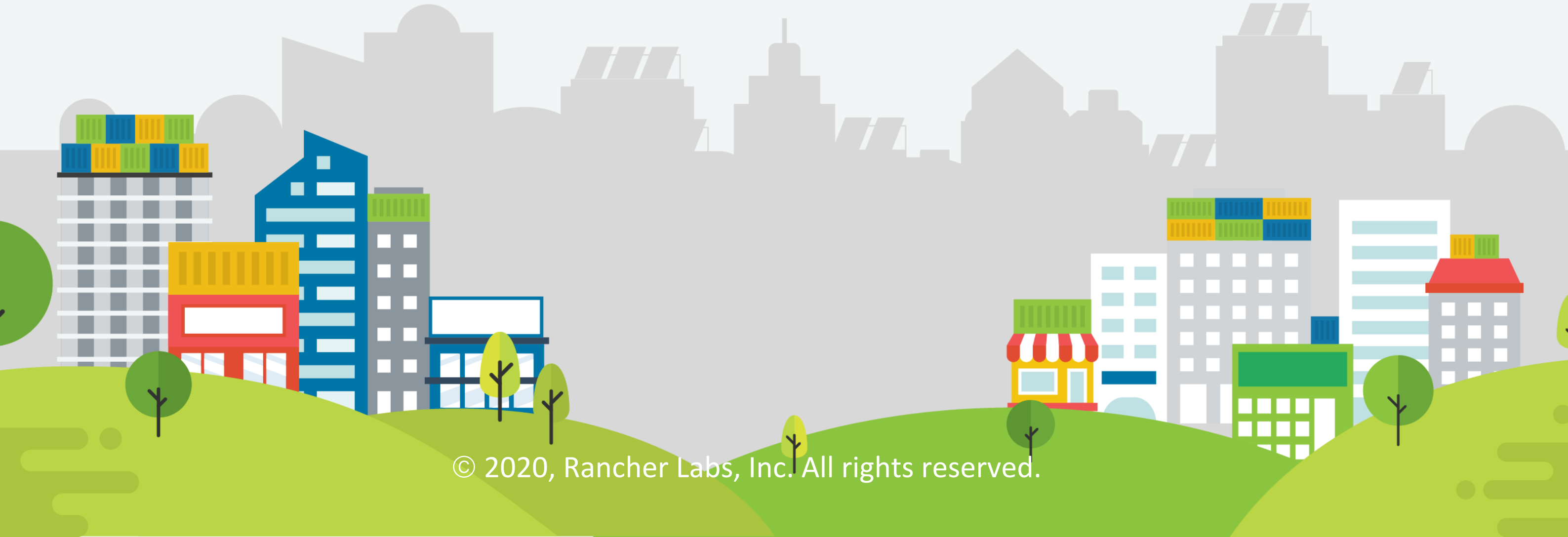
A Buyer's Guide to Enterprise Kubernetes Management Platforms

Red Hat OpenShift 4.5, VMware Tanzu 1.0, Google Anthos 1.4 and Rancher 2.5

Last Updated: September 2020



Contents

1 Executive Summary

According to 451 Research, 76 percent of enterprises will standardize on Kubernetes within the next three years because it promises a consistent set of capabilities across any infrastructure — from datacenter to cloud to the edge.[1]

By unifying their IT operations with Kubernetes, enterprises realize key benefits like increased reliability, improved security and greater efficiencies with standardized automation.

However, relying on upstream Kubernetes often isn't enough for teams deploying Kubernetes into production. Vanilla Kubernetes installations are plagued by a lack of central visibility, inconsistent security practices and complex management processes. Therefore, Kubernetes management platforms are adopted by enterprises to deliver:

- **Simplified Cluster Operations:** improved DevOps efficiencies with simplified cluster operations
- **Consistent Security Policy & User Management:** best-practice security policy enforcement and advanced user management on any infrastructure
- **Access to Shared Tools & Services:** a high level of reliability with easy, consistent access to shared tools and services

Given the transformative potential of Kubernetes, it is not surprising that the battle for Kubernetes management market leadership is heating up quickly.

Rancher Labs, which has focused on Kubernetes management since its founding in 2014, is experiencing rapid growth. Meanwhile, IT vendor stalwarts including IBM and VMware are staking their claims to this enormous market opportunity.

In July 2019, IBM completed their $34B acquisition of Red Hat, a company described in a recent GigaOm report[2] as 'semi-open source' and a 'legacy open source player'.

Google Anthos went GA in August 2019 as part of their strategy to grow enterprise adoption of Google Cloud services like GKE. As the inventors of Kubernetes, their initial GTM saw a high premium for an immature multi-cluster platform that excluded all but the largest opportunities. After a number of high-profile wins under their belt, as of September 2020, Google has introduced pay-as-you-go pricing options and a more competitively priced annual subscription offering.

More recently, VMware announced their acquisition of Pivotal for $2.7B. In March 2020, VMware released v1 of its VMware Tanzu product suite – this includes:

- vSphere Cloud Foundation Services (the Kubernetes add-on for vSphere – which we will refer to as VCFS in this document)

[1] "Kubernetes and Beyond – Effective Implementation of Cloud Native Software in the Enterprise" by Jay Lyman, Principal Analyst 451 Research – Download Whitepaper

[2] "Key Criteria for Leveraging Federated Kubernetes, Open & Closed" by David S. Linthicum, GigiaOm – Download Whitepaper

- Tanzu Kubernetes Grid (a Kubernetes distribution)
- Tanzu Mission Control (a SaaS-only central control plane for managing clusters in multiple clouds)
- Enterprise PKS still exists for on-prem use cases: given its legacy architecture and high cost, our expectation is that it will be sunsetted at some point in the future.

While there are other smaller players in the market, the scope of this guide is limited to comparing the capabilities of the four leading Kubernetes Management Platforms: Red Hat OpenShift Container Platform 4.3 (OpenShift/OCP4), VMware Tanzu Mission Control with Tanzu Kubernetes Grid (collectively referred to here as Tanzu), Google Anthos with Anthos GKE (known collectively Anthos here) and Rancher 2.5 (Rancher).

2 Capabilities Summary

2.1 Overview

In this analysis, we have used “Harvey balls” to illustrate how each vendor compares to the others by category:

- The full ball (●) is applied to the platform that is best-of-breed in that category.
- The three-quarters ball (◕) is applied to the runner-up in that category.
- The half ball (◑) illustrates acceptable capability in that category.
- The quarter ball (◔) shows weak capability in that category.
- The empty ball (○) indicates the platform has no capability in that category.

2.2 Cluster Operations

By simplifying and automating cluster operations, Kubernetes Management Platforms seek to improve DevOps efficiencies.

Feature	Rancher	OpenShift	Tanzu	Anthos
Ease of install, Config & Maintenance	●	◑	◑	◑
Intuitive UI	●	●	●	●
Multi-cloud	●	◕	◕	◑
Multi-cluster	●	◕	◕	◕
Edge Support	●	◑	◔	◑
Hosted Kubernetes Support	●	◔	◕	◕
Bare Metal, OpenStack & vSphere	●	◕	◑	◔
Import Existing Clusters	●	◕	●	◕
High Availability	●	●	◕	◑
Load Balancing	●	◕	◑	◕
Centralized Audit	◕	◕	◑	◑
Self-service Provisioning	●	◔	●	◔
Private Registry & Image Management	◕	●	◑	◑

Cluster Upgrades & Version Management	●	●	◑	◕
Storage Support	●	◕	◔	◕
Arm Support	●	○	○	○
Airgap Support	●	●	◔	○
Etcd Backup and Restore	●	◑	◑	◑

2.3 Security Policy and User Management

A key benefit of deploying a Kubernetes Management Platform is its ability to implement best practice security policy enforcement and advanced user management on any infrastructure.

Feature	Rancher	OpenShift	Tanzu	Anthos
Active Directory and LDAP Support	●	●	●	◕
Pod and Network Security Policies	●	◕	◕	◕
CIS Benchmark Adherence & Tracking	●	◑	◑	◕
Global RBAC Policies	●	◑	●	◑

2.4 Shared Tools and Services

Once deployed, Kubernetes Management Platforms encourage user adoption with easy, reliable and consistent access to shared tools and services.

Feature	Rancher	OpenShift	Tanzu	Anthos
Application Catalog	◕	●	◕	◑
Provision with Config Management Systems	●	◑	◔	●
Integration with CI/CD Solutions	●	●	◕	●
Advanced Monitoring	●	●	◔	◕
Alerts and Notifications	●	◑	◔	◑
External Log Shipping	◕	◕	○	◑
Windows Container Support	◕	○	○	◕
Integrated Service Mesh Support	●	◕	◔	◕
Enterprise SLA	●	◑	◑	◑
Community Traction	●	◕	○	◔

Please note that a glossary of terms used in this document is provided in section 4.

3 Feature Analysis

3.1 Cluster Operations

3.1.1 Ease of Installation, Configuration and Maintenance

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◑
- Anthos: ◑

3.1.1.1 Rancher

Rancher offers certified Kubernetes distributions for datacenter, cloud, and edge. Each distribution requires the bare minimum of host configuration, usually no more than a supported version of Docker. For installations that want an even smaller attack surface, Rancher offers two container operating systems expressly designed to run Kubernetes in the most efficient way possible.

Kubernetes from Rancher uses a configuration syntax designed for clarity and dynamic cluster reconfiguration with no downtime.

3.1.1.2 OpenShift

OpenShift (OCP4) ships a large installation binary that includes Terraform and a set of scripts to deploy OCP4 into a provider. Currently the only supported providers are AWS, Azure, and vSphere. Only the AWS installer was evaluated for this guide. The installer requires unrestricted access to AWS in order to create and manage resources that it will consume. Execution of the installation binary is easy because there are no options available for cluster configuration at launch time. All configuration happens from within OCP4 after the cluster is online. However, the footprint of what OCP4 creates in AWS is large and makes troubleshooting difficult. It’s unclear if changes to the AWS environment will be overwritten during cluster upgrades from within OCP4. If the user wants to deviate from the defaults provided by OCP4, then they may encounter difficulty doing so.

3.1.1.3 Tanzu

Access to Tanzu is, at the writing of this document, extremely limited so we must make some assumptions. Like its forerunner Pivotal Container Service (PKS), we should assume that its prerequisites like VMware’s paid for Wavefront tool for monitoring. If using optional features, it may also require a multi-node installation of the NSX-T control plane and Harbor. VCFS is only available as an add-on to the vSphere Cloud Foundation suite. Based on our experience with Enterprise PKS, installation and configuration of this offering will take anywhere from eight to 16 hours.

Deployment of the actual PKS cluster can take up to 30 minutes to deploy a basic cluster. Changes to the PKS configuration also take 30 minutes to apply and require a relaunch of downstream clusters. At this stage we’re assuming something similar for VMware Tanzu.

3.1.1.4 Anthos

If you’re already operating in GKE, installing Anthos is easy, and other cloud providers are only incrementally more challenging. The hurdles come with an on-prem deployment, which brings in a dependency on VMware infrastructure, as well as a permanent migration from current workloads to GKE-VMs-as-Pods, at which point they go into an infrastructure managed entirely by Anthos and Google managed services staff.

3.1.2 Intuitive UI

- Rancher: ●
- OpenShift: ●
- Tanzu: ●
- Anthos: ●

3.1.2.1 Rancher

Rancher's intent-driven user interface enables users to quickly deploy and begin management of Kubernetes clusters with almost no learning curve. It softens and streamlines complex Kubernetes concepts and workflows, making it possible to leverage Kubernetes in an organization without needing extensive training up front.

3.1.2.2 OpenShift

OpenShift's user interface is crisp and fast. Common workflows exist at the top of menus, and access to both standard Kubernetes workflows and those that are unique to OpenShift are readily available.

3.1.2.3 Tanzu

VMware appears to have spent a good deal of time improving the UI and UX of predecessor products like PKS. The result looks clean and modern. At this time, the Enterprise PKS Management Console UI and the Tanzu Mission Control UI are two different offerings with different feature sets and use cases.

3.1.2.4 Anthos

As one would expect from Google, Anthos and Anthos GKE come with a clean and crisp user experience derived from Google's years of building excellent cloud applications.

3.1.3 Multi-cloud

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◕
- Anthos: ◑

3.1.3.1 Rancher

Rancher presents the most options for where to deploy Kubernetes. It can provision hosted solutions from all major providers. It can provision compute resources in any provider for which drivers exist for Docker Machine and then install Kubernetes into that environment. It can import existing Kubernetes clusters running on any provider. It also presents a Custom option for installing Kubernetes on any system provisioned via any other means, such as Ansible, Terraform, Puppet, Chef, etc.

3.1.3.2 OpenShift

OpenShift supports cloud deployments to AWS, GCP and Azure. OpenShift also supports multi-cloud deployments, albeit only supporting on-premise or hosted versions of

OpenShift’s Kubernetes distribution. OpenShift’s lack of Kubernetes and OS distribution agnosticism continues to pose a lock-in threat to its customers.

3.1.3.3 Tanzu

Tanzu is a multi-cluster and multi-cloud solution that delivers a consistent operation experience. However, Tanzu requires VMware Cloud Foundation Services to launch local clusters and requires Tanzu Mission Control to launch cloud clusters. This combination increases the risk of lock-in. Unlike Rancher, Tanzu does not treat hosted Kubernetes providers like EKS, AKS and GKE as first-class citizens.

3.1.3.4 Anthos

The Anthos multi-cloud story is somewhat disingenuous. Their objective is to move you from where you are now into GKE, so while there is support for using instances from other providers as worker nodes, the product is designed to incentivize you to migrate to GKE for better performance and lower cost. All support services within Anthos are GCP-native services and will benefit from closer colocation of node resources.

3.1.4 Multi-cluster

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◕
- Anthos: ◕

3.1.4.1 Rancher

Rancher makes Kubernetes functionality available via a rich UI and API. This, in turn, makes it possible for users to interact with Kubernetes without needing to know where it is or how it is configured. Rancher abstracts cloud-specific resources such as Identity and Access Management and reduces lock-in by enabling operators to apply standard security policies across clusters running in different clouds. Rancher Longhorn abstracts storage and enables cross-cloud application portability by presenting a standard interface to the underlying Kubernetes primitives.

3.1.4.2 OpenShift

As of August 2020, OpenShift claims to go beyond deploying and managing just individual OpenShift clusters and now supports multiple OpenShift clusters located in multiple clouds.

3.1.4.3 Tanzu

Tanzu supports multiple clusters through Tanzu Mission Control, although many popular solutions (such as EKS, AKS and GKE) are only available if you attach existing clusters to it.

3.1.4.4 Anthos

Anthos can manage multiple clusters, infrastructure and workloads across cloud and on-premise environments.

3.1.5 Edge Support

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◔
- Anthos: ◑

3.1.5.1 Rancher

K3s is a lightweight Kubernetes distribution originally designed by Rancher to run in remote, resource-constrained environments. In August 2020, K3s was accepted as a CNCF Sandbox project to further promote establishing it as by far the most widely deployed Kubernetes distribution of its type. Rancher 2.5’s Fleet-powered continuous delivery and advanced observability capabilities allow for maximum cluster consistency and operational insight from core to cloud to edge. This latest update enables Rancher to support up to one million clusters from a single console with built-in security capabilities, running any CNCF-certified Kubernetes distribution.

3.1.5.2 OpenShift

RedHat’s approach to running Kubernetes at the edge is consistent with its technical limitations and commercial constraints. Multi-cluster support from a single console is a new concept for RedHat and OpenShift continues to tie its users into its own, certified Kubernetes distribution. The company’s idea of Kubernetes at the edge consists of deploying edge data centers running OpenShift, which in turn manage ‘dumb’ endpoints. The advantages of running Kubernetes clusters on the endpoints themselves is not something that they can leverage.

3.1.5.3 Tanzu

Tanzu has an opaque edge story that doesn’t appear to extend much beyond web pages and slideware.

3.1.5.4 Anthos

Like Tanzu, Anthos’s edge story is weak. If you’re planning to deploy Anthos infrastructure to an edge-located data center, then you can be fairly confident that it will perform equally well. Anthos documentation for edge deployments appears dependent on 5G infrastructure that is not widely available, or else it relies on a limited definition of “edge” that does not include resource-constrained environments with potentially intermittent connectivity.

3.1.6 Hosted Kubernetes Support

- Rancher: ●
- OpenShift: ◔
- Tanzu: ◕
- Anthos: ◕

3.1.6.1 Rancher

Rancher supports deployment into managed Kubernetes solutions from Amazon (EKS), Google (GKE), and Azure (AKS), as well as solutions from Alibaba, Baidu, Huawei and Tencent. If a user wishes to deploy a cluster with a new provider, they can import a driver for that provider directly from the UI. Rancher 2.5 gives operators full lifecycle management of the of EKS including node management and autoscaling, from a single pane of glass. Rancher can now import, provision, upgrade and configure and secure clusters on EKS directly using Rancher’s new unified, intuitive user experience. Additionally, Rancher-managed Amazon EKS deployments support CIS templating and scanning to minimize configuration drift between clusters.

3.1.6.2 OpenShift

OpenShift ACM now claims to have ‘limited’ support for popular hosted Kubernetes distributions like EKS, AKS and GKE.

3.1.6.3 Tanzu

Tanzu Mission Control does support hosted Kubernetes providers but cannot deploy clusters to them. Clusters must be created by the hosting provider and imported.

3.1.6.4 Anthos

Like Tanzu, Anthos enables the import and management of existing EKS and AKS clusters, in addition to the direct management of GKE resources.

3.1.7 Bare Metal, OpenStack & vSphere

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◑
- Anthos: ◔

3.1.7.1 Rancher

Rancher ships with drivers for deployment into common cloud providers such as AWS, GCP, Azure, DigitalOcean, Rackspace and others, and supports any cloud provider for whom a Docker Machine driver exists. It also ships with drivers for OpenStack and vSphere, making it possible for users of these technologies to deploy Kubernetes alongside their existing virtual machines. The Rancher Kubernetes Engine requires only a supported version of Docker, making it suitable for bare metal deployments of any Linux distribution. Users looking for a lightweight, secure operating system for bare metal deployments will find it with k3OS.

3.1.7.2 OpenShift

OpenShift supports deployment on bare metal and vSphere.

3.1.7.3 Tanzu

Tanzu supports deployment of clusters on bare metal and non-conformant Pods within vSphere. It also includes VCFS as part of its product suite at additional cost.

3.1.7.4 Anthos

For non-cloud environments, Anthos requires a VMware infrastructure. There is no option to deploy directly onto bare metal or into an OpenStack infrastructure.

3.1.8 Import Existing Clusters

- Rancher: ●
- OpenShift: ◕
- Tanzu: ●
- Anthos: ◕

3.1.8.1 Rancher

Rancher imports existing Kubernetes clusters, making them available for management in the Rancher UI. These clusters can be running in the cloud, on a hosted provider, on bare metal or virtual machines or on any other platform. If the cluster is running an unadulterated version of Kubernetes, Rancher can import it with no extra steps required. If the cluster is running a non-standard version of Kubernetes (OpenShift, Tanzu, etc.), then some extra configuration is required for Rancher to manage it.

3.1.8.2 OpenShift

The OpenShift control plane can import existing OpenShift clusters in different substrates and locations. However, take note of their “limited support’” for EKS, AKS and GKE.

3.1.8.3 Tanzu

Tanzu Mission Control can import clusters from external providers.

3.1.8.4 Anthos

While Anthos doesn’t play up the ability to import or register existing clusters and instead tries to move you to deploying fully managed solutions on GKE or GKE-on-prem, it does include the ability to register and interact with existing Kubernetes clusters. The process for doing so is convoluted and error prone, with multiple CLI commands needed to connect the cluster to Google Cloud.

3.1.9 High Availability

- Rancher: ●
- OpenShift: ●
- Tanzu: ◕
- Anthos: ◑

3.1.9.1 Rancher

Rancher deployments into hosted Kubernetes providers use the provider’s configuration for high availability. When deploying into other solutions, Rancher lets the user choose the node configuration for control plane, etcd and workers, letting them choose the high availability configuration that best suits the cluster’s role in the organization. It will also allow the user to choose in which availability zone the nodes will run. Clusters deployed with RKE can be dynamically reconfigured for 3-, 5- and 7-node HA configurations as the needs of the organization evolve.

High availability at the virtual machine level is delivered by the provider, where a solution like AutoScaling Groups (ASGs) and CloudWatch will recreate unresponsive virtual machines.

3.1.9.2 OpenShift

OpenShift always deploys a highly available Kubernetes cluster with five nodes for the control plane and etcd, independent of any worker nodes.

3.1.9.3 Tanzu

Tanzu’s deployment of Kubernetes has two options – development or production. The development cluster has a single-node controlplane and the production cluster has a 3-node controlplane. When operating in a cloud environment, the production cluster forces users to put each node in a separate availability zone. While this does increase availability in the unlikely event that a provider’s entire AZ goes offline, it also increases the cost of the cluster because communication between the controlplane nodes will incur charges for inter-AZ communication.

3.1.9.4 Anthos

At the time of this writing, HA support for user clusters in GKE on-prem is in beta mode. There is no support for HA in the admin cluster. Moreover, the control plane for the user clusters is contained in the admin cluster, and if the admin cluster is down, access to user clusters is lost. Considering how important the admin cluster is for user cluster access, not having an option for high availability is a threat to the stability of the environment.

3.1.10 Load Balancing

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◑
- Anthos: ◕

3.1.10.1 Rancher

Clusters installed by Rancher on compute instances include the NGINX Ingress Controller for load balancing. If Rancher deploys a cluster on a hosted provider that doesn't install an ingress controller by default (such as EKS), the Rancher App Catalog and Helm integration enable one-click installation of an ingress controller. This will also provision a provider specific LoadBalancer Service where appropriate. All Kubernetes clusters deployed into a known cloud provider will also support the deployment of provider-specific load balancers via the Service of type LoadBalancer. All standard ingress and load balancing solutions (including API gateways and service mesh) are compatible with Rancher-deployed clusters.

3.1.10.2 OpenShift

In addition to the standard Kubernetes ingress, OpenShift uses a proprietary software load balancer called a Route. It behaves similar to an Ingress, but it only exists within OpenShift and is not portable to other Kubernetes services. OpenShift Ingress Controllers are managed by the Ingress Operator. It deploys a default HAProxy-based load balancer to handle both Route and ingress requests.

3.1.10.3 Tanzu

Tanzu installations that don't use the VMWare NSX-T network driver require manual deployment of an external load balancer. Many customers opt to manually integrate external load balancers anyway, due to performance concerns and other operational requirements. Installations in AWS require additional manual configuration of VPC subnets and labels before the load balancer can be used with Tanzu. Installations with NSX-T have a robust load balancing solution for the Kubernetes API and user workloads, including support for TCP and UDP traffic to LoadBalancer services. NSX-T does not support services of type NodePort.

3.1.10.4 Anthos

The solution for GKE on-prem is to use the Seesaw load balancer, which is derived from the OSS LVS project. Seesaw requires dedicated VMs and address space and a management strategy outside of Kubernetes. Alternative cloud-native solutions exist such as kube-vip, MetalLB and Porter, which operate from within Kubernetes and use cloud-native strategies. However, due to the architecture of GKE on-prem and the separation between admin and user clusters, the extra burden of communication is probably what forces them to use a subpar solution like Seesaw. If you wanted to use any other load balancing solution for Kubernetes, the GKE architecture might prevent it.

3.1.11 Centralized Audit

- Rancher: ◕
- OpenShift:◕
- Tanzu: ◑
- Anthos: ◑

3.1.11.1 Rancher

Rancher can log all interaction with the Rancher API, including request and response body and metadata. This information is either logged to `stdout` or can be shipped to an external endpoint via standard means available within the platform (Fluentd, syslog, etc.). Rancher also supports the standard API logging available from Kubernetes.

3.1.11.2 OpenShift

OpenShift can log all interaction with the OCP API, including request and response body and metadata. This information is logged to files and can be queried via the `oc` command. It requires knowing the host and logfile to query. OpenShift also supports the standard API logging available from Kubernetes.

3.1.11.3 Tanzu

Like Enterprise PKS, the distributed nature of the support infrastructure required for Tanzu means that audit logs are also distributed across different components and different machines. VCF components support event logs and security event logs. These require a syslog endpoint for archival and processing.

3.1.11.4 Anthos

Anthos currently supports disk-based logging using the functionality already present in Kubernetes. There is no feature for remote access of logs outside of what is available from Kubernetes and log shipping; however, Cloud Audit Log support is an alpha feature in Anthos 1.2.

3.1.12 Self-service Provisioning

- Rancher: ●
- OpenShift: ◔
- Tanzu: ●
- Anthos: ◔

3.1.12.1 Rancher

Rancher uses a granular permissions scheme to grant or deny access to resources at the Global, Cluster and Namespace levels. Users with access to the Rancher server will only see their own clusters or projects, and the optional namespace isolation assures that multi-tenant clusters stay secure. Privilege delegation means that a global admin can grant another user the permission to create clusters that only they or their team can see. This delegation of responsibility, along with the parameters for how and where clusters are deployed, gives developers access to the resources they need while assuring that the entire environment stays secure. Provisioning of Kubernetes clusters can be done through the UI, CLI or API.

3.1.12.2 OpenShift

OpenShift is a single-cluster solution that must be deployed via the installer program. It does not contain any means for launching new clusters.

3.1.12.3 Tanzu

Through the SaaS platform and API calls, users can provision Kubernetes workloads and clusters.

3.1.12.4 Anthos

Anthos does not permit end users to launch clusters without first having administrative privileges in the environment. After an administrator launches a user cluster, end users can be given access to it according to Kubernetes RBAC boundaries.

3.1.13 Private Registry and Image Management

- Rancher: ◕
- OpenShift: ●
- Tanzu: ◑
- Anthos: ◑

3.1.13.1 Rancher

Rancher contains full support for private registries. It presents a tab in the UI where users can enter their registry credentials. These are saved as Kubernetes Secrets and used when pulling from private registries.

3.1.13.2 OpenShift

OpenShift contains full support for private registries and includes a local registry that is used for locally built images. Access to the local registry uses the credentials of the requesting user when determining permissions. Access to external registries use the OC CLI to create ImagePullSecrets and optionally attach them to service accounts.

3.1.13.3 Tanzu

Tanzu uses the features available within Kubernetes for accessing private and authenticated registries. Users must manually create registry credential objects and bind them to workloads which will use them.

3.1.13.4 Anthos

Anthos uses the features available within Kubernetes for accessing private and authenticated registries. Users must manually create registry credential objects and bind them to workloads which will use them.

3.1.14 Cluster Upgrades and Version Management

- Rancher: ●
- OpenShift: ●
- Tanzu: ◑
- Anthos: ◕

3.1.14.1 Rancher

Rancher Kubernetes Engine (RKE) runs upstream Kubernetes within Docker containers. Updates to individual Kubernetes services can be performed atomically, with complete support for rollback to previous versions. All updates to Kubernetes are performed with zero downtime to running workloads.

A complete rolling update of a 3-node cluster will take approximately 10 minutes. Rancher releases security updates to RKE within two weeks of upstream release from the Kubernetes team, and non-urgent Kubernetes updates within four weeks.

Rancher 2.5 provides full lifecycle management for Amazon EKS clusters, which includes cluster upgrading from the Rancher control plane.

3.1.14.2 OpenShift

OpenShift uses Kubernetes Operators to deploy and upgrade the Kubernetes cluster components. All updates to Kubernetes are performed with zero downtime to running workloads. A complete update of a 3-node cluster will take approximately 15 minutes.

3.1.14.3 Tanzu

According to the Tanzu documentation, Tanzu Mission Control will initially support provisioning, upgrading, and scaling clusters on AWS with other environments planned for the future. Enterprise PKS Management Console supports upgrade automation today.

3.1.14.4 Anthos

Anthos has specific restrictions around versions of admin and user clusters. If the admin cluster is upgraded, then it cannot be upgraded again until all user clusters are upgraded to the same version as the admin cluster.

3.1.15 Storage Support

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◔
- Anthos: ◕

3.1.15.1 Rancher

Rancher develops Longhorn (a persistent block storage open source project governed by the CNCF) and maintains strong partnerships with Portworx, StorageOS and OpenEBS. These vendors certify their software on Rancher releases, so users of both products can be confident that they work well together.

3.1.15.2 OpenShift

Red Hat supports in-tree and CSI storage for Kubernetes. They also ship a rebranded distribution of Rook, an open source project that delivers container storage via Ceph. Red Hat maintains Ceph and GlusterFS, and can therefore implement OpenShift-specific extensions for these solutions.

3.1.15.3 Tanzu

Tanzu offers no explicit certification of storage products other than VMware vSAN. All of the storage API functionality in VCFS is targeted at vSAN.

3.1.15.4 Anthos

Anthos supports in-tree, CSI and vSphere storage drivers.

3.1.16 Arm support

- Rancher: ●
- OpenShift: ○
- Tanzu: ○
- Anthos: ○

3.1.16.1 Rancher

RKE and k3s support installation on Arm64 and Arm7. Rancher has a partnership with Arm and works closely with their engineering team on new releases.

3.1.16.2 OpenShift

OpenShift does not support deployment on Arm processors.

3.1.16.3 Tanzu

Tanzu does not support deployment on Arm processors.

3.1.16.4 Anthos

Anthos does not support deployment on Arm processors.

3.1.17 Airgap support

- Rancher: ●
- OpenShift: ●
- Tanzu: ◔
- Anthos:○

3.1.17.1 Rancher

Rancher supports airgap installations and includes documentation on how to provision a private registry server and populate it with all images needed for the installation.

3.1.17.2 OpenShift

OpenShift supported airgap installations in OCP4.

3.1.17.3 Tanzu

At GA, Tanzu Mission Control is a SaaS-only product. VMware’s plans to support other deployment modes are unknown at this time.

3.1.17.4 Anthos

Anthos has no documentation for deploying into an airgap environment.

3.1.18 Etcd backup and restore

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◑
- Anthos: ◑

3.1.18.1 Rancher

All Rancher-deployed RKE clusters are automatically backed up to local storage at regular intervals. The operator can change this to an S3-compatible endpoint. Clusters can be restored to any snapshot from the UI or CLI. HA deployments of the Rancher server require manual configuration of the RKE cluster to perform backups. These can also write to local storage or an S3-compatible endpoint. Restoring an HA cluster requires deploying a new Kubernetes cluster, restoring the backup, and then performing a new Rancher installation. Upon completion all remote Kubernetes clusters will reconnect to the new cluster.

3.1.18.2 OpenShift

Backup of an OCP4 cluster requires manually logging into an etcd host and running a script. While this could be automated with cron, it includes no provision for saving to a remote endpoint. As a result, an effective backup solution will depend on the operator to design, install and maintain it.

3.1.18.3 Tanzu

Tanzu includes Velero, an open source backup solution created by Heptio, although there is no “automatic” integration here, similar to Rancher.

3.1.18.4 Anthos

Google provides limited support for backing up and restoring a cluster's etcd datastore and encourages users to instead contact them directly for support. The provided instructions for performing backups are manual and convoluted and do not promote designing a disaster recovery strategy for Kubernetes into standard operating procedure.

3.2 Security, Policy & User Management

3.2.1 Active Directory and LDAP support

- Rancher: ●
- OpenShift: ●
- Tanzu: ●
- Anthos: ◕

3.2.1.1 Rancher

Rancher integrates directly with Active Directory, Azure AD, OpenLDAP, FreeIPA, OAuth providers like GitHub and SAML providers such as Keycloak and Okta. Configuration of the integration takes place at the Global level, after which users and groups from the provider are available for assignment to RBAC roles and downstream clusters.

3.2.1.2 OpenShift

OpenShift runs an internal OAuth server and proxies communication to multiple backend providers. It maintains compatibility with providers based on LDAP, Keystone, OpenID and OAuth, as well as providing an interface for basic authentication and external authentication systems capable of setting a request header.

3.2.1.3 Tanzu

Tanzu authentication communicates natively to any backend provider that speaks SAML. It also provides the ability to group clusters for easier application of security policies.

3.2.1.4 Anthos

Anthos supports OIDC in Active Directory 2016 and later with limitations. Because cluster configuration is immutable, any change to the authentication scheme will require building a new cluster.

3.2.2 Pod and network security policies

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◕
- Anthos: ◕

3.2.2.1 Rancher

Rancher supports Pod Security Policy (PSP) configuration at the Global level. PSP templates are then assigned to downstream clusters. This ensures conformance and reduces the risk of human error when changing policies. PSPs can be created and edited through the UI.

3.2.2.2 OpenShift

OpenShift uses Security Context Constraints to perform the function of a Pod Security Policy object in Kubernetes. It contains a robust implementation of the SCC for the cluster. SCCs can only be edited through the `oc` command on the CLI.

3.2.2.3 Tanzu

Tanzu supports native Pod Security Policies within Kubernetes and vSphere. However, Pods running in VCFS "supervisor layer" are described as "non-conformant."

3.2.2.4 Anthos

Anthos supports Kubernetes NetworkPolicy resources. The upcoming GKE Dataplane v2 supports eBPF with Cilium. Anthos does not directly support Pod Security Policies and instead provides a proprietary resource called a Policy Controller that implements similar functionality.

3.2.3 Configurable adherence to CIS security benchmarks

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◑
- Anthos: ◕

3.2.3.1 Rancher

Rancher maintains a hardening guide and self-assessment that references CIS benchmarks with specific actions a user can take to satisfy the requirement. Rancher 2.4’s CIS Scan feature allows users to run automatic assessments against the CIS benchmark best practices and then use Cluster Templates to deploy these configurations consistently at scale.

3.2.3.2 OpenShift

OpenShift offers no additional information in their documentation about CIS benchmark adherence or guidance for their customers. Customers can use public tests for Kubernetes adherence, but this will not cover anything unique to OpenShift.

3.2.3.3 Tanzu

At this time, we were not able to find guidance on hardening Tanzu deployments. A support request from March 2019 reports that kube-bench does not work with PKS clusters, leaving users to find their own solution. We will assume the same is true for Tanzu.

3.2.3.4 Anthos

Google provides documentation on how Anthos scores against CIS benchmarks, but it does not provide a means to automatically perform scans. Instead they direct users to manual scans using the open source kube-bench utility.

3.2.4 RBAC policies

- Rancher: ●
- OpenShift: ◑
- Tanzu: ●
- Anthos: ◑

3.2.4.1 Rancher

Rancher exposes all Kubernetes RBAC and then enables the configuration and maintenance of RBAC policies at the Global level in our UI. Policies exist for Global, Cluster and Project levels, and in addition to the templates Rancher provides, users can create an infinite number of templates to define new roles. User templates can inherit from existing templates to create a hierarchy of permissions which are easily maintained.

3.2.4.2 OpenShift

OpenShift uses native Kubernetes RBAC which is managed through the ‘oc’ command. It doesn’t include RBAC management through the UI.

3.2.4.3 Tanzu

At launch, VMware spent a good deal of time promoting Tanzu’s RBAC features. We will assume that, like Rancher, Tanzu exposes all Kubernetes RBAC and then enables the configuration and maintenance of RBAC policies at the Global level in their UI.

3.2.4.4 Anthos

Anthos supports Kubernetes RBAC but does not provide a user interface for configuring it or applying it globally across user clusters.

3.3 Shared Tools & Services

3.3.1 Application catalog

- Rancher: ◕
- OpenShift: ●
- Tanzu: ◕
- Anthos: ◑

3.3.1.1 Rancher

Rancher's Application Catalog extends Helm to provide users with an easily understood form-based installation process for applications. It integrates with any external Helm repository, giving users the means to install applications from either system. Tiller, Helm's internal component, is often cited as a security risk because it is often deployed with admin-level privileges in a cluster. Rancher's app catalog does not require Tiller, and as such is a more secure implementation of Helm.

3.3.1.2 OpenShift

OpenShift integrates with Red Hat's Operator Hub, a curated list of applications that meet Red Hat's requirements for inclusion. OCP 4.5 also includes a developer perspective with resources for interacting with Helm charts.

3.3.1.3 Tanzu

Tanzu includes an application catalog to provide users with an easily understood form-based installation process for applications.

3.3.1.4 Anthos

You can deploy applications to Anthos using Helm but there's no integrated application catalog or discovery mechanism for applications.

3.3.2 Provision with Terraform / Ansible / Others

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◔
- Anthos: ●

3.3.2.1 Rancher

Rancher maintains the Terraform provider, which enables users to deploy and manage Rancher using IaC principles. Although not officially integrated with other solutions, Rancher's open API and use of Docker containers for RKE make it easy to integrate with solutions such as Ansible, Puppet, Chef, AWS autoscaling groups, cloud-init or other provisioning strategies.

3.3.2.2 OpenShift

OpenShift uses Terraform for its install, but it does so by bundling the Terraform installer and all scripts into the installer binary. These are not visible to the user or available for inclusion in a corporate IaaS workflow.

3.3.2.3 Tanzu

Rather than supporting popular open source solutions like Terraform for provisioning infrastructure-as-code, much of VMware’s solution is proprietary.

3.3.2.4 Anthos

Anthos enables users to create and update clusters with Terraform. Once Anthos is running, it includes its own configuration management solution for policies and configuration across the environment.

3.3.3 CI/CD capabilities

- Rancher: ●
- OpenShift: ●
- Tanzu: ◕
- Anthos: ●

3.3.3.1 Rancher

Rancher integrates with any CI/CD system that works with Kubernetes. If a user does not already have a CI/CD system in place, they can use the Pipeline system built into Rancher to begin using CI/CD workflows. Rancher Pipelines is based on Jenkins and connects to repositories from GitHub, Gitlab and Bitbucket.

3.3.3.2 OpenShift

OpenShift will work with any CI/CD system that works with Kubernetes. Additionally, Red Hat has released an early preview of OpenShift Pipelines, based on Tekton.

3.3.3.3 Tanzu

Tanzu should work with any CI/CD system that works with Kubernetes.

3.3.3.4 Anthos

GKE includes strong support for CI/CD solutions including GitLab, Knative, Jenkins and others.

3.3.4 Advanced monitoring

- Rancher: ●
- OpenShift: ●
- Tanzu: ◔
- Anthos: ◕

3.3.4.1 Rancher

Rancher ships with basic monitoring activated by default. Cluster admins can enable advanced monitoring with a single click in the Rancher UI. This deploys Prometheus and Grafana at the project and cluster levels and installs preconfigured dashboards that immediately enable visibility into cluster operations. Users can access Grafana and see metrics for the resources to which they have access. They can also annotate their workloads to have Prometheus begin to scrape custom metrics from them.

3.3.4.2 OpenShift

OpenShift ships with Prometheus and Grafana activated by default, with preconfigured Grafana dashboards. This installation is only available for monitoring OpenShift components. Users must install their own solution for monitoring user workloads.

3.3.4.3 Tanzu

Tanzu doesn’t include monitoring or visualization by default. The only supported solution for additional monitoring of Tanzu requires a licensed copy of VMware Wavefront.

3.3.4.4 Anthos

Anthos enables application observability through Anthos service mesh. Cluster level metrics have limited support through Cloud Logging and Cloud Monitoring or Prometheus and Grafana. Both Cloud Logging and Cloud Monitoring come at a premium.

3.3.5 Alerts and Notifications

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◔
- Anthos: ◑

3.3.5.1 Rancher

Both the default basic monitoring and the optional advanced monitoring configure alerts for critical cluster components. Users need only create notification targets. Rancher supports sending alerts to Slack, PagerDuty, WeChat, email or any webhook destination. Notifiers can be configured at the cluster and project levels, allowing delegation of responsibility for application events to the responsible teams.

3.3.5.2 OpenShift

OpenShift’s notification targets require manual configuration of AlertManager and expressly forbid deviation from a small subset of AlertManager functionality.

3.3.5.3 Tanzu

Available via VMware Wavefront, a separate paid-for monitoring solution.

3.3.5.4 Anthos

Anthos enables alerting for clusters and service mesh via Google Cloud Monitoring. Google Cloud Monitoring comes at a premium.

3.3.6 External log shipping

- Rancher: ◕
- OpenShift: ◕
- Tanzu: ○
- Anthos: ◑

3.3.6.1 Rancher

Rancher ships with connectors for Elasticsearch, Fluentd, Splunk, Kafka and syslog.

3.3.6.2 OpenShift

OpenShift can deploy an EFK stack (Elasticsearch, Fluentd, Kibana) within the cluster and use it for logging.

3.3.6.3 Tanzu

Does not include any solution for log consolidation or management as part of the base product. This functionality is offered by Wavefront (a paid add-on).

3.3.6.4 Anthos

Anthos only allows you to ship logs to Cloud Logging, Prometheus and Grafana, or approved third-party solutions – Elasticsearch, Splunk and Datadog.

3.3.7 Windows container support

- Rancher: ◕
- OpenShift: ○
- Tanzu: ○
- Anthos: ◕

3.3.7.1 Rancher

Rancher supports Windows worker nodes beginning with Rancher 2.3 and Kubernetes 1.14. Windows and Linux worker nodes can exist together (Linux nodes run the control plane, etcd and ingress) in the same Kubernetes cluster, and Rancher will deploy the appropriate workload to the appropriate node.

3.3.7.2 OpenShift

OpenShift (OCP4) does not contain production support for using Windows servers in Kubernetes clusters or deploying Windows containers into Kubernetes.

3.3.7.3 Tanzu

Windows containers on PKS was in beta in Dec 2019. That doesn’t appear to have carried over to the Tanzu product suite (yet).

3.3.7.4 Anthos

GKE and GKE on-prem support Windows container workloads. Anthos includes beta support for migrating Windows VMs into containers running on Windows node pools.

3.3.8 Integrated Service Mesh support

- Rancher: ●
- OpenShift: ◕
- Tanzu: ◔
- Anthos: ◕

3.3.8.1 Rancher

Rancher 2.5 contains one-click activation of upstream Istio 1.6 with visualization within the Rancher dashboard through Kiali. Users can immediately use the benefits of service mesh within Rancher-deployed clusters, or if they wish to use an alternative other than Istio, they can deploy that from the application catalog.

3.3.8.2 OpenShift

OpenShift installs a version of Istio modified by Red Hat to work within OpenShift. While it is functionally similar to Istio, it will not move as quickly as the upstream Istio release cadence.

3.3.8.3 Tanzu

Tanzu contains support for VMware Tanzu Service Mesh, which is part of NSX —so a paid-for, proprietary product.

3.3.8.4 Anthos

Anthos includes Google Service Mesh, which is a modified version of Istio.

3.3.9 Enterprise SLA

- Rancher: ●
- OpenShift: ◑
- Tanzu: ◑
- Anthos: ◑

3.3.9.1 Rancher

Rancher Labs provides an enterprise subscription that covers Rancher, Docker, Kubernetes, and all cloud-native software that Rancher includes. It also includes IP assurance and indemnification and is available in configurable packages for business hour or 24x7 support. Rancher’s subscription is priced by node, independent of the number of cores.

3.3.9.2 OpenShift

Red Hat provides support for OpenShift and the Red Hat software stack. Many of the OpenShift components cannot be modified or used outside of the parameters Red Hat dictates without invalidating support. Red Hat’s support model is priced by virtual core, making every upgrade of the customer’s environment an increase in support cost.

3.3.9.3 Tanzu

VMware does provide a basic support for Tanzu products up to 24/7/365 technical support. However, if you want services such as root-cause analysis, upgrade coordination services or access to engineering resources, these are part of an additional, paid support package.

3.3.9.4 Anthos

Google has support tiers that range from community support to premium 1:1 support. Each of these plans includes support for Anthos and its components, but only the free community support is included in the Anthos pricing.

3.3.10 Community traction

- Rancher: ●
- OpenShift: ◕
- Tanzu: ○
- Anthos: ◔

3.3.10.1 Rancher

Rancher has a thriving community of users and contributors across all its products and projects. With +100 million downloads and +35,000 deployments, it is the most popular open source solution for deploying and managing Kubernetes clusters.

3.3.10.2 OpenShift

Red Hat has a large community of open source users across its entire product line. Although OpenShift Container Platform is a commercial offering, components of the solution exist in an open source form. The difficulty in deploying and maintaining disparate components may lead people to either purchase the commercial version of OCP4 or use alternative solutions.

3.3.10.3 Tanzu

The open source origin of PKS was Cloud Foundry Container Service. Cloud Foundry was originally created by VMware. Although maintained by Pivotal for a while, it is now back with VMware after they purchased Pivotal in 2019. While Cloud Foundry has a large and robust open source following, the same cannot be said of Tanzu, which is both new and has many proprietary components .

3.3.10.4 Anthos

The initial pricing of Anthos targeted large enterprises with deep pockets. Their recent transition to a Pay As You Go (PAYG) model implies that uptake has been low and that they are hoping to attract a broader audience.

4 About the Author

Rancher Labs is the company behind the following open source products:

- **Rancher** - the world's most popular enterprise-grade Kubernetes management platform.
- **RKE** - a simple, lightning fast Kubernetes installer that works everywhere;
- **K3s** -a lightweight production-grade Kubernetes distribution built for embedded systems and the edge. K3s is now a CNCF sandbox project.
- **Longhorn** - first developed by Rancher but now an official CNCF sandbox project, Longhorn delivers a powerful cloud-native distributed storage platform for Kubernetes that can run anywhere. When combined with Rancher, Longhorn makes the deployment of highly available persistent block storage in your Kubernetes environment easy, fast and reliable.

Together, these products help IT operators, DevOps and technology leaders' teams address the operational and security challenges of managing certified Kubernetes clusters across any infrastructure. They also provide developers with an integrated stack of tools to build and run containerized workloads at scale.

To learn more about Rancher Labs visit www.rancher.com.

5 Glossary

5.1 Cluster Operations

- Ease of installation, configuration and maintenance
    - A Kubernetes management platform should be easy and quick to implement. Deployment should be measured in minutes rather than hours or, in some cases, days.
- Intuitive UI
    - A polished, intuitive UI should allow operations that span multiple clusters running in different regions, data centers and cloud providers.
- Multi-cloud
    - Support for popular cloud environments like AWS, Azure and GCP minimizes the commercial and technical risks associated with being locked into a single cloud provider.
- Multi-cluster
    - To run Kubernetes in production without vendor lock-in, you need to have the ability to manage multiple Kubernetes clusters using the same unified user experience, on-premise or in any cloud environment.
- Edge Support
    - A nascent paradigm in the Kubernetes community, there are obvious ultra-low latency benefits when clusters are run as close as possible to where they’re delivering the most value, the customer.
- Hosted Kubernetes support
    - There are many good reasons for users to favor the deployment speed, resilience and tooling of managed service providers like AKS, EKS and GKE. A Kubernetes management platform should give users the choice of deployment environment without favoring any single vendor.
- Bare Metal, Cloud, OpenStack & vSphere
    - To support hybrid Kubernetes deployments, the chosen Kubernetes management platform must also support common bare metal, private cloud and virtualization environments.
- Import existing clusters
    - The ability to import existing Kubernetes clusters is particularly important for those that have started their Kubernetes journey using vanilla Kubernetes or a managed Kubernetes service, but want to consolidate their management with a single interface.
- High availability
    - Kubernetes management platforms should make deploying a highly available Kubernetes cluster with stacked control plane nodes or using an external etcd cluster easy without the need to deploy additional tools like kops.
- Load balancing
    - Kubernetes automatically load balances requests to application services inside of a Kubernetes cluster. However, some services need to be exposed externally for consumption by external clients. Kubernetes does not provide an out-of-the box load balancing solution for that type of service. A Kubernetes management platform should include a robust external load

    - balancing solution or integrate seamlessly with existing commercial load balancers.
- Centralized audit
    - Users should be able to see a chronological record of calls that have been made to the Kubernetes API server. Kubernetes audit log entries are useful for investigating suspicious API requests, for collecting statistics or for creating monitoring alerts for unwanted API calls.
- Self-service provisioning
    - Developers must have self-service access to one or more Kubernetes clusters with right levels of isolation in place so only members with the right privileges can access production workloads.
- Private registry and image management
    - A container image registry is a service like Docker Hub that stores container images. A private registry allows you to share your custom base images within your organization, keeping a consistent, private and centralized source of truth for the building blocks of your architecture.
- Cluster upgrades and version management
    - New versions of Kubernetes are available every three months. A Kubernetes management platform should support rolling upgrades of clusters, such that the cluster and the cluster API is always available even while the cluster is being upgraded. Additionally, it will provide the ability to rollback to previous stable version upon failure.
- Storage support
    - Integration with enterprise-grade storage is an essential component of running Kubernetes clusters in production. Enterprises will typically want their Kubernetes deployment to integrate with storage solutions that they have already deployed (NetApp, EMC, etc.) or they may want to integrate with a container-native storage technology such as Longhorn, OpenEBS, StorageOS or Portworx.
- Arm support
    - Support for Arm chipsets is particularly important when running Kubernetes clusters in resource-constrained environments like IoT appliances or at the network edge.
- Airgap support
    - Kubernetes clusters that are used for internal applications can be installed and operated in air-gapped environments. An airgap cluster doesn't have outbound Internet access, and therefore cannot pull the application images from a public Docker registry.
- Etcd backup and restore
    - For some, the idea of backups for stateless applications is counterintuitive. But state is still necessary to restore a failed master node, and is especially important if you run a cluster with only a single master.

5.2 Security Policy & User Management

- Active Directory and LDAP support
    - Out of the box, Kubernetes authentication is not very user-friendly for end users. A Kubernetes management platform should integrate seamlessly with

Microsoft Active Directory and other common LDAP services to give the easiest authentication experience to end users.

- Pod and network security policies
    - A network security policy is a specification of how Kubernetes resources can communicate with each other and other network endpoints. A Pod Security Policy (PSP) defines security rules to which Pods must conform in order to run on the cluster.
- Configurable adherence to security benchmarks
    - Benchmarks from the Center for Internet Security (CIS) can be used by system administrators, security and audit professionals and other IT roles to establish and maintain a secure configuration baseline for Kubernetes.
- RBAC policies
    - Role-based Access Control (RBAC) policies are vital for the correct management of your cluster, as they allow you to specify which types of actions are permitted, depending on the user and their role in your organization. Common RBAC policies include securing your cluster by granting privileged operations (accessing secrets, for example) only to admin users; forcing user authentication in your cluster; and limiting resource creation (such as pods, persistent volumes, deployments) to specific namespaces or have a user only see resources in their authorized namespace.

5.3 Shared Tools & Services

- Application catalog
    - The application catalog provides easy one-click deployment for a set of pre-packaged applications that run inside of Kubernetes. It also provides developers a vehicle to build and publish their own applications so that others in their team or their organization can deploy them quickly and reliably. The application catalog enables organizations to standardize on a set of application deployment recipes or blueprints, avoiding configuration sprawl and rogue installations.
- Provision with Terraform / Ansible / Others
    - Terraform and Ansible are popular infrastructure-as-code-software tools that enable users to define, provision and manage a data center infrastructure using a high-level configuration language such as YAML or JSON. Support for these tools means teams can work with your Kubernetes management platform in the same way as the rest of your infrastructure.
- CI/CD capabilities
    - One of the most critical workloads run by developers is a Continuous Integration and/or Continuous Delivery pipeline. A robust CI/CD pipeline is critical to ensure agile development and rapid delivery of new software releases to customers.
- Advanced monitoring
    - A production Kubernetes cluster must always be monitored to detect issues that might affect cluster and application availability for users. A Kubernetes management platform must provide this capability out of the box, with

  - advanced monitoring available through integrations with open source, cloud-native monitoring solutions like Prometheus and Grafana.
- Alerts and Notifications
  - Notifications and alerts are core pillars of observability in DevOps. Even though monitoring and logging provide a way to get insight on the state of a Kubernetes cluster, notifications and alerts are used to let operators know of potentially problematic events when they occur.
- External log shipping
  - Workloads in your clusters will write information to logs, but without a central point of aggregation, parsing the log data is more challenging. An effective cluster will support log shipping to external systems like Splunk, Logstash, or Fluentd. These systems enable a broader view of multiple data streams and can more easily detect anomalies within the bigger picture.
- Windows container support
  - With countless workloads running on its many versions, Windows remains one of the most popular operating systems in datacenters. Whether the requirement is to quickly create and tear down dev or test environments, or to lift and shift legacy applications to the cloud, support for Windows containers within your Kubernetes management platform is a requirement for any business that uses Windows in production.
- Integrated Service Mesh
  - Service Mesh adds fault tolerance, canary deployments, A/B testing, monitoring and metrics, tracing and observability, and authentication and authorization to Kubernetes. It eliminates the need for developers to create custom code to enable these capabilities. Developers can focus on their business logic, and all applications benefit from a standard toolchain for complex network services.
- Enterprise SLA
  - As more organizations run their business apps on Kubernetes, IT operations teams must ensure that they can support the service level agreements (SLAs) that the business requires. To help customers realize this, each vendor delivers technical expertise and insight 24/7/365 via some form of annualized subscription. Affordability and trust are key variables when evaluating competing offerings.
- Community traction
  - Often used as a bellwether of platform innovation and maturity, the most successful open source technologies are readily embraced by their respective communities and widely deployed.

6 Legal Statements

6.1 Copyright Notice

This document and its content are copyright of Rancher Labs, Inc - © Rancher Labs, Inc 2020. All rights reserved. Any redistribution or reproduction of part or all the contents in any form is prohibited other than the following:

- you may print or download to a local hard disk extracts for your personal and non-commercial use only
- you may copy the content to individual third parties for their personal use, but only if you acknowledge the source of the material

You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

6.2 Third-Party Trademark Usage

Please note that Red Hat OpenShift and VMware Tanzu are the registered trademarks of Red Hat Inc. and VMware Inc., respectively.

6.3 Note from the Authors

The views in this whitepaper are those of Rancher Labs Inc. Every effort has been made to ensure accuracy; however, we appreciate that some readers may take issue with our conclusions. If so, we welcome your feedback at:

Web – rancher.com
Email – info@rancher.com
Twitter – @rancher_labs

Worldwide Locations

NORTH AMERICA

CALIFORNIA (HQ)

10050 N Wolfe Rd
SW1 STE SW1-272
Cupertino, CA 95014

ARIZONA

1400 E Southern Ave
Ste 1020
Tempe, AZ 85282

NEW YORK

54 W 40th St
5th Floor
New York, NY 10018

EMEA & APAC

THE NETHERLANDS

John M. Keynesplen 12,
1066 EP Amsterdam

UNITED KINGDOM

Fowler Avenue
The Hub, Farnborough Business Park
Farnborough GU14 7JF

SHENZHEN, CHINA

1809, Building 2,
Xunmei Technology Plaza,
Kehua Road, Nanshan District,
Shenzhen, China