

利用 VMware Tanzu Mission Control 管理上千个集群

操作指南

目录

内容提要	3
第 1 步：将运行在任何环境中的现有 Kubernetes 集群挂接到 VMware Tanzu Mission Control	3
第 2 步：直接在 VMware Tanzu Mission Control 中置备多个基础架构提供商的集群	5
第 3 步：按集群组或工作空间组织集群和 Namespace	7
第 4 步：利用 VMware Tanzu Mission Control 监控集群的状态和运行状况	9
第 5 步：针对您的集群或工作空间应用策略，以管理用户访问权限、安全性和合规性	11
小结	12
词汇表	13

KUBERNETES 挑战

- Kubernetes 集群可以驻留在不同环境中 - 本地部署、公有云、裸机或边缘
- 不同团队的 Kubernetes 采用速度不同，也有各自独特的 Kubernetes 需求
- 跨不同环境将 Kubernetes 作为一项服务交付到不同团队极具挑战性
- 不同环境和团队的运维方式不一致会导致安全性和合规性风险。

内容提要

竞争格局已变，企业构建软件的方式对于企业的影响越来越大。挑战者银行、在线医疗提供方、电子商务领导者和其它初创企业正在通过提供新应用赢得客户。实际上，在未来五年中，企业将构建 5 亿个新应用，这相当于过去 40 年中所构建应用的数量¹。

要有效地展开竞争，企业必须营造一种环境，支持开发人员出色地完成工作。这就需要使用现代结构（容器、微服务、API），还要能够流畅地跨云工作。这导致运维团队需要适应这种惊人的多样性。正是这些同时发挥作用的因素推动了 Kubernetes 的采用，以实现跨云编排容器的使用。

VMware® Tanzu Mission Control 使企业能够管理所有 Kubernetes 集群，无论这些集群驻留在何处。开发人员可以根据需要访问所需的资源；运维人员可以跨集群和设备应用一致的策略和安全性。

下面让我们探索 VMware Tanzu Mission Control 如何满足这两个努力构建现代应用的关键群体的需求。

第 1 步：将运行在任何环境中的现有 Kubernetes 集群挂接到 VMware Tanzu Mission Control

Kubernetes 正处在发展初期，这一技术出现才五年多的时间。而 65% 的企业已运行了两个或多个 Kubernetes 发行版²。一家典型企业的开发团队处理的容器可能会涵盖 Kubernetes 发行版软件包、代管 Kubernetes 服务和/或 DIY Kubernetes 服务。

如何管理驻留在不同环境中的所有这些集群呢？VMware Tanzu Mission Control 支持您挂接任何环境中的标准 Kubernetes 集群，提供监管和管理所有 Kubernetes 服务的集中位置，无论是在本地部署的虚拟机或裸机中，公有云中，还是通过 Kubernetes 服务提供商（例如 Amazon Elastic Kubernetes Service [EKS]、Azure Kubernetes Service [AKS] 或 Google Kubernetes Engine [GKE]）提供，或位于边缘环境，均可获得更好的可见性和控制力。

挂接集群的过程涉及三个简单的步骤：

1. 注册集群
2. 安装代理
3. 验证连接

¹ 2018 年 10 月 - IDC FutureScape - 文档编号 US44403818。IDC FutureScape: Worldwide IT Industry 2019 Predictions

² Portworx and Aqua Security: Container Adoption Study, 2019。

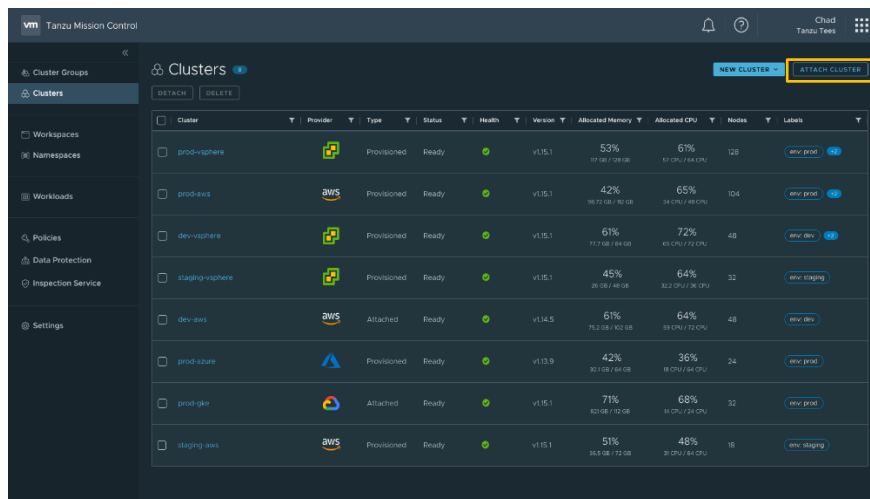
什么是 VMWARE TANZU MISSION CONTROL?

VMware Tanzu Mission Control 是一个集中管理平台，可跨多个团队和多云环境对 Kubernetes 基础架构和现代应用进行一致的运维管理和安全保护。

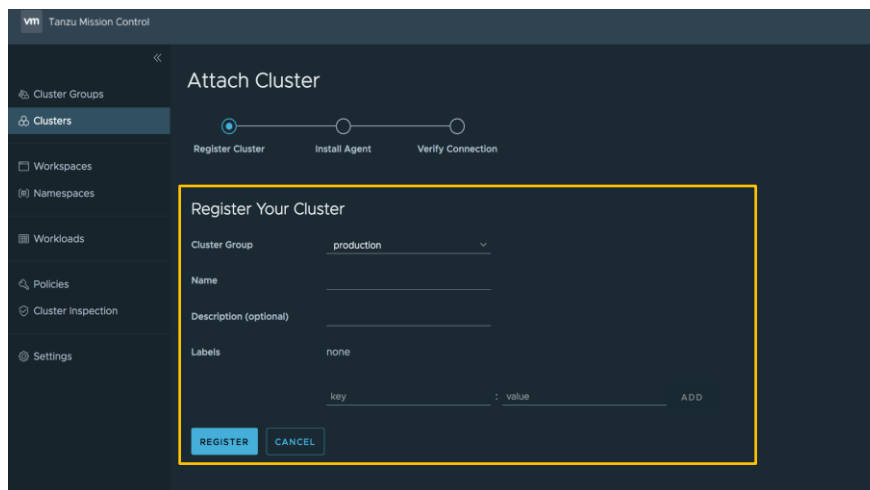
它为运维人员提供了单一控制点，使开发人员能够根据需要独立地推进业务向前发展，同时确保跨不同环境实现一致的管理和运维，以提升安全性和监管效果。

以下是 VMware Tanzu Mission Control 中的操作方法。

1. 登录您的 VMware Tanzu Mission Control 仪表盘，查看在所有环境中运行的所有 Kubernetes 集群。单击 VMware Tanzu Mission Control 中的“Attach Cluster”（挂接集群）按钮，开始挂接现有集群。



2. 要注册集群，请选择一个集群组，提供独特的集群名称和描述，并根据需要输入标签。



3. 单击“Register”（注册）后，VMware Tanzu Mission Control 会专门为此集群生成一个 YAML 脚本，并显示运行该脚本的 kubectl 命令。请在 kubectl 命令窗口中运行命令。YAML 脚本会在您的集群中运行一小组扩展，以便与 Cluster Agent 服务连接。

VMWARE TANZU MISSION CONTROL 可提供哪些帮助？

支持开发人员的独立、创新，同时不失控制。

通过 API 驱动的工作流、集中身份验证和特定于应用的策略实施，VMware Tanzu Mission Control 使开发人员能够自助访问测试和运行容器化应用所需的适当环境。

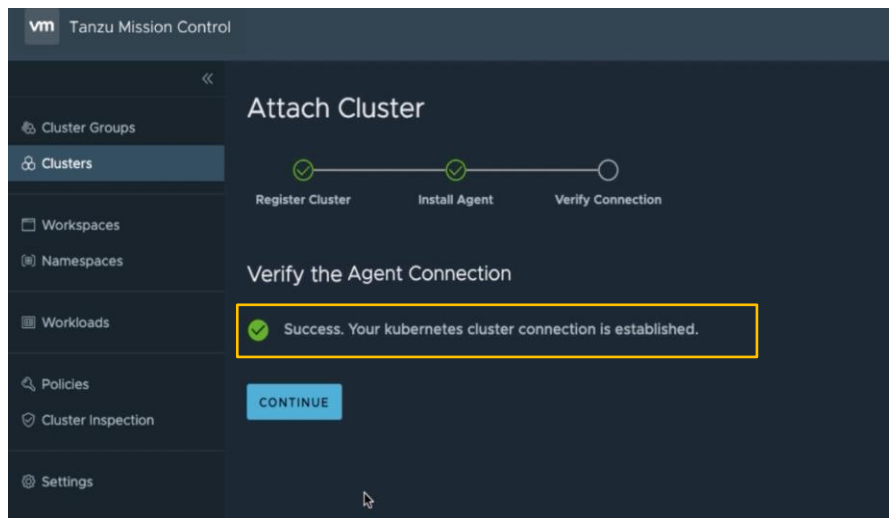
管理和运维任何位置的 Kubernetes，同时保持一致。

支持团队跨任何基础架构（vSphere、公有云、裸机）运行应用，同时保持针对集群和应用的可见性和可观察性。

保护和强化分布式系统，满怀信心。

跨不同云和集群（即使是在边缘运行的数以千计的集群）执行访问、备份、安全和合规性策略。

4. 这些扩展在您的集群中开始运行后，请返回 VMware Tanzu Mission Control 控制台，单击“Verify Connection”（验证连接）。现在您的集群已挂接成功！现在您可开始利用 VMware Tanzu Mission Control 管理集群和用户。



第 2 步：直接在 VMware Tanzu Mission Control 中置备多个基础架构提供商的集群

VMware Tanzu Mission Control 还支持用户直接通过其 UI 置备多个基础架构提供商的新集群³。它提供一组通用 API、UI 以及 CLI，用户可利用这些一致的功能特性置备 Kubernetes 集群，并处理这些集群后续的生命周期管理任务，例如升级、扩展和删除。

其背后的技术是称为 [Cluster API](#) 的开源技术，这是开源 Kubernetes 项目下的一个子项目。利用 Cluster API，社区可以构建专门的工具集，将声明性的 Kubernetes 式 API 引入到集群创建、配置和管理中。这是一款独立于云的工具，可显著改善用户体验，还能在集群生命周期管理方面实现更加复杂的自动化。现在，市场上的一些主要 Kubernetes 提供商已开始采用 Cluster API，它提升了 VMware Tanzu Mission Control 针对不同环境中的集群的生命周期管理功能。

现在，利用 VMware Tanzu Mission Control，企业可以在一些环境中将 Kubernetes 作为一项服务提供给开发人员。开发人员只需简单地单击几次，即可从 Tanzu Mission Control 中在需要的时间和位置置备集群。

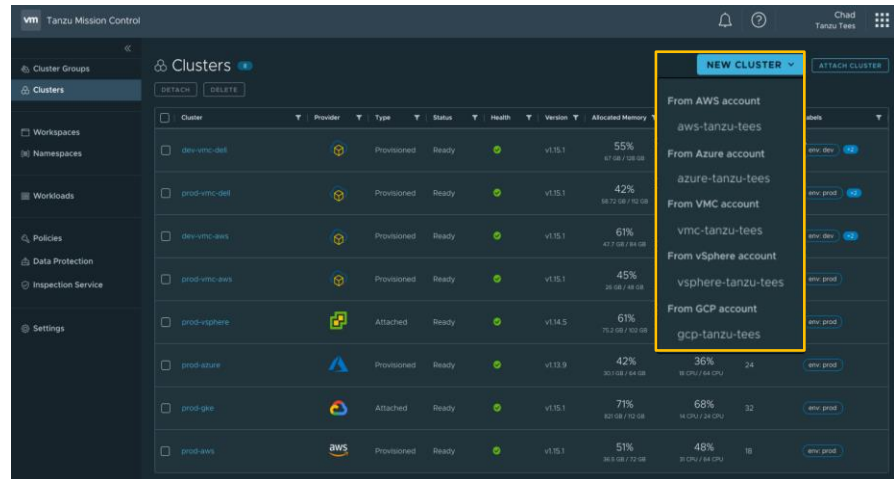
以下是如何在 VMware Tanzu Mission Control 中从 AWS 帐户环境置备新集群。

³ Tanzu Mission Control 目前支持在 AWS EC2 上置备、扩展、升级和删除集群，后续还会支持其他环境。

VMWARE TANZU MISSION CONTROL 的核心功能

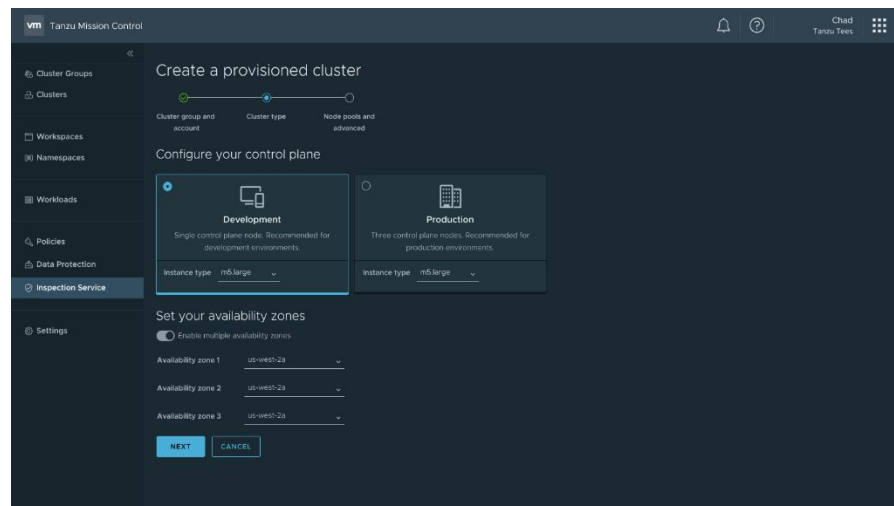
- 集群生命周期管理
- 身份认证和访问管理
- 安全性和配置管理
- 可观察性和诊断
- 审核与合规性
- 连接和流量管理

1. 要置备新集群，应首先单击 VMware Tanzu Mission Control 中的“New Clusters”（新建集群）按钮，从下拉菜单中选择 AWS 作为目标



2. 为集群命名，添加描述，输入指标，例如集群组、AWS 帐户、区域、Kubernetes 版本和 VCP CIDR，然后可以转到下一步，选择要置备的集群类型。

集群有两种类型 - 开发集群或生产集群。开发集群有一个控制平面节点，建议用于开发环境。生产集群有三个控制平面节点，建议用于生产环境。此外，如果您选择置备生产集群，要能够为您的集群启用多个可用区。



适用于多个团队的 VMWARE TANZU MISSION CONTROL

适用于基础架构团队

- 交付 Kubernetes 即服务
- 搭建现代基础架构平台
- 迁移到云环境

适用于开发团队

- 在 Kubernetes 上构建应用
- 支持开发人员自助服务和 DevOps 工作流

适用于运维团队

- 管理、运维和保护应用环境
- 管理开发人员对 Kubernetes 的访问

3. 为您的集群添加标签，定义节点池，然后单击“Create”（创建）按钮创建集群。节点池是集群中的一组节点，它们具有相同的配置。

单击“Create”（创建）后，将带您回到“Clusters”（集群）页面，您可以在这里搜索或排序，找到刚刚创建的集群。VMware Tanzu Mission Control 会在您的云服务提供商帐户中为您的集群置备必要的资源。然后它将创建集群，并挂接到企业中您指定的集群组中。

第 3 步：按集群组或工作空间组织集群和 Namespace

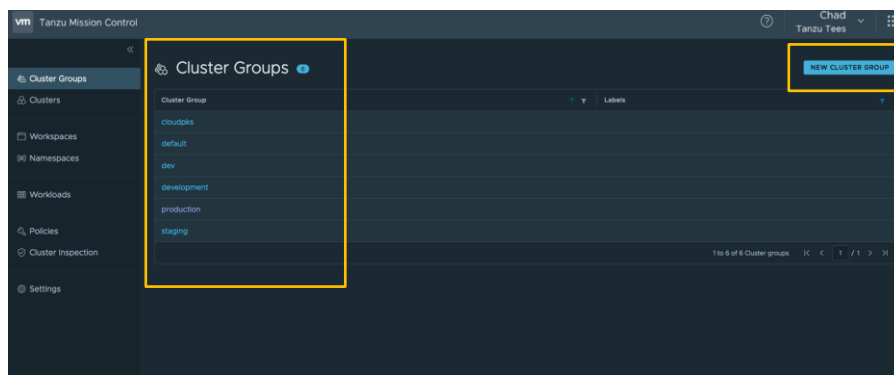
VMware Tanzu Mission Control 可对数以千计的集群保持可见性和控制力，但所有集群的清单对运维人员来说毫无用处，这些集群必须井井有条地组织起来。出于这一目的，VMware Tanzu Mission Control 引入了两个重要概念，以满足运维人员和开发人员的需求。

集群组：平台运维人员可以创建逻辑集群组，作为集群队进行管理，例如，运维人员可以为一队相似的集群应用一组通用策略，而不必为许多集群分别应用策略。集群组中可以包括存在于一个或多个环境中的集群，也可以包括多个团队共享的集群。平台运维人员可以创建、查看和删除集群组，或根据需要在组之间移动集群。

工作空间：Kubernetes Namespace 是在多个用户之间分隔集群资源的一种方式，大多数开发团队按 Namespace 组织应用服务。但开发人员经常需要跨不同集群处理某些项目，这就产生了跨一个或多个集群访问多个 Namespace 的需要。Tanzu Mission Control 利用工作空间来满足这一需求。开发人员可以使用工作空间将一个或多个集群中的 Namespace 分组，不同团队之间也可以共享工作空间。

接下来的几个步骤向您展示如何使用集群组和工作空间概念来组织您的集群和 Namespace。

1. 您可以将集群分为不同的集群组，例如“开发集群组”或“生产集群组”，还能单击“New Cluster Group”（新建集群组）按钮创建新的集群组。



2. 在挂接现有集群或置备新集群时，您能够指定将该集群与哪个集群组相关联。

The screenshot shows the 'Create a Provisioned Cluster' wizard in the VMware Tanzu Mission Control interface. The left sidebar contains navigation links: Cluster Groups, Clusters, Workspaces, Namespaces, Workloads, Policies, Cluster Inspection, and Settings. The main panel is titled 'Create a Provisioned Cluster' and has three steps: 'Cluster Group and Account', 'Cluster Type', and 'Node Pools and Advanced'. The first step is active. It includes a 'Name your Cluster' section with 'Cluster Name' and 'Description (optional)' fields. Below that is the 'Assign a Cluster Group and account' section, which contains several dropdown menus: 'Cluster Group' (set to 'default'), 'AWS Account' (set to 'Olympus-AWS'), 'Region' (set to 'us-west-2'), 'Kubernetes Version' (set to '1.14.1'), and 'VPC CIDR (IPv4)' (set to '10.0.0.0/16'). At the bottom of this section are 'CANCEL' and 'NEXT' buttons. A 'DOWNLOAD CLI' button is also visible in the sidebar.

3. 工作空间也是同样，您能够将 Namespace 分组为工作空间，也可以根据需要创建新的工作空间。当您创建新的 Namespace 时，可以指定希望将哪个工作空间与这个 Namespace 相关联。

The screenshot shows the 'New Namespace' form in the VMware Tanzu Mission Control interface. The left sidebar is the same as in the previous screenshot. The main panel is titled 'New Namespace' and has a 'Select the Location' section with two dropdown menus: 'Cluster' (set to 'gke-prod-cluster') and 'Workspace' (set to 'production'). Below this is the 'Name and Create' section, which includes 'Name', 'Description' (Optional description), and 'Labels' (set to 'none'). At the bottom are 'CREATE' and 'CANCEL' buttons.

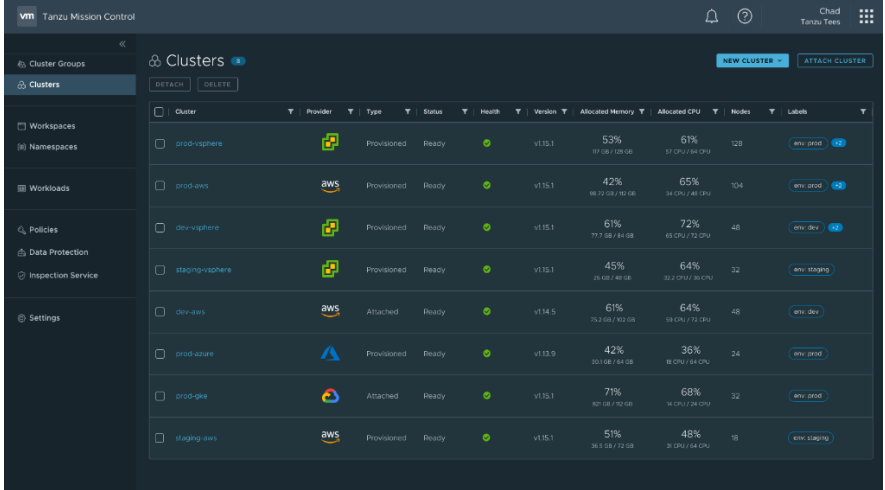
第 4 步：利用 VMware Tanzu Mission Control 监控集群的状态和运行状况

将所有集群集中到同一控制点后，可以使用 VMware Tanzu Mission Control 监管 Kubernetes 资源。您还可以了解不同环境中的 Kubernetes 集群的运行状况。VMware Tanzu Mission Control 提供整体的监控和可观察性。利用 VMware Tanzu Mission Control，您能够查看：

- 整个占用空间内现有集群的完整列表
- 集群元数据和整体资源分配和可用性信息
- 指定集群内节点、Namespace 和工作负载的列表，及其基本指标
- 所有集群中所有 Namespace 和工作负载的列表
- 所有集群组件和节点的运行状况。运行状况直观地显示在仪表盘中，可轻松进行监控。
- 集群的标准状态可确保您的集群符合最佳实践。您可以运行检查并查看报告，检查是否一切正常。

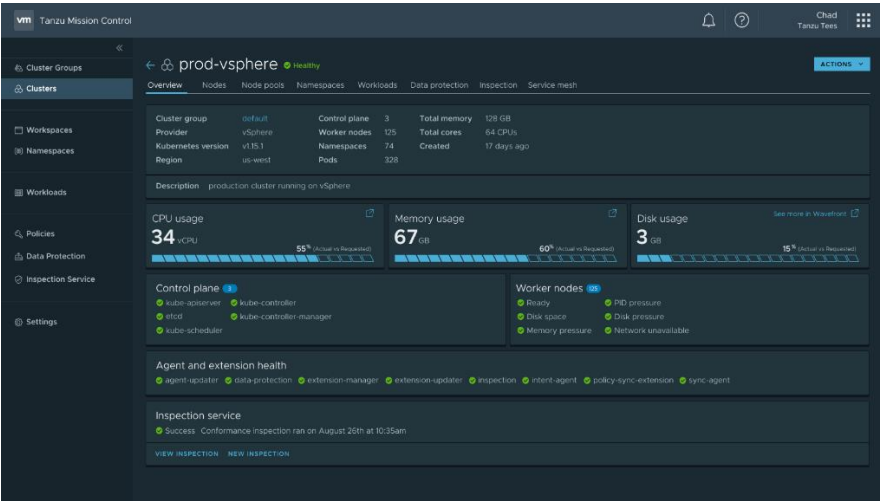
一致性测试使用 Sonobuoy 这一功能强大的开源工具运行检查。Sonobuoy 是一种诊断工具，能够以易于理解的非破坏性方式运行一组 Kubernetes 一致性测试，从而更加轻松地了解 Kubernetes 集群的状态。Sonobuoy 是 Cloud Native Computing Foundation 进行 Kubernetes 一致性测试所用的工具。

1. 查看所有环境中所有集群的完整列表。

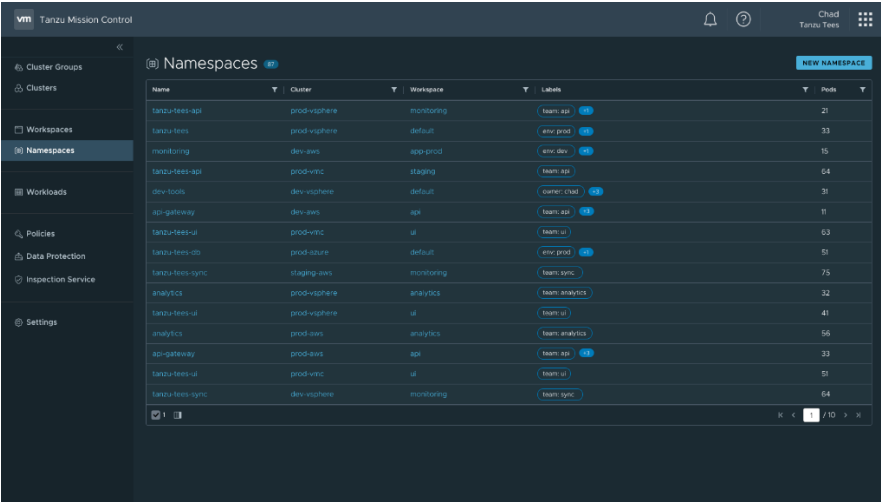


Cluster	Provider	Type	Status	Health	Version	Allocated Memory	Allocated CPU	Nodes	Labels
prod-vsphere	vsphere	Provisioned	Ready	OK	v1.15.1	53% 97 GB / 128 GB	61% 57 CPU / 64 CPU	123	env: prod
prod-aws	aws	Provisioned	Ready	OK	v1.15.1	42% 88 GB / 160 GB	65% 34 CPU / 40 CPU	104	env: prod
dev-vsphere	vsphere	Provisioned	Ready	OK	v1.15.1	67% 117 GB / 84 GB	72% 65 CPU / 72 CPU	48	env: dev
staging-vsphere	vsphere	Provisioned	Ready	OK	v1.15.1	45% 25 GB / 48 GB	64% 32 CPU / 36 CPU	32	env: staging
dev-aws	aws	Attached	Ready	OK	v1.14.5	61% 75.2 GB / 160 GB	64% 38 CPU / 72 CPU	48	env: dev
prod-azure	azure	Provisioned	Ready	OK	v1.13.9	42% 30 GB / 64 GB	36% 8 CPU / 64 CPU	24	env: prod
prod-gke	gke	Attached	Ready	OK	v1.15.1	71% 87 GB / 160 GB	68% 14 CPU / 24 CPU	32	env: prod
staging-aws	aws	Provisioned	Ready	OK	v1.15.1	51% 35.5 GB / 72 GB	48% 9 CPU / 64 CPU	18	env: staging

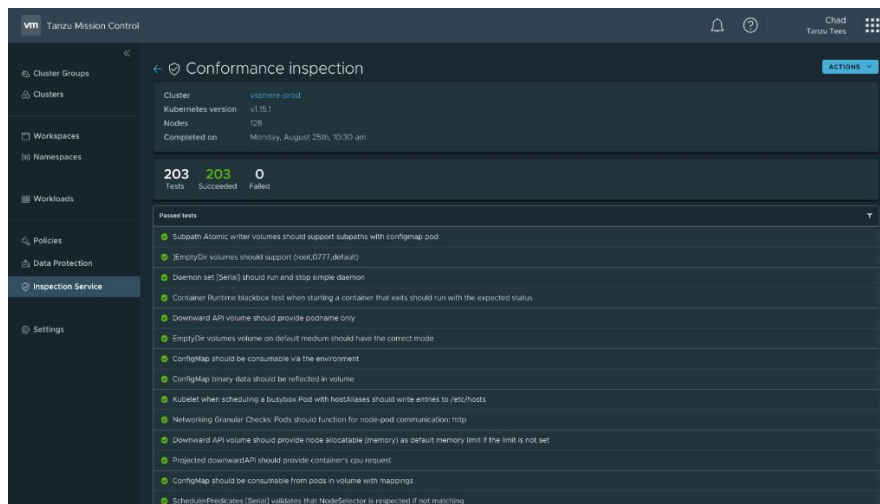
2. 集群概述可以直观展示集群的关键元数据，以及组件的运行状况，方便您轻松观察集群组件是否出现问题。



3. 查看所有集群中 Namespace 的列表



4. 运行集群检查可检查集群的标准状态，还能查看检查报告以发现问题。



第 5 步：针对您的集群或工作空间应用策略，以管理用户访问权限、安全性和合规性

在本指南的一开始，我们提到 Kubernetes 在应用和环境方面都带来了多样性。VMware Tanzu Mission Control 可利用一致的运维来支持这种多样性，这一点在处理策略的方式上表现得最为明显，这些策略包括访问策略、网络策略、安全策略等。

VMware Tanzu Mission Control 支持您对集群、应用和用户进行监管。它提供了功能强大的策略框架，使平台操作人员能够将策略应用于多种 Kubernetes 环境中的物理和逻辑资源，无论在本地还是公有云中都是如此。可以通过策略引擎应用的策略包括：

- **访问策略：**为了使人员结构和基础架构结构保持一致，VMware Tanzu Mission Control 确保了只有拥有权限的用户才能访问特定的平台功能和底层 Kubernetes 集群。通过策略引擎，运维人员可以为集群或集群组授予不同级别的访问权限，例如管理、创建、查看或编辑。
- **镜像仓库策略：**使用 VMware Tanzu Mission Control，可以限制提取镜像的镜像仓库，这样就可以更加安全地在集群中的 Namespace 部署。VMware Tanzu Mission Control 可以在企业级、工作空间级以及分别针对每个 Namespace 管理镜像仓库限制。
- **网络策略：**为了增强安全管理，也可以使用 VMware Tanzu Mission Control 管理网络限制 - 您可以创建网络策略，定义单元 (Pod) 彼此之间如何通信，以及如何与其他网络端点通信。

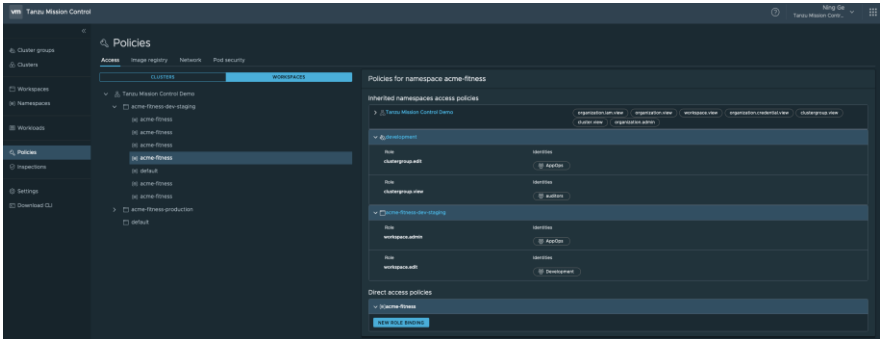
了解更多

要详细了解 VMware Tanzu Mission Control，请访问我们的网站：
cloud.vmware.com/tanzu-mission-control

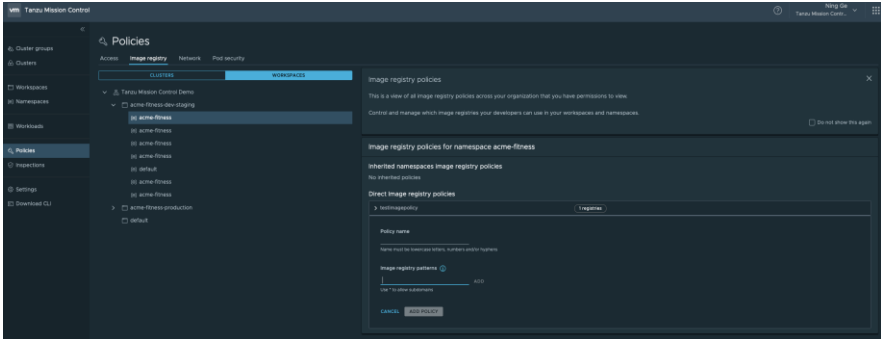
功能如此强大的引擎为运维人员提供了很大的灵活性，支持他们为不同团队管理不同类型的集群，同时可针对一组集群或 Namespace 大规模应用策略，确保效率。

以下是如何在 VMware Tanzu Mission Control 中应用策略的示例：

- 1. 应用访问策略，使某些用户可以拥有在某些工作空间中的特定访问权限。您可以为用户定义不同的角色，赋予适当的权限。用户也将自动继承所在工作空间的访问策略。



- 2. 为 Namespace 应用镜像仓库策略。镜像仓库策略可指定注册表域的白名单，在您管理的 Namespace 中只能提取这些域中的镜像进行部署。



小结

您可使用 VMware Tanzu Mission Control 从单一控制点管理所有 Kubernetes 集群，涵盖打包 Kubernetes 发行版、代管 Kubernetes 服务和 DIY 服务。

如果您是运维人员，可以全面了解所有 Kubernetes 资源的状态，随时了解每个集群的运行状况，掌握访问策略、容器镜像仓库策略、网络策略和安全策略等，对多样化的环境进行全面控制。

如果您是开发人员，可以自由地使用现代结构并自助访问 Kubernetes 资源。您不需要担心基础架构，只需专注于您的强项，即编写代码。

总之，VMware Tanzu Mission Control 可帮助您的企业在现代基础架构之上构建现代应用。我们随时准备帮助您在竞争中取胜。

词汇表

容器	容器是一个标准的软件单元，将代码和所有其他依赖项打包，使应用可以在不同计算环境中快速、可靠地运行。
Kubernetes	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。Kubernetes 这个名字源于希腊语，意为舵手或领航员。
VMware Tanzu Mission Control	VMware Tanzu Mission Control 为团队提供单一控制点，以便更加轻松地跨多种云和集群管理 Kubernetes 及运维容器化现代应用。
Namespace	Kubernetes 支持基于同一物理集群的多个虚拟集群。这些虚拟集群称为 Namespace。Namespace 专门用于多个用户分布在多个团队或项目的环境中。
Kubectl	Kubectl 是一种命令行界面，用于针对 Kubernetes 集群运行命令
工作空间	工作空间是 VMware Tanzu Mission Control 中的概念。工作空间可用于将一个或多个物理集群中的 Namespace 分组，不同团队之间也可以共享工作空间。
集群组	集群组是 VMware Tanzu Mission Control 中的概念。集群组中可以包括存在于一个或多个环境中的集群，也可以包括多个团队共享的集群。平台运维人员可以创建逻辑集群组，进行统一管理。
节点池	节点池是集群中的一组节点，它们具有相同的配置。
Cluster API 项目	Cluster API 项目是 Kubernetes 开源项目下的一个子项目。利用 Cluster API，社区可以构建专门的工具集，将声明性的 Kubernetes 式 API 引入到集群创建、配置和管理中。
集群连接代理	在 VMware Tanzu Mission Control 中，用户可以使用该代理连接其他云和环境中的现有 Kubernetes 集群，以实现集中的运维一致性。



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

北京朝阳区新源南路 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

版权所有 © 2019 VMware, Inc. 保留所有权利。此产品受美国和国际版权法及知识产权法保护。VMware 及其子公司的产品受 <http://www.vmware.com/cn/support/patents> 网站中列出的一项或多项专利保护。VMware 是 VMware, Inc. 及其子公司在美国和/或其他司法管辖区的注册商标或商标。此处提到的所有其他标志和名称分别是其所属公司的商标。项目号：vmw-wp-temp-word-104-proof

