Dell EMC VxBlock™ System 1000 with VMware Cloud Foundation 4.1

Architecture Overview

May 2021
Rev. 2

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Revision history....4

Chapter 1: Introduction....5

Chapter 2: VMware Cloud Foundation overview....6
VMware Cloud Foundation deployment....6
VMware Cloud Foundation components....7

Chapter 3: VxBlock System 1000 with VMware Cloud Foundation....8

Chapter 4: Management domain architecture....10
Physical and logical architecture....10
Network infrastructure....11
Network topology....11
Virtual infrastructure design....12
Default VLANs, port groups, and VMs....16
Scalability....18
VxBlock System multisystem management....18
Integrated Data Protection....20

Chapter 5: VI workload domain architecture....22
VI workload domain configurations....22
Cisco UCS architecture....22
Network standards....23
Virtual network segments....23
Default VLANs....24
VMware NSX-T instance deployment topologies....25
VMware NSX-T instance topologies without virtual network segments....25
VMware NSX-T instance topologies with virtual network segments....26
VMware NSX-T Edge host topologies with virtual network segments....29

Revision history

Date	Document revision	Description of changes
May 2021	2	Updated Default VLANs, port groups, and VMs.
March 2021	1	Initial version.

1

Introduction

VMware Cloud Foundation (VCF) 4.1 is an integrated platform that bundles compute, storage, and network virtualization products into a VMware validated, design (VVD) solution.

This guide provides an overview of VCF with the VxBlock System 1000 and AMP Central with VMware vSAN storage. VCF is supported with VMware vSphere 7.0 and later.

Audience

The target audience for this guide includes VxBlock 1000 administrators, Dell Technologies Sales Engineers, and field consultants.

The document assumes that the audience is familiar with the following components:

- VMware Cloud Foundation
- VxBlock 1000
- AMP Central with VMware vSAN
- VMware virtualization technologies

References

Go toVMware Docs for information on:

- VCF
- VMware vRealize Network Insight
- VMware vRealize and vCloud Suite

The Glossary provides terms, definitions, and acronyms related to Dell Technologies.

2

VMware Cloud Foundation overview

VMware Cloud Foundation (VCF) provides an integrated software-defined data center (SDDC) stack that combines core infrastructure virtualization components. VCF provides a platform for traditional enterprise and cloud-based applications with access to automatic deployment options across the private and public cloud.

VCF provides the following features for a VxBlock System 1000 with VMware vSphere 7.0 and AMP Central with VMware vSAN:

- Manages workloads on-site or in the cloud by extending the same infrastructure, operations, tools, and processes.
- Provides automated delivery including compute, storage, networking, and management tools.
- Ensures enterprise-level security with the full-stack platform that consolidates traditional VM and modern container workloads.
- Faster deployments, automated configurations, and comprehensive management solutions for the VxBlock System and AMP Central from day 0 to 2.

VCF is available in multiple editions depending on the integrated components. See VCF 4 Edition Matrix for more information. VMware professional services deploys VMware vRealize Suite components.

You can add software components that meet the compatibility requirements. The VCF edition provides the appropriate licenses for each component, except for the VMware vCenter Server. Obtain a separate VMware vCenter Server license to deploy multiple copies of VMware vSphere vCenter on the management and VI workload domain. You can obtain your VMware vCenter license from VMware or Dell Technologies.

VMware Cloud Foundation deployment

VMware Cloud Foundation (VCF) provides the deployment of the management domain and the virtual infrastructure (VI) workload domain.

A VCF workload domain combines VMware vSphere compute, network, and storage resources into a single, consumable entity. The management domain hosts the management workload to support VCF, and the VI workload domain supports external business workloads. A single VCF instance supports one management domain and up to 14 VI workload domains.

Management domain

VCF uses the management domain to combine VMware vSphere, VMware vSAN, and VMware NSX-T Data Center to provide a standardized VVD architecture. The management domain is a cluster of physical hosts that contain management VMs and applications. VCF requires four or more medium or large AMP Central servers to deploy VCF. VMware Cloud Builder deploys the management domain onto AMP Central with VMware vSAN in an integrated or stand-alone configuration. Once the management domain is deployed, VMware SDDC Manager can deploy and manage the VI workload domains.

VI workload domain

VMware SDDC Manager provisions each VI workload domain and any associated VMware vSphere clusters. The VI workload domain contains clusters of up to 96 physical hosts. A dedicated VMware vCenter Server manages the physical hosts in the clusters. VMware SDDC Manager automates day 0 to 2 tasks such as create, expand, or delete a VI workload domain. VCF supports up to 14 workload domains on the VxBlock System. VMware SDDC Manager also provisions private cloud resources on the VxBlock 1000 and monitors changes to the logical infrastructure. VMware SDDC Manager also adds life cycle management automation. Each release of VCF includes a VCF software BOM with BOM are interoperable components that align to the VxBlock 1000 or AMP Central VCF RCM.

VCF supports the optional deployment of VMware NSX-T Data Center with virtual network segments in the management and VI workload domains. Virtual network segments are VMware NSX-T overlay-backed segments in the management and workload domains. Virtual networks segments are required for VMware NSX-T Data Center to support VMware vRealize Suite.

VMware tests all VCF components for interoperability and bundles them for downloads and installation. In addition, VMware SDDC Manager provides the installation order for management and workload domains with associated VMware ESXi clusters. Once VMware SDDC manager is deployed, VMware Cloud Builder is no longer used.

VMware Cloud Foundation components

VMware Cloud Foundation (VCF) contains components that serve as the software stack for software-defined services.

The following table shows software-defined services for the VCF software stack:

Software stack	Software-defined services
Storage	VMware vSAN, vVols, and VMFS on FC
Network	VMware NSX-T Data Center
Compute	VMware vSphere and VMware vCenter Server
Security and cloud management	VMware vRealize Suite (optional VMware professional services installed components)

The following table provides an overview of VCF components:

Component	Description
VMware Cloud Builder	Deploys the management domain onto AMP Central and automates the deployment of the VCF.
VMware SDDC Manager	Deployed by VMware Cloud Builder to automate the configuration, provision, and upgrade the day-to day management and operations. VMware SDDC Manager automatically deploys VI workload domains onto the VxBlock 1000.
VMware vSphere VMware ESXi VMware vCenter Server	Transforms data centers into aggregated infrastructures that include CPU, storage, and networking resources into a unified operating environment. VMware vSphere provides administration tools for your data centers.
VMware vSAN	Required for the deployment of the management domain. Aggregates local or direct attached storage to create a single storage pool. Multiple storage policies are supported.
VMware NSX-T Data Center	Provides networking, security, automation, and operational management. VMware NSX-T instance is required in the management domain and at least one workload domain.
VMware vRealize Suite	Delivers and manages infrastructure and applications for public and private clouds, multiple hypervisors, and physical infrastructure. The optional VMware vRealize Suite contains the following components: ● VMware vRealize Log Insight ● VMware vRealize Automation ● VMware vRealize Operations Manager Virtual networks segments are required for VMware NSX-T Data Center to support VMware vRealize Suite. The virtual networks segments must be configured consistently across the management and VI workload domains. Virtual network segments can be configured as part of the initial deployment of VCF. Otherwise, engage with VMware Professional Services to deploy the VMware NSX-T Data Center with virtual networks segments.

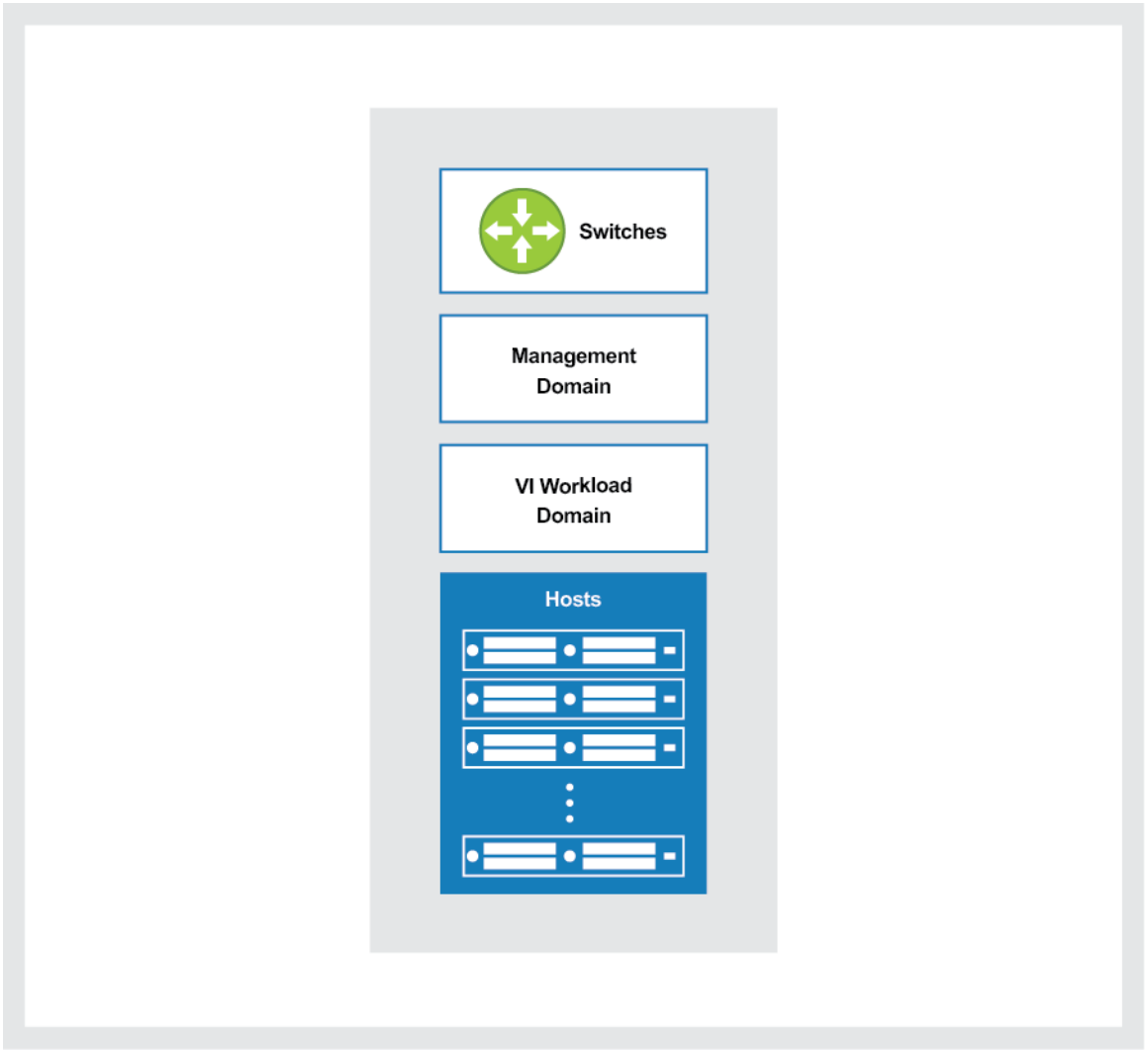
VMware tests all VCF components for interoperability and bundles them for downloads and installation. VMware SDDC Manager provides the installation order for management and workload domains with associated VMware ESXi clusters.

3

VxBlock System 1000 with VMware Cloud Foundation

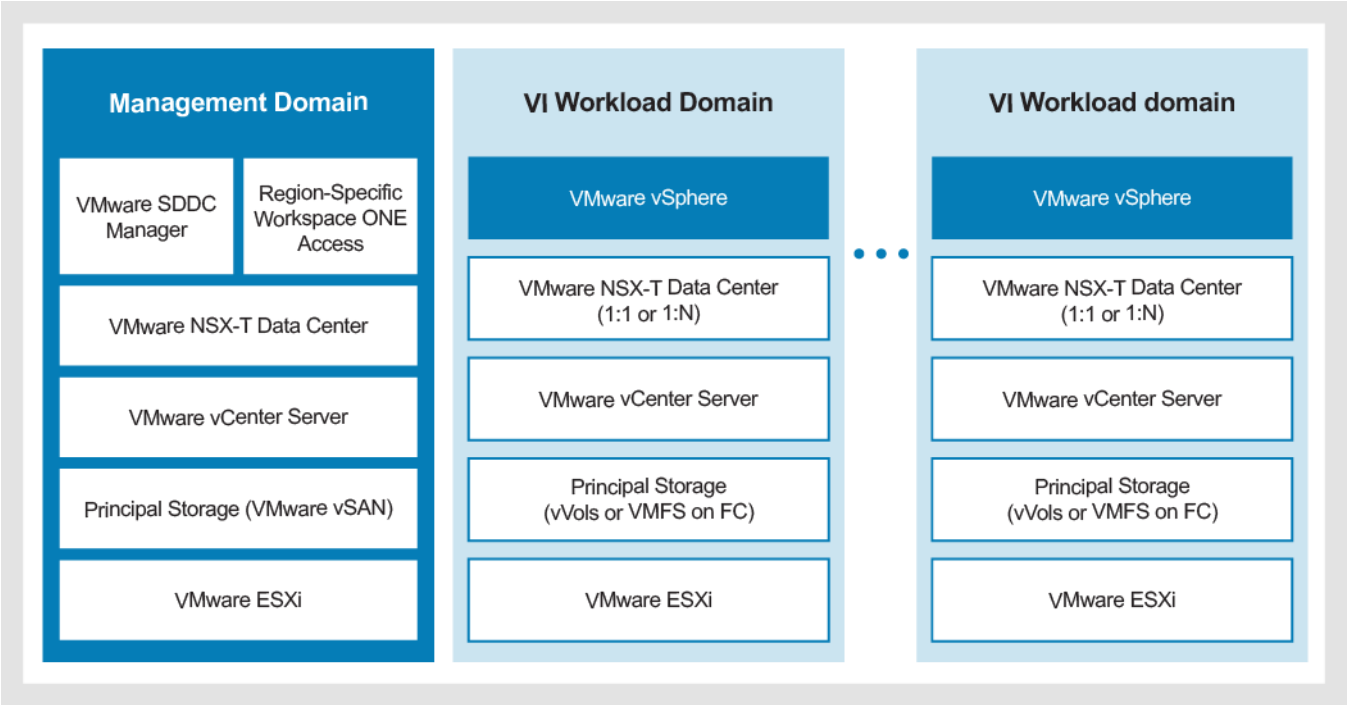
VCF on the VxBlock System supports up to 14 VI workload domains. Each workload domain has a dedicated VMware vCenter Server that supports multiple clusters. The VI workload domain in the VxBlock 1000 supports multiple storage arrays using vVols on FC or VMFs on FC datastores.

The following figure shows a VxBlock 1000 with VCF architecture:



Deploy the VMware NSX-T physical edge cluster for the first VI workload domain deployed with VMware NSX-T Data Center if virtual network segments are used. Subsequent VI workload domains can share the same VMware NSX-T physical edge cluster, or you can deploy an additional VMware NSX-T physical edge cluster. VCF uses VVD standardized architectures and configures the management and production VMware vCenter Server with VMware Embedded Link Mode.

The following figure shows the logical components of a VMware SDDC deployment that is based on the standard VCF architecture:


Management Domain
VMware SDDC Manager
Region-Specific Workspace ONE Access
VMware NSX-T Data Center
VMware vCenter Server
Principal Storage (VMware vSAN)
VMware ESXi
VI Workload Domain
VMware vSphere
VMware NSX-T Data Center (1:1 or 1:N)
VMware vCenter Server
Principal Storage (vVols or VMFS on FC)
VMware ESXi
VI Workload domain
VMware vSphere
VMware NSX-T Data Center (1:1 or 1:N)
VMware vCenter Server
Principal Storage (vVols or VMFS on FC)
VMware ESXi

4

Management domain architecture

The management domain is a cluster of physical hosts that contain the management component VMs.

A region is a single instance of VCF that contains a separate VMware SDDC instance for VCF high availability. An availability zone in the management domain is a collection of infrastructure components. Each zone is isolated to prevent failure propagation or an outage that spans a data center. The management domain provides a single availability zone to protect against failure of individual hosts.

VMware vSphere runs a dedicated VMware vCenter Server in the management domain with VMware vSAN storage. The management domain hosts VMware SDDC Manager, VMware NSX-T Managers, and AMP Central. If virtual network segments are used, two VMware NSX-T Edge node VMs connect the VMware NSX-T virtual network and the physical network components.

Before you deploy the management domain, size AMP Central with the following considerations:

- Core, optional, ECO workloads
- Optional VMware vRealize Suite products and CPU and memory requirements, and associated reservations
- Storage requirements

Physical and logical architecture

The physical and logical topology of AMP Central aligns with the physical and logical requirements of VCF. See the Release Certification Matrix (RCM) for the supported VCF release.

The following table provides a breakdown of the hardware and software components for AMP Central with VCF:

Resource	Components
Compute	4-16 Cisco UCS C220 M5 Servers VMware vSAN Ready Node AF-6 alignment
Virtualization	The VMware VCF BOM includes the following required components: • VMware Cloud Builder VM • VMware SDDC Manager • VMware vCSA • VMware ESXi • VMware vSAN • VMware NSX-T Data Center • VMware vSphere 7.0
Storage	VMware vSAN
Network	• Cisco Nexus 31108TC-V Switch • Cisco Nexus 9336C-FX2 Switch
VxBlock System management	• Secure Remote Services • PowerPath Management Appliance • Windows Server Embedded Standard Edition • Core, Optional, and Ecosystem workloads

See the *Dell EMC AMP Central Product Guide* for compute hardware configurations for AMP Central with VMware vSAN.

Network infrastructure

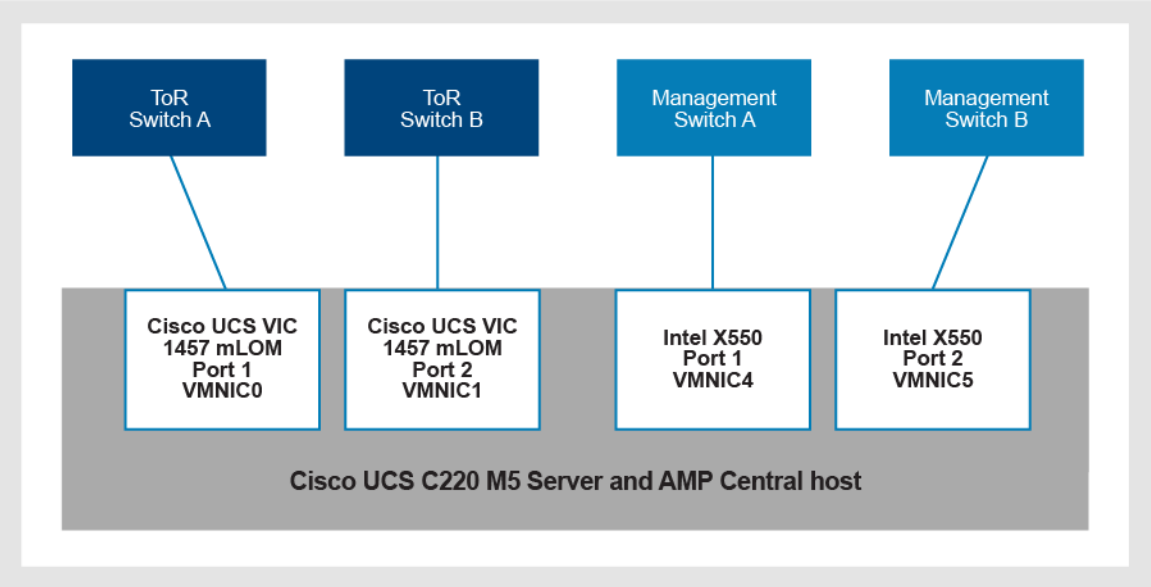
The stand-alone AMP Central uses dedicated management and ToR Cisco Nexus switches. An integrated AMP Central shares the ToR and management switches between VCF servers and the VCF resources.

The following table shows the specifications for AMP Central with VCF switches:

Switch	Specifications
Cisco Nexus ToR	Cisco UCS VIC 1457 Quad Port 10 Gb or 25 Gb SFP28 mLOM
Cisco Nexus management	Intel X550T Dual Port 10GBase-T LOM

The ToR switch uses 100 GbE QSFP breakout transceivers to provide connectivity for the Cisco UCS VIC server. The ToR switch ports support up to four 25 GbE connections. By default, two transceivers per switch connect a minimum of four servers. Two servers are configured per switch port using two breakout cables per transceiver.

The following figure shows physical connectivity for an AMP Central ready node:



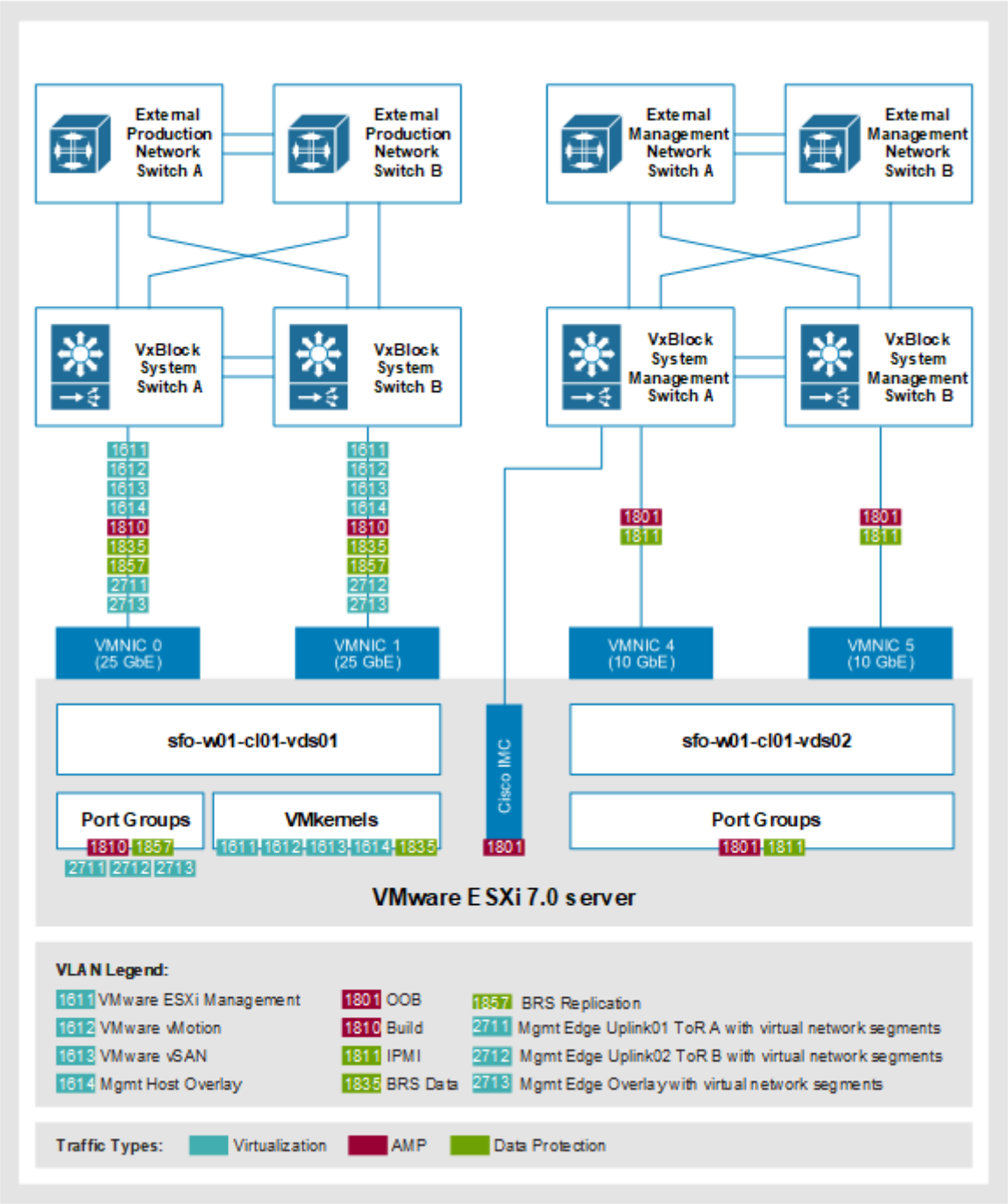
Network topology

The VCF topology aligns to the VCF domain network architecture that is based on the VMware validated design (VVD).

The VCF topology builds upon the AMP Central network topology and includes two VMware VDS. If optional VMware vRealize Suite components are to be used, the management domain deployment must include virtual network segments.

The VMware NSX-T Manager cluster is built in the management domain and consists of three VMs with an associated VIP. The VMware NSX-T host overlay network requires an additional VLAN and SVI on both ToR switches. Each management domain host requires two DHCP-assigned IP addresses for VMware NSX-T tunnel endpoints (TEPs).

The following figure shows the VCF network topology for AMP Central:



Virtual infrastructure design

The VxBlock System 1000 and the management domain follow the VMware VVD recommendations that are incorporated into VMware VCF.

The virtualization infrastructure layer contains the following components:

- VMware vSphere
- VMware vSAN
- VMware NSX-T Data Center

See Network Design for ESXi for the Management Domain for additional information. Consider the total system requirements of management components and VI workload domains when you size the compute resources for the management domain.

VMware ESXi

Host failures or maintenance should maintain a vCPU-to-pCPU ratio of less than or equal to 2:1. Do not consider hyperthreading when calculating the ratio. The number of hosts in the management domain should meet this requirement.

Consider the following for VMware ESXi host CPU capacity:

- Expected number of VI workload domains, VMware NSX-T instances, VMware NSX-T intelligence VMs.
- Optional VMware vRealize Suite requirements.
- AMP Central core, optional, and ECO workloads.
- VxBlock System multisystem management requirements

VMware ESXi is deployed with VMware ESXi Enterprise Plus license with UEFI secure boot as the default. VMware vSphere ESXI supports four to 16 medium or large AMP Central servers that are determined by the combined management and VI workload domain requirements. Management domain expansion is only supported with VMware SDDC Manager.

Follow the RCM process to perform patches and upgrades using VMware SDDC Manager.

VMware vCenter Server

The VMware vCenter Server manages the VMware ESXi hosts that are running the software components of VMware SDDC. This VMware vCenter Server supports integration with other solutions for virtual infrastructure monitoring and management. VMware vCenter is configured with an Embedded VMware Platform Services Controller (PSC) running Embedded Link Mode with up to 14 VI workload domains.

VMware SDDC Manager automation deploys the VI workload domain VMware vCenter Servers on `sfo-m01-clo1-vds01-pg-mgmt` and deploys management and VI workload domain VMware NSX-T Managers on `sfo-m01-clo1-vds01-pg-mgmt`. The first VI workload domain requires a VMware vCenter Server and associated VMware NSX-T Managers. The second VI workload domain that is deployed may only require a VMware vCenter Server.

The VMware vSphere Lifecycle Manager (vLCM) runs on the VMware vCenter Server. VMware SDDC Manager is used for life cycle management of all management and workload domains.

One VMware vCenter Server is deployed with the VMware vSphere Enterprise Plus license. The VMware vCenter Server is supported with AMP Central in a stand-alone or integrated configuration. The VCF VVD Architecture does not support VMware FT and VMware vCHA.

Follow the RCM process to perform patches and upgrades using VMware SDDC Manager.

VMware vSphere cluster

The VMware vSphere cluster requires a minimum of four VMware vSAN ready nodes in a single availability zone for the management domain. The VMware vSphere cluster automatically enables VMware HA, VMware DRS, and VMware EVC. The VMware vSphere automatically deploys three small VMs for VMware vSphere Cluster Services (vLCS) on different management domain hosts. You can view the management domain VMware vCenter Server from the **VM and template** tab.

VMware vSphere

Consider the following for VMware vSphere design:

- Place the core, optional and ECO workloads in the `sfo-m01-fd-mgmt` default folder.
- The management domain cluster uses VMware vSAN for principal storage.
- The management domain requires a minimum of four hosts to support VMware vSAN.
- The management domain does not support VMware vVols.
- Two VMware vSAN disk groups are configured per management domain host.
- At least 30 percent of the VMware vSAN datastore should be free space.
- A single availability zone uses the default VMware vSAN storage policy.
- Storage I/O control is not applicable on principal VMware vSAN datastores.

VMware SDDC Manager

Use VMware SDDC Manager to create workload domains, provision additional infrastructure and perform lifecycle management of VMware SDDC management components. The VMware SDDC Manager is assigned to the `sfo-m01-fd-mgmt` folder and automatically deploys during installation.

You can use VMware SDDC Manager to perform the following:

- Commission or decommission VMware ESXi hosts
- Deploy VI workload domains
- Extend clusters with VMware ESXi hosts in the management domain and VI workload domains
- Add clusters to the management domain and VI workload domains
- Support network pools for host configuration in a VI workload domain
- Store product licenses
- Deploy optional VMware vRealize Suite components.
- Provide life cycle management of virtual infrastructure components in the VI workload domains and optional VMware vRealize Suite Lifecycle Manager components.
- Manager certificates
- Rotate and manage passwords
- Deploy VMware NSX-T Edge clusters in the management domain and VI workload domains
- Configure backups

VMware vSphere network

VMware VDS and VMware NSX-T are used for virtual networking. The following requirements apply:

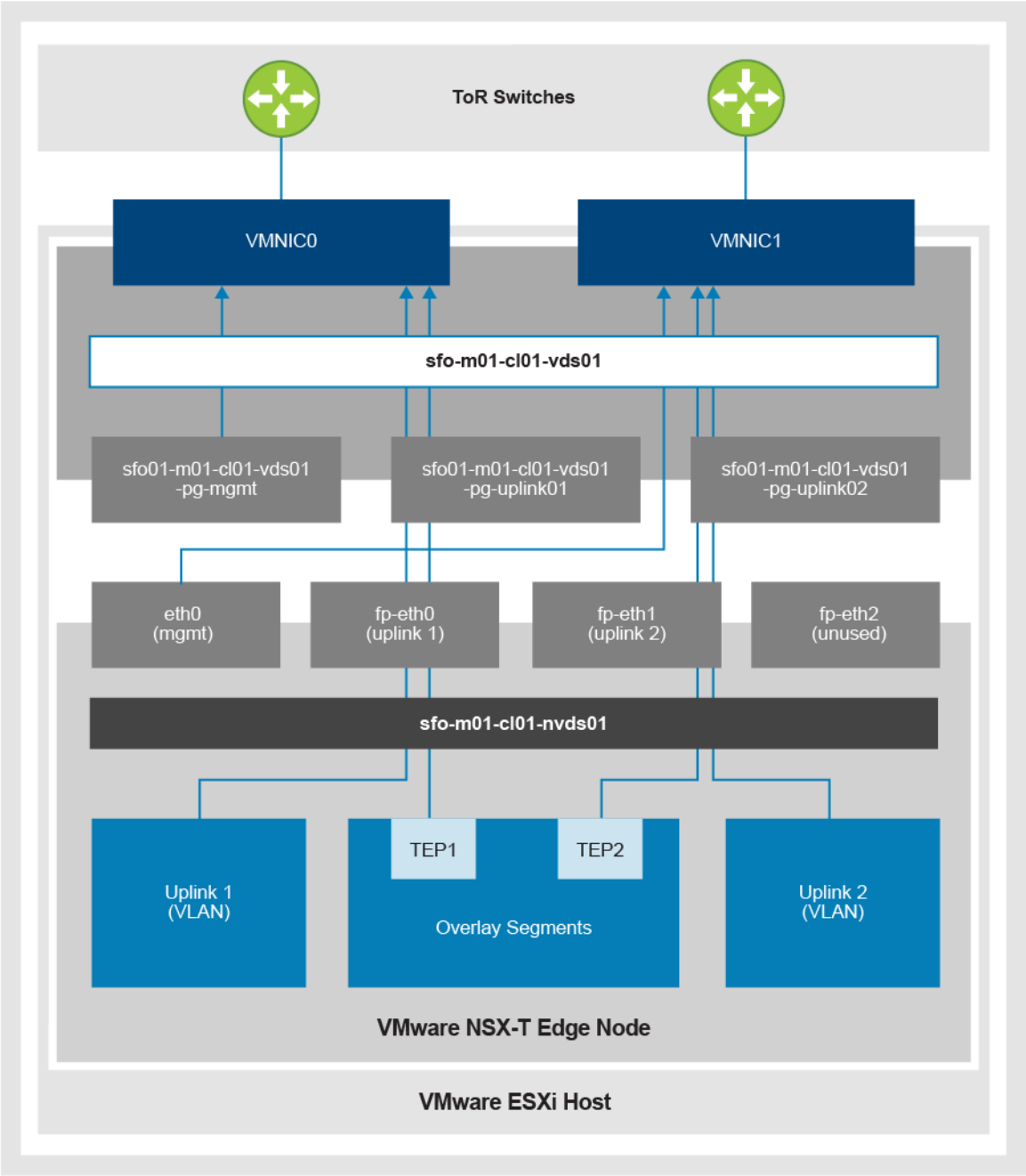
- Each VMware vSphere cluster in the management domain requires one dedicated VMware VDS for the ToR switches and a second VMware VDS and associated port group to support OOB management VMs.
- NIOC is enabled for each VMware VDS
- Route based on physical NIC load is the default network configuration for the management domain. This network configuration does not apply for the VMware NSX-T Data Center uplink port groups for the edge nodes.
  - The VLAN for the default `sfo-m01-cl01-vds01-pg-uplink01` is configured on ToR Switch A.
  - The VLAN for the default `sfo-m01-cl01-vds01-pg-uplink02` is configured on ToR Switch B.

VMware NSX-T includes the following components to provide management domain network virtualization capabilities:

- VMware NSX-T Manager implements the management and control plane for the VMware NSX-T infrastructure.
- VMware NSX-T Manager is automatically deployed with the medium configuration.
- VMware NSX-T Manager appliances are automatically deployed on `sfo-m01-cl01-vds01-pg-mgmt`.
- The VMware NSX-T management host overlay TEPs are assigned to each management host using DHCP. Each host requires two TEPs.
- If virtual network segments are deployed, the following apply:
  - VMware NSX-T Edge nodes contain the service router components and provide north-south traffic connectivity between the physical data center networks and the VMware NSX-T segments. The nodes provide east-west traffic flow support.
  - VMware NSX-T Edge VMs are deployed with the medium configuration
  - BGP is configured on the ToR switches and establish a routing adjacency with VMware NSX-T Edge nodes tier-0 service routers. Only BGP is supported as a routing protocol.
  - The ToR switch BGP configuration includes the default-originate option to inject default routes to the VMware NSX-T Edge node tier 0 gateway.
  - VMware NSX-T Management Edge overlay TEPs are manually assigned two IP addresses for each of the VMware NSX-T Edge nodes.
- VMware NSX-T Edge nodes are automatically deployed on `sfo-m01-clo1-vds01-pg-mgmt`.
- VMware NSX-T Edge nodes are implemented with a single VMware VDS. The uplink network interfaces of the VMware NSX-T Edge node are connected to VLAN trunk group ports that connected to a specific physical NIC on the host. The internal VMware VDS is required to define traffic flows through the VMware NSX-T Edge node interfaces.

NOTE: VMware SDDC Manager is used for updates, and product compatibility verification for life cycle management.

The following figure shows the VMware NSX-T Edge node configuration:



VMware NSX-T Manager

Three VMware NSX-T Managers appliances are deployed with the management domain regardless of whether virtual network segments are used.

Follow the RCM process to perform patches and upgrades using VMware SDDC Manager.

VMware NSX-T Edge VMs

Two VMware NSX-T Edge node VMs are deployed to the management domain to support virtual network segments.

Follow the RCM process to perform patches and upgrades using VMware SDDC Manager.

Default VLANs, port groups, and VMs

VMware Cloud Builder deploys two VMware vSphere Distributed Switches (VDS) and port groups that connect to the ToR switches.

The following table provides specifications to configure the VMware VDS:

Virtual port group	VMkernel port	VMkernel MTU	VMware physical adapter	Teaming and failover	VMware CoS	Load balancing
Management port group	vmk0	1500	Uplink1 (vmnic 0)	Active	Platinum CoS 6, DSCP 48	Originating port ID
			Uplink2 (vmnic 1)	Active		
			Uplink3 (vmnic 2)	Active		
			Uplink4 (vmnic 3)	Active		
VMware vMotion port group	vmk1	9000	Uplink1 (vmnic 0)	Active	Gold CoS 4, DSCP 26	Explicit failover
			Uplink2 (vmnic 1)	Standby		
			Uplink3 (vmnic 2)	Active		
			Uplink4 (vmnic 3)	Standby		
NFS port group	vmk2	9000	Uplink1 (vmnic 0)	Active	Silver CoS 2, DSCP 16	Originating port ID
			Uplink2 (vmnic 1)	Active		
			Uplink3 (vmnic 2)	Active		
			Uplink4 (vmnic 3)	Active		

VLANs and port groups

VCF can be deployed with or without VMware NSX-T virtual network segments. VCF VLANs are always required. VLANs or virtual network segments that are marked as VCF with virtual network segments are only required when deploying VCF with virtual network segments. See the `vcf-ems-deployment-parameter` spreadsheet to determine whether the virtual network segments option is required.

The following table provides sample VLAN numbers, VLAN names, port group names and VMware NSX-T virtual network segments:

VLAN	ToR switch	Port group	VLAN name	Subnet/ Netmask	Gateway	Routed	Topology
1611	A, B	sfo-m01-cl01-vds01-pg-mgmt	m-mgmt	172.16.11.0 /24	172.16.11.1	Y	VCF
1612	A, B	sfo-m01-cl01-vds01-pg-vmotion	m-vmotion	172.16.12.0 /24	172.16.12.1	Y	VCF
1613	A, B	sfo-m01-cl01-vds01-pg-vsan	m-vsan	172.16.13.0 /24	172.16.13.1	Y	VCF
1614	A, B	sfo-m01-cl01-vds01-pg-overlay*	m-host-overlay	172.16.14.0 /24	172.16.12.1	Y	VCF
2711	A	sfo-m01-cl01-vds01-pg-uplink01	m-edge-uplink01	172.27.11.0 /24	172.27.11.1	Y	VCF with virtual network segments
2712	A	sfo-m01-cl01-vds01-pg-uplink02	m-edge-uplink02	172.27.12.0	172.27.12.1	Y	VCF with virtual

VLAN	ToR switch	Port group	VLAN name	Subnet/ Netmask	Gateway	Routed	Topology
				/24			network segments
2713	B	sfo-m01-cl01-vds01-pg-edge**	m-edge-overlay	172.27.13.0 /24	172.27.13.1	Y	VCF with virtual network segments
N/A	N/A	sfo-m01-seg01	N/A	192.168.31.0 /24	192.168.31.1	VMware NSX-T BGP routed	VCF with virtual network segments
N/A	N/A	xreg-m01-seg01	N/A	192.168.11.0 /24	192.168.11.1	VMware NSX-T BGP routed	VCF with virtual network segments

*Two DHCP IP addresses in the VLAN m-host-overlay are required for the management domain TEPs on each host.

**Two static IP addresses are required per VMware NSX-T edge node in the m-edge-overlay network.

A second VMware VDS is required for the VMware Cloud Build deployment on AMP Central to connect to the management switches. The following table shows sample values:

VLAN	Management switch	Port group	VLAN name	Subnet/ Netmask	Gateway	Routed	Topology
1801	A,B	sfo-m01-cl01-vds02-pg-oob	oob	172.18.1.0 /24	172.18.1.1	Y	VCF

See the *Dell EMC AMP Central Product Guide* for information about VMware VLAN naming and numbering.

VMs

The following table describes the default VMs names and placement of port groups for the management domain using sample names:

VM type	VM	VMware VDS port group
VMware vCenter Server	sfo-m01-vc01	sfo-m01-cl01-vds01-pg-mgmt
VMware SDDC Manager	sfo-vcf01	sfo-m01-cl01-vds01-pg-mgmt
VMware NSX-T Manager Appliance A	sfo-m01-nsx01a	sfo-m01-cl01-vds01-pg-mgmt
VMware NSX-T Manager Appliance B	sfo-m01-nsx01b	sfo-m01-cl01-vds01-pg-mgmt
VMware NSX-T Manager Appliance C	sfo-m01-nsx01c	sfo-m01-cl01-vds01-pg-mgmt
VMware NSX-T Edge node 1 (VCF with virtual network segments)	sfo-m01-en01	sfo-m01-cl01-vds01-pg-mgmt
VMware NSX-T Edge node 2 (VCF with virtual network segments)	sfo-m01-en02	sfo-m01-cl01-vds01-pg-mgmt

Scalability

AMP Central with VCF aligns to the VMware Validated Designs (VVD) for VMware ESXi host CPUs with overcommitment recommendations.

The CPU overcommitment ratio for vCPU-to-pCPU is less than or equal to 2:1. Consult your Dell Technologies Sales Engineer to size the AMP and determine the number of management domain servers. Include the following minimum requirements in the complete workload:

- Management domain base workload.
- Management domain VMware NSX-T edge nodes.
- Management domain Element Managers (storage and data protection).
- Management domain core, optional and ECO workloads.
- Optional management domain VMware vRealize Suite workload
- Total number of management domain VMware vCenter Servers and associated VMware NSX-T Managers.
- Total number of XMS servers.
- Determine whether VMware NSX-T Intelligence instances are going to be deployed.
- Total number of legacy VxBlock System VMware vCenter Servers and the associated management workload.

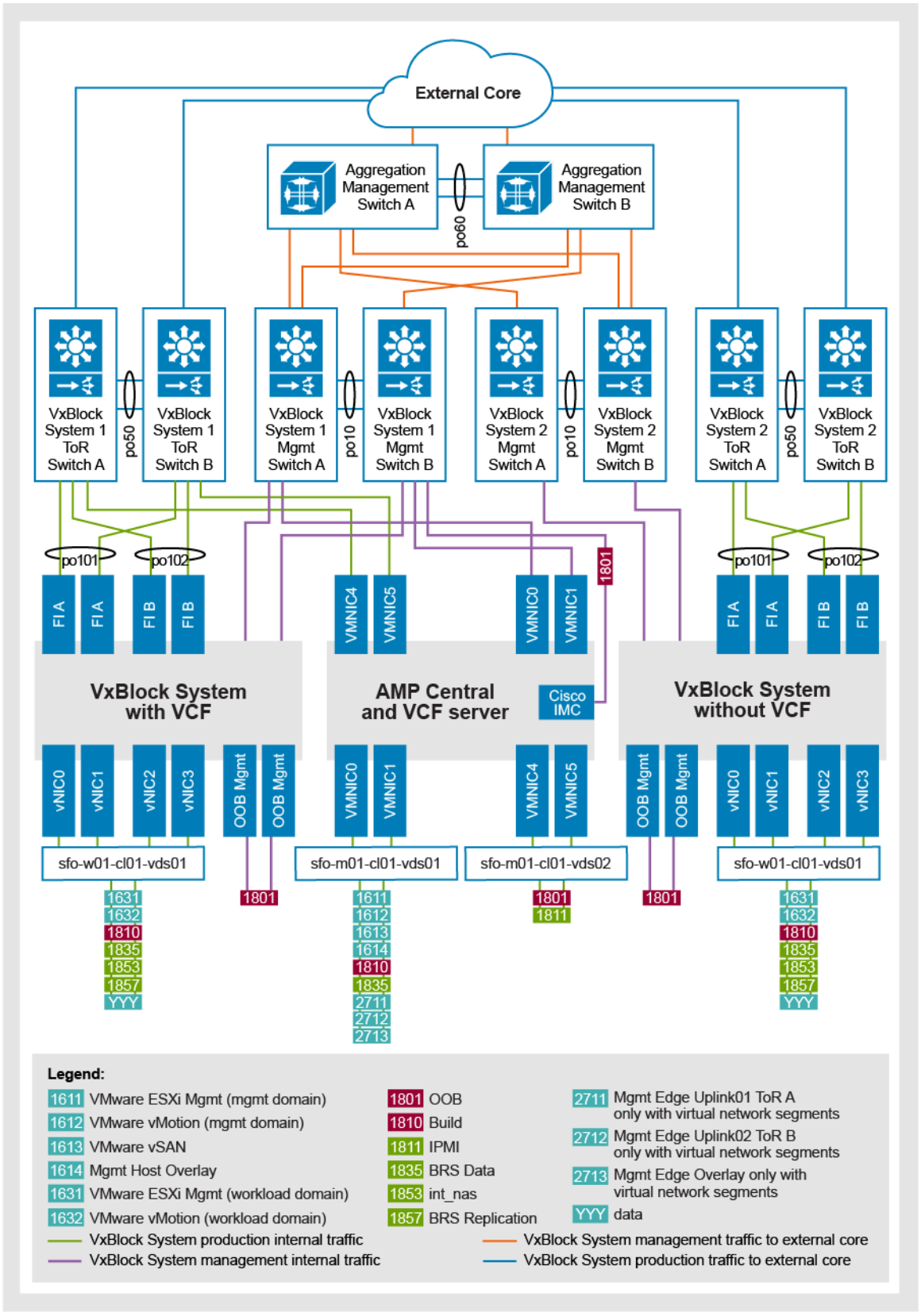
VxBlock System multisystem management

AMP Central uses available resources on the management workload cluster to manage one VxBlock System 1000 with VCF and multiple legacy VxBlock Systems. Legacy VxBlock Systems require a dedicated (non-VCF managed) VMware vCenter Server. Legacy VxBlock Systems must align to the VxBlock System RCM. You cannot convert or upgrade legacy VxBlock Systems to VMware VCF.

A stand-alone AMP Central connects to a dedicated pair of management and ToR switches that VxBlock System management traverses the external network core. An integrated AMP Central connects to a single pair of management and ToR switches within a managed VxBlock System. AMP Central must traverse the external network core to manage additional VxBlock Systems.

AMP Central hosts the production VMware vCenter Servers. You can use a single VMware vCenter Server for multiple VxBlock Systems (up to the 2000 server limit). You may also purchase more VMware vCenter Server licenses to separate the workloads for each system.

The following figure shows VCF network connectivity for an AMP Central stand-alone configuration:



See the *Dell EMC AMP Central Product Guide* for information about distributed management for VxBlock Systems, storage, virtualization, and Integrated Data Protection and management workloads.

Integrated Data Protection

Integrated Data Protection can be used on a VxBlock System 1000 with VCF for the management workload and the VI workload domain. Data Protection strategies range from basic backup and recovery to multisite data replication to support point-in-time recovery or an active/active data center. There are multiple solutions and strategies available for RTOs and RPOs.

Integrated Data Protection solutions with the VI workload domain

The following backup and recovery solutions are supported:

- Avamar Virtual Edition with Data Domain
- Avamar Single Node system with Data Domain
- Avamar Mulitnode system with or without Data Domain
- NetWorker with Data Domain
- PowerProtect Data Manager with Data Domain
- PowerProtect Cyber Recovery

The following business continuity and disaster recovery replication solutions are supported:

- RecoverPoint Classic
- RecoverPoint for VMs
- VPLEX

The following management solutions are supported:

- Data Protection Advisor
- Data Protection Central
- Data Protection Search
- PowerProtect DD Management Center

For additional information about Integrated Data Protection, see the *Dell EMC Integrated Data Protection Product Guide*.

Integrated Data Protection solutions with the management domain

Integrated Data Protection configurations within a VxBlock System back up and protect the AMP Central core management workloads. During deployment, the backup software is configured to perform VMware image level backups and file level backups. Backups run a full backup once per day and retained for 14 days.

A custom set of data protection backup scripts performs backups for a specific set of workloads. These scripts are on a Windows Server based element manager dedicated for Data Protection. Microsoft Task Scheduler is used to create tasks to run the various scripts once per day during the appropriate backup window. The backup files that are created with the scripts are programmatically moved to the Data Protection element manager. Those backup files are backed up daily by Avamar or NetWorker.

The following Integrated Data Protection configurations are supported:

- Avamar Virtual Edition with Data Domain
- Avamar Single Node system with Data Domain
- Avamar Mulitnode system with or without Data Domain
- NetWorker with Data Domain

Avamar and NetWorker performs image and file-based backups for the following workloads:

- All VMware vCSA instances
- PowerPath Management Appliances
- Element Manager for Storage Arrays
- Element Manager for Data Protection

The following backups are performed with the scripted, native command line:

- VMware vCenter file backups
- VMware vCenter Database backups
- VMware VDS exports
- PowerPath Management Appliance backups
- VMware vRealize Orchestrator instance
- VMware NSX Manager

- VMware SDDC Manager

5

VI workload domain architecture

The VMware SDDC Manager deploys, provisions, and manages VI workload domains and associated VMware vSphere clusters.

The VI workload domain consists of one or more clusters that are derived from the VxBlock 1000 domains. Each cluster has a minimum of three hosts with either Cisco UCS B-Series Blade Servers or Cisco UCS C-Series Rack Servers. Management workloads are committed to a management domain, while user workloads are deployed into separate VI workload domains.

A dedicated VMware vCenter Server manages each VI workload domain. With dedicated VMware vCenter Servers for each VI workload domain, you can deploy software updates without impacting other VI workload domains. A separate VMware vCenter Server allows for additional segregation for each VI workload domain.

VCF standard architecture provides scalability and allows for autonomous licensing and life cycle management. VCF separates management workloads from external workloads to provide better long-term flexibility and expansion options. You can only perform one VI workload domain operation at a time. When you create a VI workload domain, you cannot add a cluster to any other VI workload domain.

VCF supports up to 14 VI workload domains on the VxBlock System.

VI workload domain configurations

You can configure four vNICs per service profile for the VxBlock System 1000 with VCF.

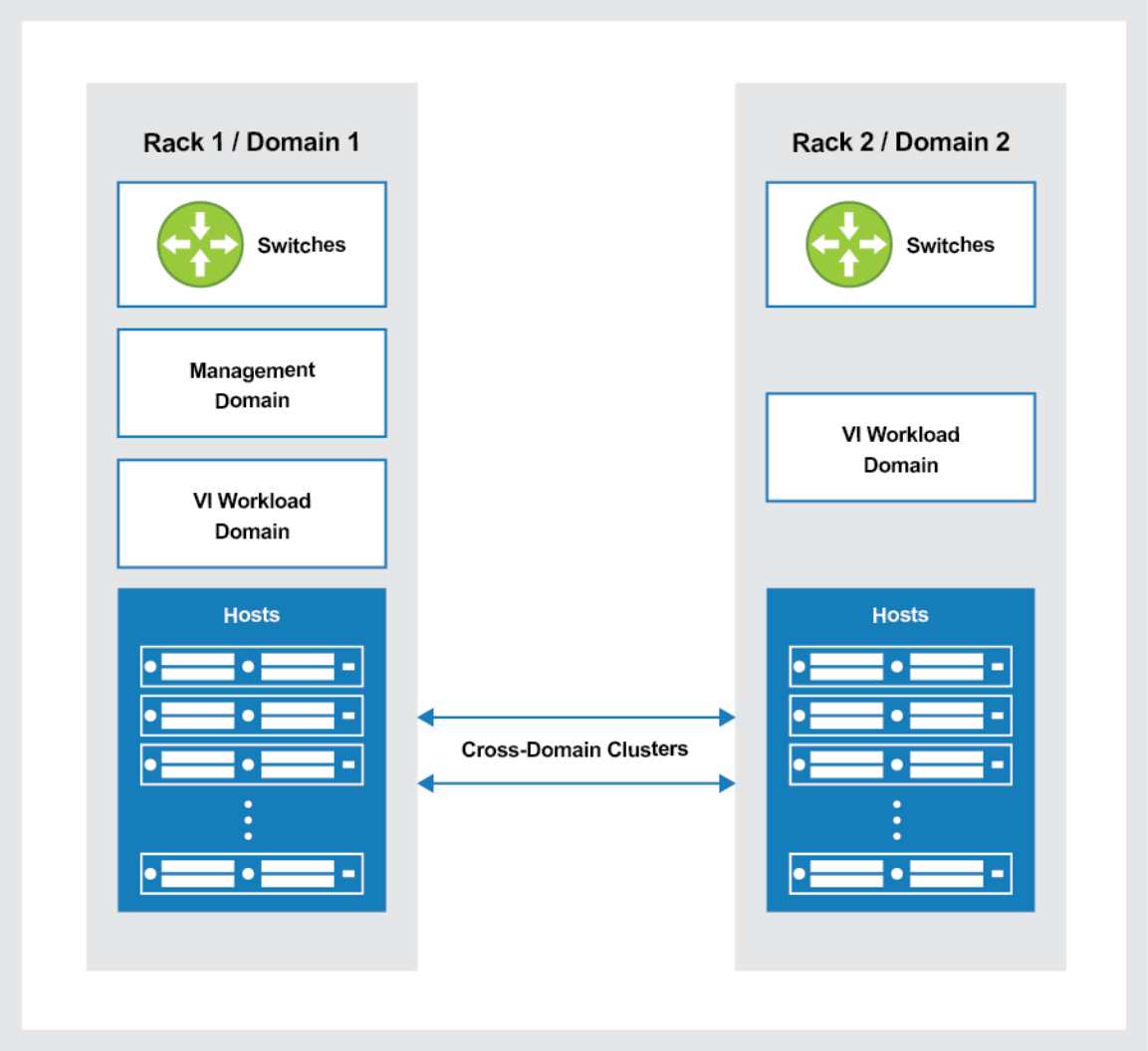
The following table shows the minimum and maximum configurations per component:

Component	Minimum	Maximum
Cisco UCS B-Series Blade Server or Cisco UCS C-Series Rack Server	3 per cluster	96 per cluster
Management domain	1	1
VI workload domain	1	14
Clusters	1	Up to 2500 hosts

Cisco UCS architecture

The Cisco UCS architecture follows the same VxBlock 1000 architecture model as a non-VCF deployment. For detailed information about Cisco UCS architecture, see the *VxBlock System 1000 Architecture Overview*.

The following figure shows a multidomain VxBlock System with hosts that are used to create multiple VI workload domains under a single management domain:



Cisco UCS B-Series Blade Server or Cisco UCS C-Series Rack Server compute hosts servers create each VCF cluster. Each cluster contains three or more Cisco UCS compute host servers from within the same VxBlock System. Clusters do not need to come from the same domain.

Network standards

VCF on the VxBlock System 1000 adheres to network standards for VMware vSphere 7.0.

For a VxBlock 1000 with VCF, the ToR switches provide the following protocols when virtual network segments are used:

- VMware NSX-T edge components use eBGP to peer to the ToR switch.
- BFD is not part of a standard VCF deployment, but it implemented on VxBlock Systems on all edge-to ToR peering connections. BFD reduces route convergence time down from 12 seconds (default) to less than two seconds in the event of a path failure.

You can configure external network uplinks with BFD regardless of whether virtual network segments are used.

Virtual network segments

Virtual network segments are VMware NSX-T managed overlay backed network segments that enable the full suite of VMware NSX-T Data Center features within a VCF deployment.

NOTE: VCF 4.1 uses the term virtual network segments. Virtual network segments were previously referred to as application virtual networks (AVN) by VMware in VCF versions before 4.1.

Virtual network segments provide the following full suite of VMware NSX-T Data Center and VMware SDDC Manager use cases, including:

- Edge firewall
- Load balancer
- NAT
- VPN
- Hybrid cloud
- Cloud DR
- Workload mobility across L3 domains
- VMware vRealize Suite of solutions

Configure virtual network segments consistently across the management domains and VI workload domains for VxBlock 1000 during the initial deployment. Deploy segments in the management domain and the VI workload domains.

Default VLANs

Default VLANs are deployed on the ToR switch and VMware NSX-T instances based on the VCF topology. VLAN IDs and names are default values, but may be customized before deployment.

The following table provides the VCF VLANs and the deployment models:

VLAN	Name	Routable	VCF without virtual network segments	VCF VMware NSX-T instances with virtual network segments			
				One VI workload domain	Two VI workload domains	Three VI workload domains	Four VI workload domains
1631	w-mgmt	Yes	Yes	Yes	Yes	Yes	Yes
1632	w-vmotion	Yes	Yes	Yes	Yes	Yes	Yes
1634	w-host-overlay	Yes	Yes	Yes	Yes	Yes	Yes
2731	w-edge-uplink01	Yes	No	Yes	Yes	Yes	Yes
2732	w-edge-uplink02	Yes	No	Yes	Yes	Yes	Yes
2733	w-edge-overlay	Yes	No	Yes	Yes	Yes	Yes
1635	w-host2-overlay	Yes	No	No	Yes	Yes	Yes
2734	w-edge2-uplink01	Yes	No	No	Yes	Yes	Yes
2735	w-edge2-uplink02	Yes	No	No	Yes	Yes	Yes
2736	w-edge2-overlay	Yes	No	No	Yes	Yes	Yes
1636	w-host3-overlay	Yes	No	No	No	Yes	Yes
2737	w-edge3-uplink01	Yes	No	No	No	Yes	Yes
2738	w-edge3-uplink02	Yes	No	No	No	Yes	Yes
2739	w-edge3-overlay	Yes	No	No	No	Yes	Yes
1637	w-host4-overlay	Yes	No	No	No	No	Yes
2740	w-edge4-uplink01	Yes	No	No	No	No	Yes
2741	w-edge4-uplink02	Yes	No	No	No	No	Yes
2742	w-edge4-overlay	Yes	No	No	No	No	Yes
1638	w-host5-overlay	Yes	No	No	No	No	No

VMware NSX-T instance deployment topologies

There are several supported deployment topologies for VMware NSX-T instances with VCF on a VxBlock System 1000. Regardless of the topology, at least three VMware NSX-T instances are deployed on AMP Central for the VI workload domain. TEPs are provisioned on each VI workload domain host, regardless of whether virtual network segments are used. The remaining components are optional.

VMware NSX-T instance topologies without virtual network segments

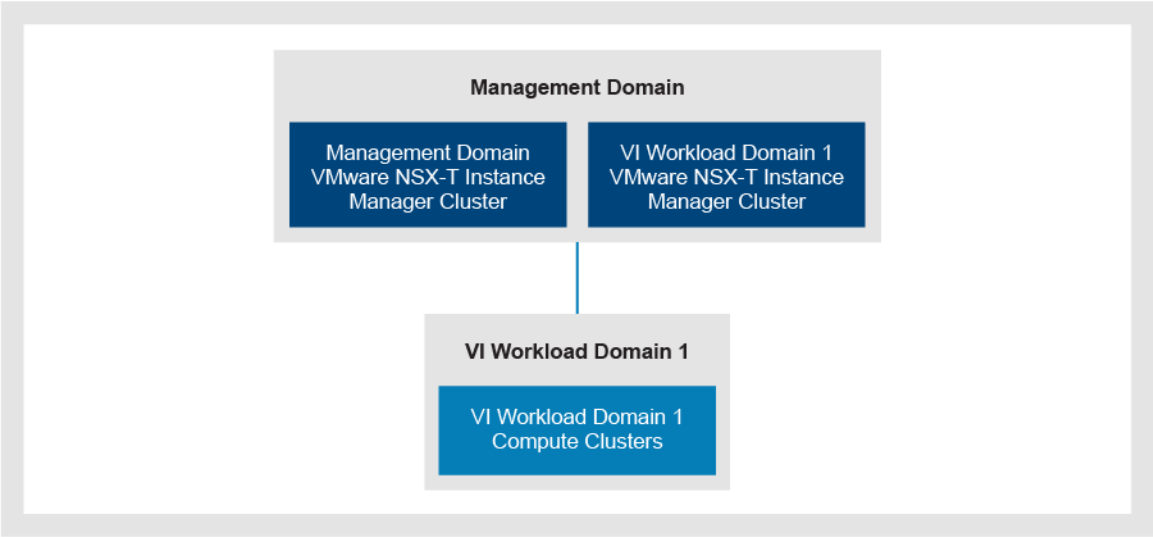
If VMware vRealize Suite is not used, virtual network segments are not required in the deployment. VMware NSX-T instance topologies that do not contain virtual network segments are provided.

Both topologies that are provided contain a single VMware NSX-T instance and a single management domain. The following table describes the attributes of the topologies that are provided for the VI workload domains:

Topology	Description
V1	• Single VI workload domain • All deployed VMware ESXi hosts participate in traditional VMware VDS virtual switching and VLAN-backed port groups. • A VMware NSX-T Manager cluster is deployed for the management domain, but is not used. This cluster is mandatory for all VCF 4.1 deployments. • A VMware NSX-T Manager cluster is deployed for the VI workload domains, but is not used. This cluster is mandatory for all VCF 4.1 deployments.
V2	• Multiple VI workload domains • All VMware ESXi hosts participate in traditional VMware VDS virtual switching with VLAN-backed port groups. • A VMware NSX-T Manager cluster is deployed for the management domain and VI workload domains, but is not used. This cluster is mandatory for all VCF 4.1 deployments.

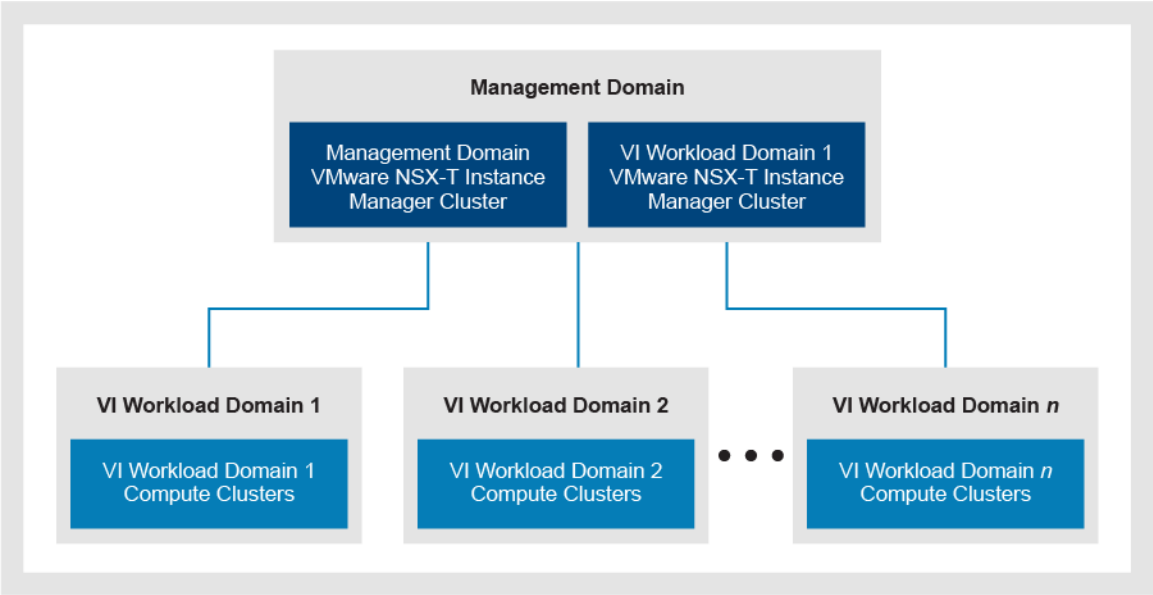
Topology V1

The following figure shows a single VI workload domain without virtual network segments:



Topology V2

The following figure shows multiple VI workload domains without virtual network segments:



VMware NSX-T instance topologies with virtual network segments

Virtual networks segments are required for VMware NSX-T Data Center to support VMware vRealize Suite. Deployments with physical VMware NSX-T Edge hosts use standard Cisco UCS C220 M5 Server edge hosts. VCF deploys dedicated, shared, compute and edge hosts even though VxBlock System standards do not use VM-based workloads on the hosts.

VCF configures hosts as VMware NSX-T transport nodes that participate in a single VMware NSX-T instance. A separate physical VMware NSX-T Edge node and VMware vSphere cluster is required for each VMware NSX-T instance in the deployment. You can not share physical hosts between VMware NSX-T instances.

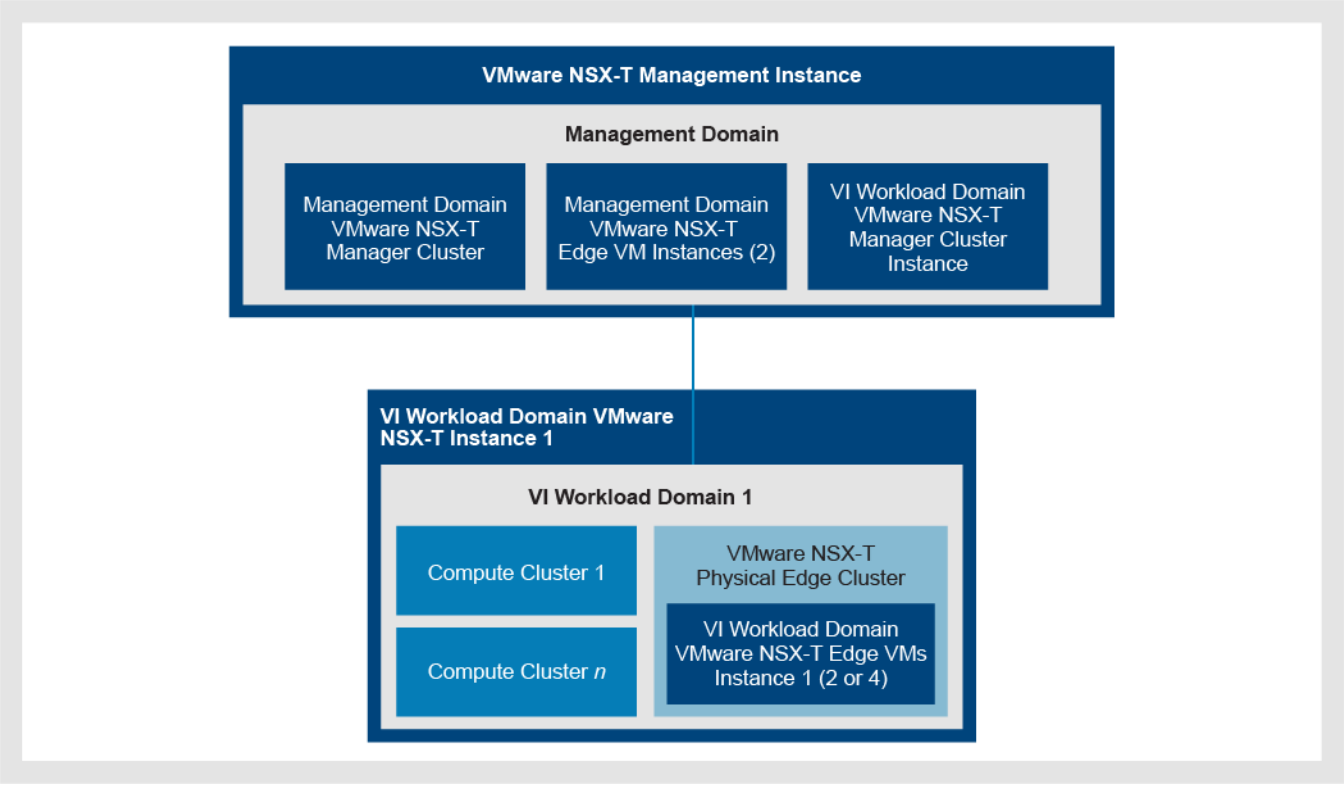
The topologies contain a single VMware NSX-T instance and a single management domain. The The following table describes the attributes of the topologies that are provided for the VI workload domains:

Topology	Description
N1	• All VMware ESXi hosts participate in traditional VMware VDS virtual switching. VMware NSX-T Data Center overlay-backed segments are available on the VMware VDS. • A VMware NSX-T Manager cluster is deployed for the management domain to provide management and control plane functions. • Two VMware NSX-T Edge VMs are deployed to the management domain VMware vSphere cluster. • A VMware NSX-T Manager cluster is deployed for the VI workload domains to provide management and control plane functions. • A dedicated physical VMware NSX-T Edge node and compute cluster consisting of at least three Cisco UCS servers is deployed as the first VI workload domain. The VMware NSX-T Edge VMs are deployed by a VCF workflow within VMware SDDC manager. • The VMware NSX-T Edge VMs handle ingress and egress between networks with and without virtual network segments, and load balancing. • One or more VI workload domain clusters are deployed to support the external workload.
N2	• All VMware ESXi hosts participate in traditional VMware VDS virtual switching. VMware NSX-T overlay backed segments are available on the VMware VDS. • A VMware NSX-T Manager cluster is deployed for the management domain to provide management and control plane functions. • Two VMware NSX-T Edge VMs are deployed by VMware Cloud Builder to the management domain VMware vSphere cluster. • A VMware NSX-T Manager cluster is deployed for the VI workload domains to provide management and control plane functions. • The dedicated VMware NSX-T Edge node and VMware vSphere cluster contains at least three Cisco servers. The VMware NSX-T Edge node and cluster are deployed as the first VI workload domain cluster. • The VMware NSX-T Edge VMs are deployed and configured on this VMware vSphere cluster by VMware SDDC manager with a VCF workflow.

Topology	Description
	• The VMware NSX-T Edge VMs handle all ingress and egress between networks with and without virtual network segments, and load balancing. • The VMware NSX-T Edge VMs cluster on each VI workload domain provides services to the workload domain clusters that are participating in the associated VMware NSX-T instance. • One or more VI workload domain clusters are deployed to support the external workload on each VI workload domain.
N3	• VCF supports up to four VMware NSX-T instances per VCF deployment. • All VMware ESXi hosts participate in traditional VMware VDS virtual switching and VMware NSX-T overlay backed segments are available on the VMware VDS. • A VMware NSX-T Manager cluster is deployed for the management domain, providing management and control plane functions. • Two VMware NSX-T Edge VMs are deployed by VMware Cloud Builder to the management domain VMware vSphere cluster. • A VMware NSX-T manager cluster is deployed for each VI workload domain VMware NSX-T instance, providing management and control plane functions for that instance. • A dedicated VMware NSX-T Edge VMware vSphere cluster consisting of at least three Cisco UCS servers is deployed as the first VI workload domain cluster. • The VMware NSX-T Edge VMs are deployed and configured on this VMware vSphere cluster by a VCF workflow within VMware SDDC Manager. • The VMware NSX-T Edge VMs handle all non-distributed VMware NSX-T services such as ingress/egress between networks with and without virtual network segments, and load balancing. • The VMware NSX-T Edge VMs cluster hosted on each workload domain provides services to the workload domain clusters that are participating in the associated VMware NSX-T instance. • One or more VI workload domain clusters are deployed to support the external workload on each VI workload domain.

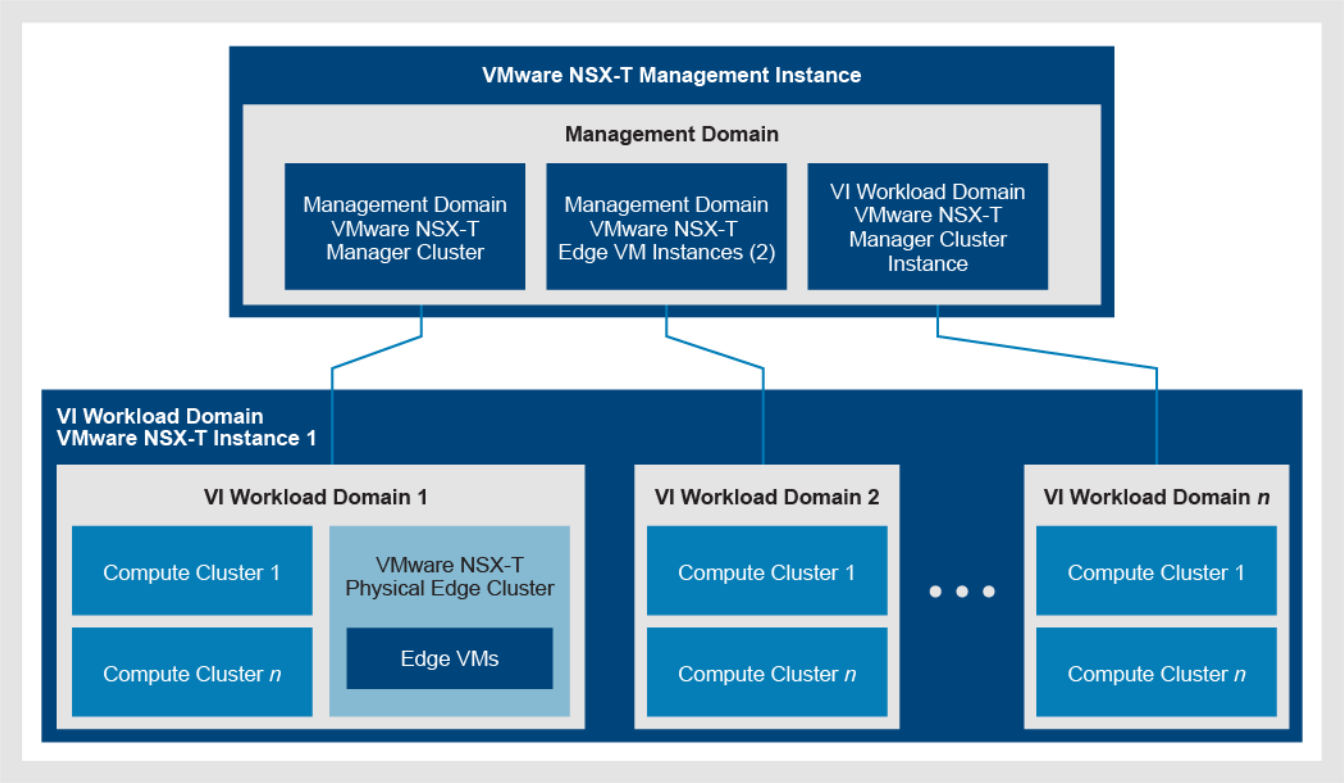
Topology N1

The following figure shows with a single VI workload domain with virtual network segments:



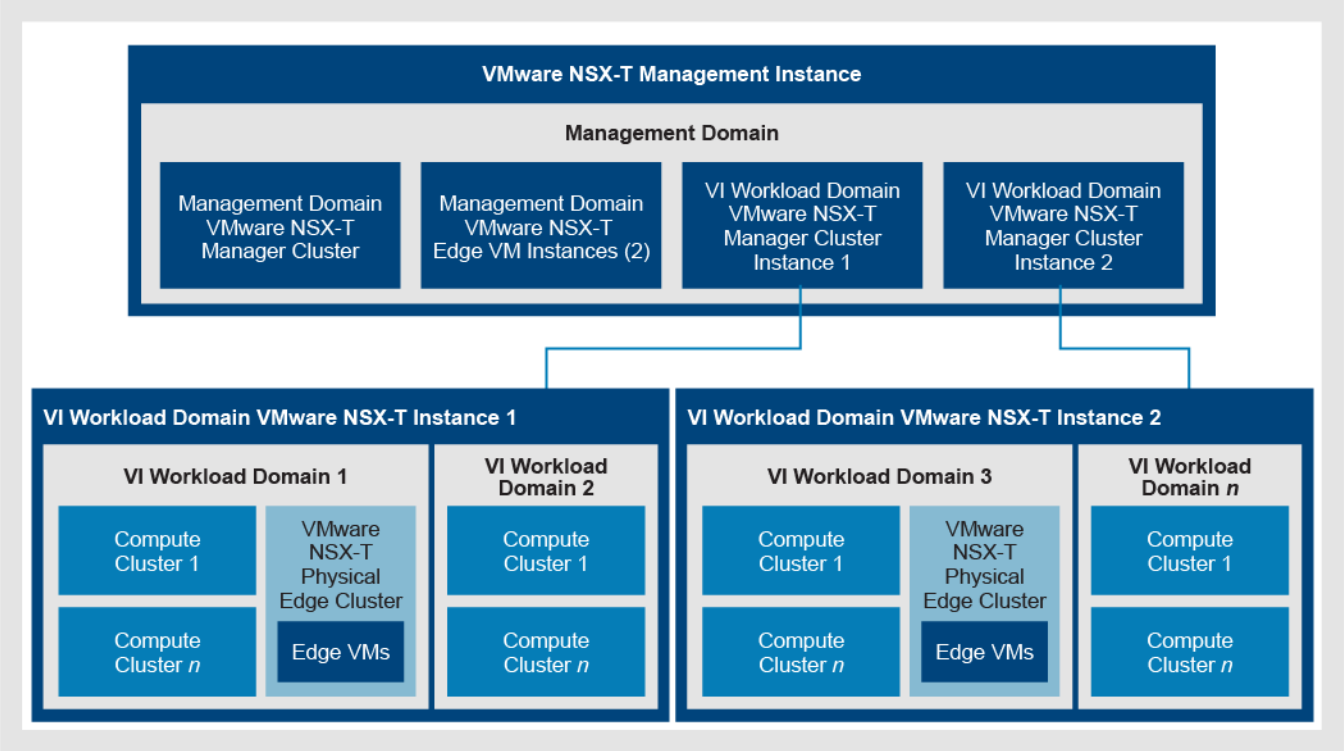
Topology N2

The following figure shows multiple VI workload domains with virtual network segments:



Topology N3

The following figure shows two VMware NSX-T instances with multiple VI workload domains and multiple VI workload domains with virtual network segments:



VMware NSX-T Edge host topologies with virtual network segments

VCF deployments use dedicated Cisco UCS server-based physical edge hosts to provide VMware NSX-T Edge services for virtual network segments. Cisco UCS manages VMware NSX-T Edge hosts. The VMware NSX-T Edge host is available in a standard and extra-large configuration with double the memory of the standard configuration.

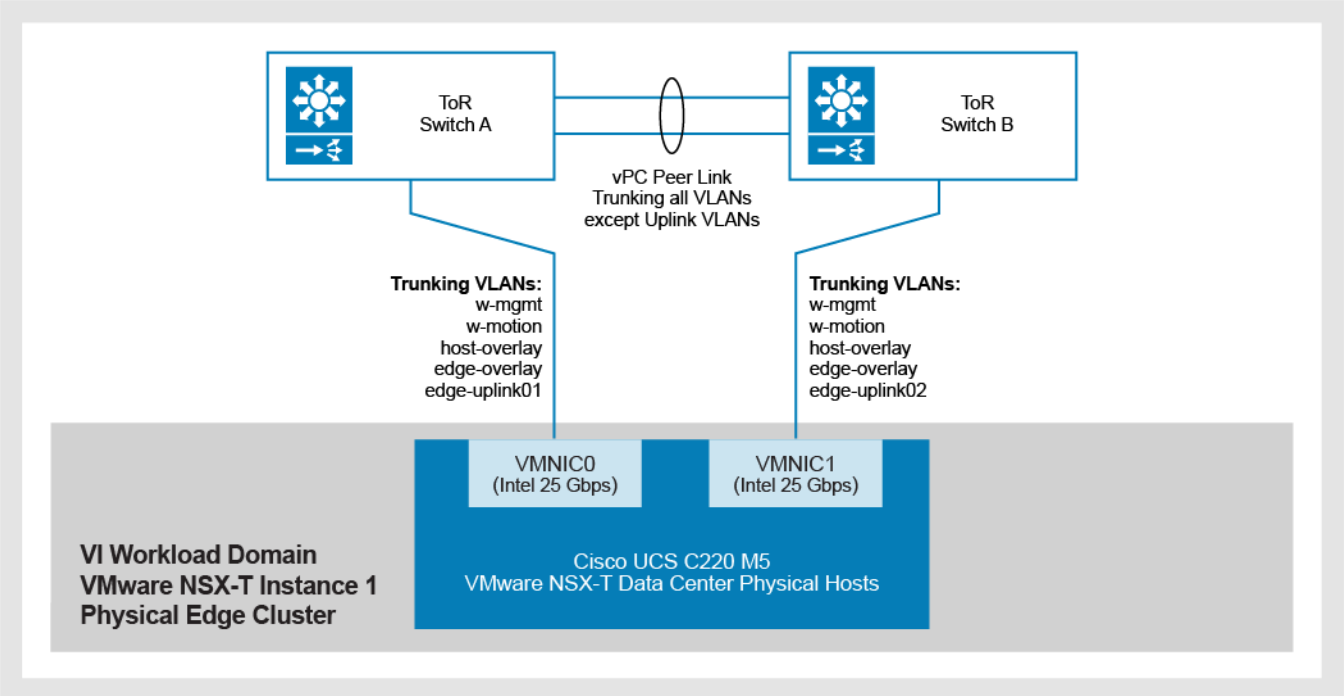
Two vHBAs provide access to the VxBlock System primary storage arrays. Cisco UCS vNICs are not deployed. All network traffic is carried on a pair of Intel XXV710-DA2 NIC ports that connect directly to the ToR switch pair. Two additional ports are available for future use.

The following table provides the specifications for the Cisco UCS C220 M5 Server:

Component	Cisco UCS C220 M5 Server
CPU	Two Intel Xeon 5218 2.3 GHz, 16 core, 22 MB cache
Memory	96 GB (6 x 16 GB DDR4-2933) standard-size host or 192 GB (12 x 16 GB DDR4-2933) extra-large host
NIC	Two Intel XXV710-DA2, dual-port 25 Gbps PCIe adapter
VIC	Cisco UCS VIC 1457 (4 x 10 Gbps or 25 Gbps SFP28 mLOM)
Storage	The Cisco UCS primary storage array provides the storage. Valid primary storage arrays are VMAX, PowerMax, Dell EMC Unity, and XtremIO X2.
Boot device	SD or boot from SAN

Physical connectivity and VLAN trunking topologies

The following figure shows a topology with a single VMware NSX-T instance with virtual network segments with the Cisco UCS C220 M5 Server:

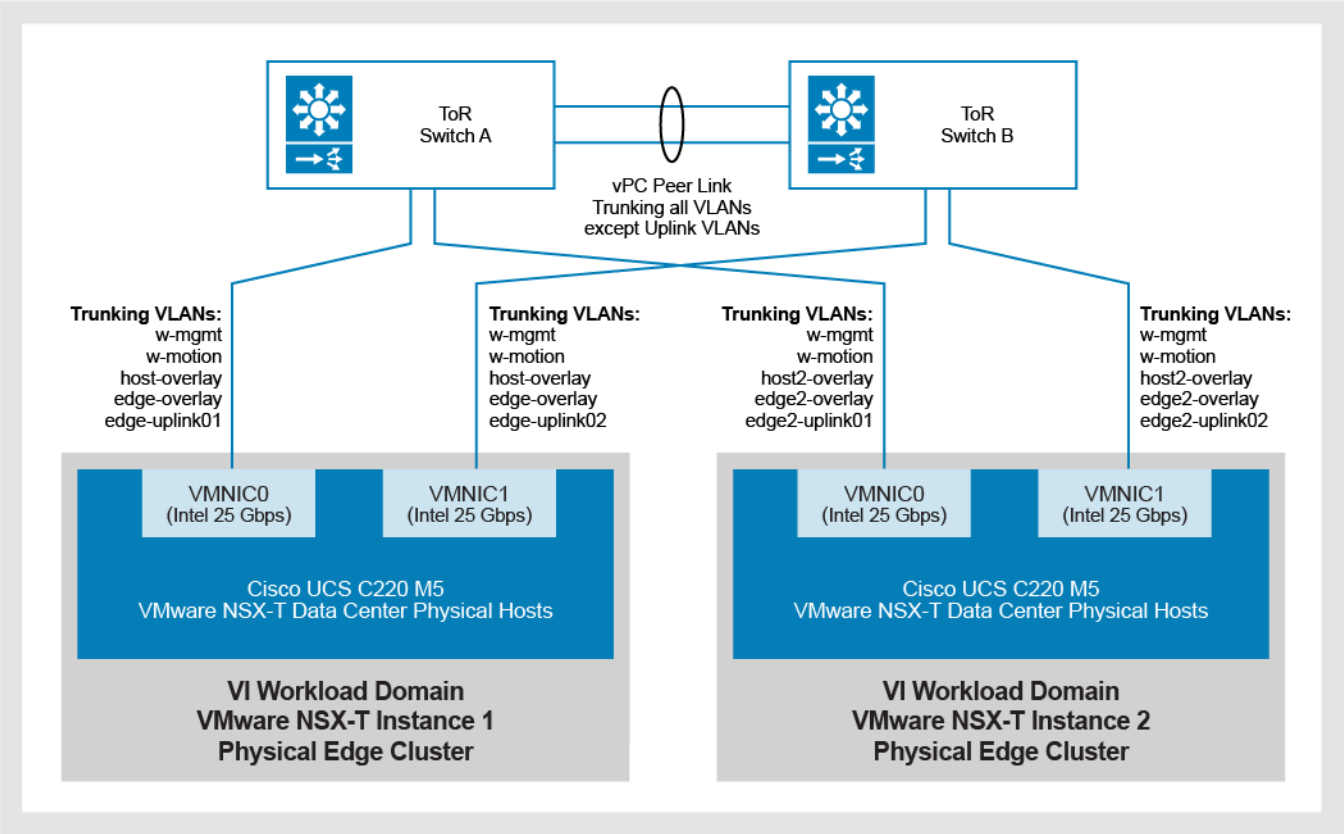


In this scenario, the following apply:

- Overlay networks are trunked on both physical uplinks from the edge host.
- The edge-uplink01 network is carried on the trunk that is connected to ToR switch A. This VLAN enables BGP peering between the Tier-0 Gateway in the VMware NSX-T Edge VM and the ToR switch on side A of the network fabric.
- The edge-uplink02 network is carried on the trunk that is connected to ToR switch B. This VLAN enables BGP peering between the Tier-0 Gateway in the VMware NSX-T Edge VM and the ToR switch on side B of the network fabric.

- The edge-uplink networks are pruned from the peer-link between the ToR switches.

The following figure shows a topology with two VMware NSX-T instances with virtual network segments and the Cisco UCS C220 M5 Server:

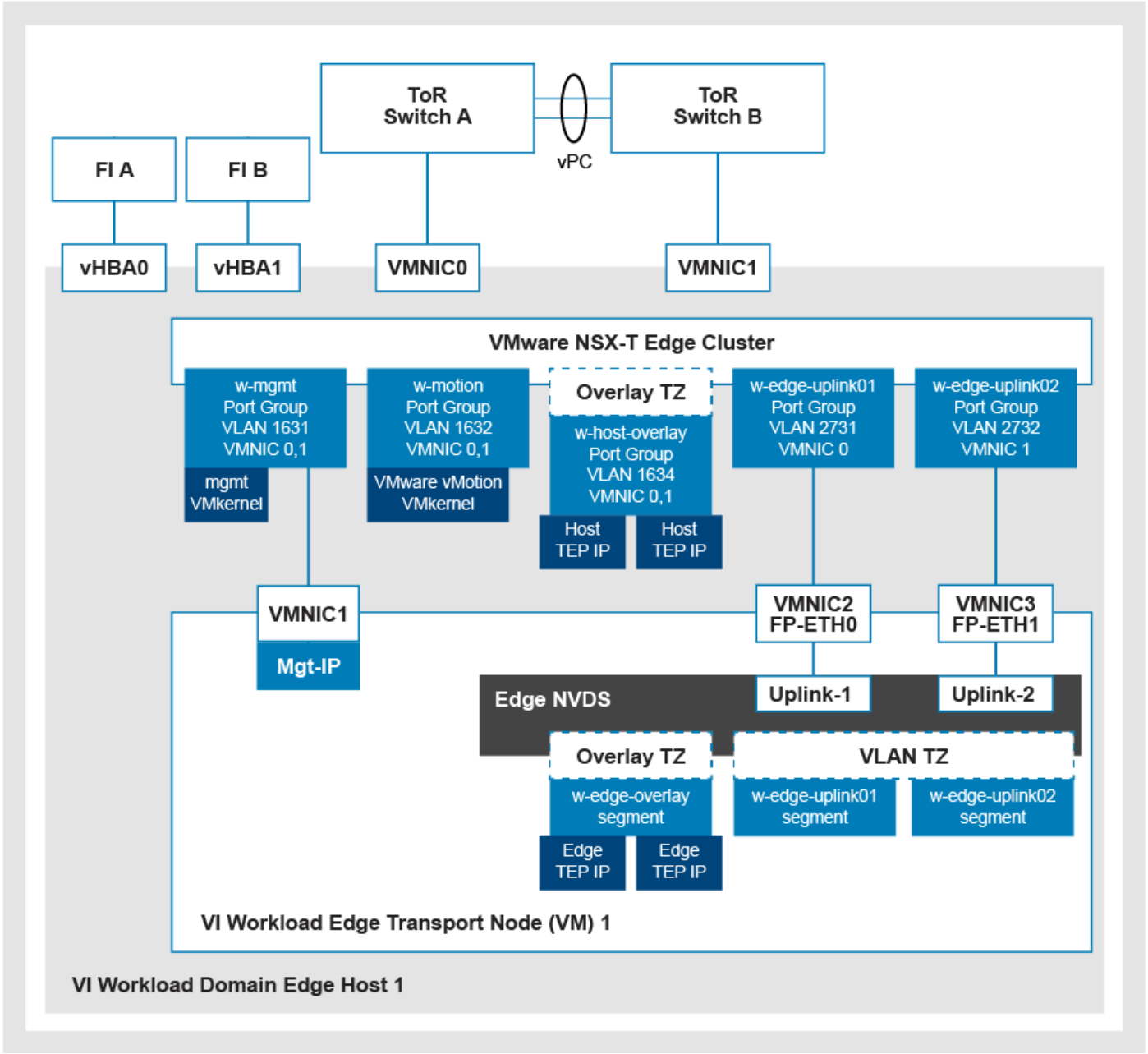


In this scenario, the following apply:

- Each VMware NSX-T instance has a unique set of overlay and uplink networks. Each physical edge cluster trunks the networks associated with the VMware NSX-T instance for which it provides edge services.
- The edge-uplink networks are pruned from the peer-link between the ToR switches.

VCF topologies

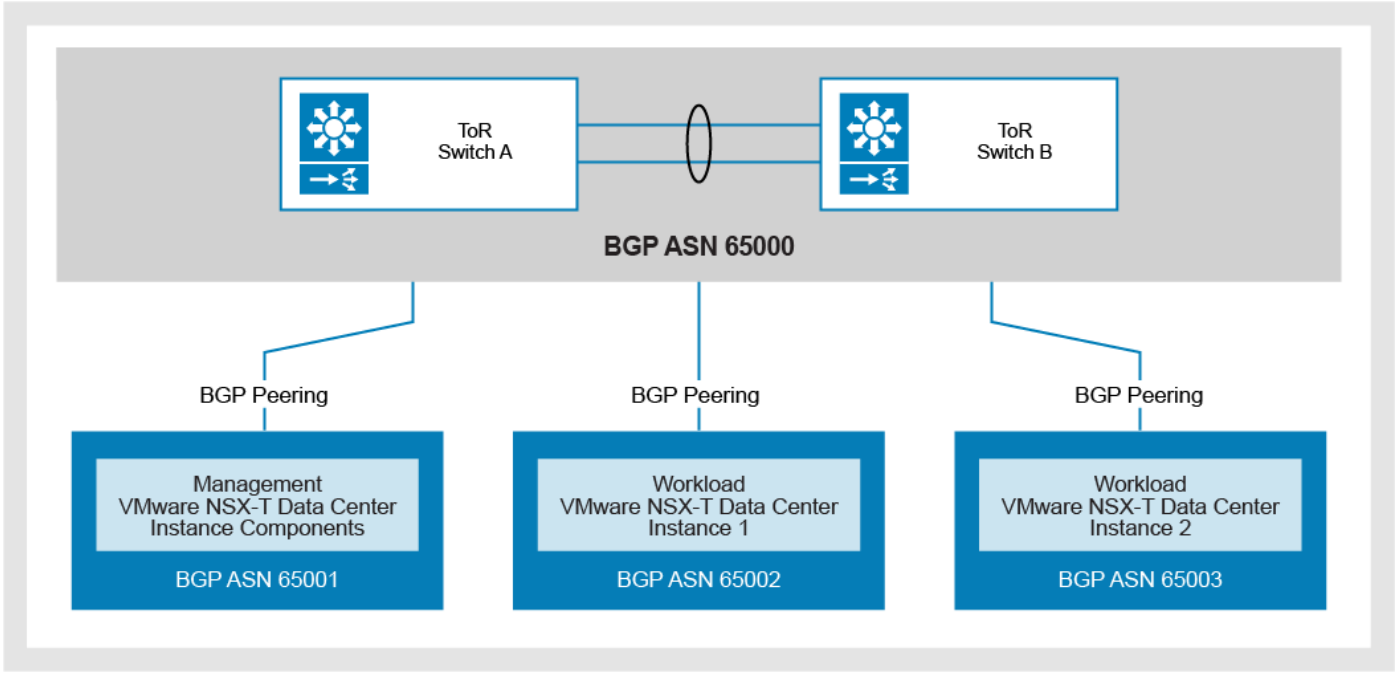
The following figure shows a topology with the VMware NSX-T Edge node for the VxBlock 1000:


ToR Switch A
ToR Switch B
vPC
FI A
FI B
vHBA0
vHBA1
VMNIC0
VMNIC1
VMware NSX-T Edge Cluster
w-mgmt Port Group VLAN 1631 VMNIC 0,1
mgmt VMkernel
w-motion Port Group VLAN 1632 VMNIC 0,1
VMware vMotion VMkernel
Overlay TZ
w-host-overlay Port Group VLAN 1634 VMNIC 0,1
Host TEP IP
Host TEP IP
w-edge-uplink01 Port Group VLAN 2731 VMNIC 0
w-edge-uplink02 Port Group VLAN 2732 VMNIC 1
VMNIC1
Mgt-IP
VMNIC2 FP-ETH0
VMNIC3 FP-ETH1
Edge NVDS
Uplink-1
Uplink-2
Overlay TZ
VLAN TZ
w-edge-overlay segment
w-edge-uplink01 segment
w-edge-uplink02 segment
Edge TEP IP
Edge TEP IP
VI Workload Edge Transport Node (VM) 1
VI Workload Domain Edge Host 1

In this scenario, the following apply:

- Each physical edge server hosts a VMware NSX-T Edge VM to connect the physical and virtual networks.
- There are two TEPs deployed on the VMware NSX-T Edge VM, which are on the w-edge-overlay VLAN.
- There are two additional TEPs deployed on the host VMware VDS connected to the w-host-overlay network.
- The w-host-overlay TEPs are not used since the physical edge hosts are dedicated for edge services.
- The edge-uplink networks are pruned from the peer-link between the ToR switches.
- These TEPs are used if non-VMware NSX-T Edge VM workloads are placed onto the host in a shared edge or compute deployment.

The following figure shows a topology with BGP on the VxBlock 1000:

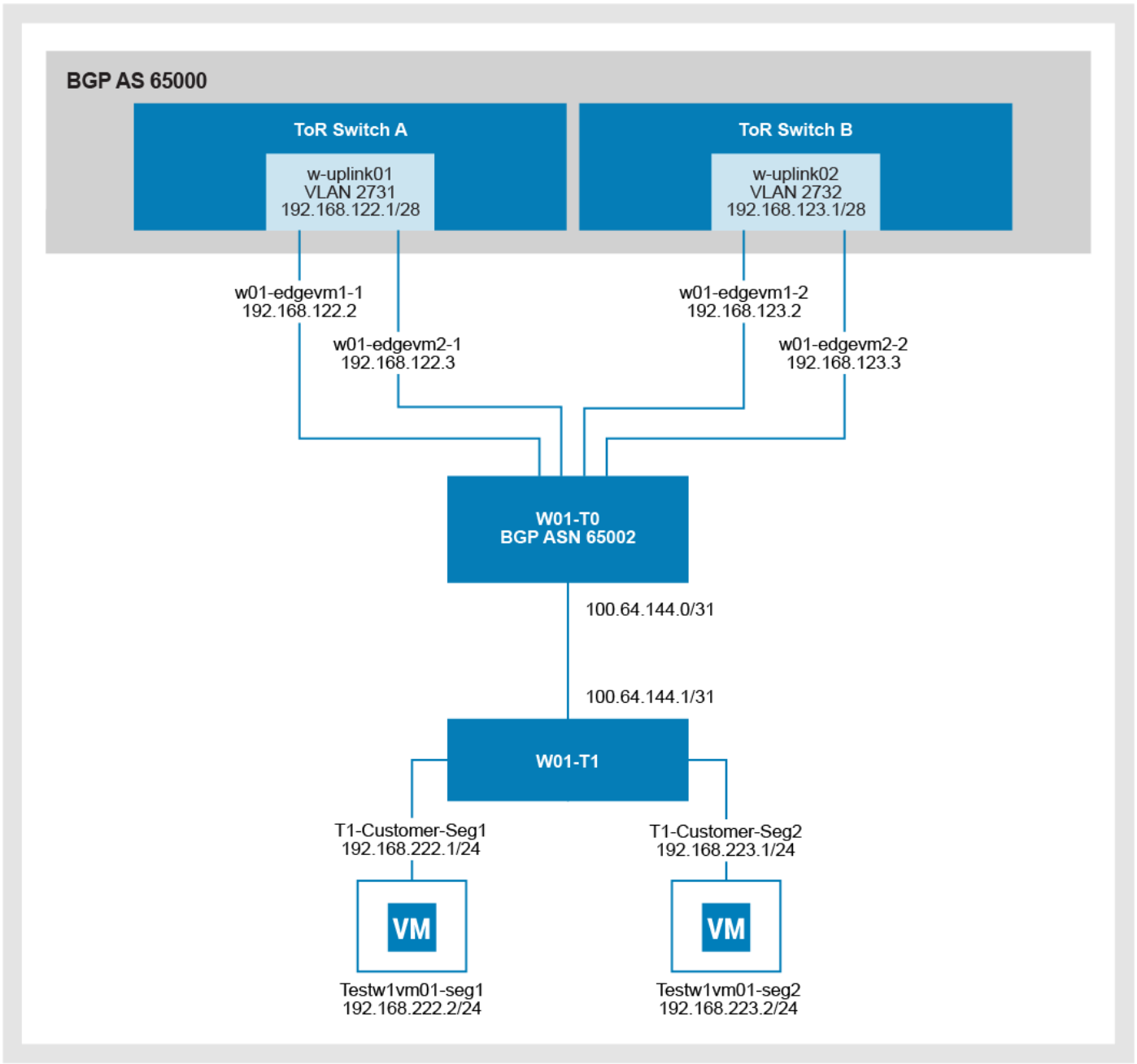

ToR
Switch A
ToR
Switch B
BGP ASN 65000
BGP Peering
BGP Peering
BGP Peering
Management
VMware NSX-T Data Center
Instance Components
BGP ASN 65001
Workload
VMware NSX-T Data Center
Instance 1
BGP ASN 65002
Workload
VMware NSX-T Data Center
Instance 2
BGP ASN 65003

In this scenario, the following apply:

- The default BGP ASN for the ToR switches is 65000. For the management domain VMware NSX-T instance, the default BGP ASN is 65001.
- The workload VMware NSX-T instance ASNs begin at 65002 and increment for each additional VMware NSX-T instance.
- The ToR switch pair supports a single BGP ASN for all VMware NSX-T components and instances to peer with. For ease of troubleshooting, a unique BGP ASN is deployed for each VMware NSX-T instance.

With virtual network segments, the Tier-0 gateway peers with the ToR Switch using eBGP. The uplink1 VLAN enables BGP peering between the Tier-0 gateway in the VMware NSX-T Edge VM and the ToR Switch on side A of the network fabric. The Uplink2 VLAN enables BGP peering between the Tier-0 gateway in the VMware NSX-T Edge VM and the ToR Switch on side B of the network fabric.

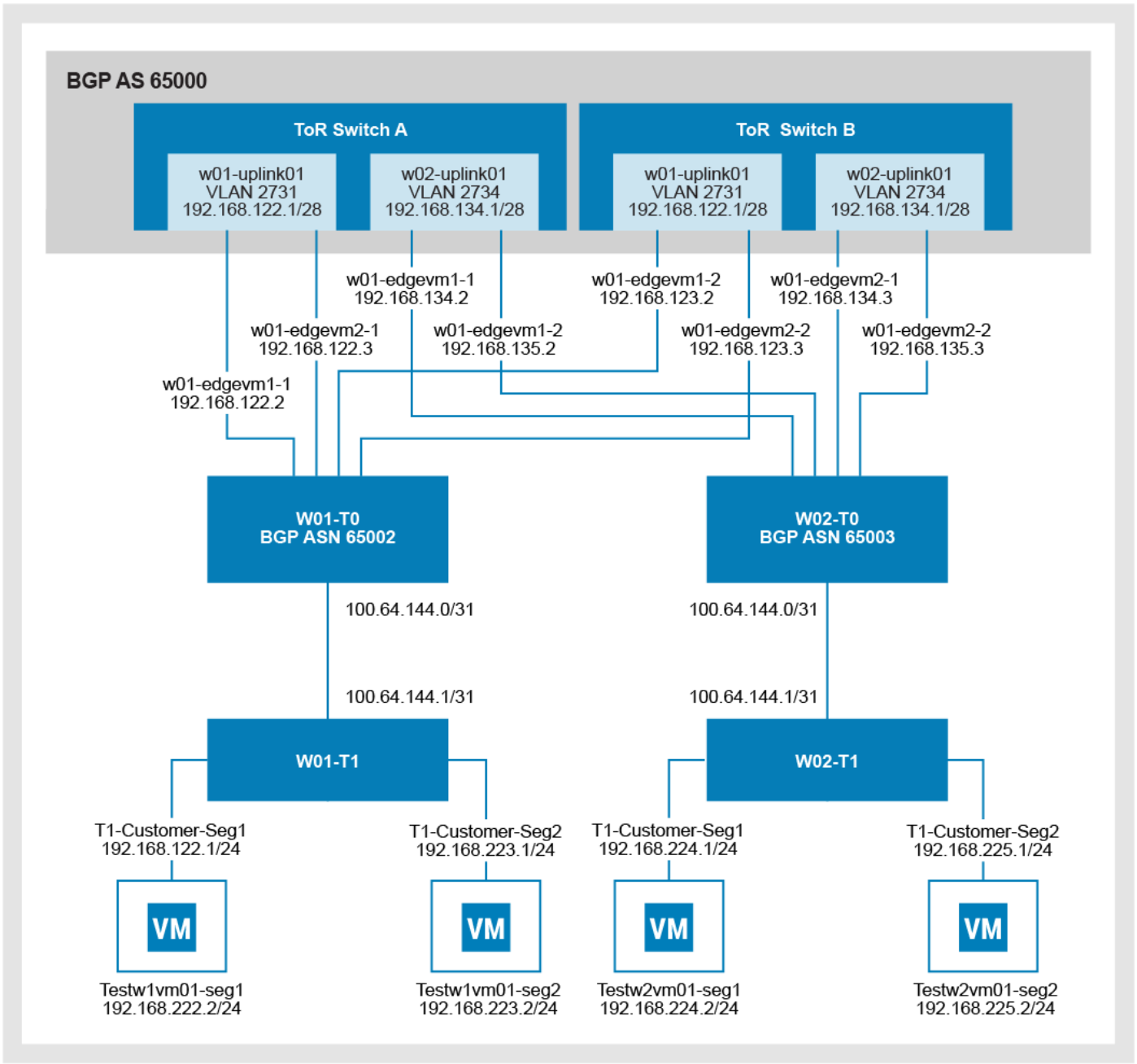
The following figure shows the routing of a single virtual network segment with multiple VMware NSX-T instances and VI workload domains:


BGP AS 65000
ToR Switch A
w-uplink01
VLAN 2731
192.168.122.1/28
ToR Switch B
w-uplink02
VLAN 2732
192.168.123.1/28
w01-edgevm1-1
192.168.122.2
w01-edgevm2-1
192.168.122.3
w01-edgevm1-2
192.168.123.2
w01-edgevm2-2
192.168.123.3
W01-T0
BGP ASN 65002
100.64.144.0/31
100.64.144.1/31
W01-T1
T1-Customer-Seg1
192.168.222.1/24
T1-Customer-Seg2
192.168.223.1/24
VM
VM
Testw1vm01-seg1
192.168.222.2/24
Testw1vm01-seg2
192.168.223.2/24

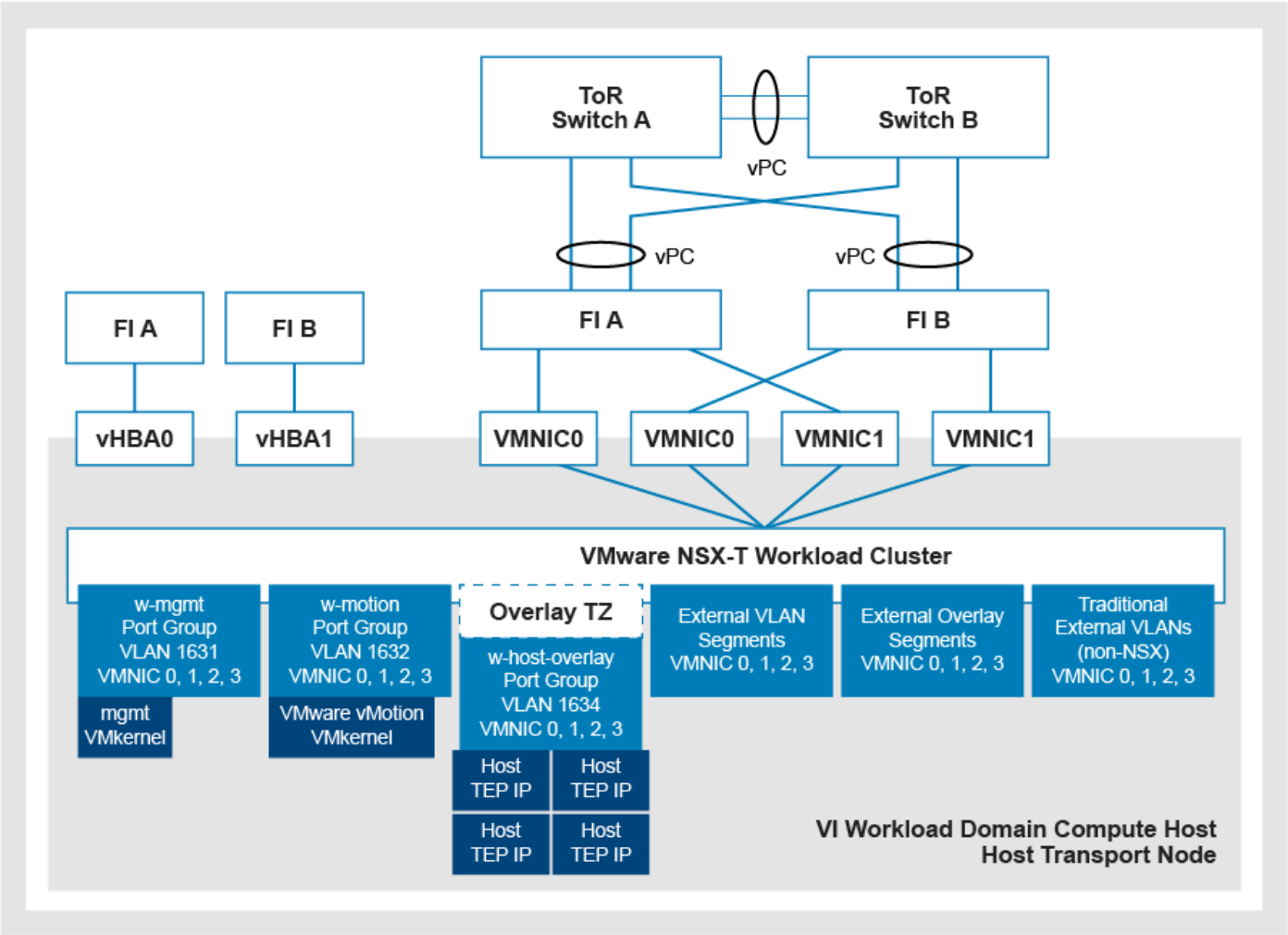
For multiple VI workload domains and VMware NSX-T instance deployments, each VI workload domain VMware NSX-T instance should have the following:

- Unique edge nodes
- Uplink01
- Uplink02
- Host overlay and edge overlay subnets
- VLANs

The following figure shows the routing of multiple VI workload domains and VMware NSX-T instances with virtual network segments:


BGP AS 65000
ToR Switch A
w01-uplink01
VLAN 2731
192.168.122.1/28
w02-uplink01
VLAN 2734
192.168.134.1/28
ToR Switch B
w01-uplink01
VLAN 2731
192.168.122.1/28
w02-uplink01
VLAN 2734
192.168.134.1/28
w01-edgevm1-1
192.168.134.2
w01-edgevm1-2
192.168.123.2
w01-edgevm2-1
192.168.134.3
w01-edgevm2-1
192.168.122.3
w01-edgevm1-2
192.168.135.2
w01-edgevm2-2
192.168.123.3
w01-edgevm2-2
192.168.135.3
w01-edgevm1-1
192.168.122.2
W01-T0
BGP ASN 65002
W02-T0
BGP ASN 65003
100.64.144.0/31
100.64.144.0/31
100.64.144.1/31
100.64.144.1/31
W01-T1
W02-T1
T1-Customer-Seg1
192.168.122.1/24
T1-Customer-Seg2
192.168.223.1/24
T1-Customer-Seg1
192.168.224.1/24
T1-Customer-Seg2
192.168.225.1/24
VM
VM
VM
VM
Testw1vm01-seg1
192.168.222.2/24
Testw1vm01-seg2
192.168.223.2/24
Testw2vm01-seg1
192.168.224.2/24
Testw2vm01-seg2
192.168.225.2/24

Hosts must have four overlay IP addresses for VCF with or without virtual network segments. The following figure shows the default VCF topology for compute transport nodes on the VxBlock 1000:


ToR Switch A
ToR Switch B
vPC
vPC
vPC
FI A
FI B
FI A
FI B
vHBA0
vHBA1
VMNIC0
VMNIC0
VMNIC1
VMNIC1
VMware NSX-T Workload Cluster
w-mgmt Port Group VLAN 1631 VMNIC 0, 1, 2, 3
mgmt VMkernel
w-motion Port Group VLAN 1632 VMNIC 0, 1, 2, 3
VMware vMotion VMkernel
Overlay TZ
w-host-overlay Port Group VLAN 1634 VMNIC 0, 1, 2, 3
Host TEP IP
Host TEP IP
Host TEP IP
Host TEP IP
External VLAN Segments VMNIC 0, 1, 2, 3
External Overlay Segments VMNIC 0, 1, 2, 3
Traditional External VLANs (non-NSX) VMNIC 0, 1, 2, 3
VI Workload Domain Compute Host
Host Transport Node

- The transport nodes connect to FI A and B through all four VMNICs.
- The four vNIC design aligns with the VxBlock System with a VMware vSphere 7.0 compute host. Service profile templates are standardized across hosts with single and dual VIC configurations.
- All port groups and VLANs are under the VMware VDS, including w-mgmt and w-vMotion.
- The overlay VLAN is added to the vNIC template for vNICs 0-3 and the ToR Switch trunk ports to FIs.