For full details about VxRail stretched cluster and its requirements, see the Dell EMC VxRail Stretched Cluster Planning Guide.

The foundation for VxRail stretched cluster is based on vSphere vSAN stretched cluster. The basic guidelines for a vSphere vSAN stretched cluster are:

- You must have three physical site locations.
- The VxRail nodes that consist of the stretched cluster instance are spread evenly over two physical sites.
- The third site supports the witness that monitors (using heartbeat) the health of the vSAN datastore that is positioned between the two sites. The required witness is a VMware virtual appliance, so the third site must have a vSphere platform at a supported VCF on VxRail version to support the witness.
- The network between the sites must meet strict latency and bandwidth requirements, since it must support synchronous I/O to vSAN for the running virtual machines in the stretched cluster.
  - 5 millisecond RTT between data node sites
  - 200 millisecond RTT between data node sites and the Witness site
Cloud Foundation on VxRail is supported on a vSphere vSAN stretched cluster as the underlying foundation, and the basic tenets for vSphere stretched cluster are applicable. There are additional networking requirements specific to Cloud Foundation on VxRail.

To ensure connectivity in the event of a site outage, the Cloud Foundation on VxRail networks must be extended across the two sites, and must adhere to specific connectivity requirements.

<table>
<thead>
<tr>
<th>Cloud Foundation on VxRail Networks</th>
<th>Connectivity Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Management</td>
<td>Layer 2</td>
</tr>
<tr>
<td>vSAN</td>
<td>Layer 3</td>
</tr>
<tr>
<td>vMotion</td>
<td>Layer 2 or Layer 3</td>
</tr>
<tr>
<td>Witness vSAN</td>
<td>Layer 3</td>
</tr>
<tr>
<td>NSX-T host overlay network</td>
<td>Layer 3</td>
</tr>
<tr>
<td>NSX-T edge overlay network</td>
<td>Layer 2</td>
</tr>
<tr>
<td>NSX-T edge node uplinks</td>
<td>Layer 2</td>
</tr>
</tbody>
</table>

- Only Layer 2 is supported for the external management network to prevent the need to re-IP the management components at the surviving site.
- vSAN must be routed over a Layer 3 network.
- vMotion can be either Layer 2 or Layer 3.
- The extension of the vSAN network to the third witness site must be routed using a Layer 3 network.
- The NSX-T host overlay network must be routed between sites over a Layer 3 network.
- If the Application Virtual Network is deployed during Cloud Foundation on VxRail, the NSX-T edge overlay network and NSX-T node uplinks must be configured between sites. Layer 2 is supported for these networks.

![Figure 37. One-to-one mapping of witness to VxRail stretched cluster](image)

In addition to providing a third site to support the stretched cluster witnesses, note that a witness can monitor and support only one VxRail stretched cluster. This means that for every VxRail stretched cluster deployed for Cloud Foundation for VxRail, a witness virtual appliance must be deployed.

To support virtual machine network traffic between Cloud Foundation domains, the MTU size must be set to a minimum of 1600 at each site. The MTU size selected must also be configured for traffic destined for the witness site.
If you deploy any Cloud Foundation on VxRail workload domains with stretched clusters as the underlying foundation, the VxRail cluster supporting the management workload domain must also be configured as a stretched cluster. If at some point in the future there is the possibility of a VI workload domain being configured with VxRail stretched clusters, it is best practice to configure the management workload domain on a VxRail stretched cluster at initial deployment. Converting an operational single site VxRail cluster instance to a stretched cluster requires additional planning and preparation as outlined in this section, as well as additional deployment work. The milestones for consideration include:

- Identify a second data center site to host the VxRail nodes to support the stretched cluster.
- Identify a third data center location for the stretched cluster witness.
- Configure the supporting networks in all sites to support VxRail stretched cluster requirements.
- Deploy the witness at the third data center site.
- Deploy additional VxRail nodes in the second data center site to balance with the VxRail nodes in the first data center site.
- Add the additional nodes into the existing VxRail cluster supporting the management workload domain.
- Convert the single site VxRail cluster to a stretched cluster.
This chapter presents the following topics:

Introduction .................................................................................................................. 58
Capture configuration settings for Cloud Foundation on VxRail ......................... 58
VxRail cluster and NSX-T networks leaf switch preparation ................................ 58
DHCP services for NSX-T host overlay network preparation .............................. 60
Application Virtual Network leaf switch preparation ............................................ 62
Layer 3 network preparation ................................................................................... 64
BGP peering preparation ......................................................................................... 65
**Introduction**

This section outlines the tasks that must be undertaken to prepare the data center network for the deployment of Cloud Foundation on VxRail.

**Capture configuration settings for Cloud Foundation on VxRail**

After the data center network architecture is defined and core network requirements are addressed, the next step is to prepare the data center network for the deployment of Cloud Foundation on VxRail. The first step is to capture and record the configuration settings for the deployment of Cloud Foundation on VxRail. Dell-Technologies professional services will work with key stakeholders to capture the required information before moving forward to the network preparation phase.

- The table in Appendix C: Cloud Foundation on VxRail VLANs describes the core VLANs that are required for the initial deployment of Cloud Foundation on VxRail.
- The table in Appendix D: VxRail network configuration describes the configuration settings to deploy a VxRail cluster by VxRail Manager.
- The table in Appendix E: Cloud Builder and management VI workload configuration describes the configuration settings required for an initial deployment of the Cloud Foundation management workload domain.
- The table in Appendix F: Application Virtual Network configuration describes the settings required for Cloud Builder to auto-configure the Application Virtual Network during the initial deployment of the Cloud Foundation management workload domain.
- The table in Appendix G: VI workload domain configuration settings describes the configuration settings required to deploy a standard VI workload domain.

The remaining tasks to prepare the data center network for initial deployment of the Cloud Foundation on VxRail, and move forward with the rest of the workflows, depends on this activity being completed.

**VxRail cluster and NSX-T networks leaf switch preparation**

While the networking requirements for VxRail and Cloud Foundation differ, there is overlap in the sense that Cloud Foundation domains depend on the networking resources enabled by VxRail for connectivity. Therefore, the supporting physical network must be properly designed and configured to support VxRail cluster network traffic, and the additional requirements for Cloud Foundation.
A leaf switch is at the lowest tier in a multi-tier architecture, and often referred to as a ‘top-of-rack’ switch. The VxRail nodes will only connect with a leaf switches in a single rack, with the upper tier switches, known as spine switches, enable multi-rack interconnectivity.

The number of Ethernet ports from each VxRail node you reserve for Cloud Foundation on VxRail networking will drive the configuration process for each switch port connected to a VxRail node port. Starting with Cloud Foundation on VxRail version 4.0.1, up to six ports on each node can be reserved for Cloud Foundation on VxRail networking.

a. In a 2-port configuration, VxRail network traffic and Cloud Foundation network traffic flow through the same pair of Ethernet ports

b. In a 4-port configuration, the VxRail network traffic flows through the first two ports on the network daughter card (NDC). The Cloud Foundation traffic flows either through the other two ports on the NDC, or on two ports on the PCIe expansion card.

c. In a 6-port configuration, the VxRail network traffic flows through the four ports on the NDC, and the Cloud Foundation traffic flows through the two ports on the PCIe expansion card.

If the VxRail network traffic and Cloud Foundation network traffic will be physically separated between the nodes and the leaf switches, the VLANs for VxRail and Cloud Foundation only need to be assigned only to the required switch ports.
The following tasks must be performed in the top-of-rack switches in order to prepare for a VxRail cluster deployment and to prepare to support NSX-T:

1. Select switches with sufficient open ports capacity to connect all the VxRail nodes, connect the inter-switch links between the leaf switches, and connect upstream to the adjacent network layer.

2. Configure at least 1600 MTU to support host overlay network traffic (9000 preferred). A minimum MTU size of 1600 (9000 preferred) must be configured on the leaf switches.

3. Ensure that the port type on the switches (RJ45, SFP+) match the port type on the VxRail nodes.

4. Configure each of the VLANs required for VxRail on the switches.

5. Configure the switch ports to be directly connected to the VxRail nodes as Layer 2 trunk ports.

6. Configure unicast on the VLAN representing the vsAN network.

7. If opting for VxRail automatic device discovery, configure IPv6 multicast on the VLAN representing the VxRail Internal Management network.

8. Configure MLD snooping and MLD querier on the VLAN representing the VxRail Internal Management Network (recommended).

9. Configure Spanning Tree on the switch ports to be directly connected to the VxRail nodes as edge ports, or in 'portfast' mode.

10. If the Layer 2 networks do not terminate at the top-of-rack switches, configure the inter-switch links to allow passage for all VLANs.

11. Configure VLAN for the NSX-T host overlay network on each switch.

12. If a switch port supports both VxRail network traffic and Cloud Foundation/NSX network traffic, configure all the VLANs for VxRail and Cloud Foundation on the switch ports.

13. If a switch port supports only VxRail network traffic or only Cloud Foundation/NSX network traffic, configure only the necessary VLANs on the switch ports.

Each VxRail node has a separate Ethernet port for out-of-band server management called ‘Integrated Dell Remote Access Controller’ (iDRAC). A separate Ethernet switch is recommended to provide connectivity for server maintenance. The server maintenance traffic can also be redirected through the existing network infrastructure. For complete details about VxRail cluster network requirements, see the Dell EMC VxRail Network Planning Guide.

The table in Appendix C: Cloud Foundation on VxRail VLANs lists the individual VLANs that must be configured on the top-of-rack switches. The example switch configuration syntax displayed in Appendix H: Example switch configuration settings offers guidance on how to configure an Ethernet switch with sample VLANs and a sample switch port configuration.

DHCP services for NSX-T host overlay network preparation
Two additional virtual NICs are created on each VxRail node to support the host overlay network during the initial deployment of Cloud Foundation on VxRail. This overlay network uses encapsulation to enable the passage of Layer 2 traffic across transport zones in the VI workload domains with a Layer 3 network. Each virtual NIC supporting the overlay network requires a routable IP address.

You can have these IP addresses input into Cloud Builder and assigned to the NICs during Cloud Foundation on VxRail deployment, or leverage DHCP services for IP address assignment. If your requirements include deploying VxRail stretched clusters to support Cloud Foundation, DHCP is the only supported method for IP address assignment.

1. Prepare a pool of IP addresses that is at least equal to double the number of VxRail nodes planned for the deployment.
2. Deploy a DHCP server in the data center, if necessary.
3. Configure the pool of IP addresses for DHCP services to support the NSX-T host overlay network.
4. Configure the data center network so that NSX-T host overlay network can reach the DHCP server.

![Figure 39. NSX-T host overlay uplinks IP addresses assigned by DHCP](image)

**Note:** If the VLAN cannot be extended out to the DHCP server, enabling ‘DHCP helper’ services on the host overlay VLAN is recommended, if supported on the leaf switches.

![Figure 40. DHCP helper connects DHCP services to host overlay VLAN](image)
Application Virtual Network leaf switch preparation

If the use cases planned for the Cloud Foundation on VxRail VI workload domains include the requirement for the vRealize applications, the leaf switches at the top of each rack must also be configured to support the Application Virtual Network.

1. Configure two VLANs to support the NSX-T edge uplinks.
2. Configure a VLAN to support the NSX-T edge overlay network.
3. The NSX-T edge uplink network and the NSX-T edge overlay network require static IP addresses. Apply Layer 3 settings to the VLANs on the leaf switches representing the NSX-T edge uplink network and the NSX-T edge overlay network.
4. Configure the VLANs on the switch ports that are supporting Cloud Foundation/NSX network traffic.
   a. If two Ethernet ports per node are reserved for Cloud Foundation for VxRail, then VxRail network traffic and Cloud Foundation/NSX network traffic is shared.
   b. For a 4-port and 6-port configuration, VxRail network traffic and Cloud Foundation/NSX network traffic is segmented.
Figure 41. VxRail, NSX-T Overlay and AVN Networks in a 2-port configuration
Layer 3 network preparation

Data center routing services must be configured for the Cloud Foundation on VxRail management networks that require upstream connectivity. The management components in the management workload domain connect upstream using Layer 2 networks. At the Layer 2 and Layer 3 boundary where the VLANs terminate, any networks requiring Layer 3 services must be configured with IP addresses to enable routing.

- The ‘VxRail External Management Network’ must pass upstream through the Layer 2-3 boundary to end users upstream, and connect to required data center services such as DNS and NTP.
- The VxRail nodes connect to the ‘NSX-T Host Overlay Network’. The overlay network must be routable within the Layer 2-3 boundary.
- The NSX-T edge nodes supporting Tier-0 gateway services connect to the ‘NSX-T Edge Overlay Network’. The overlay network must be routable within the Layer 2-3 boundary.
The VI workload domains that can be constructed in a standard architecture after the deployment of the management workload domain must be serviced with routing services upstream. If the use cases for any VI workload domains that include NSX-T based networks, including Application Virtual Networks, Border Gateway Protocol is required on the Layer 2-3 network boundary.

The best practice is to configure Border Gateway Protocol (BGP) services on the Layer 2-3 network boundary before the initial deployment of Cloud Foundation on VxRail, and establish the neighbor relationships upstream to enable connectivity to required data center services and end users, and to the external Dell Technologies and VMware support sites.

### BGP peering preparation

The virtual appliances in the Cloud Foundation management workload domain connect upstream using Layer 2 networks, where routing services in the data center are required at the defined Layer 2 and Layer 3 network boundary. For VI workload domains deployed in Cloud Foundation on VxRail, workload domains connect upstream by peering with external routing services using eBGP. A pair of NSX-T edge devices configured as Tier-0 gateways are deployed for this purpose in the management workload domain for this purpose.

If the Application Virtual Network option is enabled, the NSX-T edge devices are deployed during the Cloud Builder deployment process. The Application Virtual Network is required for the deployment of the vRealize suite of management applications. SDDC Manager depends on this network to download the vRealize Suite Lifecycle Manager and vRealize software packages.

The tables in Appendix F: Application Virtual Network configuration provide guidance on the settings that must be captured to enable BGP peering with the NSX-T Tier-0 gateways for the Application Virtual Network. The guidance provided in this section can be used for BGP peering with another NSX-T Tier-0 gateway for a future VI workload domain.
Figure 44. BGP relationship between NSX-T Edge Gateways and external routers

The NSX-T edge devices must be able to establish an eBGP peer relationship with the upstream routing services. The following tasks must be completed on the upstream switches for peering with the Edge Tier-0 gateways:

1. BGP is configured on each router instance.
   a. Configure BGP with a common Autonomous System Number (ASN) on the network devices targeted for peering with the NSX-T edge gateways.
   b. Configure the IP prefix list to allow passage of all networks between the physical and virtual networks.
   c. Configure the timer ‘keepalive’ value is set to 4.
   d. Configure the timer ‘holdtime’ is set to 12.

2. eBGP peering is configured on each router instance.
   a. Configure the IP address to establish a neighbor relationship with the first NSX-T uplink instance.
   b. Configure the IP address to establish a neighbor relationship with the second NSX-T uplink instance.
   c. Configure a password on the BGP configuration for each external router instance. This password is captured and configured on the adjacent NSX-T Tier-0 gateways.
   d. Configure the internal ASN value configured for the NSX-T Edge gateways on each BGP neighbor configuration on the external router instance.
3. Configure a VLAN on each router instance to match the VLAN assigned to the uplinks on the NSX-T Tier-0 Gateways.

4. Configure a gateway IP address on each router instance for the VLAN assigned to the uplinks on the NSX-T Tier-0 Gateways.

If the AVN option is selected during the deployment of the Cloud Foundation management workload domain, the Cloud Builder process performs the following tasks:

- Two portgroups on the virtual distributed switch in the management workload domain are configured for BGP peering.
- A VLAN is configured on the first portgroup for establishing an uplink with the first external router.
- A VLAN is configured on the second portgroup for establishing an uplink with the second external router.
- An IP address is assigned to the first virtual port on each NSX-T Edge Gateway for BGP peering with the first external router.
- An IP address is assigned to the second virtual port on each NSX-T Edge Gateway for BGP peering with the second external router.
- An ASN (Autonomous System Number) is assigned to the two NSX-T Edge Gateways.
- iBGP (Internal Border Gateway Protocol) is enabled on the Edge Gateways for connectivity with NSX-T logical routing services.
- The configuration information for eBGP peering with the upstream routing services is saved for the NSX-T Edge Gateways.

The sample switch configuration syntax displayed in Appendix H: Sample switch configuration settings provides guidance on how to configure an Ethernet switch for peering with a pair of Edge Gateways.
This chapter presents the following topics:

- Introduction ....................................................................................................... 69
- Prepare for VxRail cluster initial build ............................................................. 69
- Select the VxRail cluster VLANs ...................................................................... 69
- Select the network settings for VxRail cluster ................................................ 70
- Select the network settings for VxRail stretched cluster ............................... 70
- Create forward and reverse DNS entries for VxRail cluster ........................... 71
- Select passwords .............................................................................................. 71
Introduction

Note: Dell Technologies Professional Services will be responsible for the deployment of Cloud Foundation on VxRail per the agreed-upon statement of work. This section provides guidance on what to prepare for during that phase.

In preparation for the deployment of Cloud Foundation on VxRail, Dell Technologies will review a set of prerequisites that must be met for a successful outcome. Dell Technologies will also capture and record the settings and properties required for full deployment of Cloud Foundation on VxRail in your data center.

The data capture process is performed in the following phases:

1. The initial phase focuses on the VxRail clusters that form the resource building blocks for Cloud Foundation. Each Cloud Foundation domain requires at least one VxRail cluster.
2. The next phase captures the settings and properties for layering the Cloud Foundation management workload domain on the first VxRail cluster.
3. The next phase captures the settings and properties for the planning Cloud Foundation VI workload domains.
4. The final phase focuses on the deployment of the NSX virtual networks in the respective Cloud Foundation VI workload domains.

Prepare for VxRail cluster initial build

The initial build operation of a VxRail cluster transforms the physical nodes into a single, managed vSphere cluster with a single vSAN datastore and a single virtual distributed switch. The initial build operation occurs after the following steps are completed:

1. The adjacent top-of-rack switches are configured per VxRail requirements.
2. The VxRail nodes are installed in the racks and cabled to power and network sources.
3. The VxRail nodes are powered on.
4. VxRail performs self-discovery of the powered-on nodes, and starts VxRail Manager for input of settings to perform automated initial build.

Select the VxRail cluster VLANs

Refer to Appendix D: VxRail network configuration for guidance on all the settings that must be collected to perform VxRail cluster automated initial build.

- By default, the external VxRail management network is the native VLAN. Since the typical Cloud Foundation on VxRail deployment has more than one VxRail cluster per rack, it is advisable to select a value other than the native VLAN.
- By default, the internal VxRail management network is 3939. Since the typical Cloud Foundation on VxRail deployment has more than one VxRail cluster per leaf switch pair, it is possible that an existing VxRail Manager will detect the new
powered-on nodes in the rack. It is possible to bypass this discovery process so that the new nodes can be formed into a new cluster. If this is not desirable, a new VLAN can be set for the second and subsequent VxRail clusters. Dell Technologies will change the internal management VLAN on each VxRail node to the recorded value before cluster formation.

- The vSAN and vMotion VLANs should be unique for each VxRail cluster. Using a unique VLAN for vSAN and vMotion removes the possibility of conflicts when multiple VxRail clusters are sharing a set of switches.

Select the network settings for VxRail cluster

Appendix D: VxRail network configuration describes the settings required for VxRail cluster formation and management. The following should be adhered to when selecting these settings:

- Hostnames and IP addresses for VxRail management components are automatically assigned during initial build.
- The IP addresses must be unused and permanent IP addresses. They cannot be assigned by DHCP.
- The IP address assigned to the vCenter instance supporting the VxRail cluster must be on the same subnet as the Cloud Foundation management domain.
- The IP addresses assigned to the remaining VxRail management components must be on the same subnet.
- The NTP and DNS servers must be accessible to the VxRail external management network.

Select the network settings for VxRail stretched cluster

If your plans include the deployment of a VxRail stretched cluster, additional network settings must be captured. The second table Appendix D: VxRail network configuration includes the additional network settings required for VxRail stretched clusters.

Capture the settings to deploy the witness virtual appliance at the third site, which is required before performing initial build of the VxRail stretched cluster.

- Settings for the witness management network
- Settings for the witness vSAN network
- IP address of the vSphere host supporting the witness virtual appliance

Additional network settings need to be captured for the second site. Depending on the decisions made for the stretched cluster deployment, additional network configuration must be performed at the second site:

- Layer 3 network services are required for the VSAN network between sites.
- The vMotion network supports either Layer 2 or Layer 3 networks between the sites.
- A Layer 3 network is required between sites to support NSX-T.
Create forward and reverse DNS entries for VxRail cluster

Using the information captured in Appendix D: VxRail network configuration, create forward and reverse DNS entries for every hostname planned for the VxRail cluster. These include VxRail Manager, vCenter Server, VxRail Platform Service Controller, and each ESXi host in the VxRail cluster.

Select passwords

For VxRail cluster components, a password is required. The password policy follows VMware standards: Minimum of eight characters in length and at least one uppercase character, lowercase character, digit, and special character (example: @!#$%^).
Chapter 12 Prepare for VMware Cloud Foundation Management VI Workload Domain

This chapter presents the following topics:

Introduction ............................................................................................................... 73
Provide a temporary IP address for Cloud Builder ................................................. 73
Select the settings for the management workload domain ..................................... 73
Provide global settings for management VI workload domain ............................ 73
Select the settings for NSX-T host overlay network .............................................. 74
Create Forward and Reverse DNS Entries for the management VI workload domain ........................................................................................................ 74
Select the NSX-T host overlay VLAN .................................................................... 74
Select names for resource pools in VI Management workload domain ............... 75
Select names for portgroups in VI Management workload domain ...................... 75
Prepare passwords .................................................................................................. 75
Obtain VMware license keys .................................................................................. 75
Introduction

To configure the management workload domain, Dell Technologies will follow these steps:

1. Capture and record the settings specific to the Cloud Foundation management VI workload domain and Application Virtual Network in a workbook.
2. Download and deploy the Cloud Foundation Cloud Builder virtual appliance on the VxRail cluster.
3. Upload the settings captured in the workbook for the Cloud Foundation on VxRail to the virtual appliance.
4. Activate the Cloud Builder process. This lays down the management workload domain on top of the VxRail cluster using the uploaded settings.

See Appendix E: Cloud Builder and management VI workload configuration for guidance on all the settings that must be collected for Cloud Builder.

Provide a temporary IP address for Cloud Builder

Deploying the Cloud Builder virtual appliance requires an IP address to be accessible from the VxRail external management network.

Select the settings for the management workload domain

Select the IP subnet for the management workload domain. The IP addresses assigned to the components in the management VI workload domain

- must be on the same subnet.
- must not be in use.
- cannot be assigned by DHCP

Provide global settings for management VI workload domain

Provide the following global settings:

- The IP addresses for the DNS server(s) to support the management VI workload domain. The required forward and reverse entries to support the Cloud Foundation management workload domain must have already been completed.
- The IP addresses for the NTP server(s) to support the management VI workload domain
- The site name for single sign-on (SSO). The site name must be the same as the site name used for the underlying VxRail cluster.
- The domain name and sub-domain name
- Hostname and IP address for the SDDC Manager
• Hostnames and IP addresses for the NSX-T Manager cluster
• Hostnames and IP addresses for the NSX-T edge nodes

Select the settings for NSX-T host overlay network

If you choose to have the IP addresses for the NSX-T host uplinks assigned by CloudBuilder during Cloud Foundation on VxRail deployment, capture and record the following settings:

• A name for this static IP address pool to provide to Cloud Builder
• The IP address range to reserve for the NSX-T host uplinks in CIDR format. The range should be at least double the number of VxRail nodes planned for initial deployment.
• The starting and ending IP addresses for CloudBuilder to assign to the NSX-T host uplinks
• The gateway for the reserved IP address range

If you choose to have the IP addresses assigned dynamically during initial deployment, capture and record the following DHCP settings to support the VTEP tunnel endpoints:

• The IP address of the DHCP server that will supply two IP addresses to each VxRail node for enable connectivity to the host overlay network
• The pool of IP addresses that were configured in the DHCP server for assignment to each VxRail node. Each node requires two IP addresses.

Create Forward and Reverse DNS Entries for the management VI workload domain

Create forward and reverse DNS entries for the Cloud Foundation management VI workload domain. These are the SDDC Manager and the NSX-T Management cluster. If Application Virtual Network is enabled, include the forward and reverse entries for the NSX-T edge nodes.

Select the NSX-T host overlay VLAN

• The NSX-T host overlay VLAN must be configured on the adjacent top-of-rack switches connected to the VxRail nodes.
• The NSX-T host overlay VLAN must pass through the trunk ports connected to the VxRail nodes.
• Depending on where the Layer 2/ Layer 3 boundary is in the supporting physical network, pass the NSX-T host overlay VLAN upstream through the uplinks on the adjacent top-of-rack switches to the spine switch layer.
• IP addresses must be assigned to the switches at the Layer 2/ Layer 3 boundary to enable routing.
• Configure IGMP Snooping and an IGMP Querier on the adjacent top-of-rack switches.

Select names for resource pools in VI Management workload domain

Four resource pools will be created during the build process for the VI management workload domain. A resource pool for management components and edge components will be created for SDDC management and SDDC users. The default names provided for these four resource pools can be customized.

Select names for portgroups in VI Management workload domain

Up to four portgroups will be created during the build process for the VI management workload domain, depending on whether AVN is being configured by Cloud Builder. The default names provided can be customized.

Prepare passwords

A password is required for Cloud Foundation management workload domain components. Like VxRail, the password policy follows VMware standards: Minimum of eight characters in length and at least one uppercase character, lowercase character, digit, and special character (example: @!#$%^).

Obtain VMware license keys

Cloud Foundation on VxRail is deployed with temporary license keys. Permanent license keys must be entered before the expiration of the grace period. Licenses are required for:

• vCenter Server Standard
• ESXi Enterprise Plus (for Management and VI Workload Domains)
• vSphere Add-on for Kubernetes (Required for VI Workload Domains for Kubernetes)
• vSAN Advanced or higher
• NSX-T Data Center Advanced or higher
• vRealize Suite (if vRealize deployed)
• SDDC Manager
Chapter 13 Prepare for Cloud Foundation Application Virtual Network

This chapter presents the following topics:

- **Introduction** ....................................................................................................... 77
- **Select the Application Virtual Network region settings** ............................... 77
- **Select settings for NSX-T edge nodes** .............................................................. 78
- **Select external router settings for eBGP peering** ............................................ 79
- **Select NSX-T Edge overlay network settings** ................................................. 80
- **Select second site settings for stretched cluster** ............................................ 80
Introduction

The Application Virtual Network (AVN) is an optional deployment of the Cloud Foundation performed by Cloud Builder. The requirements for the Application Virtual Network phase are input into Cloud Builder and deployed based on the settings captured in the workbook. The tables in Appendix F: Application Virtual Network configuration represent what must be captured to deploy the Application Virtual Network by Cloud Builder.

Select the Application Virtual Network region settings

Cloud Builder will configure two regions to support the future deployment of the vRealize software on the Cloud Foundation on VxRail platform. ‘Region A’ is a virtual network segment for the vRealize management components that require mobility between regions, whereas ‘xRegion’ is for management components that are assigned to a specific region. The regions must be assigned IP addresses that can pass upstream to end users and connect to external support sites to enable software life cycle management.

Figure 45. AVN Regions and Logical Segments
The table in Appendix F: Application Virtual Network configuration outlines the settings that must be captured and input into Cloud Builder at the time of initial deployment of Cloud Foundation.

Specific details for the deployment and configuration of the vRealize software product is out of scope for this guide. See the VMware documentation VMware Validated Design Documentation for more information.

Select settings for NSX-T edge nodes

The tables in Appendix C: Cloud Foundation on VxRail VLANS outline the VLANs to support the Application Virtual Network. At the time of deployment, Cloud Builder configures two virtual switch portgroups on the virtual distributed switch configured for the VxRail cluster and assign the VLANs for the NSX-T edge appliance uplinks to each portgroup respectively in trunk mode. Cloud Builder will then connect the first NSX-T Edge node uplink to the first portgroup, and the second NSX-T Edge node uplink to the second portgroup.

- Select the VLANs to enable the BGP peering. The selected VLAN will be configured into each NSX-T edge node during Cloud Foundation on VxRail initial deployment.
- The IP address ranges for eBGP peering between the external routers and NSX-T Tier-0 Gateways in CIDR format. Ensure that the selected IP address range is large enough to support future growth of additional NSX-T edge nodes for other VNI workload domains.
- Select the gateway IP addresses to be assigned to the VLAN configured on the upstream adjacent switches. The gateway IP addresses are not required by Cloud Builder, but are required to complete the BGP peering and route sharing process.

![Diagram of NSX-T edge node uplinks](image)

Figure 46. NSX-T edge node uplinks
Select external router settings for eBGP peering

Appendix F: Application Virtual Network configuration captures what is configured on the upstream routers that will peer with the AVN Edge Service Gateways.

- The ASN values are configured on the NSX-T edge nodes during Cloud Foundation on VxRail initial deployment.
- The password is configured on the NSX-T edge nodes during Cloud Foundation on VxRail initial deployment.
- No other BGP settings outside of the default settings are configured on the NSX-T edge nodes during Cloud Foundation on VxRail initial deployment.
- For the first physical router, the receiving IP address selected must be able to send and receive traffic from the NSX-T edge uplink 1.
- For the second physical router, the receiving IP address selected must be able to send and receive traffic from the NSX-T edge uplink 2.

![Figure 47. Network settings for external routing services for eBGP peering]
Select NSX-T Edge overlay network settings

The NSX-T edge nodes must be able to pass network traffic over an edge overlay network. This edge overlay network is separate from the NSX-T host overlay network in that it enables communications between the ESX-T edge nodes only.

- The selected VLAN must be configured on each leaf switch to enable routing over the edge overlay network.
- The selected VLAN is configured into each NSX-T edge node during Cloud Foundation on VxRail initial deployment.
- An IP address from the selected ranges is assigned to each NSX-T edge node to enable connectivity over the NSX-T edge overlay network.

Select second site settings for stretched cluster

If Cloud Foundation is to be deployed on a VxRail stretched cluster, network settings must be captured for the second site. The table for the second site in Appendix F: Application Virtual Network configuration outlines the second set of settings that must be selected.

The underlying networks supporting the VxRail cluster and NSX-T are configured across the two sites in the stretched cluster to enable cross-site connectivity. The logical network switches and routers supporting the Application Virtual Network also extend between the two sites using this cross-site network connectivity. This enables a seamless failover to the surviving site in the event of a single site failure.

![Diagram](Image)

**Figure 48. Transition to surviving site for NSX-T edge devices supporting Tier-0 gateway**
To ensure uninterrupted routing services, the NSX-T edge devices configured as Tier-0 gateways peer with upstream routers in both locations in a stretched cluster deployment.

Figure 49. AVN deployed on a VxRail stretched cluster with two pairs of NSX-T Tier-0 Gateways
This chapter presents the following topics:

**Introduction** ....................................................................................................... 83

**Prepare NSX-T host overlay network** ..................................................................... 83

**Capture settings for VI workload domain** .............................................................. 84

**Prepare for vSphere for Tanzu Workload Domain** .............................................. 84

**Prepare for Multi-Region with NSX-T Federation** .............................................. 86
Introduction

Once a Cloud Foundation on VxRail management workload domain is deployed during the Cloud Builder deployment phase, the cloud platform is ready for the deployment of Cloud Foundation on VxRail VI workload domains. This milestone must be completed before moving forward with any other activities with VI workload domains.

This section provides a basic outline of how to configure a VI workload domain using SDDC Manager and describes the key steps for a deployment of Cloud Foundation with VxRail as the underlying platform.

---

**Note:** Configuring a Cloud Foundation on VxRail management workload domain assigns the VxRail cluster as the underlying resource pool to support virtual machines, and then deploys the basic management components within the domain. Additional steps are required for the buildout of the NSX-based virtual network in the domain.

---

Complete the following tasks to deploy a Cloud Foundation VI workload domain:

1. **Deploy the VI workload domain logical structure from SDDC Manager.**
   
   This task creates the workload domain logical construct in SDDC Manager and deploys a vCenter instance in the management workload domain. This vCenter instance is used to manage all VxRail clusters that are assigned to support the VI workload domain. The IP address assigned to this vCenter instance must be in the same subnet as reserved for the Cloud Foundation management domain.

2. **Deploy at least one VxRail cluster.**
   
   Use the VI workload domain vCenter as the point of management during the initial build of the VxRail cluster.

3. **Add the VxRail cluster(s) to the VI workload domain using SDDC Manager.**

4. **Decide on deploying new NSX-T management resources or use existing NSX-T management resources.**
   
   - For the first VI workload domain, three NSX-T Managers are deployed in the management domain and configured with a virtual IP (VIP).
   - Subsequent VI workload domains can share an existing set of NSX-T Managers or a new set of NSX-T Managers can be deployed.

---

**Prepare NSX-T host overlay network**

Each VI workload domain requires at least one VLAN for the NSX-T host overlay network, and connect to a host overlay network. The VLAN drives the Transport Zone selection the VI workload domain can be a member of.

- Best practice is to configure a new VLAN for each VI workload domain to support the NSX-T host overlay network.
- Applying the same VLAN to each VxRail cluster added to the VI workload domain ensures that all VxRail nodes are members of the host overlay network.
- Follow these tasks for a new VLAN for the NSX-T host overlay network:
Prepare for Cloud Foundation VI Workload Domain

- Configure the VLAN on the adjacent leaf switches providing connectivity to the VxRail nodes.
- Add the VLAN to each trunked port on the adjacent leaf switches providing connectivity to the VxRail nodes.
- Ensure connectivity to a DHCP server supplying the IP addresses for the NSX-T edge uplinks.

Capture settings for VI workload domain

Use the table in Appendix G: VI workload domain configuration settings as a guide for the VI workload domain deployment requirements.

- Each VI workload domain requires a unique name and an organization name.
- Network settings are required for the vCenter instance that is deployed in the management workload domain. Save the network settings for the vCenter instance for the subsequent phase when the VxRail cluster is assigned to the VI workload domain.
- Follow the steps to capture and record the settings for a VxRail cluster. Use the network settings for the vCenter instance from the previous step for the VxRail cluster.
- If a decision is made to deploy a new NSX-T management cluster to support the VI workload domain, then NSX-T edge nodes must be deployed to enable north-south routing services.

Prepare for vSphere for Tanzu Workload Domain

You can use the SDDC Manager in Cloud Foundation on VxRail to deploy a workload domain that will support Tanzu. Tanzu is a full distribution of the open-source Kubernetes container orchestration software that is packaged, signed, and supported by VMware. SDDC Manager will perform the configuration of the workload domain to support a Kubernetes supervisor cluster, and enable all the underlying services to support namespaces on the workload domain resources.

Under this environment, the supervisor cluster uses the services enabled in vSphere to support Kubernetes, and uses the resources provided by the ESXi hosts as worker nodes instead of Linux hosts.

Figure 50. Tanzu Kubernetes services on VI Workload Domain
To prepare for the deployment of a vSphere for Tanzu workload domain using Cloud Foundation on VxRail, ensure that there are enough resources on the planned workload domain to support the planned workload. The Tanzu Kubernetes Grid Service deploys a baseline of virtual appliances on the supervisor cluster to support management activities from a vCenter perspective, which include the creation of namespaces for DevOps. It will also deploy a pair of NSX-T edge appliances to enable connectivity upstream to the NSX-T tier-0 gateway. In addition, each time a namespace is configured by the vSphere administrator, a set of control plane virtual appliances are deployed to enable management access. The table in the appendix Cloud Foundation on VxRail Footprints for Sizing should be used to reserve resources in the supervisor cluster to support management overhead.

Figure 51. vSphere for Tanzu workload domain management components

As part of the deployment process, SDDC Manager will configure a workload network to support connectivity to the Tanzu supervisor cluster, deploy NSX-T load balancers to separate the external and internal networks within the cluster, and deploy an NSX-T tier-1 gateway for ingress and egress access. NAT rules will also be established in NSX-T to enforce the separation of the public and private networks.

Figure 52. Rules for supervisor cluster networks
Prepare for Cloud Foundation VI Workload Domain

The routable management network connects the management components in the supervisor cluster to vCenter, while the workload network uses NSX-T to support traffic to the Kubernetes APIs and to the pods created within the namespaces.

A set of IP address ranges must be reserved for usage by the vSphere for Tanzu workload domain.

- A private IP address pool used to support pods and workloads in a namespace.
- A private IP address pool used by Kubernetes applications for service exposed within the namespace. This pool is assigned to the east-west load balancer within the supervisor cluster.
- A public IP address pool for exposing services outside of the supervisor cluster through the namespace load balancer. Each namespace will get an IP assigned to be used for a NAT rule for external access.
- A public IP address pool for NAT to use for traffic outside of the supervisor cluster.

Prepare for Multi-Region with NSX-T Federation

If your business requirements including supporting Cloud Foundation on VxRail across multiple regions, there are additional preparation steps that are required.

Plan for NSX-T Global Managers

In a multi-region deployment with NSX-T Federation, one region is selected as the global manager for the NSX-T Federation. The NSX-T Local Managers in each region connect with the NSX-T Global Manager in the selected region. The Global Manager provides the administration support for NSX-T global objects across the regions.

You can also configure two regions to support global management to support active/standby failover configuration, but at least one must be selected for this purpose. The size of the virtual machines that must be deployed in the management domain selected for global management depends on the size of the multi-region NSX-T federation. See Cloud Foundation on VxRail Footprints for Sizing for guidance on sizing the virtual machines in the VCF management domain.
This appendix presents the following topics:

Appendix A: Cloud Foundation on VxRail checklist ........................................ 88
Appendix B: Cloud Foundation on VxRail footprints for sizing .................... 92
Appendix C: Cloud Foundation on VxRail VLANs ........................................ 94
Appendix D: VxRail network configuration .................................................. 95
Appendix E: Cloud Builder and management VI workload configuration ..... 97
Appendix F: Application Virtual Network configuration ............................... 99
Appendix G: VI workload domain configuration settings ......................... 100
Appendix H: Sample switch configuration settings ................................... 102
## Appendix A: Cloud Foundation on VxRail checklist

<table>
<thead>
<tr>
<th><strong>Workload Requirements</strong></th>
<th></th>
</tr>
</thead>
</table>
| **Use Cases**             | • Determination of use cases planned for VCF on VxRail integrated platform  
                            | • Determination of application availability requirements for VCF on VxRail integrated platform |
| **Workload Planning**     | • Captured performance metrics from applications targeted for VCF on VxRail integrated platform  
                            | • Completed sizing exercise with Dell-EMC VCF on VxRail sizing tool  
                            | • Converted sizing report into top-level architecture for VCF on VxRail integrated platform |

<table>
<thead>
<tr>
<th><strong>Data Center Requirements</strong></th>
<th></th>
</tr>
</thead>
</table>
| **Rack Space**              | • Calculated data center rack space and power requirements for VCF on VxRail integrated platform  
                            | • Enable redundant power sources for each data center rack. |
| **Data Center Infrastructure** | • Ethernet switch ports compatible with VxRail node ports  
                                   | • Sufficient open ports for VxRail nodes  
                                   | • Jumbo frames enabled on data center network  
                                   | • Ethernet switches supporting VCF on VxRail integrated platform support Unicast and, if applicable, Multicast  
                                   | • Ethernet switches supporting VCF on VxRail integrated platform support Border Gateway Protocol  
                                   | • Ethernet switches supporting VCF on VxRail integrated platform support hardware-based VTEP |
| **Data Center Services**    | • Domain Name Services (DNS) deployed in data center planned for VCF on VxRail integrated platform  
                            | • Network Time Protocol (NTP) services deployed in data center planned for VCF on VxRail integrated platform  
                            | • Active Directory (A-D) configured in data center planned for VCF on VxRail integrated platform (required for certain use cases)  
                            | • Dynamic Host Configuration protocol (DHCP) services configured in data center planned for VCF on VxRail integrated platform. This is not required if using static IP addresses for the host overlay networks.  
                            | • SFTP server for backups for NSX-T and SDDC Manager instances configured in data center planned for VCF on VxRail integrated platform  
                            | • Certificate generation utility (required for certain use cases) |
| **Remote Sites (if applicable)** |  |
| **WAN**                    | • Minimum 10 Mb bandwidth between the central management site and any planned remote workload sites  
                            | • Maximum 50 millisecond latency between the central management site and any planned remote workload sites  
                            | • WAN redundancy enabled between the central management site and any planned remote workload sites  
                            | • Geneve-compatible network between VCF on VxRail management domain instances across regions if NSX-T Federation is planned. |
### Licensing

<table>
<thead>
<tr>
<th>Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server Standard</td>
</tr>
<tr>
<td>ESXi Enterprise Plus (Management and VI Workload Domains)</td>
</tr>
<tr>
<td>ESXi Enterprise Plus for Kubernetes (VI Workload Domains for Kubernetes)</td>
</tr>
<tr>
<td>vSAN Advanced or higher</td>
</tr>
<tr>
<td>NSX-T Data Center</td>
</tr>
<tr>
<td>vRealize Suite (minimum 2019)</td>
</tr>
<tr>
<td>SDDC Manager</td>
</tr>
</tbody>
</table>

### Credentials

- Login credentials for Dell-Technologies support site
- Login credentials for VMware support site

### VCF on VxRail Configuration Settings

<table>
<thead>
<tr>
<th>Reserve VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>One external management VLAN for VxRail Manager, vCenter Server, ESXi, SDDC Manager and other components deployed in management workload domain requiring external access</td>
</tr>
<tr>
<td>One internal management VLAN with IPV6 multicast for VxRail node auto-discovery and device management. The default is 3939. (This VLAN reservation can be bypassed if opting for manual node discovery.)</td>
</tr>
<tr>
<td>One VLAN with IPv4 unicast for vSAN traffic</td>
</tr>
<tr>
<td>One VLAN for vSphere vMotion</td>
</tr>
<tr>
<td>One VLAN for NSX-T Host Overlay network</td>
</tr>
<tr>
<td>One VLAN for the first NSX-T Edge Uplink (if AVN is a requirement)</td>
</tr>
<tr>
<td>One VLAN for the second NSX-T Edge Uplink (if AVN is a requirement)</td>
</tr>
<tr>
<td>One VLAN for the NSX-T Edge Overlay network (if AVN is a requirement)</td>
</tr>
<tr>
<td>One VLAN for IDRAC management of the VxRail nodes</td>
</tr>
<tr>
<td>Licensing</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td><strong>Reserve IP Addresses</strong></td>
</tr>
<tr>
<td>- Determine default gateway and subnet mask.</td>
</tr>
<tr>
<td>- Reserve four or more contiguous IP addresses for VxRail nodes for each VxRail cluster.</td>
</tr>
<tr>
<td>- Reserve one IP address for vCenter Server.</td>
</tr>
<tr>
<td>- Reserve one IP address for VxRail Manager.</td>
</tr>
<tr>
<td>- Decide whether you want to use the default TCP-IP stack for vMotion, or a separate IP addressing scheme for the dedicated vMotion TCP-IP stack.</td>
</tr>
<tr>
<td>- Reserve three or more contiguous IP addresses and a subnet mask for vSphere vMotion.</td>
</tr>
<tr>
<td>- Select the gateway for either the default TCP-IP stack, or the dedicated vMotion TCP-IP stack.</td>
</tr>
<tr>
<td>- Reserve three or more contiguous IP addresses and a subnet mask for vSAN.</td>
</tr>
<tr>
<td>- Reserve IP address for SDDC Manager.</td>
</tr>
<tr>
<td>- Reserve IP addresses for NSX-T Management VIP and appliance nodes.</td>
</tr>
<tr>
<td>- Reserve IP addresses for the first NSX-T Edge Uplink (if AVN is a requirement).</td>
</tr>
<tr>
<td>- Reserve IP addresses for the second NSX-T Edge Uplink (if AVN is a requirement).</td>
</tr>
<tr>
<td>- Reserve IP addresses for the NSX-T Edge Overlay network (if AVN is a requirement).</td>
</tr>
<tr>
<td>- If witness is required for stretched cluster, reserve one IP address for the management network and one IP address for the vSAN network.</td>
</tr>
<tr>
<td>- If NSX-T Federation is a requirement, reserve IP addresses for the remote TEPs on the edge gateways in each region.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reserve Hostnames</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Determine parent and child DNS domains.</td>
</tr>
<tr>
<td>- Decide on your VxRail host naming scheme. The naming scheme is applied to all VxRail hosts.</td>
</tr>
<tr>
<td>- Reserve hostname for vCenter Server</td>
</tr>
<tr>
<td>- Reserve hostname for VxRail Manager</td>
</tr>
<tr>
<td>- Reserve hostname for SDDC Manager</td>
</tr>
<tr>
<td>- Reserve hostnames for NSX-T Management VIP and appliance nodes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Determine password structure following VMware password policy.</td>
</tr>
<tr>
<td>- Select passwords for VxRail management components.</td>
</tr>
<tr>
<td>- Select passwords for NSX-T Data Center.</td>
</tr>
<tr>
<td>- Select passwords for SDDC Manager.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prepare Data Center Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare DNS</strong></td>
</tr>
<tr>
<td>- Configure forward and reverse DNS records for VxRail Manager.</td>
</tr>
<tr>
<td>- Configure forward and reverse DNS records for vCenter Server.</td>
</tr>
<tr>
<td>- Configure forward and reverse DNS records for all VxRail nodes.</td>
</tr>
<tr>
<td>- Configure forward and reverse DNS records for SDDC Manager.</td>
</tr>
<tr>
<td>- Configure forward and reverse DNS records for NSX-T Management Cluster.</td>
</tr>
</tbody>
</table>

| **Prepare DHCP** |
| - Configure IP address scope for NSX-T host overlay network. |

| **Prepare Active Directory** |
| - If a use case for Cloud Foundation on VxRail include vRealize products to support a future VI workload domain, Active Directory must be deployed in the data center to support this requirement. |
## Licensing

<table>
<thead>
<tr>
<th>Prepare Leaf Switches</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Configure at least 1600 MTU (9000 preferred).</td>
<td>• Configure Layer 3 settings on VxRail external management network VLAN.</td>
</tr>
<tr>
<td>• Configure the required VLANs on the top-of-rack switches.</td>
<td>• Configure Layer 3 settings on NSX-T host overlay network.</td>
</tr>
<tr>
<td>• Configure Layer 3 settings on NSX-T edge overlay network (if AVN is a requirement).</td>
<td>• Configure the switch ports to be directly connected to the VxRail nodes as Layer 2 trunk ports.</td>
</tr>
<tr>
<td>• Configure Layer 3 settings on NSX-T host overlay network.</td>
<td>• Configure unicast on the vSAN network.</td>
</tr>
<tr>
<td>• Configure Layer 3 settings on NSX-T edge overlay network (if AVN is a requirement).</td>
<td>• Configure multicast on the VxRail internal management network, if applicable.</td>
</tr>
<tr>
<td>• Configure the switch ports to be directly connected to the VxRail nodes as Layer 2 trunk ports.</td>
<td>• Configure MLD snooping and MLD querier on the VxRail internal management network.</td>
</tr>
<tr>
<td>• Configure Spanning Tree on the switch ports supporting VxRail nodes as edge ports, or in 'portfast' mode.</td>
<td>• Configure inter-switch links on switches below the Layer 2/3 boundary.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prepare Routing Services</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Configure Border Gateway Protocol at the Layer 2/3 network boundary.</td>
<td>• Configure BGP peering with NSX-T Tier-0 Gateway (if AVN is a requirement)</td>
</tr>
</tbody>
</table>
Appendix B: Cloud Foundation on VxRail footprints for sizing

Use these tables to obtain footprint estimates of the resources for Cloud Foundation on VxRail.

Base Virtual Machines for every Cloud Foundation Management workload domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>SDDC Manager</td>
<td>4</td>
<td>16</td>
<td>800</td>
</tr>
<tr>
<td>Management</td>
<td>vCenter</td>
<td>8</td>
<td>24</td>
<td>500</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 1</td>
<td>6</td>
<td>24</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 2</td>
<td>6</td>
<td>24</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 3</td>
<td>6</td>
<td>24</td>
<td>200</td>
</tr>
</tbody>
</table>

Note: NSX-T Manager and NSX-T Edge devices can be deployed in three sizes: Small, Medium, Large. Cloud Builder deploys the ‘Medium’ sized NSX-T Manager virtual appliances into the management workload domain.

Virtual Machines deployed in Cloud Foundation Management workload domain for each Cloud Foundation VI workload domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>vCenter</td>
<td>8</td>
<td>24</td>
<td>500</td>
</tr>
</tbody>
</table>

Virtual Machines deployed in Cloud Foundation VI Workload Domain to support the Application Virtual Network. The default size is ‘Medium’.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workload</td>
<td>NSX-T Edge 1</td>
<td>4</td>
<td>8</td>
<td>120</td>
</tr>
<tr>
<td>Workload</td>
<td>NSX-T Edge 2</td>
<td>4</td>
<td>8</td>
<td>120</td>
</tr>
</tbody>
</table>

Virtual Machines deployed in Cloud Foundation Management workload domain for each Cloud Foundation VI workload domain which does not use a shared NSX-T management instance. The default size is ‘Large’.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>NSX-T Manager 1</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 2</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 3</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
</tbody>
</table>

Virtual Machines deployed in Cloud Foundation Management workload domain for each Cloud Foundation VI workload domain for Kubernetes which does not use a shared NSX-T management instance. The default size is ‘Large’.
<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>NSX-T Manager 1</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 2</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Manager 3</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
</tbody>
</table>

Virtual Machines deployed in one of the Cloud Foundation Management workload domains to support NSX-T Federation across regions. The size of the virtual machines depends on the size of the federation under management, either Medium or Large.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>NSX-T Global Manager 1</td>
<td>6/12</td>
<td>24/48</td>
<td>300</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Global Manager 2</td>
<td>6/12</td>
<td>24/48</td>
<td>300</td>
</tr>
<tr>
<td>Management</td>
<td>NSX-T Global Manager 3</td>
<td>6/12</td>
<td>24/48</td>
<td>300</td>
</tr>
</tbody>
</table>

The following table lists the sizing to prepare for a vRealize Suite Lifecycle Manager download and deployment.

**Note**: Cloud Foundation on VxRail does not automate the deployment or the life cycle management of the other vRealize Suite components. vRealize Suite Lifecycle Manager is used to deploy and manage those components.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>vRealize Suite Lifecycle Manager</td>
<td>4</td>
<td>16</td>
<td>135</td>
</tr>
</tbody>
</table>

The following table lists the sizing to prepare for the deployment of vSphere with Tanzu workload domain.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Component</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workload</td>
<td>Supervisor Cluster control plane</td>
<td>12</td>
<td>48</td>
<td>200</td>
</tr>
<tr>
<td>Workload</td>
<td>Registry Service</td>
<td>7</td>
<td>7</td>
<td>200</td>
</tr>
<tr>
<td>Workload</td>
<td>NSX-T Edge 1</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Workload</td>
<td>NSX-T Edge 2</td>
<td>8</td>
<td>32</td>
<td>200</td>
</tr>
<tr>
<td>Workload</td>
<td>Tanzu Kubernetes Cluster control plane</td>
<td>6</td>
<td>12</td>
<td>48</td>
</tr>
<tr>
<td>Workload</td>
<td>Tanzu Kubernetes Cluster worker nodes</td>
<td>6</td>
<td>12</td>
<td>48</td>
</tr>
</tbody>
</table>
Appendix C: Cloud Foundation on VxRail VLANs

These are the core VLANs that must be configured on the data center switches supporting the Cloud Foundation on VxRail platform Cloud Foundation on VxRail VLANs.

<table>
<thead>
<tr>
<th>Category</th>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>External Management</td>
<td>VxRail cluster and ESXi hosts</td>
</tr>
<tr>
<td></td>
<td>Internal Management</td>
<td>VxRail device discovery</td>
</tr>
<tr>
<td></td>
<td>vMotion</td>
<td>Virtual machine migration</td>
</tr>
<tr>
<td></td>
<td>vSAN</td>
<td>vSphere datastore</td>
</tr>
<tr>
<td>NSX-T</td>
<td>Host Overlay</td>
<td>NSX-T VTEP. Must be able to reach DHCP server to assign IP addresses for host overlay network.</td>
</tr>
<tr>
<td>Node Management</td>
<td>Out-of-band management</td>
<td>Dell PowerEdge iDRAC network (optional)</td>
</tr>
</tbody>
</table>

Application Virtual Network VLANs – required if Application Virtual Network is enabled.

<table>
<thead>
<tr>
<th>Category</th>
<th>VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Virtual Network</td>
<td>Uplink 1</td>
<td>NSX-T Tier-0 gateway uplink. Used for BGP peering with upstream routing services.</td>
</tr>
<tr>
<td></td>
<td>Uplink 2</td>
<td>NSX-T Tier-0 gateway uplink. Used for BGP peering with upstream routing services.</td>
</tr>
<tr>
<td></td>
<td>Edge Overlay</td>
<td>Used for edge overlay network connecting NSX-T edge nodes used for Tier-0 gateways</td>
</tr>
</tbody>
</table>
## Appendix D: VxRail network configuration

The following table lists the configuration settings required by VxRail Manager to deploy a VxRail cluster.

<table>
<thead>
<tr>
<th>Category</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VxRail</td>
<td>External Management</td>
<td>VLAN ID for the management network that passes upstream from the top-of-rack switches</td>
</tr>
<tr>
<td></td>
<td>Internal Management</td>
<td>VLAN ID for VxRail device discovery. This network stays isolated on the top-of-rack switches. The default VLAN ID is 3939.</td>
</tr>
<tr>
<td>System</td>
<td>Global settings</td>
<td>Time zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NTP server(s) IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS server(s) IP Address</td>
</tr>
<tr>
<td>Management</td>
<td>ESXi hostnames and IP addresses</td>
<td>ESXi hostname prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Separator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iterator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Offset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suffix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starting IP address for VxRail node pool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ending IP address for VxRail node pool</td>
</tr>
<tr>
<td>vCenter Server</td>
<td></td>
<td>VxRail vCenter Server hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VxRail vCenter Server IP address</td>
</tr>
<tr>
<td>VxRail Manager</td>
<td></td>
<td>VxRail hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VxRail IP address</td>
</tr>
<tr>
<td>Networking</td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>vMotion</td>
<td>Starting address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ending address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID</td>
<td></td>
</tr>
<tr>
<td>vSAN</td>
<td>Starting address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ending address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID</td>
<td></td>
</tr>
<tr>
<td>VM Networks</td>
<td>Minimum 1.</td>
<td>VM Network name and VLAN ID</td>
</tr>
<tr>
<td>Category</td>
<td>Detail</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dell Node</td>
<td>iDRAC</td>
<td>IP address for iDRAC port on each VxRail node</td>
</tr>
</tbody>
</table>

The following table applies to stretched clusters only.

<table>
<thead>
<tr>
<th>Category</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Witness</td>
<td>Management</td>
<td>Hostname</td>
</tr>
<tr>
<td>VSAN</td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Witness Site</td>
<td>vSphere Host</td>
<td>IP Address</td>
</tr>
<tr>
<td>Network</td>
<td>Witness Traffic Separation</td>
<td>Optional VLAN ID to manage traffic between two sites hosting VxRail nodes and witness site</td>
</tr>
<tr>
<td>Second Site</td>
<td>vMotion</td>
<td>Starting address for IP pool</td>
</tr>
<tr>
<td></td>
<td>Ending address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID</td>
<td></td>
</tr>
<tr>
<td>VSAN</td>
<td>Starting address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ending address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID</td>
<td></td>
</tr>
<tr>
<td>VXLAN</td>
<td>Starting address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ending address for IP pool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID</td>
<td></td>
</tr>
</tbody>
</table>
Appendix E: Cloud Builder and management VI workload configuration

This table lists the configuration settings that are required by Cloud Builder to deploy the Cloud Foundation management workload domain on the VxRail cluster platform.

<table>
<thead>
<tr>
<th>Category</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Builder</td>
<td>IP Address</td>
<td>Temporary for Cloud Builder virtual appliance</td>
</tr>
<tr>
<td>Global</td>
<td>NTP</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td>SSO Site Name</td>
<td>Must be the same site name as used for the VxRail cluster.</td>
</tr>
<tr>
<td></td>
<td>SSO Domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Zone Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP Server</td>
<td>IP address of DHCP server to assign IP addresses to VTEP tunnel endpoints for host overlay network</td>
</tr>
<tr>
<td></td>
<td>DHCP IP address range</td>
<td>Range of IP addresses in DHCP server to be assigned to VTEP tunnel endpoints for host overlay network</td>
</tr>
<tr>
<td>SDDC</td>
<td>Manager</td>
<td>Hostname</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain Name</td>
<td></td>
</tr>
<tr>
<td>NSX-T</td>
<td>Manager (VIP)</td>
<td>Hostname</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Manager Node 1</td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Manager Node 2</td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Manager Node 3</td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Appliance Size</td>
<td></td>
<td>(Small, Medium, Large)</td>
</tr>
<tr>
<td>NSX-T Host Overlay Network</td>
<td>Static IP Assignment Method</td>
<td>Name of static IP address pool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP address range in CIDR format</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Starting IP address to be assigned for host overlay network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ending IP address to be assigned for host overlay network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway</td>
</tr>
<tr>
<td></td>
<td>Dynamic IP Assignment Method</td>
<td>IP address of DHCP server to assign IP addresses to VTEP tunnel endpoints for host overlay network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range of IP addresses in DHCP server to be assigned to VTEP tunnel endpoints for host overlay network</td>
</tr>
<tr>
<td>Category</td>
<td>Detail</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vSphere Objects</td>
<td>Data Center Name</td>
<td>Default: ‘VxRail-DataCenter’. Must match value used in VxRail cluster.</td>
</tr>
<tr>
<td></td>
<td>Cluster Name</td>
<td>Default: ‘VxRail-Virtual-SAN-Cluster’. Must match value used in VxRail cluster.</td>
</tr>
<tr>
<td></td>
<td>Distributed Switch Name</td>
<td>Must match value used in VxRail cluster</td>
</tr>
<tr>
<td></td>
<td>vSAN Datastore Name</td>
<td>Default: ‘VxRail-Virtual-SAN-Datastore’. Must match value used in VxRail cluster.</td>
</tr>
<tr>
<td>vSphere Resource Pools</td>
<td>SDDC Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDDC Edge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Edge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User VM</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix F: Application Virtual Network configuration

This table lists the configuration settings required to support deployment of the Application Virtual Network by Cloud Builder during initial deployment.

<table>
<thead>
<tr>
<th>NSX-T Edge Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cluster</strong></td>
</tr>
<tr>
<td><strong>Internal ASN</strong></td>
</tr>
<tr>
<td><strong>Edge Node 1</strong></td>
</tr>
<tr>
<td>Management IP Address</td>
</tr>
<tr>
<td>Uplink 1 IP Addresses</td>
</tr>
<tr>
<td>Uplink 2 IP Addresses</td>
</tr>
<tr>
<td>Overlay IP Address</td>
</tr>
<tr>
<td><strong>Edge Node 2</strong></td>
</tr>
<tr>
<td>Management IP Address</td>
</tr>
<tr>
<td>Uplink 1 IP Addresses</td>
</tr>
<tr>
<td>Uplink 2 IP Addresses</td>
</tr>
<tr>
<td>Overlay IP Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External ASN</strong></td>
</tr>
<tr>
<td><strong>External Router 1</strong></td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td><strong>External Router 2</strong></td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Virtual Network Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Region A</strong></td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
</tr>
<tr>
<td><strong>xRegion</strong></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second Site - External Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External ASN</strong></td>
</tr>
<tr>
<td><strong>External Router 1</strong></td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td><strong>External Router 2</strong></td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>
## Appendix G: VI workload domain configuration settings

This table lists the configuration settings required to support the configuration of a standard VI workload domain by SDDC Manager.

<table>
<thead>
<tr>
<th>Category</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Domain Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization Name</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>vCenter</td>
<td>Hostname</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Account</td>
<td></td>
</tr>
<tr>
<td>NSX-T Host Overlay Network</td>
<td>VLAN</td>
<td>NSX-T VTEP. Must be able to reach DHCP server to assign IP addresses for host overlay network.</td>
</tr>
<tr>
<td></td>
<td>DHCP Server</td>
<td>IP address of DHCP server to assign IP addresses to VTEP tunnel endpoints</td>
</tr>
<tr>
<td></td>
<td>DHCP IP addresses</td>
<td>Range of IP addresses in DHCP server to be assigned to VTEP tunnel endpoints</td>
</tr>
</tbody>
</table>

Use this table only if a new NSX-T management cluster and a new NSX-T Tier-0 gateway is deployed as part of the VI workload domain.

<table>
<thead>
<tr>
<th>Category</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX-T Manager</td>
<td>NSX-T management cluster</td>
<td>IP address of NSX-T Manager VIP</td>
</tr>
<tr>
<td></td>
<td>IP address for first NSX-T Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address for second NSX-T Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP address for third NSX-T Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default Gateway</td>
<td></td>
</tr>
<tr>
<td>NSX-T Edge Uplink 1</td>
<td>VLAN</td>
<td>Used for BGP peering with upstream routing services</td>
</tr>
<tr>
<td>NSX-T Edge Uplink 2</td>
<td>VLAN</td>
<td>Used for BGP peering with upstream routing services</td>
</tr>
<tr>
<td>NSX-T Edge Overlay Network</td>
<td>VLAN</td>
<td>Used for edge overlay network connecting NSX-T edge nodes used for Tier-0 gateways</td>
</tr>
</tbody>
</table>

Use this table only if a vSphere for Tanzu supervisor cluster will be configured on the VI workload domain.

<table>
<thead>
<tr>
<th>Detail</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod CIDRs</td>
<td>Internal</td>
<td>Used by Kubernetes pods that run in the cluster</td>
</tr>
<tr>
<td>Service CIDRs</td>
<td>Internal</td>
<td>Used by Kubernetes applications that need a service IP address</td>
</tr>
<tr>
<td>Detail</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Ingress CIDRs</td>
<td>External</td>
<td>Used for load balancing</td>
</tr>
<tr>
<td>Egress CIDRs</td>
<td>External</td>
<td>Used for NAT endpoint use</td>
</tr>
</tbody>
</table>
Appendix H: Sample switch configuration settings

This set of sample syntax is for providing basic guidance on the settings that must be performed on the top-of-rack switches to configure VLANs and a switch port for a Cloud Foundation on VxRail deployment, and configuring a switch support BGP peering for the Application Virtual Network (AVN). The actual code that is required on the top-of-rack switches depends on the existing data center network infrastructure, switch operating system and routing standards.

The sample syntax highlights the following required items:

- VLAN for VxRail external management
- VLAN for VxRail internal management – node discovery
- VLAN for NSX-T host overlay network – with dhcp helper
- Switch port configuration for VxRail node

```
interface vlan <VxRail External Management>
  no shutdown
  ip address <gateway>/24
  vrrp-group <id>
  priority <priority>
  virtual-address <virtual gateway>

interface vlan <VxRail Internal Management>
  no shutdown
  ipv6 mld snooping querier

interface <Host Overlay>
  description
  no shutdown
  mtu 9216
  ip address <gateway>/24
  ip helper-address <DHCP server IP Address>
  vrrp-group <id>
  priority <priority>
  virtual-address <virtual gateway>

interface ethernet <port>
  no shutdown
  switchport mode trunk
  switchport access vlan <native vlan>
```
The sample syntax highlights the following required items:

- VLANs for AVN uplinks with assigned IP addresses
- Prefix list to permit route filtering for routes from the AVN
- BGP External ASN setting
- BGP peering with the pair of AVN Edge Service Gateways

```plaintext
interface vlan <VLAN for AVN Uplink 1>
   no shutdown
   mtu 9216
   ip address <Gateway IP address for AVN uplink 1>

interface vlan <VLAN for AVN Uplink 2>
   no shutdown
   mtu 9216
   ip address <Gateway IP address for AVN uplink 2>

ip prefix-list <Router-ESGs route map name> permit <IP address range parameters>

router bgp <External ASN>
   maximum-paths ebgp 4
   router-id <External router ID>
   address-family ipv4 unicast
   redistribute connected route-map <Router-ESG route map name>

template external-router-to-ESG
   advertisement-interval <value>
   password <password saved to Edge Gateways>
   timers 4 12

   neighbor <IP address assigned to first Edge Gateway>
      inherit template external-router-to-ESG
      remote-as <ASN assigned to Edge Gateways>
      no shutdown

   neighbor <IP address assigned to second Edge Gateway>
      inherit template external-router-to-ESG
      remote-as <ASN assigned to Edge Gateways>
      no shutdown
```