TECHNICAL WHITE PAPER
February 2025

Modern Private Cloud

with VMware Cloud Foundation

Table of contents

Introduction

Adopting private cloud infrastructure is accelerating as organizations seek greater control, security, and flexibility for their IT workloads. However, the journey to a truly modern private cloud can be complex, requiring careful consideration of infrastructure design, operational efficiency, resource consumption, security, and integration with existing systems. This white paper delves into the key technical considerations for building and managing a modern private cloud, providing a comprehensive framework for organizations to navigate this transformation effectively.

A modern private cloud is more than just a virtualized infrastructure. It represents a holistic approach to IT service delivery, encompassing several key aspects. First, it requires a robust and agile foundation. This involves carefully selecting compute, storage, and networking technologies to ensure optimal performance, scalability, and resource utilization. Decisions around virtualization platforms, server hardware, containerization, software-defined networking, and storage solutions are critical to building this solid foundation.

Secondly, streamlined and automated operations are essential. Modern private clouds leverage automation and intelligent management tools to optimize infrastructure performance, manage capacity proactively, and streamline resource configuration. Infrastructure-as-code, self-service portals, and comprehensive monitoring capabilities are key to this operational efficiency.

Furthermore, meeting diverse user needs requires a flexible approach to resource consumption. This includes self-service provisioning, API and CLI access, CI/CD integration, and a curated service catalog to empower users and automate application deployments.

Security is also paramount in any cloud environment. A modern private cloud incorporates robust security measures, including identity and access management, network security, data protection, and compliance with relevant industry regulations.

Finally, seamless integration is crucial. Integrating the private cloud with existing IT systems and third-party tools is essential for operational efficiency and maximizing the value of existing investments. This includes integrated monitoring tools, security information and event management (SIEM) systems, and other enterprise applications.

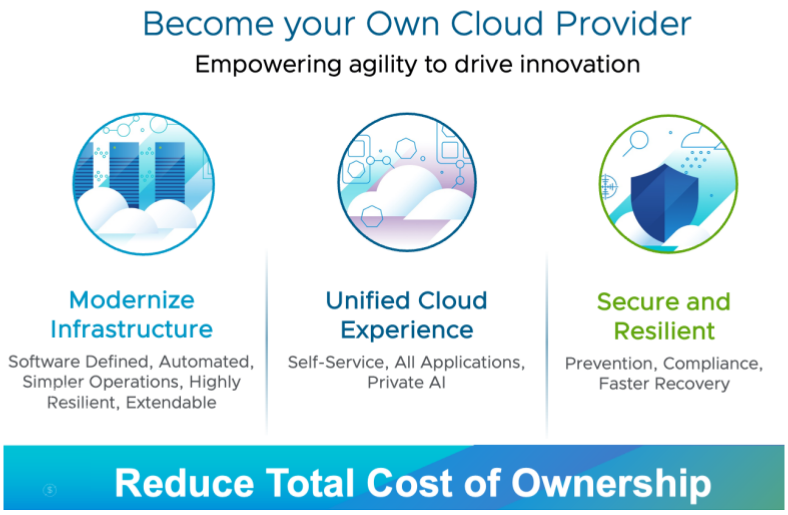

Become your Own Cloud Provider
Empowering agility to drive innovation
Modernize Infrastructure
Software Defined, Automated, Simpler Operations, Highly Resilient, Extendable
Unified Cloud Experience
Self-Service, All Applications, Private AI
Secure and Resilient
Prevention, Compliance, Faster Recovery
Reduce Total Cost of Ownership

Figure 1. Business outcomes of being your cloud provider.

What Makes a Modern Private Cloud?

Understanding how an organization establishes its vision for a private cloud is crucial. This process begins with defining the core infrastructure—the compute, storage, and network resources—that will form the foundation of the cloud environment. This involves making key decisions on:

- Compute: Choosing the right virtualization technology (e.g., vSphere), determining the optimal server hardware, and planning for scalability and resource allocation. This might involve considering bare-metal provisioning, containerization platforms like Kubernetes, and GPUs for specialized workloads.
- Storage: Selecting the appropriate storage solutions (e.g., vSAN, traditional SANs with vSphere Virtual Volumes, or cloud-native storage) based on performance, capacity, and availability requirements. This also includes data protection strategies, such as backups, replication, and disaster recovery planning.
- Networking: Designing a robust and secure network architecture with features like VLAN segmentation, software-defined networking (NSX), and integration with existing on-premises or cloud networks. This also entails considerations for network performance, security, and scalability.

Once the infrastructure is in place, the focus shifts to its operation. This involves maintaining clear visibility over the environment through comprehensive monitoring tools, optimizing infrastructure performance, managing capacity, and configuring resources effectively. This can be achieved through:

- Performance Optimization: Implementing resource scheduling, load balancing, and right-sizing virtual machines to ensure optimal application performance.
- Capacity Management: Proactively monitoring resource utilization, forecasting future needs, and scaling infrastructure accordingly.
- Automation: Utilizing infrastructure-as-code tools to automate provisioning, configuration management, and deployment processes.

Robust analytics and reporting capabilities are essential for monitoring resource consumption, identifying optimization opportunities, and ensuring resources are fully utilized or automatically repurposed/decommissioned when idle to minimize costs. This might involve leveraging tools for cost analysis, performance monitoring, and capacity planning.

Furthermore, organizations must determine how they intend to consume these resources. This could involve:

- Self-Service Provisioning: Implementing a self-service portal with role-based access control (RBAC) to empower users to provision resources on demand.
- API and CLI Integration: Providing APIs and CLIs for programmatic access to cloud resources, enabling automation and integration with other systems.
- CI/CD Integration: Integrating the private cloud with CI/CD pipelines to automate application deployments and updates.
- Service Catalog: Offering a curated catalog of services, such as databases and load balancers, to meet diverse application needs.

Security and compliance are also paramount. This encompasses:

- Identity and Access Management: Implementing strong authentication and authorization mechanisms, such as multi-factor authentication and role-based access control.
- Security Hardening: Regularly patching systems, implementing best practices, and conducting security audits to mitigate vulnerabilities.
- Network Security: Deploying firewalls, intrusion detection/prevention systems, and micro-segmentation to protect the private cloud from external and internal threats.

- Data Protection: Implementing encryption, data loss prevention (DLP) measures, and regular backups to safeguard sensitive data.
- Compliance: Ensuring adherence to relevant industry regulations and compliance standards, such as HIPAA, PCI DSS, and GDPR.

Finally, where global IT operations run 24/7, private cloud services must be highly available, protected against threats like ransomware, and capable of rapid recovery from unforeseen events. This necessitates:

- High Availability: Designing redundant infrastructure with failover mechanisms to ensure continuous service availability.
- Disaster Recovery: Implementing disaster recovery plans with regular backups, replication, and automated failover procedures to minimize downtime in case of catastrophic events.
- Ransomware Recovery: A solution that provides guided workflows, the ability to recover in an isolated recovery environment (IRE), immutable recovery points, and live behavioral analysis to identify modern ransomware strains and fileless attacks.

Why VMware Cloud Foundation?

How does VCF measure up to this standard? First and foremost, it provides a private cloud platform through its shared-nothing architecture. Each VCF deployment serves as an independent private cloud with no dependencies on shared resources. This architecture can be deployed anywhere—whether in a private data center, the public cloud, or with a managed service provider. Regardless of where it is deployed, the platform delivers consistent capabilities that align with the requirements of a private cloud. Let's outline those requirements and explain how VCF meets them.

On-demand self-service: VCF Automation offers a comprehensive solution for self-service resource consumption within your private cloud. It simplifies provisioning VMs, Kubernetes clusters, databases, and load balancers through self-service capabilities. These resources are organized into blueprints, making deploying complex applications as single service requests easier. Deployments can be managed using the VCF Automation UI or through infrastructure as code. Additionally, they can be provisioned directly from the Kubernetes API if preferred. The self-service portal is ready for immediate use and can be customized via a REST API or ServiceNow. These features empower any team to create a self-service experience in a private cloud.

Broad network access: VMware NSX is essential for operating a private cloud as it offers the software-defined networking (SDN) foundation that replicates the agility and flexibility of public cloud networking. As public cloud platforms like AWS use SDN layers to provision, connect, and secure virtual resources on demand, NSX enables organizations to achieve the same within their private cloud environments. Without NSX, constructing and managing a private cloud would be considerably more complex and less efficient, lacking the dynamic network provisioning, segmentation, and automation that are trademarks of the cloud experience. Powered by NSX, VCF simplifies the management of a wide range of network services entirely in software. Quickly expose any application—whether privately via a VPN or publicly—while securing the environment through service isolation with NSX.

Resource pooling: VCF provides robust resource pooling and multi-tenancy capabilities across the infrastructure. Workload domains enable organizations to align business needs with right-sized compute, storage, and network resource pool allocations. These pools can be subdivided into secure, isolated tenants, offering a self-service portal for administrators to manage their virtual environments. This isolation also extends to the network layer with NSX Virtual Private Clouds (VPCs), where each tenant receives a dedicated portion of the network, complete with its own address space, security policies, and routing. This granular control facilitates efficient resource allocation, enhances security, and streamlines management across diverse workloads and business units.

Rapid elasticity: VCF excels at rapid elasticity, allowing for quick scaling of resources in response to changing demands. This is achieved through VCF Operations fleet management, which continuously monitors the deployment and analyzes resource utilization trends. By assessing current and projected demand, VCF Operations enables proactive scaling—adding or removing capacity and anticipating workload fluctuations. This ensures that the private cloud environment can dynamically adapt to varying workloads, providing a seemingly limitless pool of resources while maintaining cost control and preventing over-provisioning.

Measured service: VCF delivers comprehensive metering and reporting capabilities, enabling accurate tracking and analysis of resource consumption across the entire private cloud environment. This granular visibility is provided through VCF Operations, which offers a centralized platform for monitoring resource usage across various tenants, services, and applications. This data can be leveraged for chargeback (billing internal consumers based on actual usage) and showback (providing transparency into resource consumption for cost awareness and optimization) models. VCF Operations offers detailed insights into cost and capacity, allowing administrators to plan infrastructure expenditures effectively. It includes pre-defined cost models for standard infrastructure services, which can be customized to reflect specific pricing structures or operational expenses. This allows for accurate cost allocation and forecasting, enabling informed decisions regarding resource provisioning and capacity planning.

How Does It Work?

VMware Cloud Foundation is built on top-tier technologies encompassing compute, networking, storage, management, and automation. This software-defined approach enables customers to utilize commodity hardware, separating the software from the underlying physical infrastructure. This separation offers flexibility and cost efficiency, as resources can be dynamically reallocated in response to changing demands within the data center. With the robust cloud management capabilities of VCF Operations and VCF Automation, VCF provides a genuine private cloud experience without compromise. This comprehensive platform offers:

- Simplified operations: Automated deployment, lifecycle management, and patching streamline administrative tasks, reducing operational overhead.
- Scalability and performance: VCF can scale to support thousands of virtual machines and containers, delivering high performance for demanding business-critical workloads.
- Enhanced availability: Built-in features like vSphere HA and DRS ensure continuous availability and resilience in the face of hardware or software failures.
- Integrated security: VCF integrates with NSX network virtualization, enabling centralized management, deeper visibility into virtual machine activity, and consistent network and security policies across environments.

Infrastructure Automation

VMware Cloud Foundation is deployed using an installer component, which automates the deployment and configuration of the entire software-defined data center (SDDC) infrastructure stack. This includes core components like vSphere for compute virtualization, vSAN for storage virtualization, NSX for network virtualization, VCF Operations for centralized management and monitoring, and VCF Automation for self-service consumption. The VCF Operations fleet management appliance is deployed during the initial deployment. These products provide a complete private cloud infrastructure suite, accelerating your cloud journey and modernizing your data center.

After the initial deployment, automating the scale-out and modular deployment of the core VCF stack is simple. This automation significantly reduces the complexity and time required to expand the cloud infrastructure platform. For example, adding new ESXi hosts to a cluster, expanding vSAN storage capacity, or deploying new NSX Edge services can be done with just a few clicks.

Traditional infrastructure deployment typically requires manual configuration and multiple steps, which can take weeks to finish, depending on the size and complexity of the environment. Each manual step increases the potential for human error. VCF Operations fleet management simplifies this process by utilizing automation and a self-service catalog to eliminate manual errors and ensure consistent, repeatable infrastructure deployments. This consistency speeds up time to value by lowering the need for staff retraining and specialized skill sets.

The APIs provided by VCF Operations fleet management allow for the automation of numerous tasks across storage, compute, and networking resources. This enables customers to deploy and manage their environment more efficiently, resulting in a faster time to market for their services. For example, you can use APIs to programmatically provision new virtual machines, configure network policies, or adjust storage capacity based on application demands. Cloud Foundation is built with API-first automation in mind. It offers a comprehensive and standardized set of APIs essential for customers who want to integrate their existing toolsets and automate infrastructure tasks. This API support helps accelerate private cloud adoption by simplifying the integration of VMware and third-party business systems into Cloud Foundation. Customers can protect their investments in existing IT systems by programmatically integrating them to manage and provision SDDC infrastructure as code. This gives them the power and flexibility of cloud computing within their private data centers.

Scalable Architecture

VMware Cloud Foundation (VCF) employs infrastructure automation to deploy a truly modular architecture, offering exceptional flexibility for organizations to tailor their cloud infrastructure. This allows them to start with a minimal footprint, deploying essential components like vSphere, vSAN, NSX, and VCF Operations initially and later adding advanced services as needed. Organizations can independently scale compute, storage, and network resources to meet specific application demands, optimizing resource allocation and performance. Furthermore, workload domains can be customized with tailored configurations for applications or departments, enhancing resource efficiency and performance.

Workload Domain

The term "workload domain" may be new to a vSphere administrator, but the concept is familiar. A workload domain is a modular building block of VMware Cloud Foundation infrastructure that consists of one or more vSphere clusters. Essentially, it's something you already recognize in vCenter. However, when deployed with VCF, a workload domain is provisioned using automation, and that automation adheres to a prescribed architecture.

This architecture includes deploying ESXi hosts, associating them with their dedicated vCenter instance, installing and configuring a software-defined network with NSX, and provisioning storage. Workload domains offer flexibility in storage choices, supporting vSAN, NFS, VMFS over Fiber Channel, or vVols-based storage. This allows you to tailor the storage configuration to the specific needs of your applications.

Once deployed, the workload domain is managed and monitored by VCF Operations. Think of VCF Operations as the central command center for your infrastructure. From this central point, you can automate the creation, expansion (scale out), contract (scale in), deletion, and lifecycle management of the workload domain infrastructure. This provides a cloud-like experience within your private data center, mirroring public cloud environments' self-service and operational efficiency.

Workload domains offer two main advantages: isolation and security. They create separation between applications or tenants, enhancing security by preventing unauthorized access and resource contention. This isolation also enhances resource management by enabling administrators to allocate resources to each workload domain, ensuring that critical applications receive the necessary resources.

Another benefit is simplified management. VCF Operations streamlines the management of workload domains by automating various tasks, including deployment, scaling, and lifecycle management. This automation reduces manual effort, minimizes the risk of errors, and accelerates deployment times. For example, administrators can quickly scale a workload domain by adding or removing ESXi hosts, storage capacity, or network resources with just a few clicks without requiring complex manual configuration.

Workload domains offer significant flexibility. They can be customized with different configurations, resource allocations, and security policies to meet the specific needs of various applications. This allows organizations to tailor their infrastructure to support diverse workloads, ranging from resource-intensive applications to those with strict security or compliance requirements. For example, a workload domain for a database application might be configured with high storage performance and dedicated network resources. In contrast, a workload domain for a web application might prioritize scalability and load-balancing capabilities.

Finally, workload domains have a crucial advantage of scalability. VCF allows you to quickly scale workload domains by adding or removing ESXi hosts, storage capacity, and network resources as needed. This dynamic scaling capability ensures that your private cloud can adapt to changing workloads and business requirements without significant infrastructure changes or downtime.

Organizations can use workload domains to achieve a more agile, efficient, and cloud-like operating model for their private cloud infrastructure.

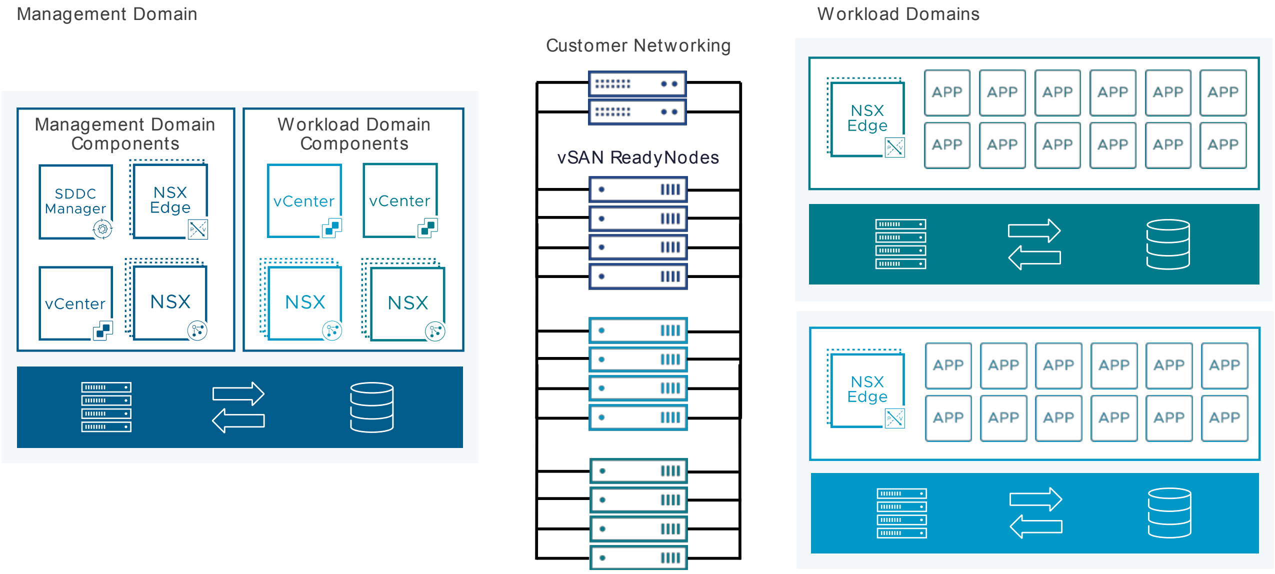


Figure 2. Management and workload domains.

Workload Domain Types

workload domains in VCF come in two flavors, each serving a distinct purpose. When you initially deploy VCF, the first type is created: the Management workload domain.

This Management workload domain houses nearly all the management components. These include the vCenter instance for managing the environment, NSX Manager appliances for network virtualization, VCF Operations and Automation appliances, and any other third-party management and operations applications you might need to operate your private cloud.

Depending on your organization’s size and needs, this single Management workload domain might be sufficient to run your management components and business applications. This is referred to as a consolidated architecture. In this scenario, VCF utilizes vSphere Resource Pools to distribute available resources within the cluster. You can configure resource reservations to guarantee that management components receive the necessary CPU, memory, and storage resources while the remaining resources are allocated to your business applications.

For larger enterprises with more demanding workloads and higher security requirements, VCF offers a second type of workload domain: the virtual infrastructure (VI) workload domain. This type is purpose-built for running business applications.

In VMware Cloud Foundation (VCF), separating management components from business applications using dedicated workload domains creates an isolated architecture with distinct advantages. This separation enhances security by reducing the attack surface and minimizing the impact of potential vulnerabilities. If a security breach occurs within a workload domain running business applications, it is less likely to affect the management components, which are crucial for controlling and maintaining the entire VCF environment.

This isolation can enhance performance by preventing resource contention between management and business applications. Management tasks, such as monitoring and lifecycle operations, can consume substantial resources. By separating these tasks into a dedicated Management workload domain, they are kept from competing for resources with business-critical applications. This guarantees consistent performance for both management functions and applications, avoiding "noisy neighbor" situations where resource-intensive tasks in one workload domain adversely affect the performance of others.

Managing separate workload domains for various purposes enhances organizational efficiency and simplifies troubleshooting. Administrators can concentrate on specific tasks within their assigned domains, streamlining operations and reducing complexity. When an issue arises, isolating and addressing it within a workload domain is easier, minimizing disruption to other parts of the environment. This separation also offers greater flexibility for applying updates and patches, allowing you to update individual workload domains independently without affecting others.

Finally, the isolated architecture allows independent scaling of the management and workload domains. This means you can scale each domain to meet its specific resource demands without affecting the other. For example, if your business applications require additional compute resources, you can scale the VI workload domain without impacting the performance or availability of the management workload domain. This granular scalability ensures that each part of your VCF environment has the resources to operate efficiently.

By offering these two types of workload domains, VCF provides the flexibility to design a private cloud architecture that aligns with your organization’s specific needs and scale.

Multiple Workload Domains

Speaking of scale, large enterprises often require more granular workload separation or additional boundaries within their private cloud environment. To address this need, VMware Cloud Foundation supports the deployment of multiple workload domains. This allows organizations to segment their infrastructure based on various factors such as departments, applications, security requirements, or compliance levels.

Each workload domain is an independent compute, storage, and network resource unit. It comes with its own dedicated vCenter instance for centralized management, is configured with NSX for software-defined networking capabilities like micro-segmentation and distributed firewalls, and offers a choice of storage backends, including vSAN, NFS, VMFS on Fiber Channel, or vVols.

Remote Workload Domains

workload domains offer even greater flexibility by enabling the deployment of remote clusters to remote sites. This capability extends the benefits of VCF to edge locations, branch offices, or disaster recovery sites, providing a consistent infrastructure and operational model across geographically dispersed environments.

When deploying a workload domain with a remote cluster, the management plane remains centralized in the Management workload domain at the primary site. This means that the vCenter instance, NSX Manager appliances, and VCF Operations and Automation appliances that manage the remote cluster are all at the primary data center.

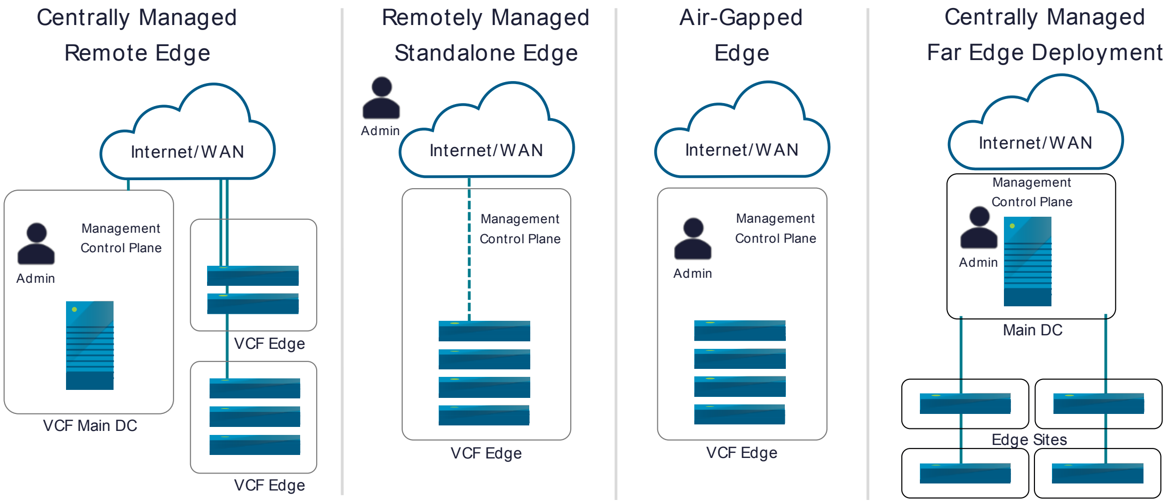


Figure 3. Deployment options for remote edge workload domains.

Isolated Single Sign On

VCF offers multiple options for organizations seeking to isolate workload domains and enhance security within their private cloud. One crucial aspect of workload domain isolation is providing independent vCenter Single Sign-On (SSO) authentication.

By default, all workload domains within a VCF deployment share the same SSO domain. This means that users authenticated in one workload domain can access resources in other workload domains if granted the appropriate permissions. However, VCF offers flexibility in SSO design to meet various security and organizational requirements.

When creating a new workload domain in VCF, you have two primary choices for SSO domain configuration:

- Join the existing Management SSO Domain: This option suits environments where a single SSO domain is sufficient for all workload domains. It simplifies user management and access control by centralizing authentication within the existing Management workload domain.
- Create a new Isolated workload domain: This option provides more robust isolation by creating a dedicated SSO domain for the new workload domain. This isolates user authentication and authorization, preventing users in one workload domain from accessing resources in another without explicit cross-domain trust configurations.

Isolated SSO domains in VMware Cloud Foundation (VCF) offer significant security and compliance advantages. By preventing unauthorized access and lateral movement between workload domains, they enhance security posture and help meet regulatory compliance requirements for strict separation of duties and access controls. For example, a user in a development workload domain cannot access resources in the production workload domain, even with valid credentials, limiting the impact of a potential security breach.

Furthermore, isolated SSO domains simplify management by enabling decentralized user administration, allowing individual teams or departments to manage their users and access controls. This is particularly crucial in multi-tenant environments, where each tenant needs complete isolation and control over their users and resources to ensure data privacy and security. By offering these SSO domain isolation options, VCF empowers organizations to tailor their private cloud environment to their specific security, compliance, and operational needs.

Multi-Cluster Workload Domains

VMware Cloud Foundation (VCF) simplifies initial deployment and provides easy scalability to accommodate growing workloads and evolving business requirements. Scaling up within VCF involves adding resources to existing workload domains while scaling out involves adding new workload domains to the environment.

Workload Domains Summary

Scaling up in VCF involves adding capacity to existing clusters within a workload domain. This could mean seamlessly adding new ESXi hosts to increase compute capacity, expanding vSAN datastore storage capacity by adding disks or new hosts, or scaling network resources to accommodate growing traffic demands. VCF Operations fleet management automates much of this process, including network configuration, storage integration, and vCenter association, simplifying the expansion of existing resources.

VCF also supports scaling out by adding new workload domains to the environment. This is particularly useful for isolating workloads based on departments, applications, or security zones, accommodating diverse requirements by deploying workload domains with tailored configurations, and supporting organizational growth by quickly adding new workload domains as needed. This flexibility allows organizations to adapt their private cloud infrastructure to evolving needs and effectively manage diverse workloads.

VCF Operations fleet management is the engine behind these scaling operations. It automates adding or removing cloud infrastructure resources, enabling organizations to adapt to changing demands without manual intervention. This automation simplifies management, reduces errors, and accelerates time to value.

Availability

VMware Cloud Foundation (VCF) is designed from the ground up to ensure high availability for your applications and provide a robust platform for running critical workloads. This is achieved through a combination of features and technologies that work together across the entire stack. By combining vSphere, NSX, and vSAN's distributed architecture, VCF provides a highly available and resilient platform for running business-critical applications. This ensures business continuity and minimizes the impact of potential failures.

Compute Availability with vSphere

VMware vSphere offers a robust suite of features that ensure high availability and resilience for your virtualized workloads. vSphere High Availability (HA) provides automatic failover of virtual machines (VMs) in case of a host failure. vSphere HA constantly monitors the health of ESXi hosts in a cluster. If a host fails, its VMs are automatically restarted on other available hosts with spare capacity, minimizing downtime.

vSphere offers advanced availability features like vSphere Fault Tolerance (FT), which ensures continuous availability for critical applications. This is achieved by creating a live shadow instance of a VM that mirrors the primary VM. In the event of a host failure, the shadow VM takes over instantly, allowing seamless failover with zero downtime. Another example is the vSphere Distributed Resource Scheduler (DRS), which dynamically balances resource allocation across hosts in a cluster, optimizing performance and ensuring VMs can access the necessary resources.

This combination of automated proactive and reactive mechanisms helps prevent resource contention and performance degradation, contributing to overall availability.

NSX Resilience

VMware NSX is designed with high availability as a core principle. It ensures that your network virtualization layer remains operational even in the face of failures. Several technical features contribute to NSX's high availability.

NSX achieves control plane redundancy by using a cluster of three or more NSX Manager nodes that handle centralized management and control functions. This ensures uninterrupted network operations, even if one NSX Manager fails. Likewise, NSX Controllers, which distribute network information and ensure consistent forwarding, are also deployed in a cluster for redundancy and fault tolerance. These controller clusters maintain a consistent view of the network environment through a distributed database, enabling seamless failover in the event of a controller node failure.

Data plane redundancy is achieved through a distributed architecture where data plane functions are spread across all hypervisors in the environment. This eliminates any single point of failure and ensures network traffic flow even during host failures. Additionally, NSX Edge nodes, which provide services like routing, firewalling, and load balancing, can be deployed in active/standby or active/active configurations for high availability. In active/standby, the standby node takes over if the active node fails, while in active/active, both nodes actively process traffic, increasing throughput and resilience.

Furthermore, NSX incorporates health monitoring and auto-remediation capabilities. It continuously monitors the health of all components, including NSX Managers, Controllers, and Edge nodes, detecting and reporting any issues. In case of a failure, NSX automatically triggers failover mechanisms to redirect traffic and maintain network connectivity. This proactive approach ensures that network operations remain uninterrupted, minimizing downtime and ensuring application availability.

Storage Availability with vSAN

vSAN, VMware's software-defined storage solution, ensures data availability and resilience. Its distributed architecture spreads data across multiple hosts in a cluster, eliminating any single point of storage failure. vSAN also provides built-in data replication and fault tolerance mechanisms.

vSAN enhances VMware Cloud Foundation (VCF) availability by distributing data across multiple hosts and providing built-in data replication. This ensures data remains accessible even during host or disk failures. vSAN automatically rebuilds data on surviving hosts to restore redundancy and proactively monitors the storage environment to address potential issues before they impact availability. Storage Policy Based Management (SPBM) also simplifies storage management by allowing administrators to define storage policies with specific availability requirements, which vSAN automatically enforces. These policies can include determining the number of failures to tolerate and the desired level of data protection (e.g., RAID 1, RAID 5, RAID 6). By combining distributed storage, data replication, proactive monitoring, and policy-driven management, vSAN delivers a highly available and resilient storage platform for VCF deployments.

Stretched Clusters for Geographic Redundancy

vSphere, NSX, and vSAN can be configured in stretched cluster deployments for even greater availability. A stretched cluster spans two geographically separated sites, providing high availability and disaster recovery capabilities. Data is synchronously replicated between the two sites, ensuring that data remains consistent and accessible even if one site experiences a complete outage.

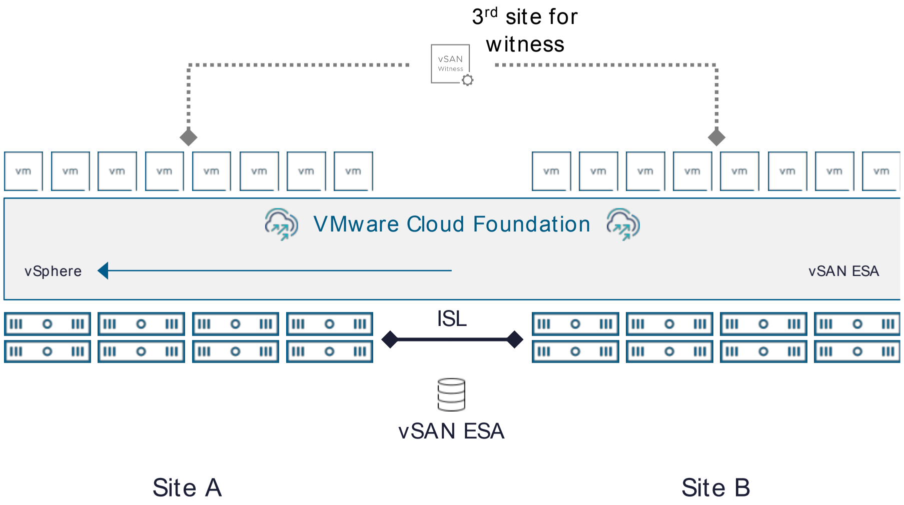


Figure 4. Availability across sites with a vSAN stretched cluster.

Lifecycle Management

Beyond simplifying architecture and deployment, VMware Cloud Foundation (VCF) Operations fleet management also provides unified lifecycle management for the core SDDC stack. This includes automating routine but critical tasks such as patching and upgrading, ensuring that all components — vSphere, vSAN, NSX, and the vCenter appliance — are consistently maintained and up to date. This automation significantly reduces the risk of errors associated with manual processes and helps maintain a healthy, secure, and compliant infrastructure.

Challenges of Manual Patching and Upgrading

Manually patching and upgrading an entire SDDC infrastructure stack is a complex task, laden with potential challenges. Administrators must carefully consider component interdependencies, as an incorrect order of patching or upgrading can result in compatibility issues and system instability. Ensuring version compatibility across all components is vital for maintaining a stable and supported environment. Minimizing downtime during these processes is crucial for business continuity, and the timely application of security patches is essential for safeguarding the infrastructure against vulnerabilities. These obstacles underscore the necessity for a more streamlined and automated approach to lifecycle management.

Automated Lifecycle Management with VCF

VCF lifecycle management streamlines and automates the entire lifecycle management process, effectively addressing the challenges associated with manual patching and upgrades. It orchestrates updates in a defined order, ensuring compatibility and minimizing downtime while automatically managing component dependencies. A centralized interface simplifies update management, making scheduling, initiating, and monitoring effortless. By automating these tasks, VCF reduces the risk of human error, resulting in a more stable and reliable infrastructure. This increased efficiency frees administrators from tedious manual tasks, allowing them to focus on strategic initiatives. Ultimately, VCF empowers organizations to maintain a healthy, secure, and up-to-date SDDC infrastructure with minimal effort and reduced risk.

Security

When designing and implementing cloud infrastructure security, there are three primary goals to remember.

Comprehensive and Flexible Security

VCF prioritizes comprehensive and flexible security by providing robust built-in security controls like vSphere hardening, NSX micro-segmentation, and vSAN encryption, which are enabled by default. Recognizing that a one-size-fits-all approach is rarely practical, VCF allows for customizing security policies to meet the unique needs of different workloads, including legacy applications that may require specific configurations. Furthermore, VCF aids organizations in meeting compliance requirements by offering tools and configurations aligned with industry standards and regulations.

Ease of Use and Operational Efficiency

To encourage adoption and minimize administrative overhead, VCF prioritizes ease of use and management for its security features. This is achieved through centralized management via VCF Operations, providing a single platform to manage security policies across the entire SDDC stack. Automating critical security tasks, such as password rotation and certificate management, further reduces manual effort and the risk of errors. Additionally, VCF streamlines security configuration and management with intuitive interfaces and workflows, making it easier for administrators to implement and maintain a secure environment.

Consistency and Pervasiveness

VCF emphasizes consistent security across infrastructure layers to minimize vulnerabilities and ensure comprehensive protection. This is achieved through integrated security features embedded across all components, from vSphere and vSAN to NSX and the VCF Operations. VCF allows for the definition and enforcement of consistent security policies across all workload domains and clusters, ensuring uniformity and reducing complexity. By integrating security throughout the stack, VCF reduces friction associated with implementing and managing security controls, promoting a secure-by-default environment.

The CIA Triad

These goals align with the core principles of information security, often referred to as the CIA Triad:

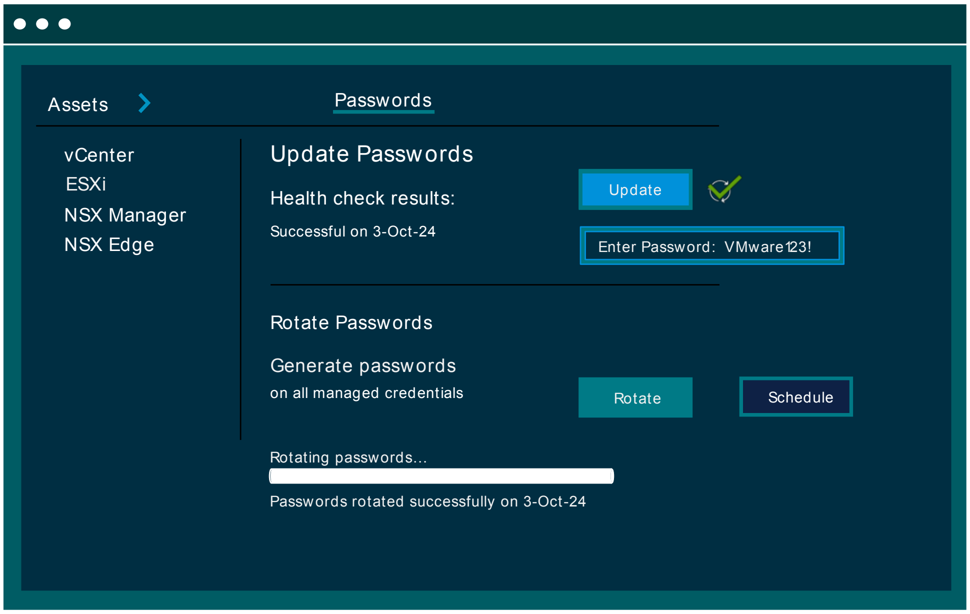
- Confidentiality: VCF protects sensitive data from unauthorized access through features like encryption, access control lists (ACLs), and micro-segmentation.
- Integrity: Ensuring that data remains accurate and unaltered. VCF provides data integrity through features like checksums, data protection mechanisms in vSAN, and secure boot for ESXi hosts.
- Availability: Guaranteeing that data and services are accessible when needed. VCF supports high availability through features like vSphere HA, vSAN data replication, and NSX Edge high availability.

Every feature within VCF can be mapped to one or more pillars, demonstrating its commitment to providing a secure and reliable platform for your critical workloads.

Password Management

VMware Cloud Foundation (VCF) provides centralized password management across the entire cloud infrastructure stack. This centralization simplifies managing passwords for various components, including compute, storage, networking, and operations services.

VCF Operations fleet management automates essential password management tasks, including password rotation to enforce vital password hygiene and synchronization across multiple components for consistency and secure password distribution to authorized users or services, streamlining access and reducing administrative overhead.



Update Passwords

Health check results:

Successful on 3-Oct-24

Enter Password: VMware123!

Rotate Passwords

Generate passwords
on all managed credentials

Rotating passwords...

Passwords rotated successfully on 3-Oct-24

Figure 5. Password rotation with VCF.

VCF integrates with existing identity management systems like Active Directory, LDAP, or SAML, enabling organizations to centralize authentication using existing identity providers, enforce consistent password management practices aligned with organizational policies, and simplify user management by managing user accounts and passwords from a central location.

To protect sensitive password information, VCF incorporates several security measures, including granular role-based access control (RBAC) to enforce least privilege principles, comprehensive audit trails and logging to track password management activities, and encryption and secure storage using industry-standard encryption algorithms and key management practices.

By centralizing, automating, and securing password management, VCF helps organizations improve operational efficiency, reduce security risks, and meet compliance requirements.

SSL Certificate Automation

VMware Cloud Foundation (VCF) simplifies SSL certificate management by automating the entire certificate lifecycle. This includes automatically generating Certificate Signing Requests (CSRs) and installing new certificates, renewing certificates before they expire to prevent service disruptions, and revoking certificates when necessary, such as when a key is compromised. These automated workflows ensure SSL certificates are always up-to-date and compliant with security policies, reducing the risk of certificate-related outages or vulnerabilities.

Furthermore, VCF provides control over SSL configuration settings. Administrators can customize SSL configurations to meet their specific security needs and regulatory requirements. This includes selecting encryption algorithms, choosing appropriate key lengths, and configuring certificate validation.

In addition to automation and customization, VCF offers comprehensive auditing and reporting capabilities for SSL certificate management activities. This includes tracking changes to SSL certificates and configurations and providing an audit trail for compliance and troubleshooting. VCF also monitors the status and validity of certificates, alerting administrators to upcoming expirations or potential issues. Furthermore, VCF can generate reports on SSL certificate usage and compliance, helping organizations meet regulatory requirements.

Data Center Privacy and Control

VCF gives organizations enhanced control over data privacy and compliance, enabling them to meet regulatory requirements and protect sensitive information.

Data Residency and Sovereignty

VCF allows organizations to maintain control over where their data resides, addressing data residency and sovereignty concerns. By offering flexible deployment options, including on-premises data centers, service providers, and edge environments, VCF enables organizations to choose locations that align with their specific data privacy and compliance requirements.

Compliance with Regulations

VMware Cloud Foundation (VCF) helps organizations demonstrate compliance with various data privacy regulations worldwide, including the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the Payment Card Industry Data Security Standard (PCI DSS) globally, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Privacy Act 1988 in Australia, the Personal Information Protection Law (PIPL) in China, and the Protection of Personal Information Act (POPIA) in South Africa. VCF provides tools and features, such as data encryption, access controls, audit logging, and data masking, to support compliance with these regulations, enabling organizations to protect sensitive data and meet their legal obligations.

Network Segmentation, Isolation, and Multi-tenancy

VMware Cloud Foundation (VCF) empowers organizations to enhance data privacy within their private cloud through robust network segmentation and isolation capabilities. VMware NSX, a core component of VCF, provides the foundation for achieving this. NSX enables the creation of secure, isolated network zones for different workloads and applications, preventing unauthorized lateral movement of data and limiting the impact of security breaches.

NSX achieves this granular network segmentation. It allows administrators to define security policies based on various criteria, such as virtual machine attributes, user identity, and application type. By enforcing these policies, NSX restricts network traffic flow, ensuring only authorized communication is permitted. This helps prevent unauthorized access to sensitive data and minimizes the blast radius of potential security incidents.

Furthermore, NSX provides advanced networking capabilities like Virtual Private Clouds (VPCs). VPCs enable multi-tenancy by allowing you to create isolated network segments for different tenants or departments within your private cloud. Each VPC has its dedicated network resources, including IP address ranges, security policies, and routing tables. This ensures strong isolation between tenants, prevents interference, and enhances data privacy. By combining micro-segmentation with VPCs, VCF provides a comprehensive network security and data privacy solution in a multi-tenant environment.

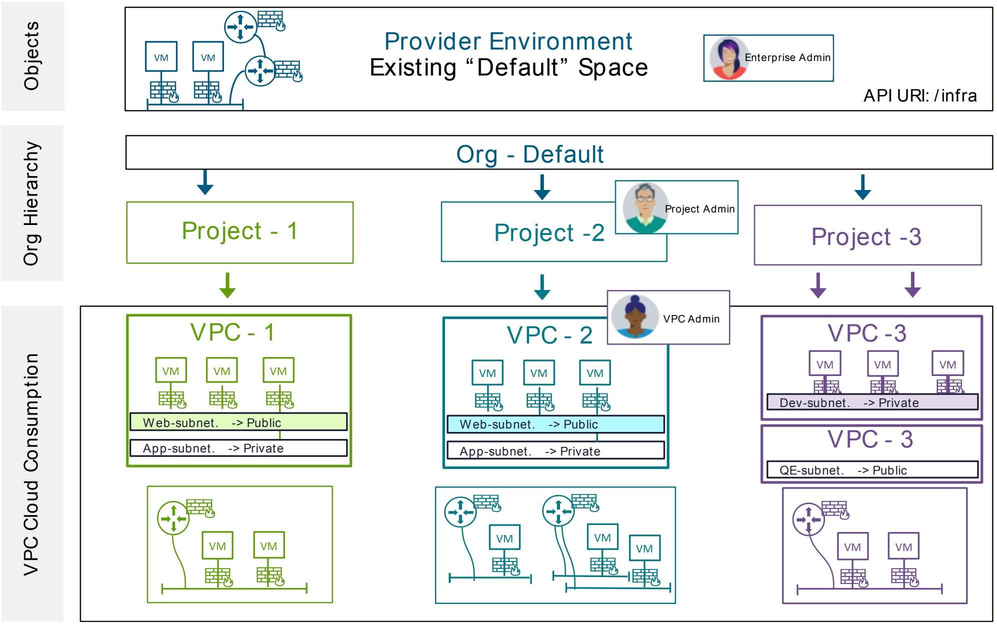


Figure 6. NSX Virtual Private Cloud (VPC).

Centralized Management and Automation

VCF Operations fleet management streamlines data privacy and compliance efforts through centralized management and automation capabilities. This encompasses defining and enforcing data privacy policies across the entire infrastructure, automating tasks like data encryption, access control configuration, and compliance reporting, and providing tools for monitoring data access and generating compliance reports, thereby reducing manual effort and the risk of errors. Furthermore, VCF can integrate with security information and event management (SIEM) tools to give real-time visibility into security events and suspicious activities, enabling proactive threat detection and response. It also supports the integration of posture management tools that continuously assess the compliance of the VCF environment against security benchmarks and industry best practices. This aids in identifying and remediating configuration drift and vulnerabilities, ensuring ongoing compliance.

Operations

Fleet management provides capabilities to better run and scale VCF infrastructures, including management capabilities for licenses, configurations, identity, and certificates. Together, they allow for better consistency and resource management across the VCF infrastructure, whether running one cloud or many.

Fleet Management

VCF Operations fleet management provides comprehensive capabilities for managing and scaling VMware Cloud Foundation (VCF) deployments, offering centralized control over various aspects of the infrastructure. These capabilities include streamlined management of licenses, ensuring compliance and cost optimization; standardized configurations to maintain consistency and reduce errors; integrated identity management for user authentication and access control; and automated certificate lifecycle management for enhanced security. Together, these features enable better consistency, resource management, and operational efficiency across VCF environments, whether running a single private cloud or multiple deployments across different locations. By streamlining these critical management functions, VCF Operations fleet management empowers organizations to optimize their private cloud deployments, reduce administrative overhead, and ensure consistent security and compliance across their entire infrastructure.

Operations Management

VCF Operations fleet management provides continuous performance monitoring to optimize VCF compute, storage, and network infrastructure resources. This involves proactively monitoring the environment to ensure the delivery of Service Level Agreements (SLAs) and to accelerate troubleshooting. The full-stack visibility provides a unified view of the entire infrastructure, from virtual machines to physical hosts, across workloads, storage, and network components. Additionally, AI-driven troubleshooting and remediation capabilities lead to faster issue resolution and better performance. This intelligent remediation can automatically identify and resolve performance bottlenecks, optimize resource allocation, and proactively address potential issues before they impact users.

Beyond performance monitoring, VCF Operations also includes detailed cost and capacity visibility and management features. These provide comprehensive cost assessment, optimization, and capacity planning across your private cloud environment to reduce costs and improve efficiency. For example, you can track resource usage by department, application, or workload, allowing for accurate cost allocation and chargeback. Efficient cost and capacity management enable innovative procurement to maximize compute, storage, and network utilization at a minimal cost. This includes assessing capacity and addressing shortfalls based on historical resource utilization and real-time predictive projections. Users can automate cost savings by identifying and reclaiming unused resources. The greater infrastructure visibility and workload planning capabilities support current and future workloads, reducing the total cost of ownership (TCO). Costs can also be managed through showback and chargeback to allocate costs based on actual usage and expenses, providing accurate cost visibility across your IT business.

Security Management

VCF Operations helps improve the security of your VMware Cloud Foundation environments by enabling compliance with regulatory standards, adherence to hardening guidelines, and support for governance initiatives. It can report on your current compliance posture against built-in regulatory standards, such as PCI DSS, HIPAA, and GDPR, helping you identify and address potential compliance gaps. This proactive approach to compliance strengthens your security stance and reduces the risk of audits and penalties.

VCF Operations also provides a streamlined event auditing process across all VCF resources. Audit records are generated for various platform interactions, including searches, logins, logouts, capability checks, and configuration modifications. These records are easily searchable and viewable within the VCF Operations console, ensuring that cloud administrators are quickly aware of any VCF infrastructure changes. This real-time visibility helps reduce the time to take remedial action, if required and provides insights into suspicious access events and policy violations. Additionally, it increases user accountability as each action is registered and associated with the user who performed it.

The configuration drift capabilities in VCF Operations enable cloud administrators to check the configuration status of vCenter instances and identify any deviations from defined baselines. Cloud administrators can define vCenter configuration templates and compare them against the actual configurations of vCenter instances to detect any deltas or drift. Maintaining consistent configurations across the environment ensures a more secure and stable environment, reducing the likelihood of issues arising from misconfigurations. For example, you can ensure that all ESXi hosts have consistent security settings, such as firewall rules and password policies.

By combining compliance checks, detailed auditing, and proactive configuration management, VCF Operations empowers organizations to strengthen their security posture, simplify compliance efforts, and maintain a consistent and secure VCF environment.

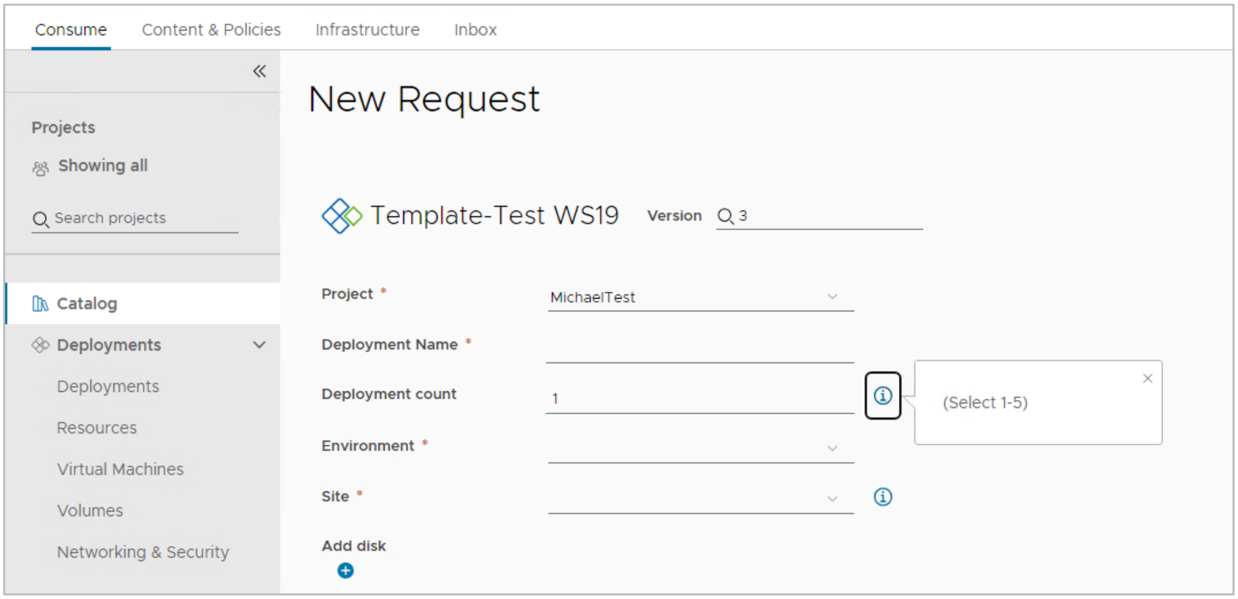
Automation

Many organizations have embraced the public cloud for some business needs, experiencing the advantages of cloud infrastructure and operations. Now, they seek to replicate the public cloud's self-service experience within their on-premises environments. Industry research confirms this trend, with IT professionals recognizing self-service as an efficiency and transformation enabler for IT teams and end-users. IDC predicts that "by 2028, 80% of IT buyers will prioritize as-a-service consumption for key workloads that require flexibility to help optimize IT spending, augment ITOps skills, and attain key sustainability metrics."[1]

Public cloud solutions are valuable for many applications and digital initiatives but are not universal. Due to data sovereignty, security regulations, integration with legacy systems, and cost considerations, specific applications and workloads may need to reside in on-premises environments. Additionally, workloads might need to move between different environments over time based on evolving needs and consumption patterns. Self-service delivery models enable IT organizations to abstract infrastructure complexities and provide users with the resources they need when they need them. This gives IT the flexibility to move workloads on the back end while maintaining control and compliance, optimizing the use of strategic corporate infrastructure resources.

Many IT organizations find building and delivering a self-service private cloud challenging. Maintaining it can be costly, operating it is complex, and keeping pace with the latest cloud-native technologies is difficult. IT teams encounter an increased demand for digital resources and support for modern software development practices from developers, DevOps engineers, and platform engineers. This strains IT staff, which are already limited, creating an unsustainable situation. There is growing pressure on IT to drive innovation collaboratively with developers in a secure, compliant, agile, and scalable way. Additionally, finding and retaining skilled IT professionals with expertise in infrastructure automation, DevOps, and cloud-native technologies, including knowledge of specialized coding and scripting languages, poses a significant challenge in today's competitive job market.

VCF Automation assists organizations in overcoming these challenges and accelerating their journey to a self-service private cloud. It empowers existing VI administrators to leverage their skills and transition into cloud administrators capable of delivering a genuine cloud consumption experience. This includes offering developers, DevOps teams, and platform engineers self-service access to Kubernetes and cloud infrastructure resources "as a service" through a modern IaaS consumption model. Templates reduce or eliminate the manual processes in building virtual infrastructure and supporting services. These templates can be deployed rapidly to enhance productivity.



New Request

Template-Test WS19 Version 3

Project * MichaelTest

Deployment Name *

Deployment count 1

(Select 1-5)

Environment *

Site *

Add disk

Figure 8. VCF Automation template deployment.

VCF Automation enables iterative development with infrastructure as code and the delivery of virtually anything as a service, including Kubernetes clusters, load balancers, private AI infrastructure, and more. It accomplishes this within a secure private cloud environment, with policy-based governance and automated workload lifecycle management.

VCF Automation helps organizations release new and updated applications more frequently, enabling the rollout of new products and services that support business growth and global operations. The solution also better uses existing resources, making IT and development teams more productive. Development teams gain an improved, secure, and compliant consumption experience with better request reliability. In contrast, IT teams free up time spent on helpdesk tickets and infrastructure maintenance to focus on more strategic initiatives and complex issues, driving innovation.

Conclusion

Many businesses have adapted to cloud consumption and understand cloud platforms' ease of deployment. However, they also face challenges in managing the rising public cloud costs and are striving to achieve similar efficiencies with private cloud deployments. VCF enables organizations to adopt a cloud operating model anywhere, allowing IT administrators to evolve into cloud administrators who can offer a self-service experience.

This transition is essential because businesses increasingly require agile and responsive IT services. Traditional data center operations often compel development teams to navigate complex, siloed deployment processes. Each service delivery component must be managed individually, making it difficult to coordinate changes and slow to implement them. VCF enhances agility by abstracting the data center into resource pools—compute, storage, and network—rather than managing discrete devices. It automates and oversees the entire infrastructure stack needed to deliver modern applications at the speed of business.

Most developers and IT managers prefer cloud infrastructure because of its agility. This agility enables rapid iteration and faster validation of ideas. VCF delivers that same agility to any infrastructure, whether in a public cloud or a private data center. This empowers businesses to innovate faster, respond more effectively to market changes, and optimize their IT investments.

Next Steps

The Total Economic Impact of VMware's VMware Cloud Foundation

Private Cloud Maturity Model Assessment

VMware Cloud Foundation Jumpstart Workshops

VMware Certified Professional - VMware Cloud Foundation

1. Source: https://www.idc.com/research/viewtoc.jsp?containerId=US50401023

Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24