WHITE PAPER
October 2024

Why NSX for VCF

Enabling the Cloud Operating Model for your Network in Private Cloud

VMware Cloud Foundation (VCF) - Technical Marketing

Author: Puneet Chawla

Special contribution from: Andrew Voltmer, Devyani Pisolkar, Dimitri Desmidt, Francois Tallet, Jeff Hunter, Jerome Catrouillet

vmware® by Broadcom

Table of contents

VMware Cloud Foundation

VMware Cloud Foundation (VCF) streamlines the creation of self-service private clouds, offering customers a seamless experience with consistent operations and governance. Its rapid deployment capabilities empower users to quickly access and provision resources, fostering business and IT agility. By leveraging VCF, organizations unlock modern use cases, driving productivity and efficiency while remaining adaptable to evolving demands.

VMware NSX

VMware NSX, a key component of VMware Cloud Foundation, embodies network virtualization, enabling seamless integration with existing infrastructure. It facilitates a cloud operating model on-premises, delivering simplified operations, self-service automation, visibility, and robust security. This integration optimizes application delivery and enhances infrastructure security.

Executive Summary

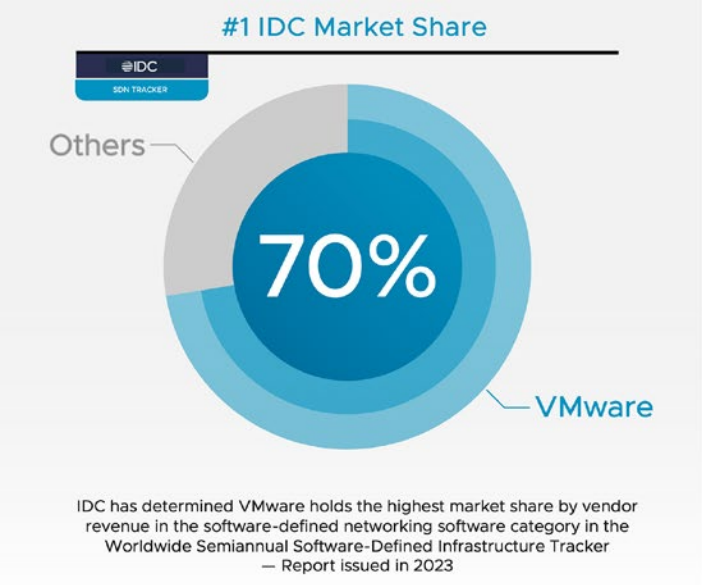
Cloud Operating Model for your Private Cloud

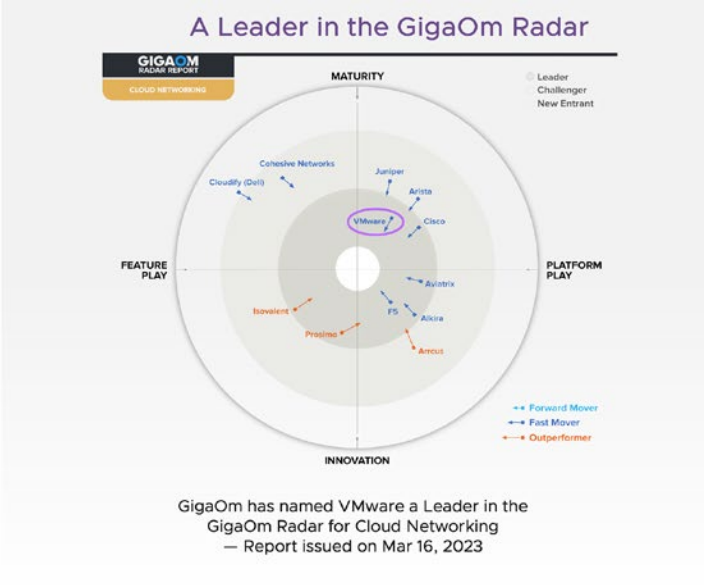
Organizations are increasingly seeking to replicate the self-service capabilities of cloud infrastructure within their on-premises environments to address the challenges of rapid digital transformation and cloud-native application adoption. This shift necessitates a cloud operating model, encompassing a comprehensive transformation of people, processes, and technology.

VMware Cloud Foundation (VCF), integrated with NSX, delivers a powerful solution to meet this demand. NSX's network virtualization and automation capabilities empower VCF to provide the agility, scalability, resiliency, and security essential for a successful cloud operating model.

NSX's software-defined networking (SDN) capabilities address challenges posed by traditional networking approaches. By decoupling network functions from hardware, NSX enables IT admins to provision and manage resources programmatically, automate tasks, and enforce both global and granular security policies. When combined with VCF, NSX creates a fully integrated and automated platform for building and managing a private cloud infrastructure that is both agile and secure.

The business benefits of using NSX with VCF are substantial, providing a strong return on investment through accelerated application delivery, improved operational efficiency, and enhanced security. This translates to significant cost savings, reduced time-to-market, and improved business agility.





VCF Networking: 11+ years of technological innovations, proven performance, and scale

Learn more

Learn more about VMware Cloud Foundation online: https://www.vmware.com/products/cloud-foundation.html

Try online for free Hands-On-Lab: https://www.labplatform.vmware.com/HOL/catalog/lab/14179

For more information or to purchase VMware products

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit vmware.com/products, or search online for an authorized reseller.

For detailed product specifications and system requirements, please contact VMware sales online https://www.vmware.com/company/contact_sales.html.

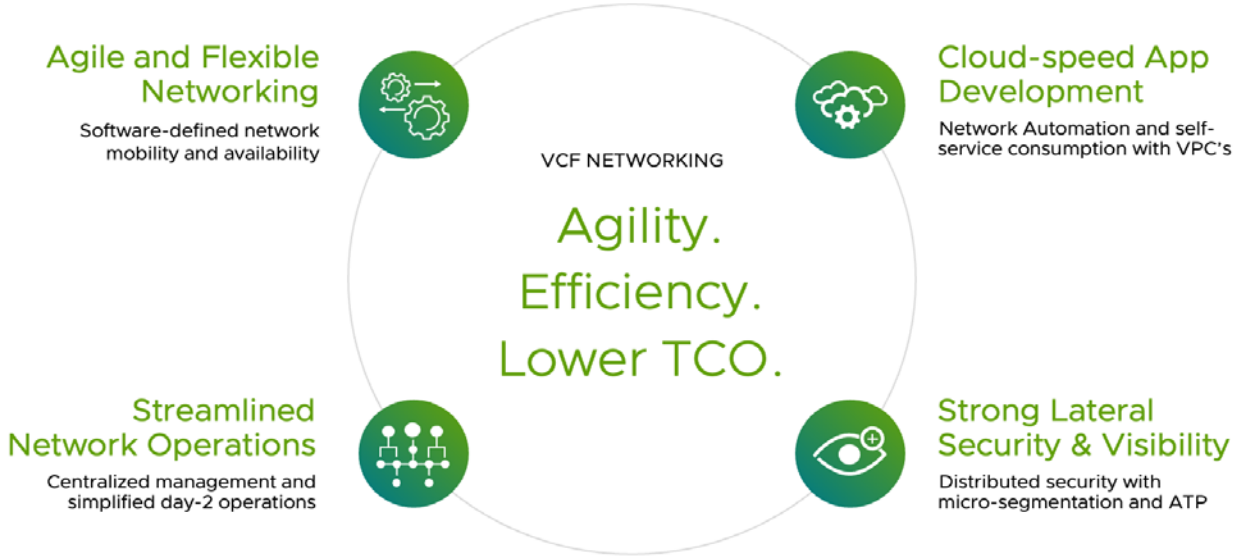
Why Network Virtualization Matters

Introduction

In the realm of Private Cloud infrastructure facilitated by VMware Cloud Foundation (VCF), VMware NSX stands as a cornerstone Software-Defined Networking (SDN) solution, reshaping network virtualization paradigms. NSX within VCF abstracts network services from physical hardware, allowing organizations to architect entire virtual networks comprising switches, routers, firewalls, and load balancers as distributed virtual appliances. This abstraction liberates businesses from the constraints of hardware-centric networking, fostering agility, security, and operational efficiency within their IT environments.

Leveraging NSX, VCF enables the creation of virtual networks - Virtual Private Cloud (VPC) independent of underlying hardware, facilitating dynamic provisioning, and scaling to meet evolving requirements. Moreover, NSX supports native vSphere Distributed Switch (VDS) [version 7 & above] and doesn't require network change for existing workloads to utilize NSX.

Additionally, vDefend Security (an add-on to VCF licensing) bolsters security with features like micro-segmentation, empowering organizations to implement granular security policies at the workload level. Through the integration of NSX within VCF, enterprises can expedite their digital transformation journeys, streamline network operations, and mitigate costs traditionally associated with hardware-based networking infrastructures.



Benefits	NSX Virtual Networking
Simplified Networking	Offers a complete network virtualization solution, consolidating all network functions into a single platform simplifying network management and reducing complexity across your entire infrastructure through a centralized NSX Manager.
Scalable Network and Automation	Scales linearly to accommodate growth, leverages a software-defined approach for dynamic network changes, and automates network provisioning by using declarative APIs and support for tools like VMware Cloud Foundation Automation, vCloud Director, NSX SDKs, Terraform, Ansible, and PowerShell.
Centralized Multi-site Network Management and Visibility	Centralizes network management across multiple environments, providing consistent policies and granular visibility for proactive troubleshooting.
Application Mobility and Disaster Recovery	Simplifies disaster recovery through features like stretched networking, federation, and integration with VMware Live Recovery for automated recovery without changing application IP addresses.
Multi-Tenancy and Self-Service Networking	Provides true multi-tenancy with granular control over resource allocation, network isolation, and global security policies. Plus, simplified network creation and micro-segmentation for each VPC through self-service portals.
Modern Applications	Provide full-stack networking and security for your containerized apps and microservices, just like your VMs. Simplify Kubernetes networking with features like Antrea for enhanced performance, visibility, and flexibility.
Zero Trust Security	Enables Zero Trust security with add-on features like vDefend distributed firewall, IDS/IPS, and malware prevention for a defense-in-depth approach.

Full list of NSX Features available here

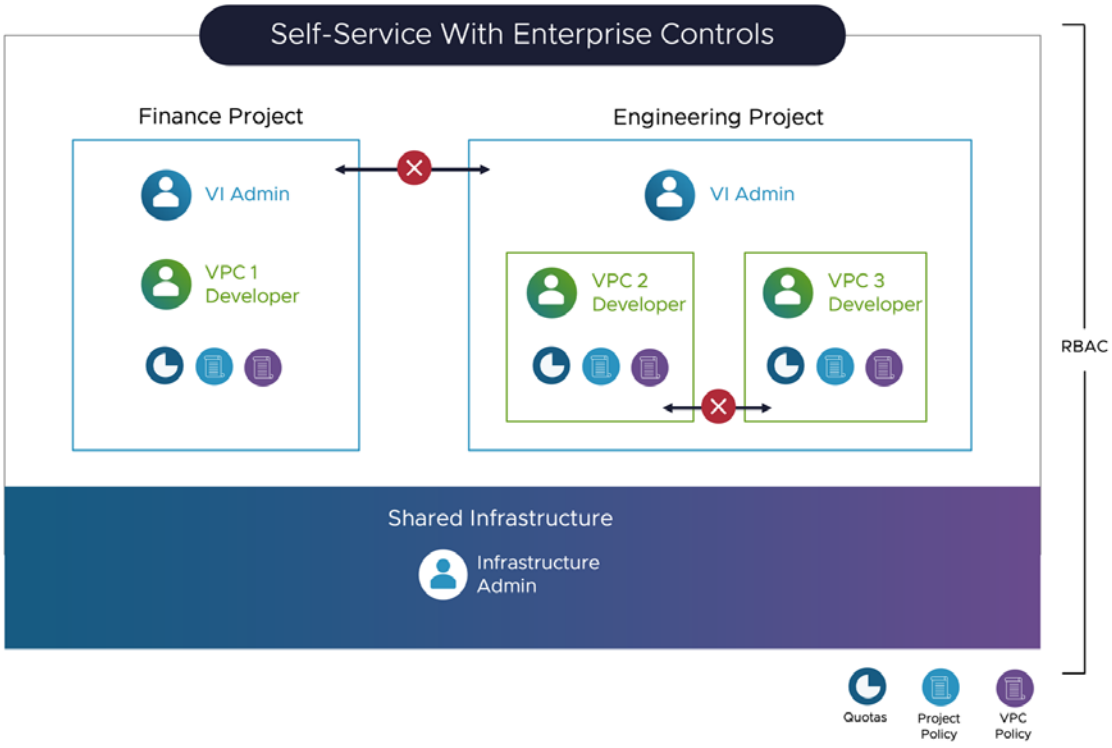
VCF Use Cases with NSX and Highlights

VMware NSX revolutionizes network virtualization through software-defined networking (SDN), decoupling network functions from hardware for agile, scalable, and secure virtual networks. Following are some of the key highlights and use cases:

Self-Service Networking with VPC

One of the key highlights of VMware NSX is its ability to create Virtual Private Clouds (VPC) functionality in VCF Private Cloud. NSX VPC offers organizations a self-consumption model for networking resources within predefined guardrails established and managed by network administrators. NSX VPC enables the creation of isolated virtual network environments over shared infrastructure that mimic the characteristics of traditional public clouds, providing tenants with dedicated networking resources while maintaining centralized oversight and control. This empowers business units and application owners to independently provision and manage their network infrastructure within the constraints set by network administrators, fostering agility and autonomy without compromising security or compliance requirements.

With NSX VPC, organizations can define policies and templates that govern network provisioning and configuration, ensuring consistency and compliance across VPC instances. Network administrators retain granular control over resource allocation, security policies, and connectivity options, while empowering tenants with self-service capabilities to deploy and scale their network environments on-demand. This self-service model not only fosters collaboration and innovation but also frees up IT time for more critical tasks, resulting in a reduction in support tickets and accelerated time-to-market for new services and applications.



Networking Infrastructure Automation

VMware NSX revolutionizes network automation by providing complete automated provisioning of virtual routers, switches, load balancers, firewalls, virtual networks, subnets, and many other network services. This comprehensive approach reduces manual configuration overhead, accelerates network infrastructure deployment, and empowers organizations to achieve greater agility, efficiency, and scalability. The power of NSX declarative APIs further streamlines network operations, allowing you to define the desired state of your network, and NSX will automatically configure and enforce the necessary changes, ensuring your network always aligns with your requirements.

Infrastrucutre as Code (IaC)

NSX seamlessly integrates with orchestration platforms like VMware Cloud Foundation Automation and third-party Infrastructure as a Code (IaaC) tools like Terraform and Ansible. This integration allows for the automation of network provisioning, configuration, and management tasks through declarative code templates and workflows. By treating network infrastructure as code, organizations can achieve consistent, repeatable, and auditable deployments across different environments, fostering a DevOps culture and accelerating time-to-market for new services and applications.

Automation within the NSX

NSX also incorporates automation directly within its product, simplifying complex network operations. For instance, when deploying a Virtual Private Cloud (VPC), NSX automatically provisions and configures the necessary network components. This eliminates the need for manual configuration, reducing errors and accelerating deployment times.

Furthermore, NSX automates the upgrade process for all networking services, including routers, switches, load balancers, firewalls, VPCs, and edge virtual appliances. This single solution upgrade simplifies lifecycle management and ensures consistent network configurations across the entire infrastructure, saving significant time and effort compared to managing upgrades for disparate networking products individually.

Application Mobility

NSX's software-defined networking (SDN) capabilities allow organizations to create virtualized network environments that are decoupled from physical infrastructure, making it easier to move applications and workloads between data centers. By encapsulating network services, such as virtual switches, routers, load balancer, and firewall within software-defined constructs, NSX enables organizations to maintain consistent network connectivity & policy, security, and performance characteristics

Multi-Site Network Support

Another standout feature of VMware NSX is its support for multiple environments. With NSX, organizations can extend their network seamlessly across multiple private data centers and deploy consistent networking and security policies regardless of where workloads are deployed. This enables enterprises to embrace very large scale VCF Private Cloud deployment strategies with confidence, leveraging the agility and scalability of the private cloud while maintaining control over security and compliance requirements everywhere. By abstracting networking functions from the underlying infrastructure, NSX simplifies the complexity of managing disparate environments, providing a federated networking fabric that spans across private clouds.

Disaster Recovery

NSX plays a crucial role in enabling Disaster Recovery (DR) by providing a virtualized network that facilitates seamless replication, failover, and failback of critical workloads between geographically dispersed data centers. This virtual network acts as a conduit for data replication, ensuring continuous connectivity and policy synchronization between primary and secondary sites. NSX's network virtualization capabilities allow the creation of logical network segments that encapsulate application workloads and associated network services. These virtual networks can be replicated and synchronized across multiple data center sites, maintaining identical network configurations and policies. NSX's distributed routing and switching functionality ensures seamless communication between workloads, regardless of their physical location, while its distributed firewall capabilities enforce consistent security policies across the entire network infrastructure. Additionally, NSX supports both active-active and active-standby network architectures, providing flexibility in DR strategies. Integration with disaster recovery solutions like VMware Live Recovery (SRM) further enhances automation and orchestration of failover processes, ensuring rapid recovery and minimal downtime. By offering a resilient and agile network infrastructure, NSX empowers organizations to achieve continuous network availability to mitigating the impact of unforeseen disruptions.

Data Center Consolidation, Migration, and M&A Integration:

Application mobility facilitates the consolidation and migration of applications and workloads between disparate data center environments, enabling organizations to streamline operations, reduce infrastructure costs, and simplify management overhead. Additionally, in the context of mergers and acquisitions (M&A), application mobility enables organizations to seamlessly integrate and migrate applications and workloads from acquired entities into their existing infrastructure without the need to change IP addresses. NSX allows organizations to maintain the same IP ranges from both companies on separate virtual networks, avoiding duplicate IP conflicts and ensuring seamless communication between applications. By leveraging NSX's network virtualization capabilities, organizations can achieve a fast but smooth transition and consolidation of IT assets during M&A activities while minimizing disruption to business operations.

Hybrid-Cloud Support:

VMware Cloud Foundation (VCF) and NSX enable organizations to seamlessly integrate and manage both on-premises environments and public clouds, leveraging consistent infrastructure across both. Since VCF, including NSX, is available on all major hyperscalers like AWS, Azure, Google Cloud, Oracle, and others, customers benefit from the same technologies in both environments, avoiding vendor lock-in. NSX provides a unified platform for networking and security, allowing custom automation of policies to ensure consistency across multiple clouds. This hybrid-cloud approach enables organizations to efficiently scale resources, quickly provisioning additional compute, storage, and networking capacity to meet demand, while maintaining consistent security and network policies across all environments.

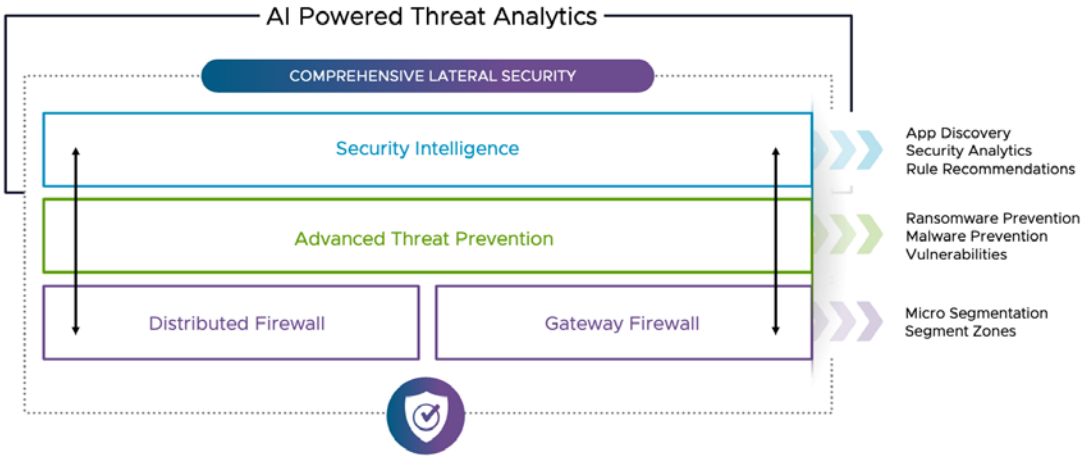
Network Security

vDefend add-on to VCF licensing, a standout feature of VMware NSX is its capability to implement micro-segmentation within the network without necessitating any changes to the underlying network infrastructure or requiring the deployment of any agents on individual workloads. This approach allows organizations to apply granular security policies at the hypervisor level for each workload, significantly bolstering overall security posture. With micro-segmentation, traffic between workloads can be tightly controlled based on predefined rules, thereby reducing the attack surface and mitigating the potential impact of security breaches. This feature is particularly crucial in modern data center environments characterized by the proliferation of applications and services, where a robust approach to network security is paramount.

Full vDefend security licensing add-on to VCF also includes Advanced Threat Protection (ATP) capabilities, including ransomware protection, to further enhance security defenses. With vDefend ATP, organizations gain AI driven threat detection and mitigation capabilities, enabling them to detect and respond to advanced threats, including ransomware attacks, in real-time. By leveraging sophisticated behavioral analysis and machine learning algorithms, ATP provides comprehensive protection against evolving cyber threats, safeguarding critical assets and ensuring business continuity. This integrated security functionality complements vDefend DFW (micro-segmentation) capabilities, offering organizations a holistic approach to network security that is both effective and efficient.

vDefend Security Architecture

(add-on only)



High Performance Networking (DPU-based Accelerators/Smart NIC)

The introduction of Data Path Units (DPUs) or SmartNICs into VMware's NSX platform significantly enhances network performance. These specialized hardware accelerators, integrated into network interface cards, offload network processing tasks from the hypervisor, reducing CPU overhead and improving overall system performance.

NSX DPUs leverage hardware-based packet processing engines to provide key network functions, enabling wire-speed packet processing and low-latency network performance even under high traffic loads. They seamlessly integrate with the VMware Cloud Foundation (VCF) stack, offering unified management and operations.

Key benefits of NSX DPUs include resource optimization and security isolation. By offloading network processing tasks to NSX DPUs, customers can free up valuable resources within their infrastructure, allowing them to allocate those resources to critical workloads instead. Additionally, they enhance security effectiveness by offloading security processing tasks to dedicated hardware, ensuring robust security without compromising. NSX DPUs also provide hardware-based packet capture and analysis capabilities for real-time traffic monitoring and troubleshooting.

Further amplifying the performance and availability benefits of NSX DPUs by using dual-DPUs on a host, the throughput capacity is effectively doubled, with each DPU operating independently to provide high Performance. Moreover, dual DPUs can be configured for High Availability with active-standby mode, providing redundancy and ensuring uninterrupted network connectivity even in the event of a DPU failure. This enhancement is particularly valuable for mission-critical workloads and environments requiring high network availability.

Build with Confidence

In today's digital landscape, delivering exceptional application experiences around the clock is paramount for customer satisfaction. Organizations need to deploy applications rapidly and with certainty to meet these demands. By leveraging complete end-to-end automation spanning Layer 1 through 7, VCF customers can confidently deploy NSX knowing they have the support of meticulously tested and validated designs from VMware by Broadcom. This prescriptive architectural approach, ensures seamless integration into implementations, eliminating the risk of networking being an afterthought or deployed with mix a of hardware vendors. As a result, operational and testing efforts are significantly reduced.

Moreover, NSX adheres to rigorous standards compliance, including the Federal Information Processing Standards (FIPS) such as FIPS 140, ensuring that organizations can trust in the security and reliability of their network virtualization infrastructure. The FIPS 140 standards specify the cryptographic and operational requirements for modules within security systems that protect sensitive information. By meeting these and other industry standards like, DISA STIG EAL NDCPP NIAP USGv6 IPv6 ready, etc. NSX provides assurance that critical security requirements are met, further bolstering confidence in its capabilities. This commitment to standards compliance underscores NSX's dedication to maintaining the highest levels of security and integrity, essential for protecting sensitive data and ensuring regulatory compliance.

VMware offers a range training and certifications that validate expertise in network virtualization and security, further bolstering confidence in practitioner's capabilities. These certifications, such as VMware Certified Professional - Network Virtualization (VCP-NV) and VMware Certified Advanced Professional - Network Virtualization Deployment (VCAP-NV), demonstrate proficiency in designing, implementing, and managing NSX environments. With certified professionals at the helm, organizations can trust in the expertise and knowledge backing their NSX deployments, ensuring optimal performance and security.

Visibility and Troubleshoot Faster

NSX accelerates troubleshooting and enhances visibility with centralized monitoring tools, offering comprehensive insights into the network environment. Through a unified management interface, administrators gain real-time access to metrics, logs, and performance data across the entire NSX deployment. This centralized visibility simplifies the detection and diagnosis of network issues, enabling administrators to identify root causes more rapidly and proactively address potential problems.

NSX's distributed architecture, leveraging distributed routing and switching, minimizes the impact of network disruptions by reducing single points of failure and optimizing traffic flows. In the event of a network issue, NSX's distributed nature ensures that traffic can continue to flow uninterrupted, mitigating downtime and minimizing service disruptions.

Furthermore, NSX offers a rich set of troubleshooting and diagnostic tools that streamline the identification and resolution of network issues. These tools include packet capture, traceflow, live traffic analysis (LTA), and analysis capabilities, allowing administrators to inspect network traffic at various points within the NSX environment. By capturing and analyzing packet-level data, administrators can pinpoint issues with network connectivity, performance, or security, facilitating faster resolution of network-related problems.

The integration with VMware Cloud Foundation Network Operations, included in VCF, further elevates NSX's troubleshooting capabilities by providing advanced analytics and deep visibility into the NSX infrastructure. This integration offers a holistic view of the network, encompassing both virtual and physical components, enabling administrators to understand the interdependencies and potential bottlenecks within their environment.

Network Operations' comprehensive visualization and topology mapping features help administrators grasp the relationships between different network components and identify potential points of failure. This visualization simplifies troubleshooting by providing a clear overview of the network environment and facilitating navigation between interconnected components. Moreover, the proactive monitoring and alerting capabilities within Network Operations enable administrators to detect potential issues before they impact service availability or performance. By setting up custom alerts and thresholds, administrators can receive notifications for deviations from expected behavior, allowing them to take preemptive action to prevent downtime or service degradation.

VCF Simplified Operations across the Lifecycle

VMware Cloud Foundation (VCF) incorporates comprehensive lifecycle management capabilities, encompassing the entire journey of the Software Define Data Center (SDDC) stack, including its intrinsic NSX component. This unified management approach, driven by declarative APIs and robust automation tools, streamlines and simplifies the initial deployment, ongoing configuration adjustments, seamless upgrades, and routine maintenance of the entire VCF environment. By automating these processes, VCF significantly reduces manual effort, mitigates the risk of human error, and accelerates the realization of value for organizations adopting the platform. This efficiency gains allow IT teams to shift focus from laborious operational tasks to strategic initiatives that foster innovation and business growth.

Cloud Builder

Cloud Builder serves as the initial catalyst for deploying a VCF environment, guiding users through the setup process and automating the configuration of crucial components such as compute, storage, networking (inherently leveraging NSX), and management elements like SDDC Manager. By streamlining the initial bring-up, Cloud Builder empowers organizations to establish their SDDC infrastructure rapidly and efficiently. It also plays a pivotal role in facilitating ongoing expansion, allowing for the seamless addition of new resources and capabilities to the environment as organizational needs evolve. This scalability ensures that the VCF environment can adapt and grow in alignment with business requirements.

SDDC Manager

SDDC Manager functions as the central orchestrator of VCF's lifecycle management. It provides a single pane of glass from which administrators can oversee and manage the deployment, configuration, upgrade, and monitoring of the entire SDDC stack, encompassing the NSX network virtualization layer. By automating routine tasks and ensuring consistency across the environment, SDDC Manager significantly reduces manual effort and the potential for configuration drift. Moreover, it offers insightful visibility into the health and performance of the SDDC stack, empowering administrators with the ability to proactively identify and address potential issues, ensuring optimal performance and reliability.

VCF - 4 Network Architecture options

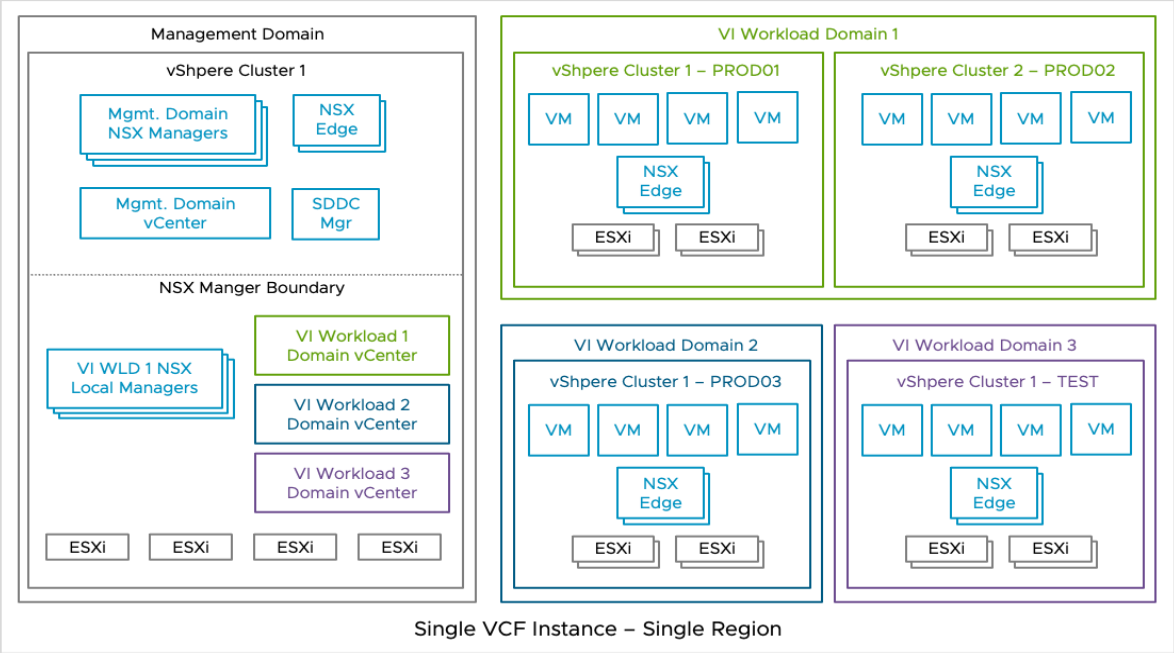
[Standard deployment architecture consists of a separate management plane while Consolidated deployment architecture has both management and compute as one. Any of the four following topologies can be used with the Consolidated or Standard architecture. And both architectures are supported for production deployment. Difference between both boils down to having one more level of redundancy in the Standard architecture compared to Consolidated architecture.]

1. VCF Single Instance Deployment (Standard)

Overview: This architecture embodies the core essence of VMware Cloud Foundation in its simplest form. All essential Cloud Foundation components (SDDC Manager, vCenter Server, NSX Manager, etc.) are consolidated within a single vCenter Server instance, sharing a unified management domain. This shared management domain serves as the control center, overseeing the configuration, deployment, and lifecycle management of the entire software-defined data center (SDDC).

Workload Isolation: While the management components are centralized, workload domains are strategically isolated from the management domain. This isolation is achieved by deploying workloads within separate VI workload domains, each managed by a dedicated vCenter Server instance. This architectural separation ensures that workloads operate independently, minimizing the risk of conflicts and resource contention.

Simplified Management: The single instance deployment simplifies the operational overhead of managing the Cloud Foundation environment. Administrators can manage the entire infrastructure from a single vCenter Server instance, streamlining tasks like monitoring, provisioning, and troubleshooting.



Single VCF Instance – Single Region

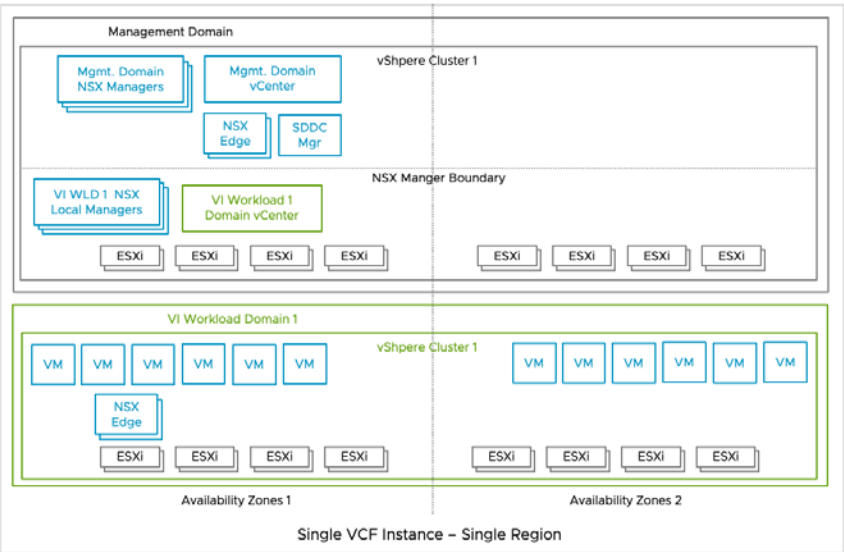
When to Use:

- Small to medium-sized environments: Ideal for organizations with a limited number of hosts and workloads.
- Limited resources: Organizations with constraints on infrastructure or IT staff can benefit from this architecture's simplicity.
- Initial deployments: This architecture serves as a starting point for organizations exploring VMware Cloud Foundation and can later be expanded or transitioned to other architectures as needs evolve.
- Test and development environments: Provides a cost-effective and easily manageable platform for non-production workloads.

2. VCF Single Instance in Multi Availability Zone (AZs) Deployment

Overview: This architecture extends the single instance model by strategically distributing workload domains across multiple availability zones within a region. This enhances the availability and resilience of the SDDC by providing protection against failures within a single zone.

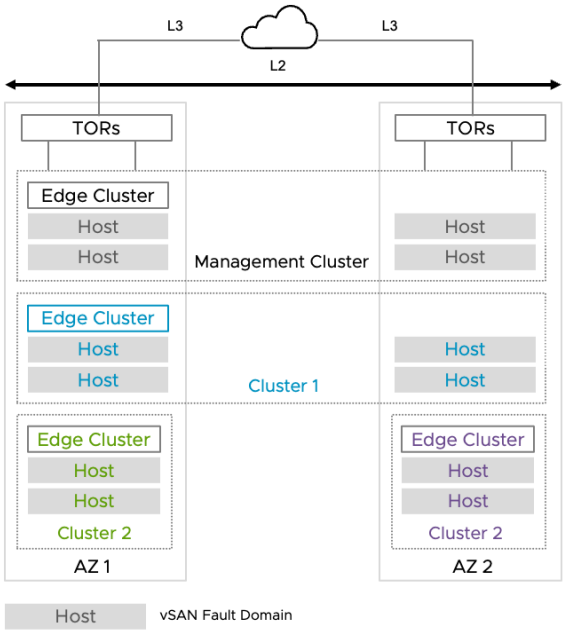
Workload Mobility: One of the key advantages of this architecture is the ability to seamlessly move workloads between availability zones. This is achieved using vSphere's native features like vMotion and Storage vMotion. In the event of a failure in one zone, workloads can be quickly migrated to another zone with minimal disruption, ensuring business continuity.



Availablity Zone is a fault domain that protects VMs in a vSphere cluster leveraging vSAN stretched cluster. It protects VMs against partial host failures in clusters, therefore, the scope is a single data center.

When to Use:

- High availability requirements: Organizations with critical workloads that require continuous availability and minimal downtime can benefit from this architecture.
- Regional resilience: This architecture provides protection against localized failures within a data center, between Availability Zones, ensuring business continuity.
- Disaster recovery: This architecture can serve as a foundation for a disaster recovery strategy, allowing for failover of workloads to another zone in case of a primary zone outage.

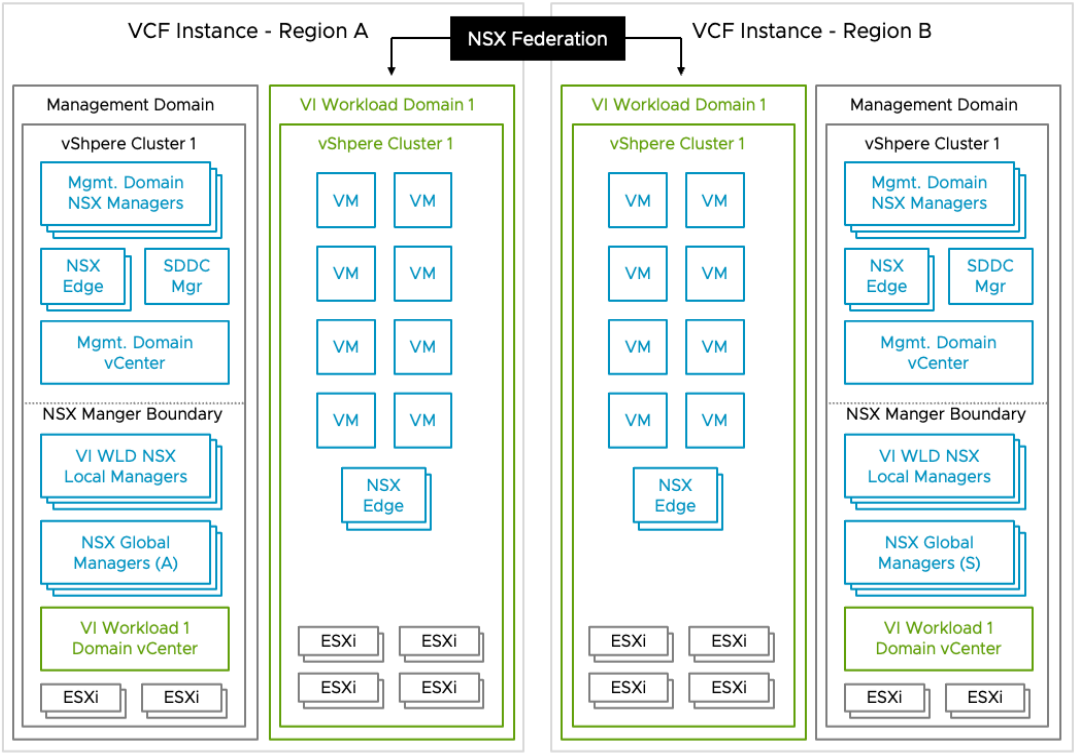


Protected clusters stretched across AZ's
Mandatory for default cluster of Management Workload Domain Optional for other clusters
Separated vSAN fault domains for host protection
vSphere HA to recover VMs in failed hosts
Flat L2 network for Edge Node networks using physical fabric
N-S traffic forwarded through AZ1 TORs for stretched clusters in normal conditions

3. VCF Multi Instance, Multi Region Deployment

Overview: This architecture involves deploying multiple independent Cloud Foundation instances across different regions or data centers. Each instance functions as a self-contained SDDC with its own management domain and workload domains. This provides geographic redundancy and the flexibility to tailor each instance to specific regional requirements or regulatory compliance.

Centralized Management: While each instance is independent, they can be linked together using vCenter Linked Mode or NSX Federation for centralized management and visibility. This allows administrators to manage multiple instances from a single console, simplifying operational tasks and providing a holistic view of the entire environment. NSX Federation is a manager of manager approach i.e. NSX manager (Global manager) has visibility and control over the other NSX managers and their components. Deployment of NSX Federation is not automated via SDDC Manager but it is supported in VCF and can easily be deployed and configured manually on multi-site VCF architectures.



Region is a fully fault tolerant design that protects the entire VM infrastructure against catastrophic failures. It requires one or more standby VCF instances that provide backup services

When to Use:

- Geographically dispersed operations: Organizations with multiple data centers or operations in different regions can leverage this architecture to ensure data locality and compliance with regional regulations.
- Disaster recovery: This architecture can be used to implement a robust disaster recovery strategy by replicating workloads across multiple instances in different locations.
- Resource segmentation: Organizations can dedicate specific instances to different business units or departments for better resource control and isolation.

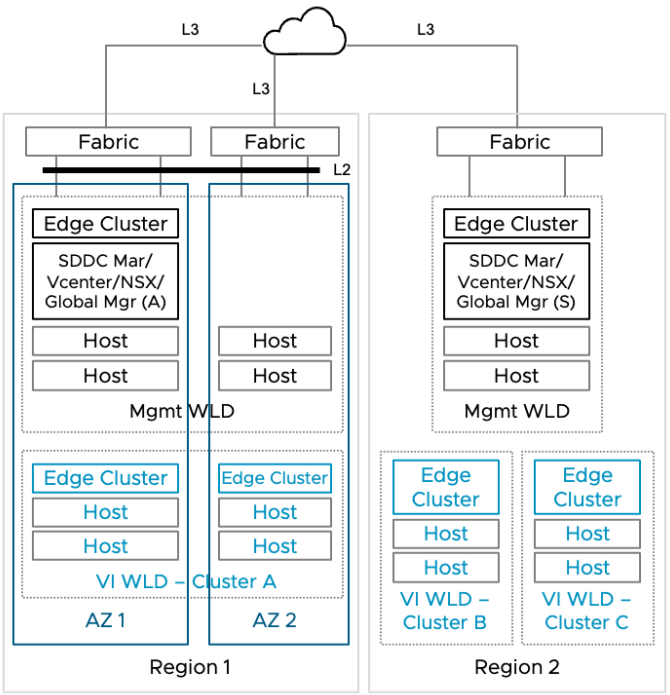
4. VCF Multi Instance, Multi Region, Multi Availability Zone Deployment

Overview: This architecture represents the pinnacle of resilience and availability within the VMware Cloud Foundation framework. It combines the benefits of multi-instance and multiple availability zone architectures, offering the highest level of protection against failures at multiple levels: within a zone, within a region, and across regions.

Global Redundancy: This architecture provides true global redundancy by distributing workloads across multiple availability zones within multiple regions. In the event of a failure at any level, workloads can be automatically migrated to another available zone or region, ensuring uninterrupted service delivery.

When to Use:

- Mission-critical workloads: Ideal for organizations with critical applications and services that require continuous availability and cannot tolerate downtime.
- Global enterprises: Organizations with a global presence and diverse regulatory requirements can benefit from this architecture's flexibility and resilience.



Protected Workload Domains use stretched NSX gateways
Single or Multiple AZ on each region for added local protection
VMware Live Recovery to recover VMs in failed regions
NSX Federation for IP portability
N-S traffic forwarded through Region 1 for stretched NSX gateways in normal conditions

Conclusion

In conclusion, the integration of VMware NSX within VMware Cloud Foundation (VCF) delivers a powerful and transformative solution for organizations seeking to embrace the cloud operating model within their private cloud environments. By virtualizing network services and decoupling them from hardware, NSX empowers organizations with agility, scalability, and enhanced security, driving significant operational efficiencies essential for modern IT infrastructures.

Through its self-service networking, automation capabilities, application mobility features, and robust security measures, NSX enables organizations to streamline network operations, accelerate application delivery, and enhance overall security posture. The combination of NSX and VCF creates a unified platform that simplifies the deployment and management of private clouds, fostering innovation, agility, and efficiency while ensuring the highest levels of security and compliance. As organizations continue their digital transformation journeys, the integration of NSX within VCF stands as a testament to the power of software-defined networking in enabling a truly cloud-like experience on-premises.

vmware® by Broadcom

Item No: why-nsx-on-vcf-whitepaper SW2-3 10/24