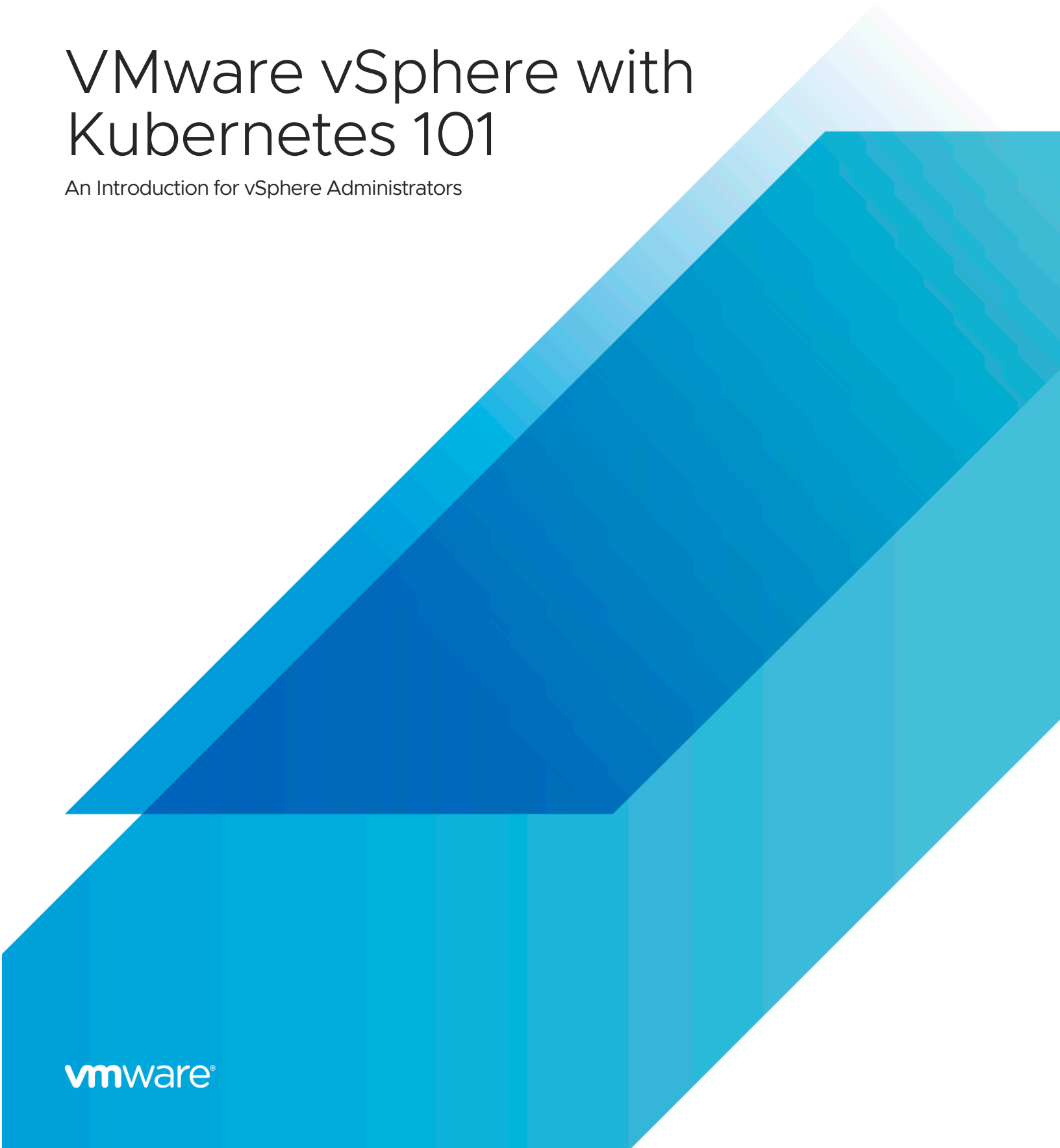
# VMware vSphere with Kubernetes 101

An Introduction for vSphere Administrators



## Table of Contents


Introduction 3

Goals 3

What is Kubernetes? 3

What is vSphere with Kubernetes? 4

What components make up a Kubernetes Cluster? 4

How does vSphere with Kubernetes work? 5

Advantages for the VMware Administrator 6

What comes with vSphere with Kubernetes? 6

- vSphere Pod Service 7
- Tanzu Kubernetes Cluster 7
- vSphere with Kubernetes & Cloud Foundation Services 7
- VMware NSX 7

Tanzu Kubernetes Cluster or vSphere Pod Service: Which do I choose? 9

- Tanzu Kubernetes Cluster: 9
- vSphere Pod Service: 9

The Best Way to Get Started: VMware Cloud Foundation 9

Conclusion & Takeaways 10

Resources 11

## Introduction

If you spend time in the information technology world you've likely heard the word "Kubernetes," often in conjunction with containers and developers. Containers first started on Linux in 2008 and are a lightweight & portable way to distribute and run applications across operating systems and clouds. Containers are not virtual machines, and by being lightweight they don't have the same well-defined boundaries — security, performance, or even political — that virtual machines have. As you might expect, this has both challenges and advantages.

Containers can be incredibly useful for developing applications. Kubernetes was created to help manage many of the challenges around deploying those applications, most notably by helping automate and orchestrate deployments and availability.

Kubernetes itself is an open-source project, governed by the Cloud Native Computing Foundation. VMware contributes heavily to the open-source Kubernetes software base and is deeply involved in Kubernetes communities and governance.

Kubernetes is extremely API-driven, which lends itself well to automation. It is very appealing to application developers as they seek to implement modern development practices, with short or continuous development cycles, well-defined APIs, and clearly separated and defined services which are often referred to as microservices.

vSphere and Virtual Infrastructure administrators often find themselves positioned between developers seeking to implement modern application development practices and more traditional IT infrastructure and governance rooted in decades of practice. This guide is intended to help admins understand what vSphere with Kubernetes is, how it helps build bridges, and how to get started with this new and exciting form of infrastructure for modern, cloud-native applications both on-premises and in public clouds.

## Goals

At the end of this document it is our goal that you will understand:

- What VMware vSphere with Kubernetes is
- The value that a Kubernetes Namespace brings to both the VMware Administrator and developers
- The differences between a vSphere Pod Service and a Tanzu Kubernetes Cluster
- How to get started with vSphere with Kubernetes & VMware Cloud Foundation Services

## What is Kubernetes?

According to Kubernetes.io, Kubernetes is "a portable, extensible, open-source platform for managing containerized workloads and services, which facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available."

What does that mean to a VMware Administrator? Kubernetes is an innovative approach for orchestrating the deployment and ongoing lifecycle management of modern, container-based workloads. Perhaps a brief history of the different approaches to application deployment will help aid our understanding of how Kubernetes fits in the modern enterprise:

- Traditional Deployment

  Applications and workloads deployed directly to physical servers are considered "traditional" deployments. Deployments of these types tended to be inflexible, hard to scale, and wasted costly resources by trapping them on specific systems.

- Virtualized Deployment

  VMware ESXi, a hypervisor, adds a layer of abstraction that allows for the creation of "virtual machines" which mimic the functions of a standardized physical server such that a workload does not know it is not running directly on a physical server. Each virtual machine has its own set of allocated resources as well as an operating system and can provide isolation of resources from other virtual machines. VMware ESXi also provides numerous availability features like vMotion, Dynamic Resource Scheduling, High Availability, and more, all of which provide massive advantages over traditional workload deployments.

- Containerized Deployment

  Containers are like VMs but are lightweight and do not have the rigid boundaries that VMs have. This makes them more portable and agile within a family of guest operating systems (such as Linux). A container's operating system comes from the system the container is running on and is shared among all containers running on a host. However, containers have their own filesystems and resource

allocation mechanisms. Containers are popular because of the ability to have continuous development and integration for deployment, a capability made possible by their lightweight nature.

## What is vSphere with Kubernetes?

VMware vSphere with Kubernetes was announced at VMworld 2019 as Project Pacific. It adds Kubernetes capabilities to vSphere in ways that respect the traditional experiences of both developers and vSphere Admins.

To a developer, vSphere with Kubernetes looks and acts like a standard Kubernetes cluster. Their tools and processes work across implementations. They can use the Kubernetes "declarative syntax" to define what resources they need, such as storage, networking, and even relationships & availability requirements. By using the industry-standard Kubernetes syntax they don't need direct access to, or knowledge of, the vSphere APIs, clients, or infrastructure.

To a vSphere Admin, vSphere continues operating just as it has for decades but now with new workload management features to better meet the needs of developers. Management of vSphere is still done through the vSphere Client, PowerCLI, and APIs, as it has been done for years. vSphere Admins can deploy "namespaces" – the Kubernetes term for managing resources and policies – and manage the security, resource consumption, and networking capabilities available to the developers.

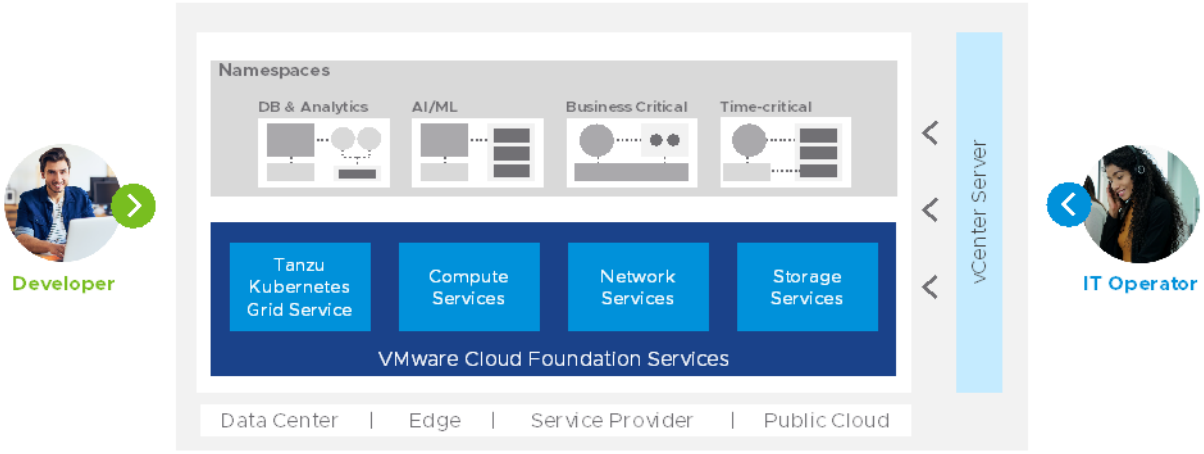



*Figure 1 - Overview of vSphere with Kubernetes*

vSphere with Kubernetes provides a unified approach to infrastructure that is uniquely suited for hosting both traditional workloads, and modern, cloud-native applications. For application developers, it is Kubernetes. For vSphere administrators, it is vSphere. For the business, it is a consistent, standardized approach for deploying and managing traditional workloads alongside modern, cloud-native applications, while safeguarding the security, compliance, and control of the IT infrastructure.

## What components make up a Kubernetes Cluster?

There are many components that are part of a Kubernetes Cluster. Here is an explanation of the ones relevant to deploying and configuring vSphere with Kubernetes:

- Nodes

  There are two main node types in Kubernetes, a Master and Worker. A master node is a management node, what you would expect of vCenter Server. A worker node is what you would expect of an ESXi host, allowing you to run Pods.

- Pod

  A Pod is a group of one or more containers. If we map this to a VMware Administrator construct think of Pods as an object similar to a virtual machine. Pods are managed by the Kubelet that runs on each node. Kubelet watches Podspecs assigned to it and handles all lifecycle by comparing actual Pod state to the desired state stored in the Podspec.

- Storage

  The files stored within a container are ephemeral, which means on each container restart the data is lost. This is both an advantage and disadvantage. If you wish to have data be persistent it must be stored in a persistent volume. There are many different types of volumes available to Kubernetes. VMware vSAN has native container storage capabilities, allowing workloads to mount persistent volumes inside the VMware Cloud Foundation deployment. vSphere Cloud Native Storage provides the capability to back Kubernetes persistent volumes with vSphere volumes. The CNS provider supports VSAN and any other VMFS based datastore.

- Namespace

  A Namespace is used as the unit of management in environments with many users across multiple teams or projects. Namespaces are a way to divide cluster resources and separate permissions between users. When a Namespace is created you assign CPU, Memory and Storage limits to restrict the amount of resources a workload can consume, not unlike a vSphere Resource Pool. Where Namespaces differ from Resource Pools is that they also incorporate controls such as security. For example, from a security perspective via Namespaces you can manage access controls by using edit or read-only groups. You also have the ability through security policies to limit ports, audit changes and force encryption of data. To encrypt all containers and/or VMs in a Namespace is done by setting one property rather than going to each VM and encrypting individually.

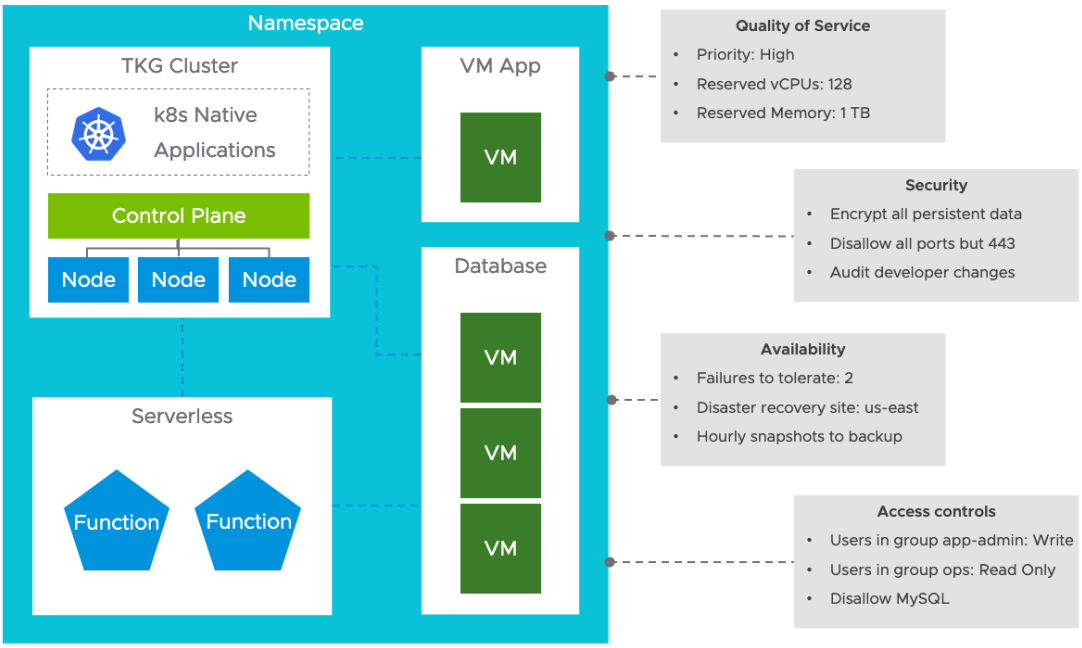



*Figure 2 - vSphere Namespace*

## How does vSphere with Kubernetes work?

vSphere with Kubernetes introduces Kubernetes APIs as a new Developer API that provides a cloud service consumption experience analogous to what they would get in a public cloud while providing a new control plane, or management interface, for vSphere via the extended Namespace construct. This allows for deep orchestration and governance of workloads, whether they are containers, applications, or even virtual machines.

vSphere with Kubernetes embeds the Kubernetes API, together with a custom management agent called a Spherelet, directly into the ESXi hypervisor. The Spherelet is based on the Kubernetes "Kubelet" and enables the ESXi hypervisor to act as a native Kubernetes node which can participate in a Kubernetes cluster. With this, every ESXi host can host containers directly on the hypervisor without the requirement for a separate Linux operating system (OS) instance. To accomplish this, we have added a new container runtime to ESXi called the CRX. This is presented to Kubernetes as an ESXi vSphere Pod Service.

The vSphere Pod includes a purpose-built and lightweight Linux kernel that is responsible for running containers inside the guest. Since this Linux kernel is provided by the hypervisor, VMware has been able to make numerous optimizations to para-virtualize the container, boosting its performance and efficiency. Additionally, because the CRX kernel does not load a full Linux guest OS, the instantiation of new pods is very fast.

Along with embedding Kubernetes directly into the hypervisor, the vSphere Client has also been made Kubernetes aware. Using the traditional vSphere Client, we can now view and manage Kubernetes objects alongside our virtual machines. Conversely, Kubernetes can also specify and control some aspects of traditional virtual machines, helping to seamlessly blend traditional and container workloads together to form a cohesively managed application.

Under the covers and invisible to the developers who consume Kubernetes clusters, vSphere with Kubernetes abstracts storage, network, and other resources. The developer can deploy containers or virtual machines without having to know or use traditional vSphere APIs. They use Kubernetes the way they always have.

## Advantages for the VMware Administrator

For the VMware Administrator, the introduction of Kubernetes as a control plane for vSphere opens possibilities for new workload management and orchestration in the future while still protecting your investments & efforts today. vSphere traditionally has been about management of virtual machines and infrastructure while being somewhat indifferent to the actual applications running on the VMs.

With vSphere with Kubernetes both the developer and the VMware Administrator can now easily create workloads and policies that govern containers, VMs, or both simultaneously. All aspects of application workload management are now first-class citizens in a vSphere environment.

Developers may already be running container workloads in your environment, but as a VMware Administrator you have no awareness nor visibility into them, making governance and troubleshooting difficult. With vSphere for Kubernetes, administrators gain visibility into Kubernetes workloads running on their virtual infrastructure. Enabling vSphere with Kubernetes allows you, as a VMware Administrator, to provide the platform based on the same performance, security, and availability criteria you use today for your traditional virtual machine workloads. Developers will still be able to use their same tools to code, test, deploy, and support their applications. This gives you as a VMware Administrator the ability to apply existing governance processes & tools to the environment, while developers have access to the modern application self-service components they enjoy.

The following is an example of the visibility the vSphere Administrator has of the Tanzu Kubernetes Grid instances running in their environment.

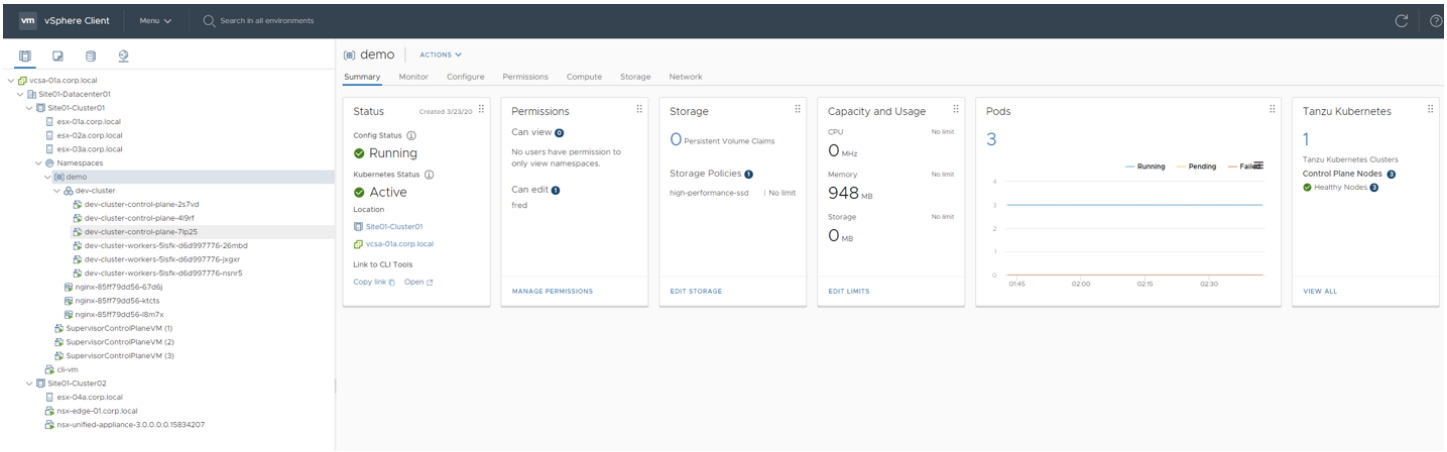



*Figure 3 - vSphere Client showing a TKG cluster*

## What comes with vSphere with Kubernetes?

There are many ways to deploy Kubernetes. Options including managed, cloud, on-premises virtual, and on-premises bare metal. There are tools such as the open source Minikube that have been developed to install and operate a Kubernetes cluster on a single host, which

is great for training. For enterprise use, though, most deployments require extensive setup work, new processes, and retraining of staff to install and operate Kubernetes effectively. This is where vSphere with Kubernetes and the VMware Cloud Foundation Services shine, with ease of installation and operation that fits naturally into your existing IT infrastructure and processes.

Within vSphere there are two types of Kubernetes clusters that run natively: a "Supervisor" Kubernetes cluster control plane known as the vSphere Pod Service and the Tanzu Kubernetes Cluster, sometimes also referred to as a "Guest Cluster."

### vSphere Pod Service

The vSphere Pod Service is a special kind of Kubernetes cluster that uses ESXi as its worker nodes instead of Linux. This is achieved by integrating the worker agents, Spherelets, directly into the ESXi hypervisor. The Spherelet doesn't run in a VM, it runs directly on ESXi via vSphere Pods. The vSphere Pod Service is a Kubernetes cluster of ESXi nodes instead of Linux nodes. The vSphere Pod Service uses vSphere Pods to run container workloads. vSphere Pods draw deeply on the exceptional security, availability, and performance of the ESXi hypervisor.

### Tanzu Kubernetes Cluster

While the vSphere Pod Service uses Kubernetes, it's not a conformant Kubernetes cluster. This is by design, as it intends to use Kubernetes to improve vSphere, rather than trying to turn vSphere into a Kubernetes clone. To deliver Kubernetes clusters to your developers that are standards-based and fully conformant with upstream Kubernetes you can use Tanzu Kubernetes Clusters, also referred to as "Guest" clusters.

A Tanzu Kubernetes Cluster is a Kubernetes cluster that runs inside virtual machines on the Supervisor layer and not on vSphere Pods. Since a Tanzu Kubernetes Cluster is fully upstream-compliant Kubernetes it is guaranteed to work with all your Kubernetes applications and tools. Tanzu Kubernetes Clusters in vSphere use the open source Cluster API project for lifecycle management, which in turn uses the VM Operator to manage the VMs that make up the cluster.

### vSphere with Kubernetes & Cloud Foundation Services

The main components that make up vSphere with Kubernetes and differentiate it from other Kubernetes implementations are the services that are used. When a cluster is enabled for vSphere with Kubernetes, we deploy the following services.

- vSphere Pod Service

  The vSphere Pod Service allows developers to run containers natively & securely on vSphere without managing virtual machines or Kubernetes clusters.

- Registry Service

  The Registry Service allows developers to store, manage and secure Docker and OCI images using Harbor. Harbor is an open source container image registry that secures images with role-based access control, scans images for vulnerabilities, and signs images as trusted.

- Storage Service

  The Storage Service allows vCenter Server storage policies & devices to be consumed as Kubernetes storage classes and be used as persistent disks for use with containers, Kubernetes, and virtual machines.

- Network Service

  The Network Service allows developers to define virtual routers, load balancers and firewall rules for use with their application.

- Virtual Machine Service

  Going forward, the Virtual Machine Service will allow you to deploy and manage traditional virtual machines using Kubernetes.

- Tanzu Kubernetes Grid Service for vSphere

  Part of the Tanzu Runtime Services, The Tanzu Kubernetes Grid Service allows developers to manage consistent, compliant, and conformant Kubernetes clusters. These are Tanzu Kubernetes Clusters.

### VMware NSX

NSX is designed into vSphere with Kubernetes from the ground up as the default pod networking & network security solution. NSX provides a rich set of networking capabilities including distributed switching and routing, firewalling, load balancing, and more.

Integrations with Kubernetes enables context-aware security policies that follow Kubernetes namespaces, providing easy-to-use isolation and security.

Native integration with the Kubernetes Cluster API allows application developers to specify load balancers and access policies, enabling applications to be easily published and supported outside of the Kubernetes cluster. Furthermore, NSX-aware tools like vRealize Network Insight help bring deep performance monitoring, security analytics, and troubleshooting capabilities to bear on modern applications running inside vSphere with Kubernetes, just as they do for traditional workloads.

## Tanzu Kubernetes Cluster or vSphere Pod Service: Which do I choose?

Tanzu Kubernetes Cluster:

- Kubernetes clusters that are fully conformant with upstream Kubernetes
- Flexible cluster lifecycle management independent of vSphere, including upgrades
- Ability to add or customize open source & ecosystem tools like Helm Charts
- Broad support for open-source networking technologies such as Antrea

vSphere Pod Service:

- Has additional capabilities that are inherent in the vSphere environment and are available to Kubernetes via the kubectl command
- Provides the ability to manage virtual machines just as you would manage containers
- Provides stronger security and resource isolation due to the use of vSphere Pods
- Performance advantages of vSphere Pods

## The Best Way to Get Started: VMware Cloud Foundation

Getting started with vSphere with Kubernetes happens with VMware Cloud Foundation. Cloud Foundation employs deep data center automation so new applications and services can be deployed and consumed quickly. It is a full suite approach to everything from deployment to day 2 operations such as patching, upgrades, and reconfiguration, for all the components in the software-defined data center (SDDC).

Cloud Foundation provides standardized and repeatable architecture & methods for implementing, operating, and maintaining a modern hybrid cloud, complete with vSphere with Kubernetes. vSphere administrators can use the advanced automation capabilities of VMware SDDC Manager to fully automate vSphere deployments into their private cloud. The automation includes the deployment and configuration of VMware vSAN as well as the implementation of a VMware NSX-T fabric.

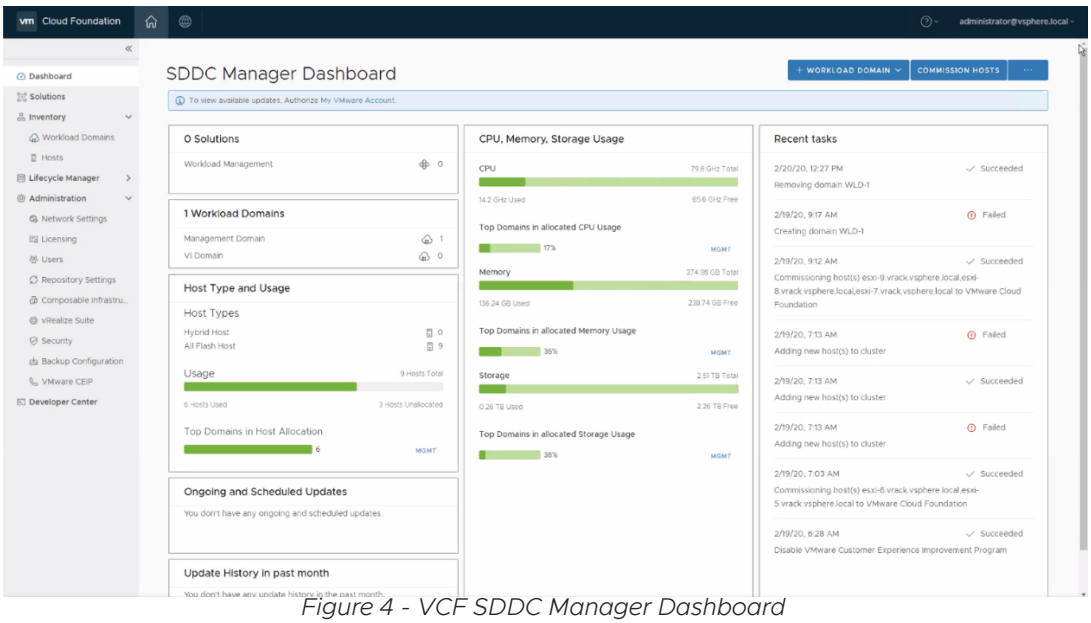



*Figure 4 - VCF SDDC Manager Dashboard*

Cloud Foundation is a dynamic platform, allowing infrastructure to be elastically scaled, shrunk, and repurposed in software to suit the demands of modern business. SDDC Manager is Kubernetes aware and provides the ability to orchestrate the deployment of the

Kubernetes vSphere Pod Service in preparation for hosting container-based workloads alongside your virtual machines. After the implementation, the SDDC Manager makes it easy to apply ongoing software patches and updates, streamlining day 2 operations and making it easy to keep your environment updated and secure.

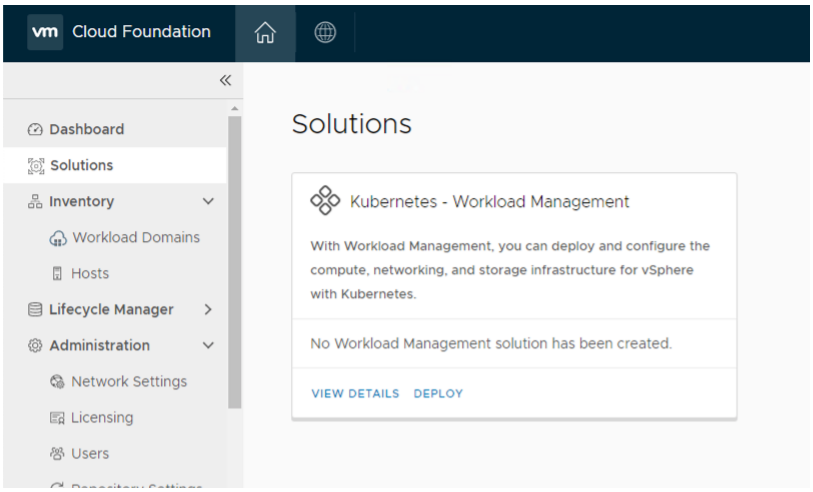



*Figure 5 - VCF Solutions*

## Conclusion & Takeaways

vSphere with Kubernetes is the best of both worlds. VMware Administrators can continue to leverage the vSphere environment they've known for decades with their traditional workloads, while simultaneously providing a world-class environment for the containerized workloads of a modern application.

- Open source Kubernetes installation and operation can be challenging for many reasons. VMware vSphere with Kubernetes and the VMware Cloud Foundation bring Kubernetes to enterprises in a way unlike anything else in the industry. The approach these products take recognizes & respects investments in infrastructure, people, processes, and existing workloads while positioning the enterprise for the future.
- Kubernetes namespaces are poised to change the way we think about application management inside virtual infrastructure. They allow developers freedom and self-service within operational and security boundaries set by the business. Namespaces also allow workload administrators, developers, and VMware Administrators new levels of flexibility to define and describe their workloads, letting Kubernetes orchestrate placement, availability, security, and other operational details.
- Namespaces allow VMware Administrators to have as much or as little interaction with the workloads as they want or need. VMware Administrators can bring their existing tools and knowledge to bear on the specifics of each workload. Both VMware Administrators and developers benefit from the large and growing ecosystem of tools, from the VMware vRealize Suite to Tanzu Mission Control.
- VMware vSphere with Kubernetes offers different types of Kubernetes clusters. The vSphere Pod Service is managed tightly with vSphere and offers better security and performance but differs from upstream Kubernetes offerings. Tanzu Kubernetes Clusters are completely conformant to upstream Kubernetes releases and are more flexible for developers when it comes to lifecycle operations.
- The VMware Cloud Foundation is how enterprises get started with vSphere with Kubernetes. The Cloud Foundation SDDC Manager automates deployments, infrastructure changes, and lifecycle operations for as much or as little of the VMware product stack as a customer desires and takes complexity out of operating a private cloud.

## Resources

To learn more about VMware vSphere with Kubernetes, VMware Cloud Foundation, and open source Kubernetes please visit the following resources:

- https://blogs.vmware.com/vsphere
- https://vspherecentral.vmware.com
- https://storagehub.vmware.com/t/vmware-cloud-foundation/
- https://k8s.vmware.com/kubernetes-on-vsphere-for-dummies/
- https://kube.academy/
- https://kubernetes.io/
- https://pathfinder.vmware.com/path/enterprisepks
- https://goharbor.io/

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.