VCF 9.0 admin exam guide

9.0 whats new

simplified workflow to set up network connectivity and perform network configuration. It improves the operational efficiency of VPC environments by providing a simple way to establish external connectivity and installing Edge nodes and Edge clusters, using either NSX or vCenter

theTo simplify the deployment process leverages many defaults settings that are recommended by Broadcom, such as transport zones and uplink profile

Centralized Connectivity:

Create a Centralized connection if you have an environment that requires full-scale NSX networking services, such as DHCP, NAT, and Layer 3 services. It connects the Transit Gateway through a Tier-0 router provisioned from NSX. The Tier-0 is deployed on NSX Edge nodes and provides the interconnection to the physical fabric. Centralized connectivity supports stateful services either at Tier-0 level or at the Transit Gateway level (NAT) and supports dynamic routing, BGP/OSPF, with the physical fabric. The Centralized connectivity requires setting up of Edge nodes.

Distributed Connectivity:

Distributed Connection allows a distributed connection to the data-center fabric that requires a minimal physical fabric configuration (only VLAN/IP) and without the need to deploy Edge nodes or configure dynamic routing.

In addition to on-demand networking and distributed routing, other services available when using distributed connections are 1:1 NAT and distributed DHCP. The Distributed connectivity connects the Transit Gateway directly to a VLAN provisioned in the fabric. This happens directly on the host, which implies that the VLAN needs to be available on the ESX (on physical uplinks used by NSX vmkernel).

Virtual Private Cloud (VPC) in vCenter

VCF 9.0 supports a common networking framework aligned with industry standards for consumption from vCenter, VKS NSX, and VCF Automation. This feature allows administrators to consume natively from vCenter Networking pane virtual networks through VPCs.

VPC in vCenter provides the ability to create VPCs, and subnets inside those VPCs which can be private or publicly advertised (public network), exposing VMs to the outside through External IPs.

VPCs are fundamental in the Supervisor Service and bring a Cloud consumption model for networking in VCF. Inside a VPC users can deploy resources including StaticRoute, SecurityPolicy, K8s NetworkPolicy, TKG Cluster, PodVM and VM.

NSX VPC Transit Gateways (TGWs) simplify and streamline inter-VPC and VPC-to-external network communication by acting as a central hub for routing traffic. The TGW provides an abstraction layer, eliminating the need for tenants to configure infrastructure components directly thus avoiding misconfigurations. Tenants can attach external connections based on their needs, with support for both centralized (CTGW) and distributed (DTGW) connection types.

VPC-Ready Workload Domains

When a workload domain is created, all the prerequisites for consuming a Virtual Private Cloud (VPC) are fulfilled. This provides for the deployment of applications in a VPC onset of the deployment in NSX, vCenter and VCF Automation.

Edge Host Affinity

Edge Host Affinity improves traffic mgmt. via the Edge Node during host upgrade using vSphere Life Cycle Manager, (inimizes disruption to network operations of the Edge Node.) Instead of leveraging vMotion to migrate Edge nodes, the feature relies on higher-level

protocols to seamlessly failover traffic between Edges. This feature helps to improve Edge Cluster High Availability.

NSX Edge Platform Usability

The installation and configuration of NSX Edge Nodes and Edge Clusters have been significantly streamlined through vCenter. This enhancement simplifies workflows, reduces complexity, and improves operational efficiency for VPC environments.

Gateway Firewall Disabled by Default

Starting with NSX 9.0, Gateway Firewall is automatically disabled by default for all greenfield deployments of Tier-0 (T0) or Tier-1 (T1) Gateways. This update can enhance performance and optimize resource utilization in modern network environments.

NSX

Starting with NSX 9.0, a standalone upgrade of NSX is not supported. You must use the VCF BOM and follow the recommended process to upgrade NSX 4.x to VCF 9.0.

NSX Manager gets installed as part of VCF or when a workload domain is created so that VCF enables customers to use virtual networking features, such as VPCs.

NSX vibs are on ESXi by default and they support ESX Live Patch

NSX config is integrated with vsphere config profiles (VCPs)

NSX and vsphere upgrades are aligned / streamlined

NSX System Health Monitoring Improvement and Integration with VCF Operations

The NSX UI features a **System Health** page for centralized monitoring of the overall health of management cluster, transport nodes, and edge nodes, giving users quick insight to items such as status, alarms, resource utilization, API usage, and compute manager reachability.

NSX Certificate Management

It is best practice to run the CARR script prior to upgrading NSX Manager. The goal of running the CARR script is to ensure that the Transport Node (TN) certificates are not expiring within 825 days. If any TN certificate expires within 825 days, the CARR script can be invoked again to replace the certificate.

nsx components

NSX host component upgrade bundles are included in ESX upgrade bundles and are not available separately. NSX host components are now upgraded as part of the ESX upgrade.

other

VCF installer

VCF 9.0 ships with VCF Installer, which replaces Cloud Builder

workload domain deployment

can be done with new UI (Inventory > select VCF Instance > Add Workload Domains). During this you can deploy and config a vSphere Supervisors, and deploy / conig distributed or centralized network

Fleet Management:

license, id / access, cert mgmt. pswd mgmt. config mgmt., tag mgmt.,

VCF Health

continuously monitors the operational state of the VCF components in your environment to ensure they are functioning as expected. By proactively identifying potential issues such as

expired certificates, NTP drifts, DNS misconfigurations, and configuration errors, you can take preventative actions before these issues escalate into significant problems

Diagnostics Findings

feature offers a consolidated view of known product issues, VMSA-based security exposures, and best-practice recommendations across your VCF environment. Diagnostic Findings helps VCF administrators gain enhanced visibility into potential issues and risks, prioritize resolution efforts, and achieve uninterrupted operations.

Storage Overview

Provides visibility into health, performance, and capacity of vSAN and non-vSAN datastores

VCF Operations 9.0 introduces an integrated log management solution enabling you to explore logs, configure log-based alerts, and create dashboards directly within VCF Operations.

- Centralized Log Collection and Standardization
- Log Analysis
- Unified Cloud Proxy for Log Collection

VCF operations (formerly Aria Ops) includes fleet mgmt. and workload mobility

VCF 9 concepts

Cloud Services

Last Updated August 11, 2025

VCF Automation provides a set of cloud services which are accessible on a self-service basis using multiple interfaces, including UI, CLI, and API.

With this interface, users can provision the following types of workloads:

- VMs
- Kubernetes workloads
- Networking
- Volumes
- Secret stores
- Databases
- Harbor container registries
- External DNS
- Certificates
- AI workloads

vSphere Supervisor

VMware vSphere Supervisor ® is the foundation of VCF consumption and can be enabled during workload domain creation or directly in vCenter.

It transforms vSphere clusters into modern application platforms by embedding a platform-level Kubernetes control plane directly into ESX hosts, exposing a unified declarative API surface. This integration allows end users to provision and manage workloads, including VMs, containers via vSphere Pods, full Kubernetes clusters through VKS, OCI image registries, and data services through a consistent API interface.

vSphere Supervisor maintains enterprise-grade governance, security, and operational consistency through vCenter, VCF Operations, and VCF Automation. Its vSphere Namespaces provide the foundation for multi-tenancy, enabling GitOps-based workflows, and delivering cloud-like self-service in private data centers.

Single-Zone Deployment

A Single-Zone Supervisor deployment uses a single vSphere cluster to host both workloads and Supervisor management components.

Multi-Zone Deployment

A Multi-Zone Supervisor deployment uses three vSphere clusters, placing each cluster into a vSphere Zone. vSphere Zones are used by workloads and Supervisor management components to deliver high availability and expose each cluster as an independent, consumable availability zone. This configuration provides a resilient, HA-capable platform.

Additional vSphere Zones can be added after initial enablement. However, these additional zones will be available for workload consumption only, not for Supervisor control plane components.

Single Host

Also a Single-Zone Supervisor with a single Control Plane VM deployed to a single ESX host, with vSphere HA disabled.

Easy Supervisor

This is a Single-Zone deployment that uses VDS-based workload networking, designed as a fast and simple starting point for proof-of-concept environments and production deployments leveraging VDS.

An Easy Supervisor deployment consists of:

One Supervisor Control Plane VM

A shared network for both workload and management traffic

No load balancer

You can deploy only VMs.

Additional services, such as VKS, can be enabled by configuring a load balancer after the initial deployment.

Getting started

The first step in building a VCF platform is deploying a VCF fleet or a VCF Instance in a VCF fleet.

NOTE: for environments without Internet connection, you can use the VCF Download Tool for download required binaries.

Deploy a VCF Fleet or a VCF Instance - 3 approaches

The first step in building a VCF platform is deploying a VCF fleet or a VCF Instance in a VCF fleet.

Deploying a New VMware Cloud Foundation or vSphere Foundation Private Cloud.

Deploy a new VCF fleet. You deploy the components of the VCF fleet and of the first VCF Instance with the initial management domain. In addition to the management components of the VCF Instance, the initial management domain hosts the components of the VCF fleet too.

Deploy a new VCF Instance within an existing VCF fleet. You deploy a VCF Instance with its management domain.

Converging Your Existing Virtual Infrastructure to VMware Cloud Foundation Platform.

Converge to a new VCF fleet. You can use VMware Aria Operations and other VMware Aria Suite components in your environment as the VCF fleet. The vCenter instance and ESX hosts running VMware Aria Operations become the first VCF Instance with the initial management domain. If your environment does not have VMware Aria Operations, then you can make a vCenter and its managed hosts the first VCF Instance and deploy VCF Operations and the other required fleet components on it.

Converge to a new VCF Instance within a VCF fleet. You can add a vCenter and its managed ESX hosts as a VCF Instance with its management domain that is managed by an existing VCF fleet.

Upgrade Your Management Domain to VCF.

Upgrade the existing VMware Aria components and management domain components. Then, deploy the rest of the VCF fleet components that you need.

If VMware Aria Operations is not included in your VCF 5.2 environment, deploy VCF Operations and then VCF Operations fleet management. Then, upgrade the the other VMware Aria components in your environment and the management domain. Deploy the rest of the VCF fleet components that you need.

Add Workload Domains to a VCF Instance

After you deploy the VCF fleet and VCF Instances, you can start adding workload domains with infrastructure for consumer workloads to the VCF Instances in one of the following ways:

Deploy new workload domains.

Import vCenter instances, managing consumer workloads, as workload domains. You can import components that are compatible with VCF 5.x and upgrade to version 9.0 after you import them as a workload domain.

Add a vCenter Instance to the VCF Fleet

You can add virtual infrastructure under a vSphere Foundation license to a VCF fleet. See vSphere as a data source in VCF Operations.

Complete the Configuration of the VCF Fleet, VCF Instances, and Workload Domains

After you deploy the VCF fleet or VCF Instance or add a workload domain to a VCF Instance, complete its configuration by performing the following tasks. Assigning a license must be done right after you complete deployment.

- Assign a license to the VCF fleet, VCF Instance or workload domain.
- Configure depot settings.

- Configure identity and access management.
- Configure backup of the management components.
- Configure certificate management in VCF Operations.
- Configure password management.

Add Workload Domains to Your Cloud Organization Structure

You can add workload domains to an organization in VCF Automation provider management for consumption by end users. You can create two types of organizations in VCF Automation - All Apps Organizations for workload domains with Supervisor clusters that run both containers and VMs, and a VM Apps Organization for workload domains with clusters that run only VMs.

You cannot use the same workload domain in an All Apps Organization and a VM Apps Organization.

- Deploy and configure vSphere Supervisor.
- Add an identity provider for your organizations.
- Create organizations for all applications for the workload domains with Supervisor instances.
- Create an organization for VM applications for the workload domains that do not run Supervisor instances.

When creating an Organization for All Applications, during the regional networking setup steps, the system will deploy and configure a default VPC, a provider tier-0 gateway, a VPC connectivity profile, and outbound default SNAT rules

Detailed Journeys

For visual guides to the sequences of getting started operations, see the following VCF journey maps.

- Build Journey - Install a New VMware Cloud Foundation Deployment link
- Build Journey - Converge Your Infrastructure to VMware Cloud Foundation from Existing vSphere and VMware Aria Operations link

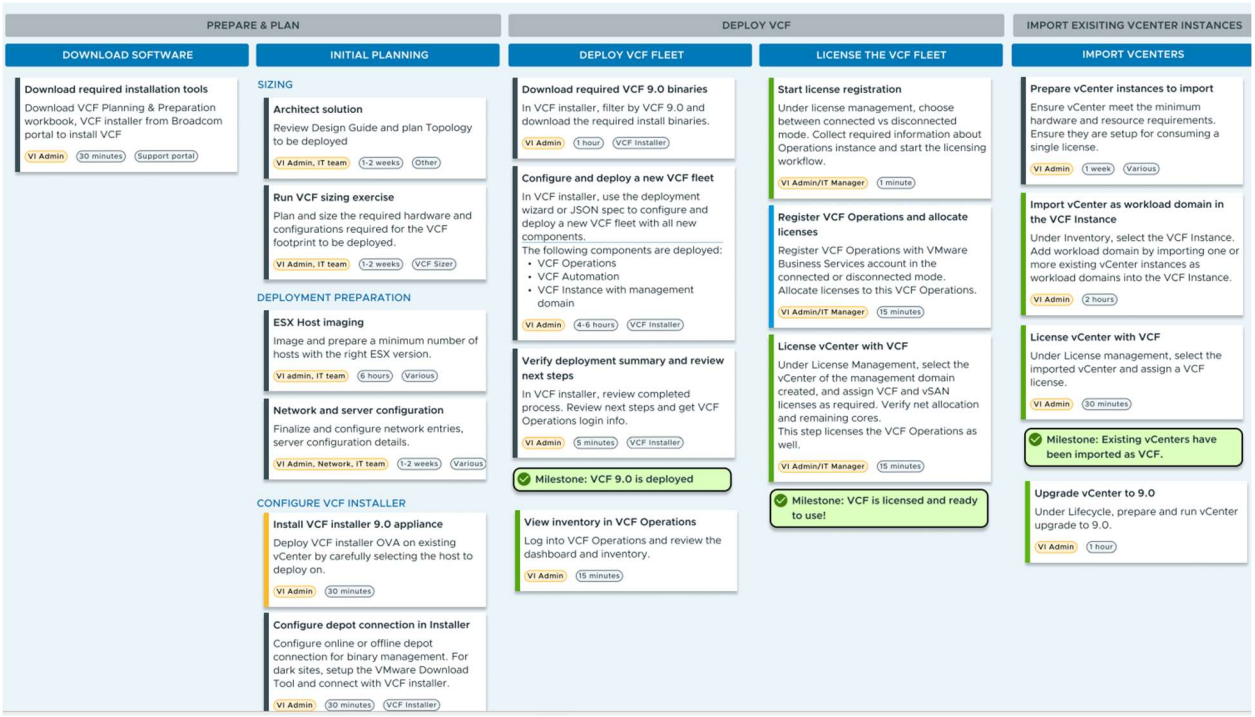
- Holistic Journey - Fully Adopt VMware Cloud Foundation from Existing vSphere and VMware Aria Operations link

Planning and Preparation

VCF planning / prep workbookd: link

VCF Planning Tools maximums ports

Install a new VCF Deploy Journey



Converging your existing components to vSphere Foundation or VCF with version 9.0

Before converging

Before deciding which convergence path to follow, you can independently upgrade your existing pre-version 9.0 standalone components, that are not yet part of a VCF Instance, to version 9.0. For example, you can upgrade your vCenter, ESX, and Aria Operations to version 9.0. This component configuration is the minimum requirement to evaluate the capabilities of verion 9.0, for up to 90 days, before you licence the products from VCF Operations.

Starting with VCF and vSphere Foundation 9.0, you manage your licenses through VCF Operations across your entire fleet and can manage licenses for multiple VCF Operations instances from the VCF Business Services console (vcf.broadcom.com), a part of the Broadcom Support Portal

Converging Existing Virtual Infrastructure to a VCF or a vSphere Foundation Platform

The process for converging includes complying with the general requirements and scenario-specific prerequisites, manual upgrade procedures of your existing components, and deployments and configurations performed by VCF Installer. In the supported scenarios, the manual high-level steps upgrade your existing components to version 9.0 and prepare your infrastructure for the VCF Installer workflows. By using the VCF Installer workflows, you can converge the components to a new VCF Fleet or a new VCF Instance in an existing VCF fleet.

Converging a vSphere ONLY environment on vSphere 8 to VCF 9, requires you to deploy the following new items:

- VCF Installer (which becomes SDDC Manager)
- VCF Ops
- VCF Ops collector (to collect data for VCF Ops from VCs, etc)
- Fleet Manager

Supported scenarios:

Summary: requires VC / ESXi. vROps is optional, with or without Aria LCM, Automation is optional but requires Aria LCM

- Converging a vCenter Instance and ESX Hosts
- Converging a vCenter Instance, ESX Hosts, and VMware Aria Operations
- Converging a vCenter Instance, ESX Hosts, VMware Aria Suite Lifecycle, and VMware Aria Operations
- Converging a vCenter Instance, ESX Hosts, VMware Aria Lifecycle, and VMware Aria Automation
- Converging a vCenter Instance, ESX Hosts, VMware Aria Lifecycle, VMware Aria Operations, and VMware Aria Automation

Converging existing NSX instances is not supported in VCF 9.0. Instead, you deploy a new NSX instance during the converge operation by using VCF Installer

- You can choose between an HA deployment model with a cluster of 3x NSX Managers or a Simple-node deployment model with 1 NSX Manager.
- You can choose to configure overlay traffic on a management VMkernel or on a VLAN-backed segment.

Supported Storage

- Sufficient free space for VCF components
- Datastore writeable across all hosts in the clusters
- Simple deployment
    - Min 3 hosts for vSAN, or 2 hosts for share storage
    - High availability deployments: 4 hosts
- Any supported vSphere storage type.
- If the default cluster includes multiple datastore types, VCF determines the primary datastore using the following priority:
    - vSAN
    - NFS v3
    - VMFS
    - NFS 4.1
    - vVols*

- If you are using a JSON specification file to converge, you can use the existingDatastoreName property to override the priority order and use a specific datastore.
- vSAN Stretched Clusters (ESA, OSA, or ESA storage clusters) with at least 3 ESX hosts in each availability zone and a witness host deployed in a vSAN witness zone that is different from the availability zones
- Two-node vSAN clusters for remote offices/branch offices (ROBO) with two ESX hosts and one witness host for VCF simple deployments
- vSAN OSA clusters, where deduplication and compression are either both activated or both deactivated
- vSAN OSA clusters with activated compression only

Supported network

- Virtual Distributed Switch (VDS) 8.0 or later
- Ports aligned with VMware Ports and Protocols
- vCenter instance with temporary IP address
- Statically assigned VMkernel IP addresses
- Dedicated network for VMware vMotion
- vSphere Distributed Switches (VDS) with enabled link aggregation control protocol (LACP)
- ESX hosts with a combination of standard switches and VDS
- ESX hosts with multiple physical uplinks of minimum of 10Gbps, that are assigned to a vSphere Distributed Switch
- ESX hosts with a single pNIC with a minimum of 10 Gbps speed, that is connected to a standard switch
- Clusters using shared vSphere Distributed Switches
- ESX hosts with a single Physical Network Adapter (pNIC)

Not supported network

- Cisco virtual switches
- vCenter instances without a vSphere Distributed Switch
- Custom vCenter ports for client connections
- Environments using ports not aligned with VMware Ports and Protocols

- vCenter instances with existing NSX registrations
- Multiple VMkernel interfaces for vMotion traffic
- Dynamically allocated VMkernel IP addresses
- You can move to statically assigned IP addresses. See Edit a VMkernel Adapter Configuration.
- Shared networks for VMware vMotion
- Multiple NSX Manager instances in a vCenter instance
- NSX Bare Metal Edge nodes

Supported compute

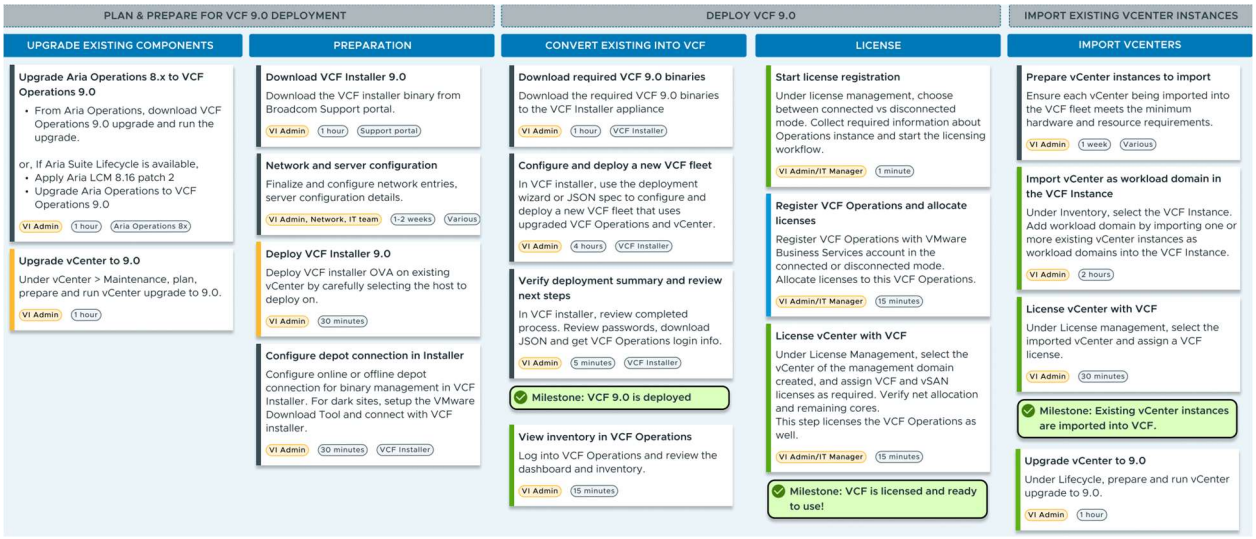
- Virtual machine of vCenter instance hosted on one of the clusters that is managed by the same instance. You can move the virtual machine to a supported location by using VMware vMotion. See Migrating Virtual Machines Between vCenter Systems.
- Clusters using vSphere Configuration Profiles
- Clusters using vSphere Lifecycle Manager images. You can convert clusters that use baselines to use images before upgrading to ESX 9.0. See Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images.
- Clusters using fully automated Dynamic Resource Scheduler (DRS)
- Standalone ESX hosts and single ESX host clusters, if your vCenter instance has an additional cluster that meets the cluster requirements. You can manually perform the lifecycle management of the standalone ESX hosts and single ESX host clusters by using the vSphere Client.
- Clusters using fully automated Dynamic Resource Scheduler (DRS)

Unsupported compute:

- Clusters managed by Dell VxRail
- vCenter instance VM hosted on a cluster that is managed by a different vCenter instance
- Clusters using baselines for lifecycle management
- vCenter instances with Enhanced Linked Mode (ELM). You can remove your vCenter from the ELM. See Splitting Enhanced Linked Mode (ELM).
- Clusters using manual or partially automated Dynamic Resource Scheduler (DRS). You can set the automation level to fully automated. See Edit Cluster Settings.

- Password Management of imported ESX hosts via the Password Management Console of VCF Operations
- Adding hosts to imported clusters without the use of the vSphere Client
- Partial import of clusters
- All clusters managed by a vCenter instance are imported together
- Clusters that use vCenter High Availability (VCHA). You can deactivate VCHA and re-enable it after the converge process. See Remove a vCenter HA Configuration.

Convert (converge) existing environment to VCF 9.0



#	VCF Component	Converging existing standalone components to VCF 9.0
1	Aria Suite Lifecycle	Yes*
2	Aria Operations / VCF Operations	Yes, automated or manual
3	Aria Automation / VCF Automation	Yes
4	Aria Automation Orchestrator / VCF Operations orchestrator	Yes
5	Aria Operations for Networks / VCF Operations for networks	Yes
6	Aria Operations for Logs / VCF Operations for logs	No**
7	SDDC Manager	N/A
8	HCX / VCF Operations HCX	Yes
9	NSX	No***
10	vCenter	Yes
11	ESX	Yes
12	vSAN	Yes

* VMware Aria Lifecycle is not upgraded to version 9.0. After the VCF Operations fleet management appliance is deployed, the existing connection with VMware Aria Operations is imported to the new appliance.

** No upgrade path for VMware Aria Operations for Logs. Redeploy of VCF Operations for logs 9.0 is required.

*** NSX 4.x deployments that are not part of VCF instances can be upgraded to version 9.0 only after they are first imported to existing VCF instances as workload domains.

The upgrade to VCF Operations 9.0 upgrades your VMware Aria Operations instance to VCF Operations 9, installs the VCF Operations fleet management appliance, and transfers the existing VMware Aria Operations and VMware Aria Automation integrations from the VMware Aria Suite Lifecycle appliance to the newly deployed fleet management appliance. You later use that VCF Operations instance to upgrade other management components.

Upgrade existing VCF 5.2 to 9.0

If you have existing VCF 5.2, you can upgrade to 9.0

#	VCF Component	Upgrading to version 9.0
1	Aria Suite Lifecycle	Yes*
2	Aria Operations / VCF Operations	Yes
3	Aria Automation / VCF Automation	Yes
4	Aria Automation Orchestrator / VCF Operations orchestrator	Yes
5	Aria Operations for Networks / VCF Operations for networks	Yes
6	Aria Operations for Logs / VCF Operations for logs	No**
7	SDDC Manager	Yes
8	HCX / VCF Operations HCX	Yes
9	NSX	Yes
10	vCenter	Yes
11	ESX	Yes
12	vSAN	Yes

* VMware Aria Lifecycle is not upgraded to version 9.0. After the

VCF Operations fleet management

appliance is deployed, the existing connection with VMware Aria Operations is imported to the new appliance.

The upgrade from VCF 5.2 to VCF 9.0 begins with upgrading SDDC Manager. After SDDC Manager is upgraded to 9.0, then other components (VC, ESXi, NSX, Ops) are made available to download.

Ops for Logs

No upgrade path for Aria Operations for Logs. Deployment of VCF Operations for logs 9.0 is required.

You can use the Log Data Transfer option in VCF Ops > Administration > Control Panel to transfer up to 90 days old dat from Aria Ops for Logs 8.x, choose Initiate Transfer

Paths to building workload domains with version 9.0

After you create your management domain, you can proceed with the analogous, workload domains-specific guidance.

create a new workload domain

general requirements

A vSphere Lifecycle Manager cluster image must be available for the default vSphere cluster of the workload domain. See Managing vSphere Lifecycle Manager Images for VMware Cloud Foundation.

Hosts must be commissioned with the target principal storage type. See Managing ESX Hosts in VMware Cloud Foundation.

If you are using vSAN principal storage type, SSD disks or NVMe disks without pre-existing disk partitions must be available with each host.

If you are using vVols principal storage type, add a VASA provider to the inventory. See Add a VASA Provider for vVols Storage in Workload Domains.

> Starting with VMware Cloud Foundation 9.0 and vSphere Foundation 9.0, the vSphere Virtual Volumes capability, also known as vVols, is deprecated and will be removed in a future release of VMware Cloud Foundation and vSphere Foundation

Networking requirements:

A static IP pool or a DHCP server configured and advertising IP addresses on the workload domain's NSX host overlay (HOST TEP) VLAN.

Each host must have at least one physical NIC, with a minimum of 10 Gbps speed, connected to a standard switch.

A network pool with free IP addresses must be available.

The IP addresses and Fully Qualified Domain Names (FQDNs) for the vCenter and NSX Manager instances must be resolvable over DNS

VMware Cloud Foundation supports creating workload domains with a vSphere Distributed Switch with link aggregation control protocol (LACP) enabled, but you must use the SDDC Manager API to do so.

1. In VCF Operations, select Inventory > Detailed View.
2. Expand VCF Instances and browse to the VCF instance in which you want to create a new workload domain.
3. Click Add Workload Domain > Create New.
4. Review the prerequisites, click Select All, and click Proceed.
5. Enter the General Information details and click Next. Options:
    a. Workload domain name
    b. Enable vsphere supervisor
    c. Sso domain name
    d. Password creation
6. Enter VC details (FQDN, root password)
7. Enter cluster details (name, vsphere zone name, select cluster image)

8. NSX Manager details
    a. Deployment size, app size,
    b. appliance 1-3 FQDNs, app cluster FQDN
    c. admin password, auditor password
    d. configure network connectivity and VPC external IP blocks
        i. If you select Centralized Connectivity, configure it after the workload domain is created to make it VPC-ready.
        ii. If you select Distributed Connectivity, enter the following:
            1. **VLAN ID:** A dedicated VLAN network is required for the distributed gateway's external connectivity.
            2. **Gateway CIDR IPv4 Address**: The gateway CIDR IP address should be the same as the VLAN default gateway configured in the external router (TOR).
            3. **External IP Block:** Advertised CIDRs that allow outside connectivity to VPC workloads either on public subnets or through external IPs. The external IP block must be the same as, or a sub-block of, the configured Gateway CIDRs.
            4. **Private - Transit Gateway IP Block:** Private CIDRs that are available for inter-VPC (Virtual Private Cloud) communication and are not advertised by the Transit Gateway to the outside datacenter.
9. **Storage details**
    a. vSAN (optionally select Enable vSAN ESA) vSAN storage clusters (formerly known as vSAN Max) require vSAN ESA
    b. NFS
    c. VMFS on FC
    d. vVol
10. vSAN details
    a. FTT, space efficiency,
    b. Vsan cluster type (vSAN HCI, vSAN storage)
    c. Network option: select **vSAN Storage Client Network** to isolate client or application network traffic from vSAN Storage
    d. Storage policy
11. NFS details
12. vVOL details
13. Select the ESX hosts to use for creating the workload domain and click Next.

14. The ESX hosts must be commissioned with the same storage type as the primary cluster of the workload domain. For example, select hosts commissioned for vSAN ESA storage for a vSAN ESA workload domain.
15. vDS details (select a profile: default, storage traffic separation, NSX traffic separation, storage traffic and nsx traffic separation, cusom switch config)
16. vSphere Supervisor details
    a. supervisor name and CIDR
    b. ESXi mgmt. vmk settings
    c. Vlan id
    d. Control plane ip range, mask, GW
    e. vDS
    f. NSX project
    g. VPC connectivity profile
    h. Private (transit GW) CIDR
    i. Private CIDR
    j. Workload DNS, NTP
17. Review, click finish , watch for successful validation
18. Monitor progress using : Fleet ManagementTasks to monitor progress.

Import an existing vcenter to create a workload domain

https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/building-your-private-cloud-infrastructure/working-with-workload-domains/import-an-existing-vcenter-to-create-a-workload-domain.html

To import existing infrastructure as a workload domain

you can import a VC, with or without NSX Manager (if without, you can deploy NSX manager during the import). Includes All vsphere clusters (cannot choose a subset)

minimum versions

- VCF 9.0 instance from which to perform the import
- vCenter 8.0 Update1
- ESX 8.0 Update 1

- NSX Manager 4.1.0.2

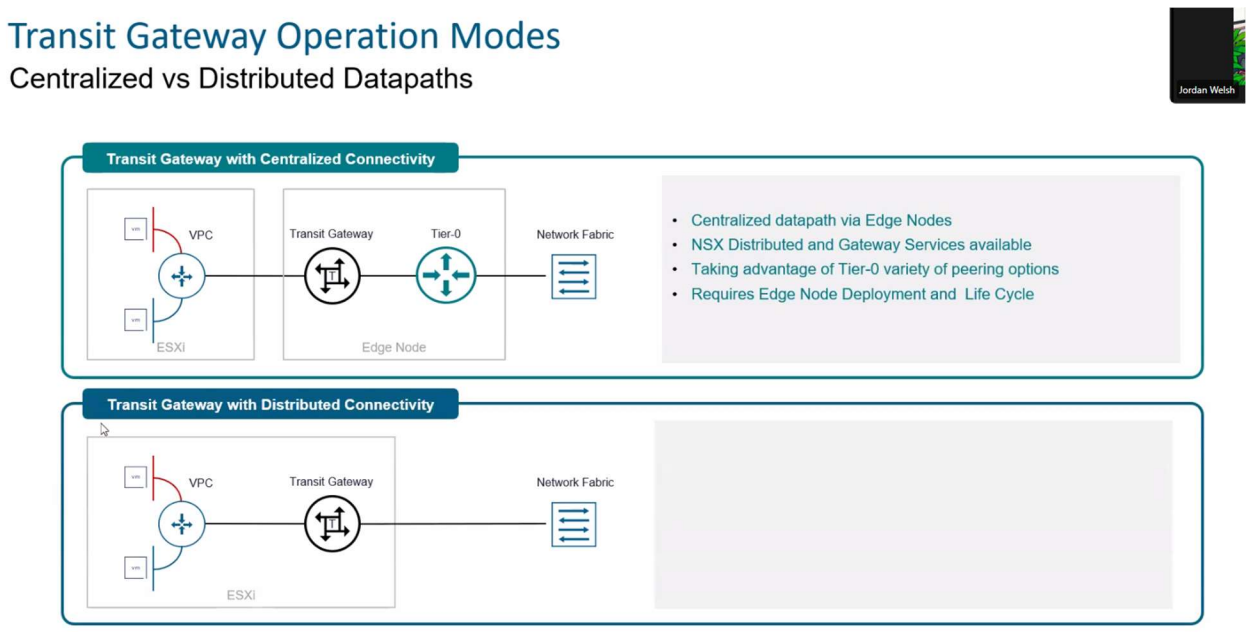
Nearly identical supported / unsupported compute, storage,network as for convergence

- In VCF Operations, select Inventory > Detailed View.
- Expand VCF Instances and browse to the VCF Instance into which you want to import a workload domain.
- Click Add Workload Domain > Import a vCenter.
- Enter a workload domain name and click Next.
- Select a vCenter and optionally an NSX Manager instance to import as a workload domain and click Next.
    - If VC is connected to NSX Manager, then select the VC, activate the toggle, and enter NSX details (Mgr VIP FQDN, admin pswd, root pswd, audi pswd)
        - If NSX Manager is 9.0 or later, the Edge nodes are imported and their passwords reset (can be retrieved from VCF credential store)
        - Choose Enable Edge Cluster Sync and Import NSX Edge node VMs to ensure this is applied now and to Edge nodes added later
    - Otherwise, provide VC details (FQDN, root pswd, SSO user, SSO pswd)
- Conform certificate thumbprints for VC, and NSX
- If you are Not importing the NSX manager connected to the VC, then enter the NSX details (choose to create a new NSX Manager or join an existing one)
    - Choose an existing NSX
    - Otherwise, provide details for a new NSX Manaager instance
        - Deployment size, appliance size
        - App 1-3 FQDN, Cluster FQDN
        - Admin password, auditor pswd,
        - NSX overlay netwoking
- Run validations, prechecks, review, click Finish

upgrade your workload domain components

Transit GW

Centralized vs Distributed



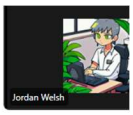
Distributed does not require edge node framework. Does not allow Gateway servercies, but does allow NSX distributed services. Transit GW is provided by ESXi

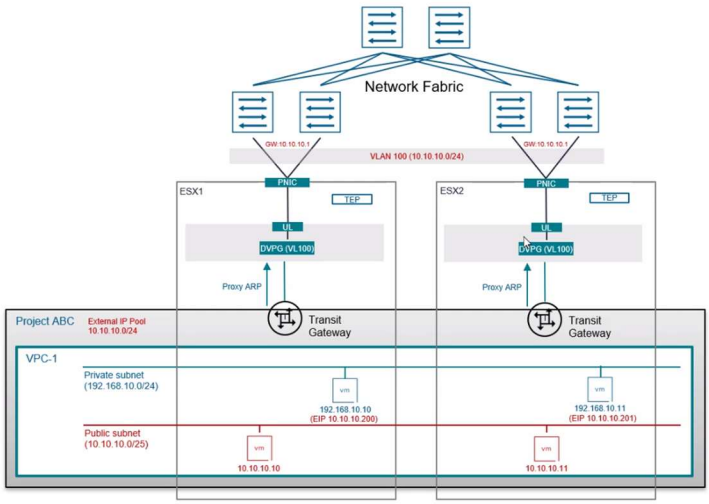
Centralized requires Edge node deployment, and supports NSX distributed and Gateway services. Transit GW is provided by Edge Node.

Example model of distr connectivity

Transit Gateway with Distributed VLAN Connectivity

Simplified External Connectivity Model





Feature

Simplified external connectivity model that does not require deploying edge nodes and the advanced routing configuration

Compatible with existing VLAN networking model

Benefit

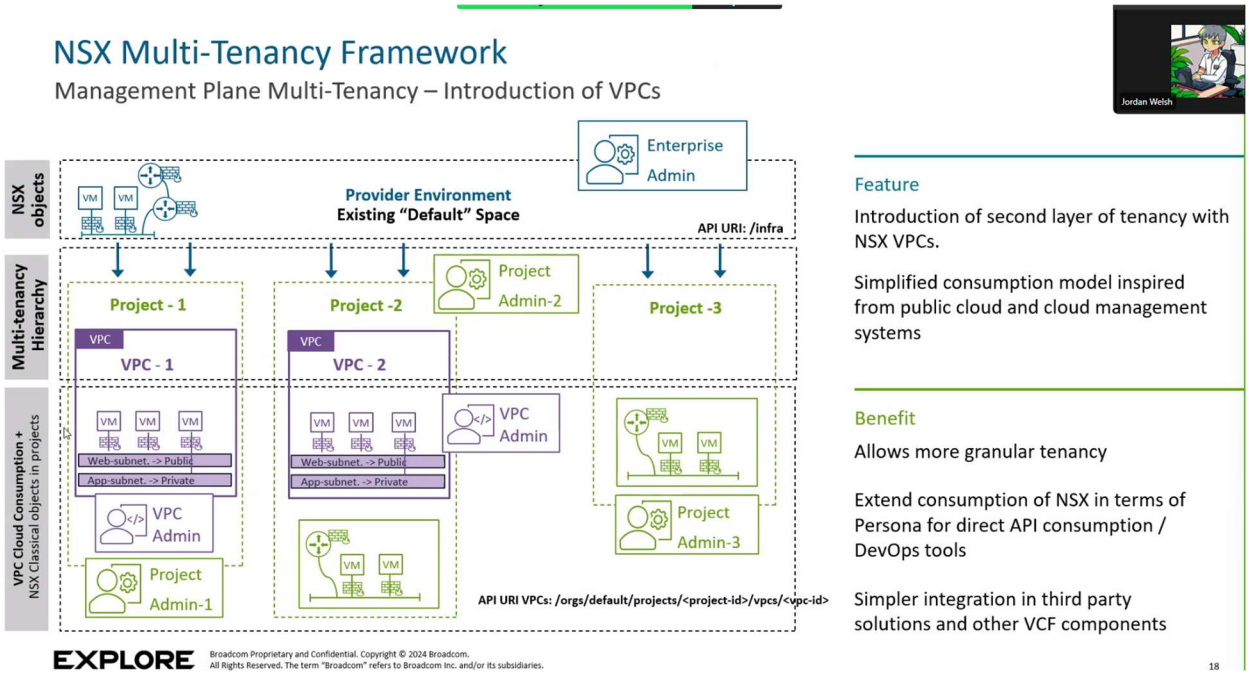
Easy to Deploy

Reduced Footprint

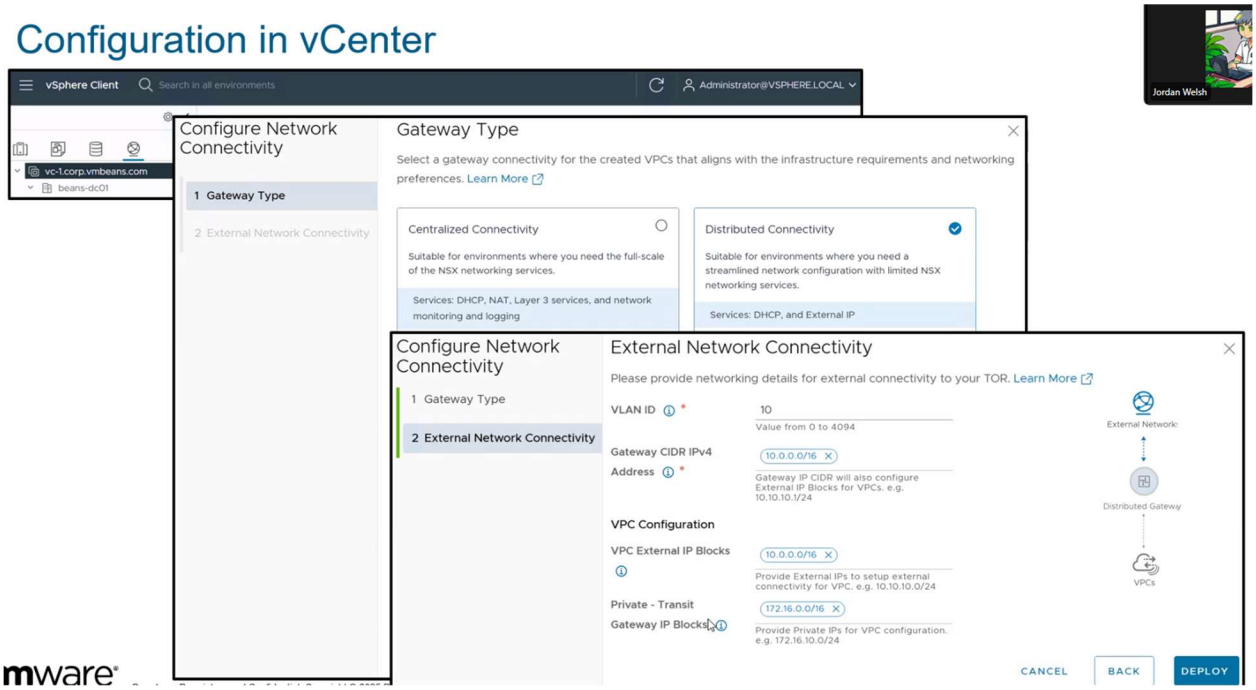
Path to full NSX virtual networking adoption

vmware

Nsx multi-tenancy framework



VCP / GW Config steps



You are viewing Jordan Welsh's screen REC View Options

Base NSX Logical Design with VPC

Simplest way to organize workload is at segment and the VPC level

Single VC and NSX Domain (Singe VI WLD)

Single Active/Active Stateless Tier-0 Gateway

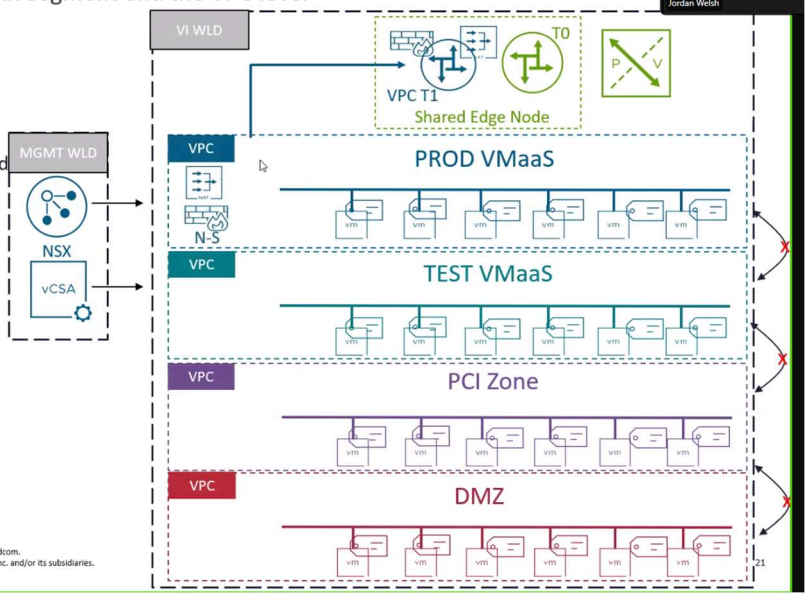
A VPC is mapped to a workload type or a tenant

Shared NSX Edge Cluster for the Tier-0 gateway and the stateful VPCs

Each VM has 5 to 8 Tags

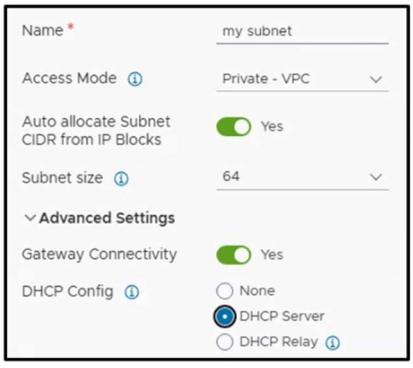
- Tags paves the way to manage inventory, grouping, seed the baseline security policy
- VPCs provide a first level of workload organization

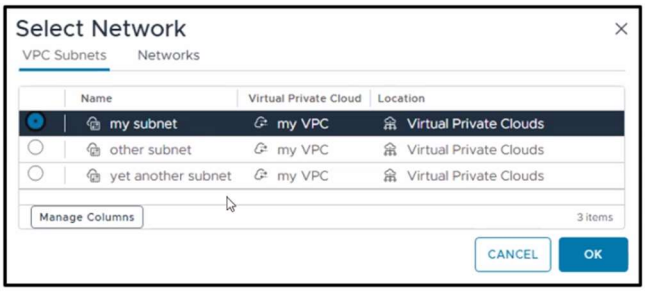
Security policies can be centrally managed by the Enterprise Admin or offloaded to the VPC Admin



EXPLORE
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

VPC Admin – Create network





VCF password management

On the password management page, you can manage passwords for VC, ESXi, backup, nsx edge, nsx manager, psc

For example for nsx maanger, you can:

- **Update** – in VCF Ops, You use the Update action to provide a new password for an account and change that password on the server side (where the account resides) and on the client side (where the account is used).
- **Rotate** – in SDDC Manager, You use the Rotate action to change the password with an auto-generated password on both server (where the account resides) and client (where the account is used) sides.-
- **Remediate**: in VCF Ops, You use the Remediate action to provide the new password on the client side (where the account is used) after the password is changed on the server side (where the account resides)

In VCF Ops, you can Update and Remediate:

VCF Instance / Domain Components	Local Account
ESX	root
vCenter	root
SDDC Manager	backup
NSX	root admin audit
VCF Management Components	**Local Account**
VCF Operations	root admin
VCF Operations fleet management	root admin@local
VCF Operations for networks	consoleuser

VCF Instance / Domain Components	Local Account
	support admin@local
VCF Operations for networks collector	consoleuser support
VCF Operations for logs	root admin
VCF Automation	admin
VCF Identity Broker	vmware-system-user

You can also use the SDDC Manager API to look up and manage credentials.

Update

- Requires **Fleet Management: Passwords** > **Manage** and **View**
- Can only update one pswd at a time
- In VCF Operations, click **Fleet ManagementPasswords** > **Passwords**
- Select **VCF Management** or **VCF Instances,** select a VCF, select a component
- Click **Update Password**
- Enter a password

Remediate

- Requires **Fleet Management: Passwords** > **Manage** and **View**
- Can only remediate one pswd at a time
- In VCF Operations, click **Fleet ManagementPasswords** > **Passwords**
- Select **VCF Management** or **VCF Instances,** select a VCF, select a component, where you already manually changed the password
- Click **Remediate Password**
- Enter a password

Network models

Network Fabric Models

There are three

Network Fabric Models

which a vSphere cluster is built upon:

- Single-Rack Network Fabric Model
- Multi-Rack Network Fabric Model
- Multi Availability Zone Network Fabric Model

VPCs in VMware Cloud Foundation provide isolated cloud environments, allowing different tenants, projects, or departments to operate securely and independently with self-service access to subnets, network services (like NAT), firewall rules, and load balancing.

VPC networking model

1. **Provider Gateway (Tier-0 Gateway):** The provider gateway is a virtual router that connects the virtual network to the physical infrastructure. It handles dynamic or static routing to the physical network, advertising the network ranges of the virtual network, including public subnets, NAT IPs, and load balancer VIPs. In VCF 9.0, the provider gateway is essentially the same as the Tier-0 or VRF gateway found in the NSX segment networking model. The provider gateway can be shared among one or more tenants, enabling them to link their VPCs to the physical fabric via the transit gateway.
2. **Transit Gateway (TGW):** The transit gateway's primary role is to interconnect VPCs among each other and to the provider gateway. The transit gateway can bypass the provider gateway and directly connect to the physical fabric via an external VLAN,

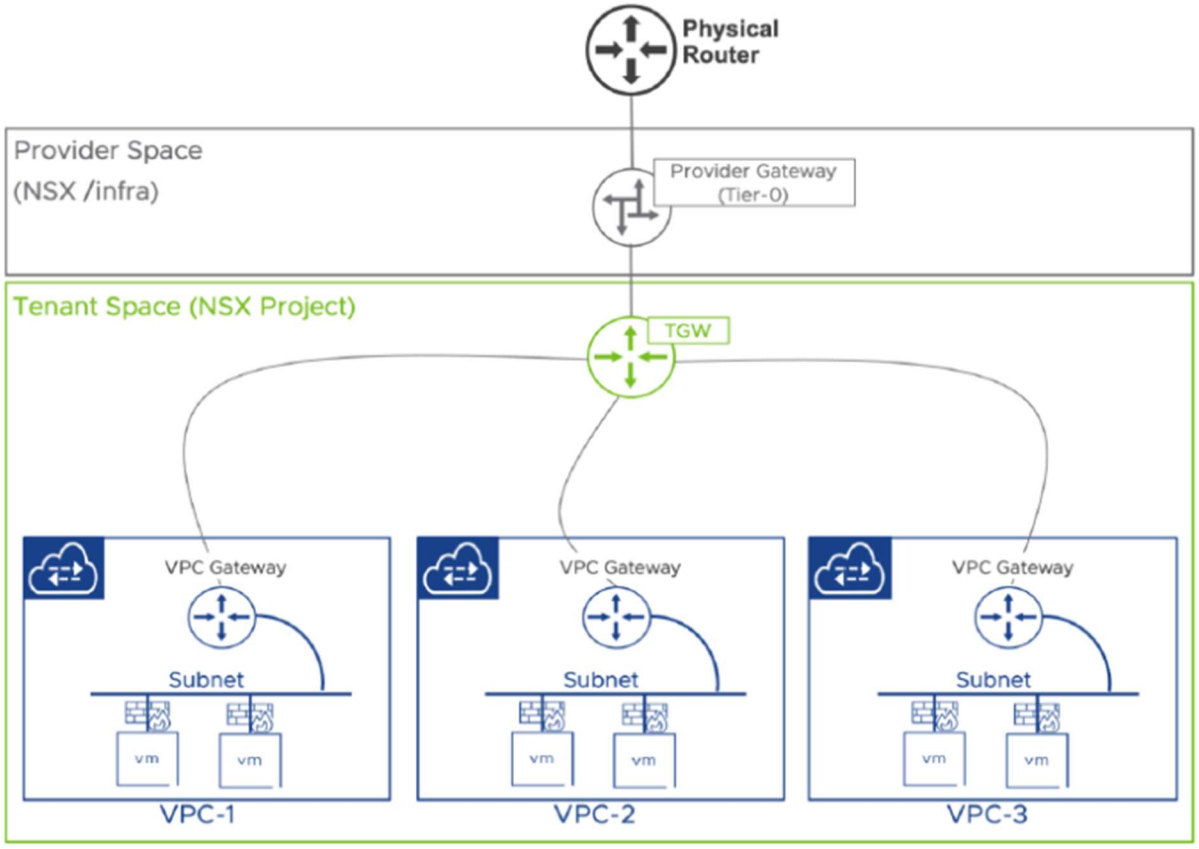
eliminating the need for NSX Edge nodes or any routing to the physical fabric. This setup is called the Distributed Transit Gateway (DTGW) because its functionality is fully distributed. DTGW does not support VCF Automation or Supervisor integration, as services like Source NAT and Load Balancing are unavailable. However, 1:1 NAT using an external IP can be configured for VPCs connected to a DTGW.

3. **VPC (Virtual Private Cloud):** A VPC is a dedicated networking domain available to a cloud user, where workloads are connected based on network requirements. A VPC consists of subnets, which are essentially NSX logical networks in the VPC Networking Model. Each VPC is automatically assigned a VPC Gateway that routes traffic between subnets within the same VPC. East-West traffic is permitted unless restricted by a Distributed Firewall (DFW). Connectivity to external endpoints requires the VPC to be connected to a transit gateway (TGW) and depends on the type of subnet in which the workloads are placed. There are three subnet types within a VPC:

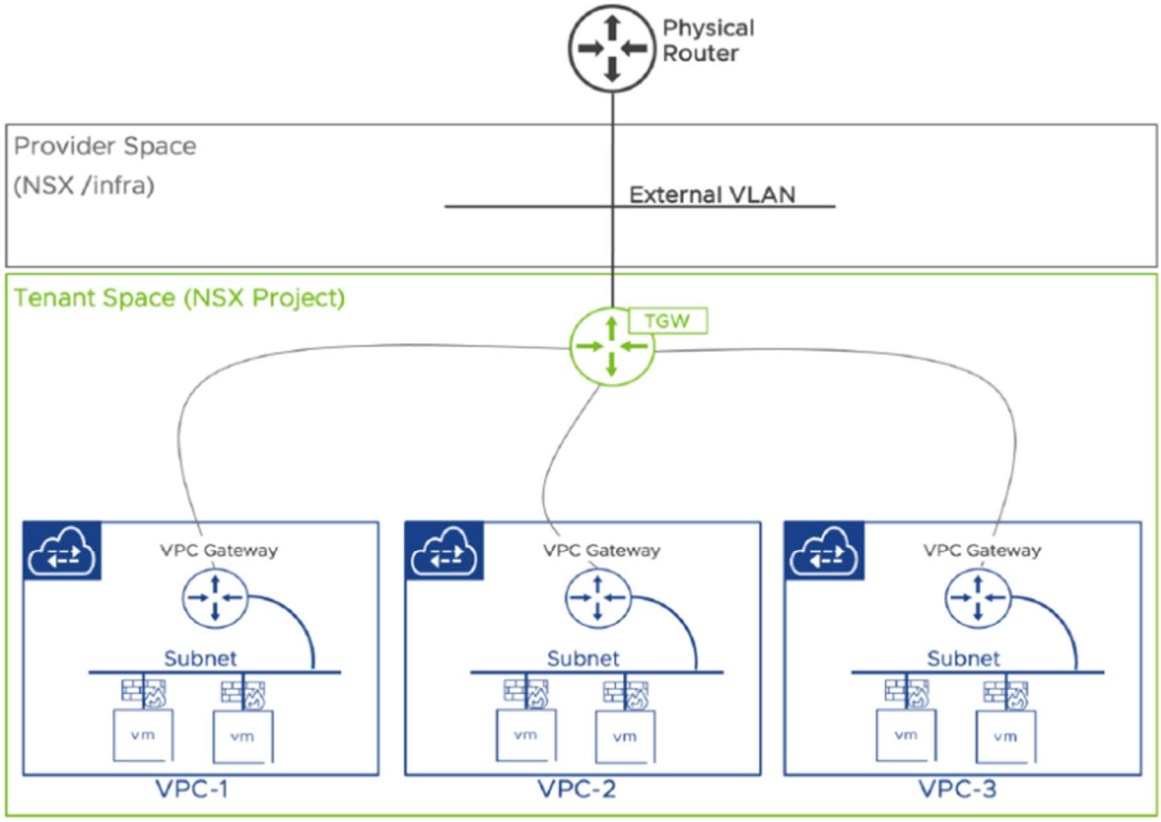
-
    - **Private VPC:** Not routable outside the VPC. Workloads in a private VPC subnet require NAT to communicate with external workloads.
    - **Private TGW:** Not routable north of the TGW. Workloads on a private TGW subnet need NAT to communicate with workloads north of the TGW but can connect with workloads south of it.
    - **Public:** Routable north of the TGW. Workloads in a public subnet are generally accessible from external endpoints, depending on the routing configuration of the provider gateway.

The diagrams below, taken from the VCF 9.0 NSX design guide, illustrate the architectu

VPC Networking Model with Centralized TGW



VPC Networking Model with Distributed TGW



The table below lists the major differences between the 2 gateway connectivity types:

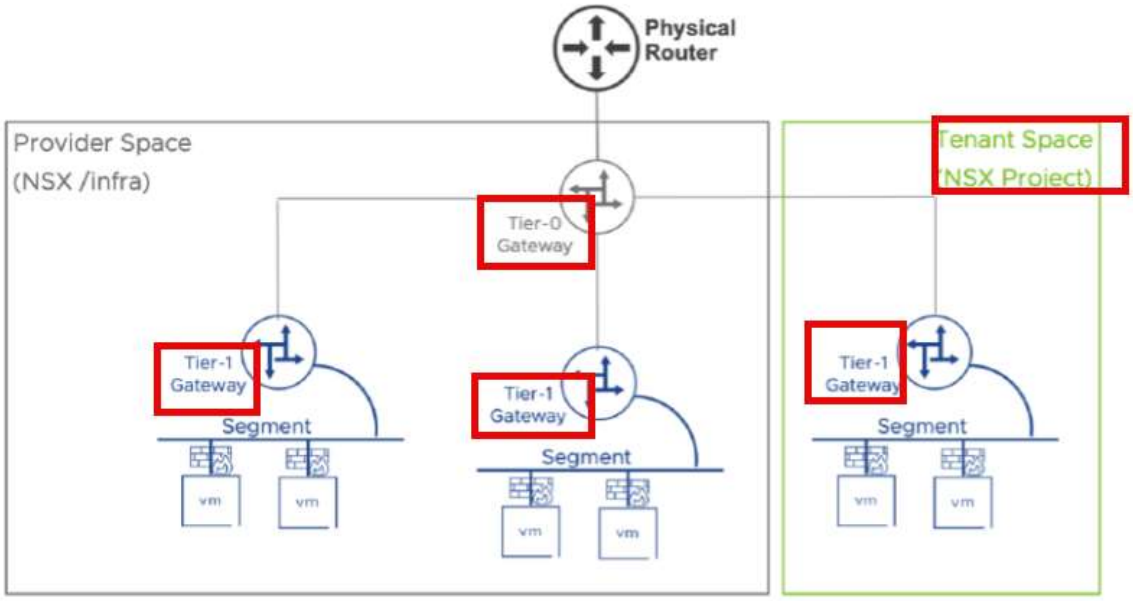
Feature	Centralized Connectivity	Distributed Connectivity
External IP (1:1 NAT)	No	Yes
NAT (SNAT/DNAT)	Yes	No
VPC Default Outbound NAT	Yes	No
DHCP (distributed)	Yes	Yes
E/W Firewall	Yes	Yes
N/S Firewall	Yes	No
AVI Load Balancer	Yes	Yes
VCF Automation	Yes	No
Supervisor Integration	Yes	No

Segment Networking Model

The Segment Networking model is a 2-tier logical network layout that has been known to NSX users for ages and is based on the following components:

- **Tier-0 Gateway:** The Tier-0 Gateway is essentially the same as the provider gateway in the VPC Networking model. It connects the physical infrastructure to the virtual network. It supports both dynamic and static routing, advertising the network ranges of the virtual network. The Tier-0 Gateway is always managed by the provider admin.
- **Tier-1 Gateway:** The Tier-1 Gateway serves as the default gateway for workloads connected via logical segments. A Tier-1 Gateway cannot connect directly to the physical fabric; it must connect to a Tier-0 Gateway. Tier-1 Gateways can be managed either by the Provider Admin or by a Tenant Admin (if created as part of an NSX Project). A typical NSX deployment has one or more manually configured Tier-0 Gateways, with a larger number of Tier-1 Gateways, depending on application needs. The Tier-1 Gateway is similar to the VPC Gateway in the VPC Networking Model.

- **Segment:** A segment represents an NSX logical network in the NSX segment model. Segments can be managed by either the provider admin or the tenant admin when created as part of an NSX Project. Typically, segments are connected to tier-1 gateways. The Segment object corresponds to the VPC Subnet object in the VPC Networking Model.



Licensing

License modes

Connected: Connected mode is easiest for the customer, as within **every 180 days, a customer needs to click one button** to send in their license usage information.

Disconnected: Customers with disconnected mode will have to **manually upload their license usage file** to the Broadcom support portal vcf.broadcom.com, **then download the license file to VCF Operations within every 180 days** to stay compliant with licensing.

Register

Starting with version 9.0, you access and manage the licenses for your environment by using VCF Operations and the **VCF Business Services console**. You must register the VCF Operations instance with the VCF Business Services console.

Register in Connected mode

- Log in to VCF Operations , and select **License ManagementRegistration**.
- connected mode pane > **Start Registration**.
- **Log in** to the **VCF Business Services console by using your Broadcom Support** Portal credentials.
    - In the wizard, **Select the Site ID** , click Next
    - **Enter a unique display name** for your VCF Operations instance
    - **Save** and **Next**.
    - **Select licenses** to add to your VCF Operations instance, and click **Save** and **Next**
    - View the summary of the registration, and click **Generate Activation Code**.
    - To complete the registration, you must **copy the activation code and enter it in VCF Operations** . Click **Copy**, and **Finish**.
- In **the VCF Operations** instance, navigate to **License ManagementRegistration**.
    - In the connected mode pane, click **Enter Activation Code**.
    - **Paste** the activation code, and click **Activate**.
    - In the VCF Operations instance, navigate to License ManagementRegistration.
    - In the connected mode pane, click **Start Registration**.
- **Log in to the VCF Business Services console**. by using your **Broadcom Support Portal c**redentials.
    - **Select the Site ID to** which you want to register this VCF Operations instance and click Next.
    - A new activation code is presented.
    - **Copy the activation code and click Finish**.

VCF Automation – Provider Management

Infrastructure resources

are an abstraction of their underlying vSphere and NSX resources. The infrastructure includes Supervisors, regions, provider gateways, and region quotas and networking configurations for each organization.

Supervisor

A VMware vSphere Supervisor is a collection of one or more clusters on a vCenter instance that provide and manage Kubernetes resources. The Supervisor is the component that owns the physical infrastructure resources and runs organization workloads on those resources. Each Supervisor can only be associated with one region.

VCF Automation supports only Supervisor deployed with NSX Virtual Private Cloud (VPC) networking

Zone

Zones represent vSphere clusters that provide compute resources for Supervisors. A Supervisor can span across multiple zones.

In VCF 9.0, a zone can consist of only a single vSphere cluster. When enabling a Supervisor, you must choose between two configuration types:

- **HA mode**: Controller nodes are distributed across three zones, offering high availability. This mode requires exactly three zones.
- **Default mode:** All controller nodes are placed in the first zone. You can add additional zones to isolate workloads and management functions. This mode provides flexibility for physical separation while maintaining simplicity.

While it is technically possible to add many zones to a Supervisor, consider limiting the number to 1 or 3 zones per Supervisor. Each zone is exposed to the end user as a selectable compute location, and too many options can degrade the user experience.

Region

In VCF Automation, a region combines compute, storage, memory, and networking resources from one or more Supervisors across one or more vCenter instances that are managed by the same NSX Manager instance.

You can create regions for different geographies, business units, or performance needs, but all Supervisors within a region must have homogeneous configurations:

- Identical names and definitions for storage classes
- Matching Kubernetes versions
- A consistent set of IaaS services

VCF Automation does not support heterogeneous configurations within a region

Resources in a region can be dedicated to a single organization or shared across multiple organizations.

Region Quota of an Organization

A region quota defines the compute and storage resources allocated to an organization for a given region. The key aspects of a region quota are:

VCF Automation Networking

To leverage the networking capabilities of VCF Automation for organizations for all applications, you can add and manage your infrastructure and cloud networking resources through the Provider Management Portal.

The networking capabilities of organizations for all applications are defined in two categories:

- **Tenancy** to support overall tenancy story with organizations for all applications
- **Self-service networking** for organization administrators and users

After creating a tier-0 gateway in NSX Manager, you define networking configurations for regions in the VCF Automation Provider Management Portal. See Add an Tier-0 Gateway.

1. Determine the set of IPs that organizations have access to and define IP spaces for these IPs. At least one IP space is required per region. The IP Spaces are used to define the routing for the provider gateway. You must define in NSX the external IP spaces that are being routed.

2. Define provider gateways that organizations can use for north-south connectivity. You define provider gateways by discovering your preexisting tier-0 gateways in Active Standby mode from NSX . You must have at least one provider gateway per region.
3. Verify that all edge clusters are synchronized.
4. Assign resources to organizations.

Organizations

VCF Automation supports multi-tenancy by using organizations. An organization is a top level entity that represents a line of business or a tenant. Each organization operates in a secure and isolated environment where users can access only allocated services and resources.

Content Libraries

A VCF Automation provider content library is an abstraction in VCF Automation that provides a single interface for provider administrators to share content with organizations across regions and to manage their content across the regions. Content libraries contain VM images hosted in vCenter that can be used in blueprints or IaaS services. The provider content libraries are read-only to the users of the organizations.

Services

Services in VCF Automation are value-added solutions provided by Broadcom and third-party vendors. The VCF Automation services enhance and extend the functionality of the VCF platform

Provider Administrator Workflow Example

As a Provider Administrator, you manage the overall infrastructure in VCF Automation. You must create one or more organizations and assign resources to those organizations. You can use the following as a sample workflow of your primary tasks as a Provider Administrator.

1. **Configure an identity provider.** See Managing Identity Providers in VCF Automation.

2. **Configure the VCF Automation access control**. See Configuring the VCF Automation Access Control.
3. **Create a Region** in Your VCF Automation.
4. **Create an organization** for All Apps or VM Apps. See Create an Organization for All Applications, or Create an Organization for VM Applications.
5. **Configure the Region Network Configurations** of a VCF Automation Organization.
6. **Add Region Quota to an Organization.**
7. **Configure the networking resources.** See Managing Networking Resources in the VCF Automation Provider Management Portal.
8. **Upload a Service to Your VCF Automation**.

Organization Management

Organizations in VCF Automation are created by the provider administrator in the VCF **Automation Provider Management Portal**. The provider administrator can create two types of organizations: an All Apps organization and a VM Apps organization. VM Apps organizations can run VM-based applications, while All Apps organizations are enabled to run a comprehensive set of built-in cloud services. For more information about creating VCF Automation organizations in the provider portal, see Managing Organizations.

Regardless of the type, each organization has its own organization portal where users log in to consume resources and services. Every organization has its own identity source that they connect to and can import users from.

All Apps Organizations in VCF Automation

All Apps organizations offer application teams a comprehensive set of built-in cloud services to provision VMs, Kubernetes, networking, volumes, Secret Store, databases, Harbor container registries, external DNS, certificates, and AI workloads. These cloud services can be consumed on a self-service basis through a curated catalog or self-service interfaces.

Organizations enable line-of-business or tenant organization administrators to further organize and govern resources that are allocated to them among application teams through the following capabilities:

- Resource management for project teams.

- Centralized content management for the organization.
- Policy-based governance on usage of resources.
- Quota-based management of networking resources.
- Workflow orchestration and extensibility through event subscriptions.
- Integration with identity providers of their choice.

Provider Consumption Organizations in VCF Automation

A Provider Consumption organization (PCO) is a special type of All Apps organization in VCF Automation that the provider administrator enables in the VCF Automation Provider Management Portal. The provider administrator can enable only one Provider Consumption organization

The PCO is intended for use when the provider wants to have their own consumption service for their users and/or they want to share catalog items with other organizations under their management.

PCOs are administered in the same way as other All Apps organizations, but they offer some additional capabilities on top of what a standard All Apps organization provides.

- PCOs come with a preconfigured VCF Operations orchestrator instance that is embedded in the organization portal, which you access on the Orchestrate tab.
- As a PCO administrator, you can publish VCF Operations orchestrator objects as catalog items to other organizations that use the same embedded VCF Operations orchestrator instance.
- You can publish catalog items to other organizations that use VM images from a provider content library.

VM Apps Organizations in VCF Automation

VM Apps organizations help existing VMware Aria Automation users transition to VCF Automation 9.0 without any impact to infrastructure, automation, or end-user experience.

In VM Apps organizations, the allocation of resources, like cloud accounts, cloud zones, profiles, image mappings and so on, is contained in the organization itself. The organization administrator defines and works with the infrastructure; the provider administrator does not allocate resources to organization of this type.

If you upgrade an existing VMware Aria Automation 8.x deployment to VCF Automation 9, your organizations are automatically mapped to VCF Automation for VM Apps

organizations. You continue to use vIDB and VMware Aria Suite Lifecycle to manage vIDM to maintain legacy authentication.

Organizations and Projects

Organization and projects are the top-level grouping objects used to define isolated sets of users and resources. A tenant is fully isolated from other tenants, with separation at the resource, network and identity layers. One tenant has no knowledge of any other tenants. This is typically used when multiple separate entities share a common infrastructure – either with a service provider model, or a centralized corporate IT department providing resources with self-service workload deployment and billing to different business units within the broader organization.

Within a tenant, there is further grouping possible, as vSphere Namespaces are created within the scope of a project. This allows compute and network resources to be defined independently for each vSphere Namespace. VPCs can be shared or dedicated as needed (to any projects or vSphere Namespace within the Organization, but not outside of the Organization). Access definitions can be managed at the project level, allocated by the Tenant Manager. These separations help reduce the need for requests to central infrastructure teams (Provider and Infrastructure Managers) and moving the operations closer to the consumers of the service.

Each Organization has a dedicated NSX project created when the provider creates the Region Network Configuration. This gives each Organization their own Transit Gateway and IP block allocation which they can carve up into VPCs and subnets to deploy different workloads

Aria Automation Policies

Content Sharing Policy

As a Automation Service Broker administrator, you can create a **content sharing policy that** entitles allAutomation Service Broker users in a project to shared content defined in the policy.

Content sharing policies control what items and actions are available in the Automation Service Broker catalog for users and user groups. If you have catalog items that require additional governance, you can apply content sharing policies to those items.

You share content at the project level where all users and user groups that are associated with a project can be granted access to specific catalog items. When you add a content source or a catalog item to a content sharing policy, you allow the users specified in the policy to request the items in the Automation Service Broker catalog.

- You can create content sharing policies per project, and then provide additional governance at the content source or at the catalog item level for all content that is associated with a specific project.
- You can share content with users and user groups that are associated with a specific project.
- Multiple content sharing policies can be created per project.

Procedure:

- Select Content and Policies > Policies > Definitions> New Policy > Content Sharing Policy
- Configure:
    - Scope: specify the project
    - Content Sharing: click add items > Content Sources
    - Users: click Add Users

Deployment limit policy

To limit resource consumption when users deploy cloud templates in Automation Assembler and request catalog items in Automation Service Broker, you can create a limit policy using the Policies API. The policy applies limits to all deployments in an organization by default.

You define deployment limit policies to control the amount of resources that deployments can consume when users deploy templates in Automation Assembler and request catalog items in Automation Service Broker.

How are deployment limit policies enforced

- When the policy is enforced, users can provision deployment resources within the specified limits.
- Multiple deployment limit policies can be enforceable. If there are multiple policies defined for a deployment, the lowest limit value is enforced for each resource.
- If there are resource quota policies and approval policies defined that affect the deployments within the policy scope, deployment limits are enforced before the other policy types.
- If a deployment requests no resources, such as a workflow deployment, the policy is not enforced on that deployment.

Procedure:

- Content and Policies > Policies> Definitions > New Policy > Deployment Limit Policy
- Set scope: such as a specific organization
- Set CPU, VM, memory, and storage max values

Security

Certificate Management

You can use the VCF Operations console to view and manage the certificates for all VMware Cloud Foundation components.

Access to all management component interfaces must be over a Secure Socket Layer (SSL) connection. During deployment, each component is assigned a certificate from a default signing Certificate Authority. You should replace the default certificates for the management domain components with trusted enterprise CA-signed certificates to provide secure access to each component.

Use the VCF Operations console to:

- View certificates and certificate alerts.
- Enable automatic renewal of certificates.

- Configure a certificate authority (CA).
- Generate certificate signing requests (CSRs).
- Replace certificates.

VCF management components only support Microsoft Certificate Authority. VCF Instance components support both Microsoft Certificate Authority and OpenSSL

Configure a CA for VCF

Procedure – navigate as follows:

- Logon to VCF Ops console
- Fleet Management > Certificates
- Select a VCF instance
- Configure CA
- Enter details (CA url, user, password, country, org, etc)

Replace a cert with an external CA-signed cert

If you do not want to configure a Certificate Authority in VCF Operations, you can generate a CSR, request a signed certificate from your external Certificate Authority, import the certificate, and then use it to replace an existing certificate for a VMware Cloud Foundation component.

Procedure – navigate as follows:

- Logon to VCF Ops console
- Fleet Management > Certificates
- Select a VCF instance
- Generate CSR
- Enter details (CA url, user, password, country, org, etc)
- Download CSR
- Import certificate ****ONLY PEM encoded certs are supported ***
- Provide name, source

- Choose validate, Save and Replace with Imported Certificate

Configuration drift

For VC config drift

- **create a Config Template** in VCF Operations
- in the wizard, select a VC source
- edit config template as you wish
- in the **Assign vCenters using Policy** page, you can:
    1. Use the Default Policy to apply to all VCs
    2. Create additional policies, or edit the list of VCs impacted by the default policy
- Drill to **Fleet Management > Configuration Drift.**
- Select a VCF instance.
- Select one ore more vCenters
- click **Detect Drift**
- After it runs, looks for differences in the VC config (left pane), and template (right pane)
- To remediate, do so manually. (future features may include a Remediate button)

Optionally, you can schedule config drift check jobs

For ESXi config / cluster drift

use configuration profiles – set your environment to use cluster images

create a configuration profile

- in vsphere Client (vCenter, not vROps):
- select the cluster
- select **Configure** > **Desired State** – **Configuration**.
- Click **Create Configuration**
- vCenter will run a quick pre-check to ensure that the vCenter Profiles are supported.
- Choose a reference host

- Click **Import**

To check for compliance and remediate:

- For the cluster, choose **check compliance**
  - **chose pre-check**
  - then choose **Apply changes**
  - navigate thru**remediation setting**s page and **Review Impact** page
  - click **Remediate**
- In the wizard, …. Then click **Apply Changes**

Manage VCF Domain Configuration Drift

If you make any out-of-band changes from vCenter or NSX Manager, you can use VCF Operations to update SDDC Manager with these changes and sync the SDDC Manager and vCenter inventories.

If the SDDC Manager and vCenter inventories get out of sync, some workflows may be blocked. You can use this procedure to unblock these tasks.

The sync workflow requires you to select a VCF domain to sync, ONE VCF domain at a time If you need to sync multiple workload domains, you will have to run the sync workflow multiple times.

- In VCF Operations, select **InventoryDetailed** View.
- Expand VCF Instances and browse to the VCF instance that contains the VCF domain you want to sync.
- **Click the VCF** domain name.
- Click **ActionsSync Inventory**.
- Review the information and click Sync Inventory.

If your existing NSX Manager instance has one or more Edge clusters, the sync process adds the discovered Edge node VMs to the VCF inventory, including their user credentials. During the sync process, the Edge node credential passwords will be reset. You can retrieve the updated passwords from the VCF credential store.

Select the Enable Edge cluster sync and import NSX Edge node VMs check box to perform the password reset operation for all the nodes in the existing Edge cluster, as well as for any nodes added later.

Kubernetes / Supervisor – other details

Kubernetes permissions

In Kubernetes RBAC, **ClusterRoleBindings** is used to grant permissions to resources that are not scoped by a namespace, such as a cluster-wide resource

Velero

Velero is an opn-source Kubernets backup and restore solution integrated into VCF

VM Class

A VM Class defines the hardware for a Kubernetes managed VM. It includes parameters such as: number of CPUs, memory capacity, and reservations

VCF – Cluster API

The API for creating, configuring, and managing Kubernetes workload clusters

CNIs

Container Network Interface for VMware Kubernetes

One more important aspect of Kubernetes networking is the Container Networking Interface, or CNI. The CNI connects Pods across nodes, acting as an interface between a network namespace and a network plug-in or a network provider and a Kubernetes network. There are many different CNI providers and plug-ins to choose from with different sets of features and functionality. CNI plug-ins have the ability to dynamically configure a

network and resources as Pods are provisioned and destroyed. They provision and manage IP addresses as containers are created and deleted. Kubernetes is the default networking provider for Kubernetes, but CNI plug-ins such as Flannel, Calico, Canal, and Weave Net offer additional features.

Antrea

Antrea is the default Container Network Interface (CNI) used for VMware Kubernetes Services (VKS) workload clusters. When deploying a new VKS workload cluster, an Antea CNI is automatically enabled to provide pod to pod and pod to service networking.

Calico

When used for Pod connectivity, Calico uses the Linux bridge with BGP, where Antrea uses Open vSwitch.

Flannel

Not normally recommended … not available with vSphere Supervisor 8.0

Flannel is a simple overlay network CNI plugin for Kubernetes, which can be selected during deployment on platforms like VMware Tanzu Kubernetes Grid. A common issue is that the default Flannel backend (VXLAN) may not work with VMXNET3 network interfaces in VMware; in this case, it's recommended to use Intel e1000 interfaces or configure Flannel to use a different backend like host-gw

IaaS Resource Policies

https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/organization-management/creating-policies-for-all-apps-orgs/vcfa-iaas-policy.html

https://blogs.vmware.com/cloud-foundation/2025/10/01/vmware-cloud-foundation-automation-infrastructure-resource-policy-overview/

Practice in HOL

Search the VMware Hands on Labs for any labs where VCF (preferable VCF 9.x) is deployed.

If you want, you can ignore the lab book and try your own experiments:

- VCF deployment, convergence
- Workload domain imports
- VCF Automation
    - Configure orgainizations, groups, tenants
- VCF Operations
    - VCF Health
    - VCF Storage Overview
- Licensing
- Certificate management
- Password management
    - Rotate, update, etc
- Configuration drift
- NSX
    - VPCs
    - NSX projects
- In HOL labs with Kubernetes (Tanzu):
    - Create / configure supervisor clusters
    -