VMware vSphere with Kubernetes 基础知识

vSphere 管理员简介

目录

简介

如果您从事信息技术领域的工作，则您很可能听说过“Kubernetes”一词，它通常与容器和开发人员关联在一起。容器最早出现在 2008 年的 Linux 上，它是一种轻量级和可移植的媒介，用于在操作系统和云端分发和运行应用。容器不是虚拟机，由于具有轻量级特征，它们并不像虚拟机那样有明确定义的边界 - 安全性、性能、甚至策略。如您所料，这既是挑战，也是优势。

在开发应用方面，容器非常有用。Kubernetes 旨在帮助管理与部署这些应用有关的众多挑战，它最主要的作用是帮助自动化和编排部署及可用性。

Kubernetes 本身是一个开源项目，由云原生计算基金会负责监管。VMware 为开源 Kubernetes 软件基础做出了巨大贡献，并深入参与了 Kubernetes 社区和监管。

Kubernetes 主要由 API 驱动，因此非常适合自动化。它对应用开发人员非常有吸引力，因为他们寻求实施现代开发做法，它具有较短或连续的开发周期、定义明确的 API 以及明确独立和定义的服务（通常称为微服务）。

vSphere 和虚拟基础架构管理员发现自己面临两难境地：一边是寻求实施现代应用开发做法的开发人员，一边是传统的 IT 基础架构和已推行了几十年的管理模式。本指南旨在帮助管理员了解 vSphere with Kubernetes 是什么、它如何帮助消除上述困境，以及如何着手针对本地部署和公有云中的现代云原生应用，采用这种令人兴奋的、全新形式的基础架构。

目标

在本文结束时，我们的目标是让您了解：

- VMware vSphere with Kubernetes 是什么
- Kubernetes Namespace 给 VMware 管理员和开发人员带来的价值
- vSphere Pod Service 与 Tanzu Kubernetes 集群的区别
- 如何开始使用 vSphere with Kubernetes 和 VMware Cloud Foundation Services

什么是 Kubernetes

根据 Kubernetes.io 的定义，Kubernetes 是一种可移动、可扩展的平台，用于管理容器化的工作负载和服务，促进声明性配置和自动化。它拥有一个庞大的、快速发展的生态系统。Kubernetes 服务、支持和工具广泛可用。

这对 VMware 管理员意味着什么？Kubernetes 是一种创新的方法，用于编排基于容器的现代工作负载的部署和后续生命周期管理。也许，通过了解不同应用部署方法的简要历史，将有助于我们理解 Kubernetes 如何切合现代企业的需求：

- 传统部署

  直接部署在物理服务器上的应用和工作负载被视为“传统”部署。这些类型的部署往往缺乏灵活性，难以进行扩展，并且，由于将昂贵的资源局限在特定系统上，造成了巨大的浪费。

- 虚拟化部署

  VMware ESXi 是一个 Hypervisor，它增加了一个抽象层，允许创建“虚拟机”来模拟标准化物理服务器的功能，这样一来，工作负载会认为自己是直接在物理服务器上运行。每个虚拟机都分配了一组资源以及一个操作系统，可以做到将资源与其他虚拟机隔离。VMware ESXi 还提供了众多可用性功能，比如 vMotion、动态资源调度、高可用性等，这些功能对于传统工作负载部署而言提供了巨大的优势。

- 容器化部署

  容器和虚拟机一样，但是具有轻量级特征，没有虚拟机那样的明确边界。在客户机操作系统（比如 Linux）家族中，上述特性使得它们更加便携和敏捷。容器的操作系统来自于容器所运行的系统，并且在主机上运行的所有容器之间共享。但是，容器有自己的文件系统和资源分配机制。容器之所以受欢迎，是因为它能够进行持续开发和集成部署，这种能力源自于其轻量级的特性。

什么是 vSphere with Kubernetes

VMware vSphere with Kubernetes 在 VMworld 2019 大会上以 Project Pacific 的形式发布。它将 Kubernetes 功能添加到了 vSphere 中，其采用的部署方式尊重开发人员和 vSphere 管理员的传统体验。

对于开发人员来说，vSphere with Kubernetes 的外观和行为类似于标准 Kubernetes 集群。他们的工具和流程可以跨多项实施使用。他们可以使用 Kubernetes 的“声明性语法”来定义他们所需的资源，比如存储、网络，甚至可以定义关系和可用性要求。通过使用行业标准的 Kubernetes 语法，他们不需要直接访问或了解 vSphere API、客户端或基础架构。

对于 vSphere 管理员来说，vSphere 的运行方式与过去几十年没什么不同，但现在增添了新的工作负载管理功能，可以更好地满足开发人员的需求。对 vSphere 的管理仍然通过 vSphere Client、PowerCLI 和 API 来完成，这与多年来的做法一致。vSphere 管理员可以部署“Namespace”（Kubernetes 术语，用于管理资源和策略），并管理开发人员可用的安全性、资源消耗和网络功能。

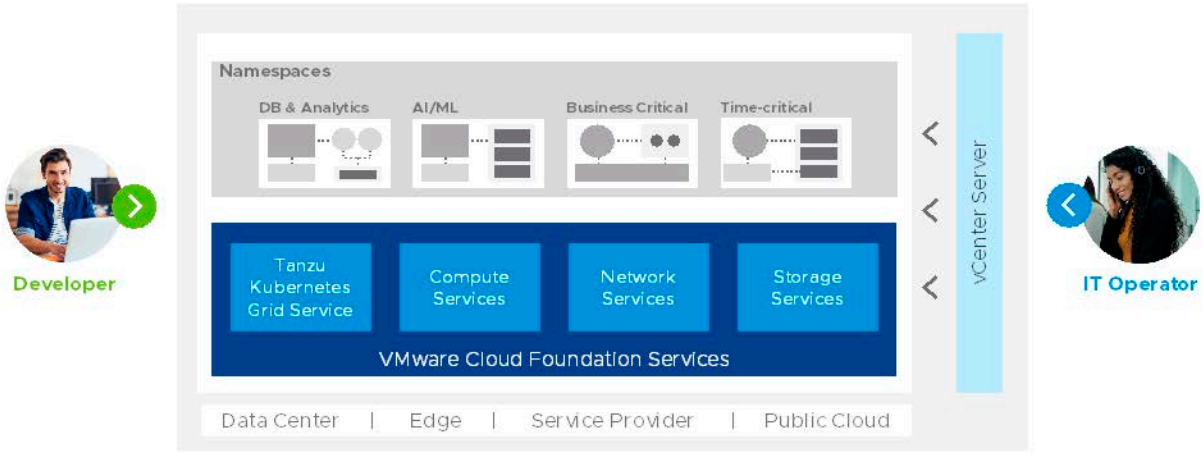

图 1 - vSphere with Kubernetes 概述

vSphere with Kubernetes 提供了一种统一的基础架构策略，专用于同时托管传统工作负载和现代云原生应用。对于应用开发人员来说，它是 Kubernetes。对于 vSphere 管理员来说，它是 vSphere。对企业而言，它是一种一致的标准化方法，用于部署和管理传统工作负载以及现代云原生应用，与此同时，保障 IT 基础架构的安全性、合规性和对它的控制。

Kubernetes 集群由什么组件组成

有许多组件是 Kubernetes 集群的一部分。下文说明了与部署和配置 vSphere with Kubernetes 相关的组件：

- 节点

  Kubernetes 中主要有两种节点类型 - 主节点和 Worker 节点。主节点是一个管理节点，这是您期望 vCenter Server 提供的功能。Worker 节点是您期望 ESXi 主机提供的功能，允许您运行 Pod。

- Pod（单元）

  Pod 是由一个或多个容器组成的组。如果我们将其对应到 VMware 管理员结构中，请将 Pod 视为一个类似于虚拟机的对象。Pod 由运行在每个节点上的 Kubelet 管理。Kubelet 观察分配给它的 Podspec，并通过比较实际的 Pod 状态和 Podspec 中存储的期望状态来处理所有生命周期。

- 存储

存储在容器中的文件将临时存在，这意味着，在每次容器重启时数据都会丢失。这既是优势，也是劣势。如果您希望数据持久存在，它必须存储在一个永久性卷中。Kubernetes 可以使用许多不同类型的卷。VMware vSAN 具有原生容器存储功能，允许工作负载在 VMware Cloud Foundation 部署内挂载持久性卷。vSphere Cloud Native Storage 可通过 vSphere 卷为 Kubernetes 持久性卷提供支持。CNS 提供商支持 VSAN 和任何其他基于 VMFS 的数据存储。

- Namespace

在特定的环境中（有跨多个团队或项目的众多用户），Namespace 被用作管理单元。Namespace 是在用户之间划分集群资源和分离权限的一种手段。创建 Namespace 后，您可以分配 CPU、内存和存储限制，以限制工作负载可消耗的资源量，这与 vSphere 资源池不同。Namespace 与资源池的不同之处在于，它们还加入了安全性等控制措施。例如，从安全角度来看，通过 Namespaces，您可以使用编辑或只读组来管理访问控制。您还可以通过安全策略来限制端口，审查更改和强制加密数据。要加密一个 Namespace 中的所有容器和/或虚拟机，您只需要设置一个属性，而不是对每个虚拟机单独加密。

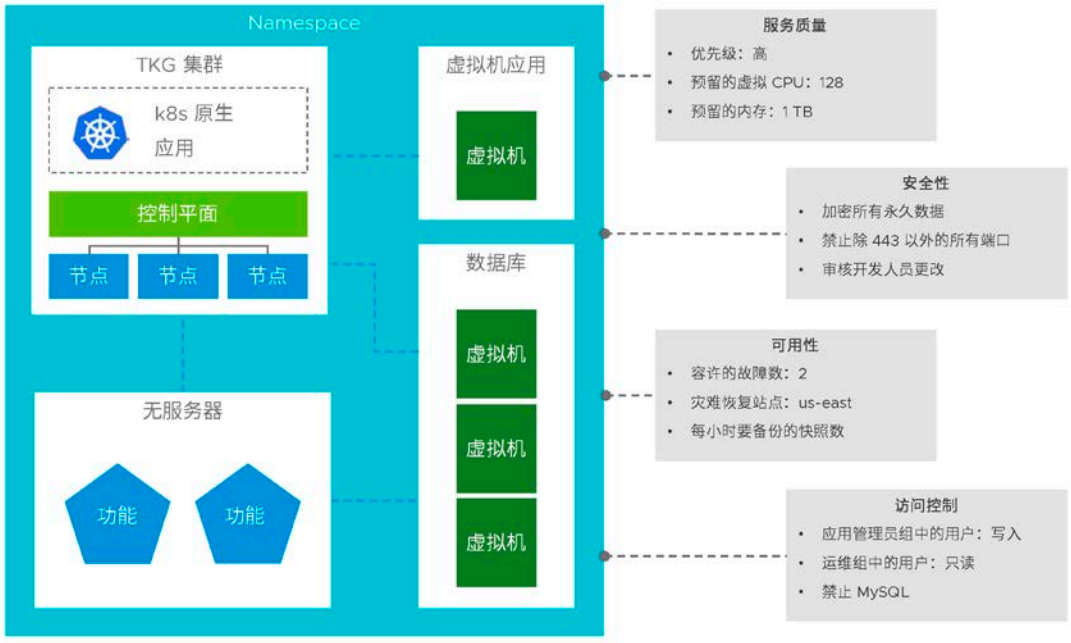

图 2 - vSphere Namespace

vSphere with Kubernetes 的工作原理是什么

vSphere with Kubernetes 引入了 Kubernetes API 作为新的开发人员 API，该 API 提供的云服务使用体验类似于公有云中提供的体验，与此同时，通过扩展的 Namespace 结构，为 vSphere 提供了一个新的控制平面或管理界面。这样一来，可以对工作负载（容器、应用、甚至虚拟机）进行深入编排和监管。

vSphere with Kubernetes 将 Kubernetes API 以及名为 Spherelet 的自定义管理代理直接嵌入到 ESXi Hypervisor 中。Spherelet 基于 Kubernetes“Kubelet”，使 ESXi Hypervisor 能够作为原生 Kubernetes 节点参与 Kubernetes 集群。借助此功能，每个 ESXi 主机都可以直接在 Hypervisor 上托管容器，而不需要单独的 Linux 操作系统 (OS) 实例。为了实现这一点，我们向 ESXi 添加了一个名为 CRX 的新容器运行时。此对象以 ESXi vSphere Pod Service 的形式呈现给 Kubernetes。

vSphere Pod 包含一个专门设计的轻量级 Linux 内核，负责在客户机内部运行容器。由于此 Linux 内核由 Hypervisor 提供，因此，VMware 能够执行大量优化，以准虚拟化容器，从而提升它的性能和效率。此外，由于 CRX 内核不加载完整的 Linux 客户机操作系统，因此，新 Pod 的实例化速度非常快。

除了直接将 Kubernetes 嵌入到 Hypervisor 中，vSphere Client 也可以识别 Kubernetes。通过使用传统的 vSphere Client，我们现在可以查看和管理 Kubernetes 对象及虚拟机。反之，Kubernetes 也可以指定和控制传统虚拟机的某些方面，有助于将传统工作负载和容器工作负载无缝融合在一起，形成一个聚合代管应用。

vSphere with Kubernetes 在后台运行，不会被 Kubernetes 集群的开发人员看见，它抽象化了存储、网络和其他资源。开发人员可以部署容器或虚拟机，而无需了解或使用传统 vSphere API。他们可以按照习惯的方式使用 Kubernetes。

VMware 管理员获得的优势

对于 VMware 管理员来说，通过引入 Kubernetes 作为 vSphere 的控制平面，为未来实现新的工作负载管理和编排开辟了可能性，同时还能保护您当下的投资和工作成果。vSphere 过往一直注重的是虚拟机和基础架构管理，而对虚拟机上运行的实际应用却有些忽视。

借助 vSphere with Kubernetes，开发人员和 VMware 管理员现在可以轻松创建工作负载和策略，以管理容器、虚拟机或同时管理两者。现在，在 vSphere 环境中，应用工作负载管理的各个方面都得到了重视。

开发人员可能已经在您的环境中运行容器工作负载，但作为 VMware 管理员，您既不了解、也无法监测这些工作负载，这使得监管和故障排除变得困难。借助 vSphere for Kubernetes，管理员可以监测在其虚拟基础架构上运行的 Kubernetes 工作负载。启用 vSphere with Kubernetes 后，作为 VMware 管理员，您仍然可以按照如今为传统虚拟机工作负载使用的性能、安全性和可用性标准来提供该平台。开发人员仍可使用相同的工具对其应用进行编码、测试、部署和支持。这使您 - 作为 VMware 管理员 - 能够将现有的监管流程和工具应用到环境中，而开发人员可以访问他们喜欢的现代应用自助服务组件。

以下是 vSphere 管理员对其环境中运行的 Tanzu Kubernetes Grid 实例的可见性示例。

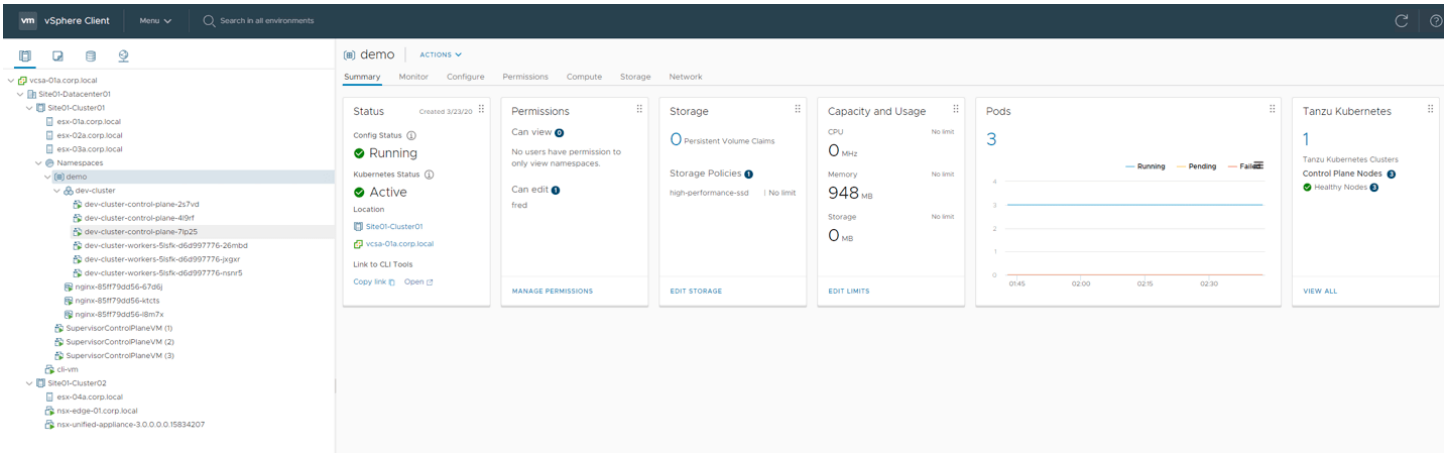

图 3 - vSphere Client，显示了 TKG 集群

vSphere with Kubernetes 附带了什么

部署 Kubernetes 的方式有很多。选项包括代管、云端、虚拟本地部署和裸机本地部署。已开发了一些工具（比如开源的 Minikube），可以在单台主机上安装和操作 Kubernetes 集群，这有利于开展培训。但对于企业而言，大多数部署都需要大量设置工作、新的流程以及重新培训员工，才能有效地安装和操作 Kubernetes。这正是 vSphere with Kubernetes 和 VMware Cloud Foundation Services 的优势所在，它们易于安装和操作，可以自然地融入您现有的 IT 基础架构和流程。

在 vSphere 内，有两种原生运行的 Kubernetes 集群：一种是称为 vSphere Pod Service 的“主管”Kubernetes 集群控制平面，另一种是 Tanzu Kubernetes 集群，有时也称为“客户机集群”。

vSphere Pod 服务

vSphere Pod Service 是一种特殊的 Kubernetes 集群，它使用 ESXi（而不是 Linux）作为其 Worker 节点。通过将 Worker 代理 Spherelet 直接集成到 ESXi Hypervisor 中来实现此目的。Spherelet 不在虚拟机中运行，它通过 vSphere Pod 直接在 ESXi 上运行。vSphere Pod Service 是由 ESXi 节点（而非 Linux 节点）组成的 Kubernetes 集群。vSphere Pod Service 使用 vSphere Pod 来运行容器工作负载。vSphere Pod 深入利用了 ESXi Hypervisor 的卓越安全性、可用性和性能。

Tanzu Kubernetes 集群

虽然 vSphere Pod Service 使用 Kubernetes，但它并不是一个符合标准的 Kubernetes 集群。这是设计上有意而为之，因为它打算使用 Kubernetes 来改进 vSphere，而不是试图将 vSphere 变成一个 Kubernetes 克隆体。为了向您的开发人员提供基于标准且完全符合上游 Kubernetes 的 Kubernetes 集群，您可以使用 Tanzu Kubernetes 集群，也称为“客户机”集群。

Tanzu Kubernetes 集群是一个 Kubernetes 集群，它运行在虚拟机内部的“主管”层上，而不是 vSphere Pod 上。由于 Tanzu Kubernetes 集群是完全符合上游标准的 Kubernetes，因此可以确保与您的所有 Kubernetes 应用和工具兼容。vSphere 中的 Tanzu Kubernetes 集群使用开源 Cluster API 项目进行生命周期管理，而该项目又使用 VM Operator 来管理组成集群的虚拟机。

vSphere with Kubernetes 和 Cloud Foundation Services

组成 vSphere with Kubernetes（并使它与其他 Kubernetes 实施有所区别）的主要组件是使用的服务。为 vSphere with Kubernetes 启用集群时，我们会部署以下服务。

- vSphere Pod 服务

  vSphere Pod Service 让开发人员能够以原生方式在 vSphere 上安全地运行容器，无需管理虚拟机或 Kubernetes 集群。

- 镜像仓库服务

  镜像仓库服务使开发人员可以使用 Harbor 存储、管理和保护 Docker 及 OCI 镜像。Harbor 是一种开源容器镜像仓库，可通过角色访问控制来保证镜像安全。

- 存储服务

  Storage Service 让我们可以将 vCenter Server 存储策略和设备用作 Kubernetes 存储类别，还可以用作永久磁盘，与容器、Kubernetes 和虚拟机配合使用。

- 网络服务

  Network Service 让开发人员能够定义配合应用使用的虚拟路由器、负载均衡器和防火墙规则。

- 虚拟机服务

  未来，Virtual Machine Service 将允许您使用 Kubernetes 部署和管理传统虚拟机。

- Tanzu Kubernetes Grid Service for vSphere

  Tanzu Kubernetes Grid Service 是 Tanzu Runtime Services 的一部分，允许开发人员管理一致且合规的 Kubernetes 集群。它们是 Tanzu Kubernetes 集群。

VMware NSX

NSX 作为默认的 Pod 网络连接和网络安全解决方案，经过重新设计并集成到了 vSphere with Kubernetes 中。NSX 提供了一套丰富的网络功能，包括分布式交换和路由、防火墙、负载均衡等。与 Kubernetes 的集成实现了可感知上下文的安全策略（遵循 Kubernetes 的 Namespace），从而提供易于使用的隔离和安全功能。

与 Kubernetes Cluster API 的原生集成允许应用开发人员指定负载均衡器和访问策略，使应用能够在 Kubernetes 集群之外轻松发布和获得支持。此外，vRealize Network Insight 等 NSX 感知工具有助于运用深入的性能监控、安全分析和故障排除功能来管理 vSphere with Kubernetes 内运行的现代应用，就像对待传统工作负载一样。

Tanzu Kubernetes 集群或 vSphere Pod Service：我该选择哪个

Tanzu Kubernetes 集群：

- 完全符合上游 Kubernetes 标准的 Kubernetes 集群
- 独立于 vSphere 的灵活集群生命周期管理，包括升级
- 能够添加或自定义开源和生态系统工具，比如 Helm Charts

vSphere Pod Service：

- 拥有 vSphere 环境中固有的其他功能，并可通过 kubectl 命令向 Kubernetes 提供这些功能
- 提供管理虚拟机的能力，就像管理容器一样
- 由于使用了 vSphere Pod，提供更强大的安全性和资源隔离
- vSphere Pod 的性能优势

最佳入门方式：VMware Cloud Foundation

通过 VMware Cloud Foundation 开始体验 vSphere with Kubernetes。Cloud Foundation 采用了深入的数据中心自动化，因此可以快速部署和使用新的应用和服务。它是一种完整套件策略，适用于软件定义的数据中心 (SDDC) 中所有组件的管理 - 从部署，到后续运维，比如修补、升级和重新配置。

Cloud Foundation 为实施、运维和维持现代混合云（其中包括 vSphere with Kubernetes）提供了标准化和可重复的体系架构与方法。vSphere 管理员可以使用 VMware SDDC Manager 的高级自动化功能，以全自动的方式将 vSphere 部署到私有云中。自动化功能包括 VMware vSAN 的部署和配置，以及 VMware NSX-T 架构的实施。

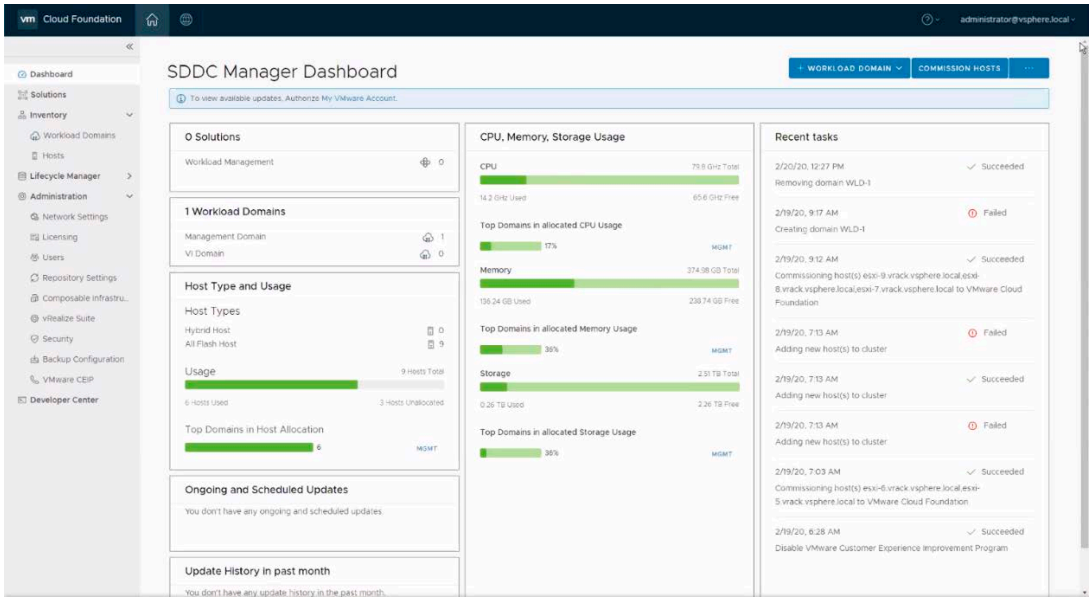

图 4 - VCF SDDC Manager 仪表盘

Cloud Foundation 是一个动态平台，允许基础架构以软件的形式弹性扩展、缩减和调整用途，以适应现代业务的需求。SDDC Manager 可感知 Kubernetes，还能够编排 Kubernetes vSphere Pod Service 的部署，从而准备好托管虚拟机和基于容器的工作负载。实施后，SDDC Manager 可轻松应用后续软件补丁和更新，从而精简后续运维，并轻松让环境保持更新和安全。

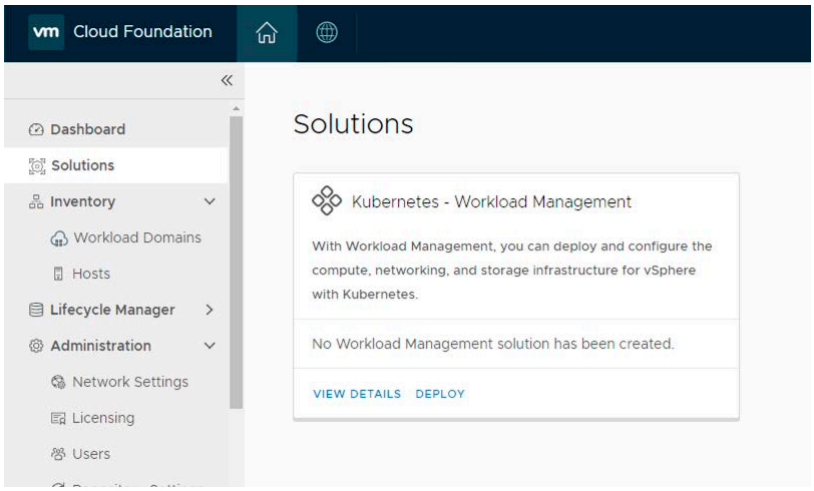

图 5 - VCF 解决方案

结论与要点

vSphere with Kubernetes 可以实现两全其美。VMware 管理员可以继续利用他们几十年来熟知的 vSphere 环境来处理传统工作负载，同时提供一个出色的环境来处理现代应用的容器化工作负载。

- 由于许多原因，开源 Kubernetes 的安装和运维可能具有挑战性。VMware vSphere with Kubernetes 和 VMware Cloud Foundation 以一种不同于业界其他产品的方式将 Kubernetes 提供给企业使用。这些产品所采用的方法认可并尊重企业对基础架构、人员、流程和现有工作负载做出的投资，与此同时还能让企业对未来做好充分准备。
- Kubernetes Namespace 将改变我们对虚拟基础架构内的应用管理的看法。它们允许开发人员在企业设置的运维和安全边界内自由行事和执行自助服务。Namespace 还为工作负载管理员、开发人员和 VMware 管理员赋予了更大的灵活性来定义和描述他们的工作负载，使得 Kubernetes 可以编排放置、可用性、安全性和其他运维细节。
- Namespace 允许 VMware 管理员根据自己的意愿或需求，与工作负载进行任意程度的交互。VMware 管理员可以利用他们现有的工具和知识来应对每个工作负载的具体情况。VMware 管理员和开发人员都能从庞大且不断增长的工具生态系统（从 VMware vRealize Suite 到 Tanzu Mission Control）中获益。
- VMware vSphere with Kubernetes 提供了不同类型的 Kubernetes 集群。vSphere Pod Service 通过 vSphere 实现紧密管理，它提供了更出色的安全性和性能，但与上游 Kubernetes 产品有所不同。Tanzu Kubernetes 集群完全符合上游 Kubernetes 版本标准，在生命周期运维方面，对于开发人员来说更加灵活。
- 企业通过 VMware Cloud Foundation 开始使用 vSphere with Kubernetes。Cloud Foundation SDDC Manager 可根据客户的需求，自动完成 VMware 产品堆栈的任意部署、基础架构变更和生命周期运维，并消除私有云运维的复杂性。

vmware

资源

要了解有关 VMware vSphere with Kubernetes、VMware Cloud Foundation 和开源 Kubernetes 的更多信息，请访问以下资源：

- 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
威睿信息技术（中国）有限公司
中国北京办公室 北京市朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真：852-3696 6101 www.vmware.com/cn

项目号：vmw-wp-tech-temp-word-102-proof 5/19