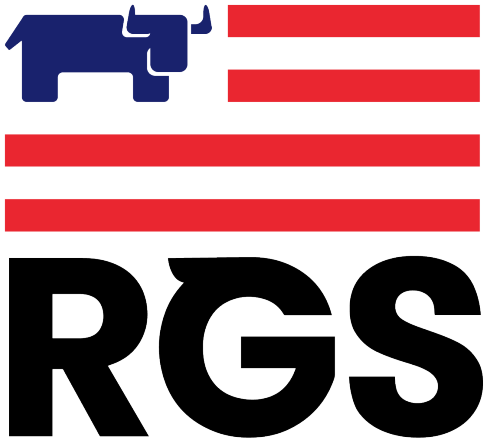
A Buyer's Guide to Enterprise Kubernetes Management Platforms



RGS
Rancher Government Solutions

Red Hat OpenShift 4.7, VMware Tanzu 1.3, Google Anthos 1.8, and Rancher 2.6

Updated August 2021

Content

01 Executive Summary

Government Organizations modernizing their infrastructure continue to choose cloud-based technologies to power their digital transformation. As they move away from their legacy environments to hybrid, multi-cloud stacks, enterprises are creating new opportunities to unify their IT operations with containers and Kubernetes. The recent Forrester Wave report[1] stated that these cloud-native technologies are quickly becoming the preferred way for global organizations to build and modernize their applications and services at scale.

The popularity of containers and Kubernetes is evident with Gartner[2] predicting that by 2022 more than 75% of worldwide organizations will run containerized applications in production. This forecasted growth demonstrates the value of cloud-native technologies for developers, who look for solutions to help them build applications quickly without compromising on reliability, agility and security.

Relying on upstream Kubernetes isn't enough for teams deploying Kubernetes into production. Basic Kubernetes installations are plagued by a lack of central visibility, inconsistent security practices, and complex management processes.

Therefore, Kubernetes management platforms need to confidently deliver:

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

[1] "The Forrester Wave™: Multicloud Container Development Platforms, Q3 2020" by Dave Bartoletti, Charlie Dai with Lauren Nelson, Duncan Dietz, Han Bao, Bill Nagel, Forrester –

[2] "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024" by Susan Moore, Gartner –

Given the transformative potential of Kubernetes and the growth of the cloud-native sector, the battle for market leadership in Kubernetes management remains very competitive.

Rancher is available as an open source project that anyone can use. Rancher's growth has continued to accelerate, with downloads now exceeding 102 million.

Rancher has extended its success in the Government market by maintaining double digit growth year on year. Its latest release, SUSE Rancher 2.6 is a showcase of the acquisition's success and includes a new user-experience designed for the enterprise user, full lifecycle management across the three major hyperscalers, and a strengthened security posture.

Following its merger with IBM in 2019, Red Hat continues to command market share. By leveraging their existing relationships with global enterprises, Red Hat has been successful with their "semi open source approach," as described by GigaOm's recent report[3] on Federated Kubernetes.

Since launching to a lukewarm reception in 2019, Google Anthos has found a niche in the market as part of the wider Google Cloud portfolio. Their initial go-to-market strategy saw a high premium for an immature multi-cluster platform. In 2020, Google introduced a new pay-as-you-go pricing model and invested heavily in developing new features for Anthos in order to remain competitive in the market.

In the last three years VMware has acquired a number of companies, including Pivotal, Heptio, and Bitnami, to expand their experience in the cloud-native space and maintain market share that was threatened by the absence of a Kubernetes management story. In March 2020, VMware released v1 of its VMware Tanzu product suite that differentiated itself by leveraging Project Pacific, a re-architecture of vSphere with Kubernetes as its control plane.

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 4.7 (OpenShift/OCP4), VMware Tanzu Mission Control with Tanzu Kubernetes Grid Integrated Edition (collectively referred to as Tanzu in this guide), Google Anthos with Anthos GKE (collectively referred to as Anthos in this guide) and SUSE Rancher 2.6.

[3] "Key Criteria for Leveraging Federated Kubernetes, Open & Closed" by David S. Linthicum, GigaOm –

02 Capabilities Summary

_02.1 Overview

In this analysis, we use "Harvey balls" to illustrate how each vendor compares to the others by category:

FEATURE	Rancher	OpenShift	Tanzu	Anthos
Ease of install, Config & Maintenance	4	3	3	2
Intuitive UI	4	4	3	4
Multi-cloud	4	3	3	2
Multi-cluster	4	2	3	3
Edge Support	4	1	1	2
Hosted Kubernetes Support	4	1	2	2
Bare Metal, OpenStack & vSphere	4	3	2	3
Import Existing Clusters	4	3	3	2
High Availability	4	4	3	2
Load Balancing	4	2	2	3
Centralized Audit	4	3	2	1
Self-service Provisioning	4	2	2	0
Private Registry & Image Management	4	4	4	2

FEATURE	Rancher	OpenShift	Tanzu	Anthos
Cluster Upgrades & Version Management	4	4	2	2
Storage Support	4	3	4	3
Arm Support	4	0	0	0
Airgap Support	4	3	3	0
Etcd Backup and Restore	4	2	3	2

- The full ball (**4**) is applied to the platform that is best-of-breed in that category.
- The three-quarters ball (**3**) is applied to the runner-up in that category.
- The half ball (**2**) illustrates acceptable capability in that category.
- The quarter ball (**1**) shows weak capability in that category.
- The empty ball (**0**) indicates the platform has no capability in that category.

_02.2 Cluster Operations

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

_02.3 Security Policy and User Management

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

FEATURE	Rancher	OpenShift	Tanzu	Anthos
Active Directory and LDAP Support	4	4	4	3
Pod and Network Security Policies	4	3	2	2
CIS Benchmark Adherence & Tracking	4	3	2	2
Global RBAC Policies	4	2	3	2

_02.4 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	4	4	2	1
Provision with Config Management Systems	4	2	2	4
Integration with CI/CD Solutions	4	4	2	4
Advanced Monitoring	4	4	2	2
Alerts and Notifications	4	4	1	2
External Log Shipping	4	4	2	3
Windows Container Support	4	4	0	3
Integrated Service Mesh Support	4	3	1	4
Enterprise SLA	4	2	2	2
Community Traction	4	3	0	1

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

03 Feature Analysis

_03.1 Cluster Operations

_03.1.1 Ease of Installation, Configuration, and Maintenance

Rancher	4
OpenShift	3
Tanzu	3
Anthos	2

_03.1.1.1 Rancher

Rancher operates across any certified Kubernetes distribution from the cloud to core and at the edge. Each distribution requires the bare minimum of host configuration, usually no more than a supported version of Docker. For edge deployments, Rancher does not need Docker containers when used with distributions such as K3s and Rancher Kubernetes Engine 2 (RKE2). For installations that want an even smaller attack surface, Rancher can utilize an operating system such as openSUSE MicroOS to help run Kubernetes in the most efficient way possible.

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

_03.1.1.2 OpenShift

OpenShift Container Platform 4 (OCP4) ships a large installation binary that includes Terraform and a set of scripts to deploy OCP4 into a provider. Installation guides are provided for public and private cloud providers, along with guides for bare metal and "any other provider." Cloud provider installers require administrator access to the environment to create the resources but can operate without administrative access once installation is complete. Executing the installation binary is easy because there are minimal options available for cluster configuration at launch time. All configuration happens from within OCP4 after the cluster is online. OCP4 requires a minimum of three control plane nodes and zero, two, or more worker nodes, plus a bootstrap node for installation that can be deleted after the cluster is online. The bootstrap and control plane nodes must run Red Hat Enterprise Linux CoreOS.

_03.1.1.3 Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) ships an installer that runs from the local computer. Installation of the TKG Management Cluster and application clusters happens through the installer GUI or via command-line directives that use a YAML configuration file. Clusters can only run on vSphere, Amazon EC2, or Microsoft Azure nodes. Downstream Kubernetes clusters are installed through the CLI only.

Upgrades are bound to the version of the TKGI CLI and require that users download and install virtual machines and base image templates before performing the cluster upgrade. A cluster upgrade replaces the virtual machines and must be performed on the management cluster first. The documentation lists multiple pages of prerequisites and post-upgrade re-registration tasks, which may make the process of upgrades a challenge for cluster administrators.

The exception to these rules is if the environment uses Tanzu Mission Control (TMC), a VMware SaaS offering for cluster management. If so, then TMC acts as the management cluster and can provision and manage downstream TKG clusters.

_03.1.1.4 Anthos

If you're already operating in GKE, installing Anthos is easy, and using Anthos with AWS is only incrementally more challenging. Anthos can use VMware infrastructure, physical infrastructure, or virtual machines from other providers for on-premises deployments. The on-prem installation process is manual and requires Internet connectivity. If you use your own infrastructure (VMware or bare metal), Anthos is 3x more expensive per vCPU than if you use GKE or AWS.

_03.1.2 Intuitive UI

Rancher	4
OpenShift	4
Tanzu	3
Anthos	4

_03.1.2.1 Rancher

Rancher's updated interface enables users to quickly deploy and begin managing Kubernetes clusters with almost no learning curve. It has been designed with a logic-based approach to soften and streamline complex Kubernetes concepts and workflows, making it possible to leverage Kubernetes in an organization without needing extensive training upfront.

_03.1.2.2 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.

_03.1.2.3 Tanzu

TKGI does not come with a management interface. Instead, VMware offers visual cluster management through a SaaS product called Tanzu Mission Control (TMC). TMC is part of VMware Cloud Services. TMC has a well-designed user interface that comes in two versions: Standard and Advanced. Standard is only available with the purchase of Tanzu Standard, and Advanced is available as a standalone purchase or comes with the purchase of Tanzu Advanced. TMC Standard contains a reduced feature set for security and policy management for role-based access control (RBAC), quotas, CIS benchmarks, and other important areas.

_03.1.2.4 Anthos

Anthos and Anthos GKE come with a clean and crisp user experience derived from Google's years of building excellent cloud applications providing existing users of Google Cloud a familiar, cohesive experience.

_03.1.3 Multi-cloud

Rancher	4
OpenShift	3
Tanzu	3
Anthos	2

_03.1.3.1 Rancher

Rancher presents the most options for where to deploy Kubernetes. It can provision hosted solutions across major cloud providers, including AWS, Azure, GCP, and vSphere. 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. Rancher also offers a Custom option for installing Kubernetes on any system provisioned via any other means, such as Ansible, Terraform, Puppet, Chef, etc.

_03.1.3.2 OpenShift

OpenShift provides installation guides for AWS, GCP, Azure, IBM Cloud, and VMware Cloud. Each cluster must be installed independent of the others and exists autonomously. There is no option to deploy OCP4 control plane or worker nodes across multiple clouds for a single cluster. All control plane nodes must run Red Had Enterprise Linux CoreOS. The only published solution for connecting workloads in different clusters uses Submariner, a project jointly developed by SUSE and Red Hat engineers. OpenShift's lack of Kubernetes and OS distribution agnosticism continues to pose a lock-in threat to its customers.

_03.1.3.3 Tanzu

Tanzu is a multi-cluster and multi-cloud solution that delivers a consistent operations experience. However, its strongest features, such as Tanzu Mission Control (TMC), are provided via SaaS-only options, and within those components, the best features are restricted to higher-cost tiers. This increases the risk of lock-in and makes it difficult to change platforms at a future date. It also only supports a subset of public cloud providers, which limits user choice.

_03.1.3.4 Anthos

Anthos can deploy clusters into Amazon EC2. Support for deploying clusters into Microsoft Azure has been "under development" since early 2020. AWS clusters offer a subset of the features available for clusters deployed into Google's own platform, making their "multi-cloud" offering somewhat disingenuous and instead appearing as a funnel for moving customers from other cloud providers to GKE to receive the full benefits that Anthos offers. All support services within Anthos are GCP-native services and will benefit from closer colocation of node resources.

_03.1.4 Multi-cluster

Rancher	4
OpenShift	2
Tanzu	3
Anthos	2

_03.1.4.1 Rancher

Rancher makes Kubernetes functionality available via its new UI and API. This, in turn, makes it possible for users to interact with Kubernetes without knowing where it is or how it is configured. In addition, SUSE 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. SUSE Rancher also utilizes Longhorn to abstract storage and enable cross-cloud application portability by presenting a standard interface to the underlying Kubernetes primitives.

_03.1.4.2 OpenShift

Red Hat customers can only manage multiple Kubernetes clusters through Red Hat Advanced Cluster Management for Kubernetes, an additional paid subscription service.

_03.1.4.3 Tanzu

Tanzu Kubernetes grid can deploy and support multiple clusters through the open source Cluster API. This includes on-premises clusters running in vSphere and clusters running on cloud infrastructure from Amazon EC2 or Microsoft Azure. In addition, Tanzu Mission Control can import existing clusters, which is the only way to support popular hosted Kubernetes solutions like Amazon EKS, Google GKE, or Microsoft AKS.

_03.1.4.4 Anthos

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

_03.1.5 Edge Support

Rancher	4
OpenShift	1
Tanzu	1
Anthos	2

_03.1.5.1 Rancher

K3s is a lightweight Kubernetes distribution originally developed 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 the most widely deployed Kubernetes distribution of its type.

Rancher's Fleet-powered continuous delivery and advanced observability capabilities allow for maximum cluster consistency and operational insight from core to cloud to edge. In addition, Fleet enables Rancher to support up to one million clusters from a single console with built-in security capabilities, running any CNCF-certified Kubernetes distribution.

_03.1.5.2 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 certified Kubernetes distribution. The company's idea of Kubernetes at the edge consists of deploying edge data centers running OpenShift, which manages 'dumb' endpoints. The advantages of running Kubernetes clusters on the endpoints themselves is not something that they leverage.

_03.1.5.3 Tanzu

The Tanzu edge story is built around vSphere Remote Office Branch Office (ROBO), in which a central vCenter data center deployment manages edge locations that run vSphere with a 2-node vSAN cluster. These environments, in turn, run Tanzu Kubernetes Grid and are remotely managed by the Tanzu Mission Control and Tanzu Observability SaaS solutions.

The proposed solution does not consider resource-constrained environments or a management solution that does not include additional paid VMware services.

_03.1.5.4 Anthos

The Anthos edge story used to revolve around 5G connectivity to Google-managed nodes in a telco facility, but they stopped promoting this in early 2021. Instead, they now direct users to deploy Anthos on-premises and manage their own connectivity and backhaul. Although Anthos can run on small form-factor nodes such as an Intel NUC, the bare-metal requirement for Internet connectivity rules out resource-constrained environments or environments with limited connectivity. The tripling in cost for running Anthos on bare-metal also diminishes the value of running Anthos in the large edge environments of the future.

_03.1.6 Hosted Kubernetes Support

Rancher	4
OpenShift	1
Tanzu	2
Anthos	2

_03.1.6.1 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 2.6 gives operators full lifecycle management of clusters from EKS, AKS, and GKE from a single pane of glass. Rancher can now import, provision, upgrade and configure and secure clusters across all three environments directly using SUSE Rancher's updated unified, intuitive user experience. Additionally, Rancher-managed Amazon EKS, Microsoft AKS, and Google GKE deployments support templating and CIS benchmark scanning to maintain high security and minimize configuration drift between clusters.

_03.1.6.2 OpenShift

Red Hat OpenShift is a single-cluster solution with no support for hosted Kubernetes solutions from any provider. For an additional fee, Red Hat Advanced Cluster Management for Kubernetes (ACM) can import and manage pre-built clusters on EKS, GKE, AKS, and IBM Cloud. However, it cannot create, upgrade, or destroy a cluster on these platforms.

_03.1.6.3 Tanzu

Tanzu Mission Control supports the management of hosted Kubernetes clusters but cannot deploy or delete them. Instead, clusters must be created directly with the hosting provider and then imported.

_03.1.6.4 Anthos

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

_03.1.7 Bare Metal, OpenStack & vSphere

Rancher	4
OpenShift	3
Tanzu	2
Anthos	3

_03.1.7.1 Rancher

Rancher ships with drivers for deployment into common cloud providers such as AWS, GCP, Azure, DigitalOcean, and Rackspace. Rancher also 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. For environments that do not utilize Docker, RKE2 and K3s ship with containers.

_03.1.7.2 OpenShift

OpenShift supports deployment on bare metal and vSphere.

_03.1.7.3 Tanzu

Tanzu deploys Kubernetes clusters on vSphere infrastructure. vSphere can also deploy non-conformant Pods directly on vSphere-managed ESXi hosts through proprietary VMware extensions that replace the container engine and the standard Kubernetes kubelet.

_03.1.7.4 Anthos

Anthos supports deployment within a vSphere environment or on bare metal or virtual machines.

_03.1.8 Import Existing Clusters

Rancher	4
OpenShift	3
Tanzu	3
Anthos	2

_03.1.8.1 Rancher

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

_03.1.8.2 OpenShift

Red Hat ACM (an additional paid service) can import existing OpenShift clusters in different substrates and locations.

_03.1.8.3 Tanzu

Tanzu Mission Control (TMC) can import clusters from external providers. TMC is a SaaS-only solution.

_03.1.8.4 Anthos

While Anthos doesn't play up the ability to import or register existing clusters and instead tries to move you to deploy fully managed solutions on GKE or GKE-on-prem, it does include the ability to register and interact with existing Kubernetes clusters. Anthos prices these attached clusters the same as clusters deployed within GCP. Although you can attach any conformant Kubernetes cluster, Anthos features are only available on a small list of "approved" cluster types. RKE, one of Rancher's CNCF-certified Kubernetes distributions, is included in this list.

_03.1.9 High Availability

Rancher	4
OpenShift	4
Tanzu	3
Anthos	2

_03.1.9.1 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.

The provider delivers high availability and node healing at the virtual machine level, where a solution like AutoScaling Groups (ASGs) and CloudWatch will recreate unresponsive virtual machines.

_03.1.9.2 OpenShift

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

_03.1.9.3 Tanzu

Tanzu's deployment of Kubernetes has two default options – development or production. The development cluster has a single-node control plane, and the production cluster has a 3-node control plane. When operating in a cloud environment, the production cluster defaults to placing 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 control plane nodes will incur charges for inter-AZ communication. This can be overridden at install time.

_03.1.9.4 Anthos

High availability within Anthos varies by deployment type. For vSphere clusters, the admin cluster does not have an HA control plane. User clusters can have one or three (HA) control plane nodes managed by the admin cluster. For bare-metal clusters, the admin cluster can have an HA control plane. In both of these deployment scenarios, the control plane nodes for the user cluster are worker nodes within the admin cluster. During the time that an admin cluster is down, no user cluster can be managed.

For AWS clusters, there is a management service that controls the creation and management of user clusters in AWS. One management service is required for each VPC where user clusters run. This service runs in a single availability zone (AZ) and is not an HA service. Therefore, user clusters can have multiple control plane nodes.

For GKE clusters, there is no admin cluster or management service, and GKE is presumed to be HA on its own.

This lack of a unified standard in how Anthos handles high availability increases the cognitive load of the operations staff, despite the standards for high availability in Kubernetes being standardized throughout the rest of the industry.

_03.1.10 Load Balancing

Rancher	4
OpenShift	2
Tanzu	2
Anthos	3

_03.1.10.1 Rancher

Clusters installed by Rancher on compute instances include the NGINX Ingress Controller for load balancing. If SUSE Rancher deploys a cluster on a hosted provider that doesn't install an ingress controller by default (such as EKS), the SUSE 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.

_03.1.10.2 OpenShift

OpenShift uses a proprietary software load balancer resource called a Route. It behaves like an Ingress, but it only exists within OpenShift and is not portable to other Kubernetes clusters. OpenShift Ingress Controllers are managed by the Ingress Operator. It deploys a default HAProxy-based load balancer to handle both Route and ingress requests. OpenShift pollutes the API space by placing Route (an OpenShift-specific resource) under "v1," making it appear to be a common Kubernetes resource. When a user creates an Ingress (a standard Kubernetes resource), OpenShift uses the instruction to create a Route instead. This crosstalk makes it more challenging to utilize the same Kubernetes manifests in a non-OpenShift cluster.

_03.1.10.3 Tanzu

Installations in EC2 receive a Classic Load Balancer. Installations in Azure receive an Azure load balancer.

Installations of Tanzu Kubernetes Grid Integrated Edition (TKGI) on vSphere or VMware Cloud on AWS receive the NSX Advanced Load Balancer (ALB) Essentials Edition by default. This is a Layer 4 load balancing solution that includes a Kubernetes operator to manage the lifecycle of load balancing and ingress resources within the Kubernetes cluster. Unfortunately, the NSX ALB requires a separate controller and cluster configuration that adds additional proprietary knowledge workload to the operations team. The Essentials Edition offers a limited set of features that are sufficient for Kubernetes. Still, if a single deployed environment wishes to use advanced features of the Avi (NSX ALB) controller, every connected environment must be relicensed to support the Advanced or Enterprise controller features.

_03.1.10.4 Anthos

The solution for Anthos in vSphere and on bare metal is to use the Seesaw load balancer, which is derived from the open source LVS project. Seesaw requires dedicated VMs, 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 most likely what forces them to use a sub-par solution like Seesaw. If you wanted to use any other load balancing solution for Kubernetes, the GKE architecture might prevent it.

Anthos in GKE and AWS use the load balancers available for those cloud environments.

_03.1.11 Centralized Audit

Rancher	4
OpenShift	3
Tanzu	2
Anthos	1

_03.1.11.1 Rancher

Rancher has updated its logging capabilities and now utilizes Banzai Cloud Logging operator to power logging across the platform. Logging is easily deployed across each cluster in Rancher via Cluster Explorer, completely removing the need for any manual configuration. The logging operator utilizes Fluent Bit to query the Kubernetes API and enriches logs with metadata on pods. Fluentd then filters, transfers, and logs to multiple outputs. Rancher also supports the standard API logging available from Kubernetes.

_03.1.11.2 OpenShift

OpenShift can log all interactions 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.

_03.1.11.3 Tanzu

TKG ships with Fluent Bit for collecting and forwarding logs. Logs can go to an Elasticsearch, Kafka, Splunk, syslog, or HTTP endpoint. It also exposes some metrics to Prometheus and Grafana. The deployment and configuration of Fluent Bit is a manual process that must happen on each Kubernetes cluster.

_03.1.11.4 Anthos

Anthos currently supports disk-based logging for GKE on-prem (vSphere) and bare metal, using the functionality already present in Kubernetes. These clusters can also send log data to Google Cloud for long-term storage. GKE clusters, however, only use Cloud Audit Logging. Anthos clusters running on AWS do not have Cloud Audit Logging, but presumably, a cluster administrator can manually configure disk-based audit logging by following the Kubernetes documentation.

Cloud Audit Logging for GKE on-prem has been a preview feature since December 2019 and offers fewer features than those available for GKE.

_03.1.12 Self-service Provisioning

Rancher	4
OpenShift	2
Tanzu	2
Anthos	0

_03.1.12.1 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.

When Rancher is used with RKE, the admin can also use RKE templates to standardize cluster configurations. Rancher will guarantee that every cluster it provisions from an RKE template is uniform and consistent in the way it is produced.

_03.1.12.2 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. However, Red Hat ACM (an additional paid service) can deploy OpenShift clusters in multiple environments.

_03.1.12.3 Tanzu

Authorized users can deploy, configure, and interact with TKG clusters using the vSphere plugin for kubectl. Self-service deployments are also available through Tanzu Mission Control (TMC).

_03.1.12.4 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 access it according to Kubernetes RBAC boundaries.

_03.1.13 Private Registry and Image Management

Rancher	4
OpenShift	4
Tanzu	4
Anthos	2

_03.1.13.1 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.

_03.1.13.2 OpenShift

OpenShift contains full support for private registries and includes a local registry 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 ocCLI to create ImagePullSecrets and optionally attach them to service accounts.

_03.1.13.3 Tanzu

vSphere with Tanzu embeds a central Harbor registry that can be enabled on the management cluster. Once configured, all downstream clusters can use it for private images.

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 that will use them.

_03.1.13.4 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 that will use them. Google provides the Google Container Registry as part of the GCP service offering and encourages its use in Anthos clusters. This is an additional paid service.

_03.1.14 Cluster Upgrades and Version Management

Rancher	4
OpenShift	4
Tanzu	2
Anthos	2

_03.1.14.1 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. SUSE 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 also enables upgrades in air-gapped environments with Helm template options.

_03.1.14.2 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.

_03.1.14.3 Tanzu

TKGI supports cluster upgrades from the CLI. Upgrades are bound to the version of the TKG CLI and require that users download and install virtual machines and base image templates before performing the cluster upgrade. A cluster upgrade replaces the virtual machines and must be performed on the management cluster first. The documentation lists multiple pages of prerequisites and post-upgrade re-registration tasks, which may make the process of upgrades a challenge for cluster administrators. It is not clear from the documentation if user-deployed self-service clusters will require that a cluster administrator perform the upgrade. However, the dependency on the management server and the number of steps needed implies that upgrades are not user-friendly.

Clusters deployed through Tanzu Mission Control can be upgraded through that interface.

_03.1.14.4 Anthos

Anthos changed its upgrade process for GKE on-prem (vSphere) in 1.3.2, then again in 1.7. The current process for 1.7 or later clusters is to upgrade the admin workstation, then the user clusters, and finally (optionally) the admin cluster.

For Anthos on AWS, users must first upgrade the management service, followed by user clusters.

For Anthos on bare metal, users must upgrade the admin cluster, followed by user clusters. User clusters must not be more than one minor version number behind the new version of the admin cluster before upgrading the admin cluster. The documentation does not say what will happen to those clusters if they deviate from this requirement. Upgrades are restricted to the single supported cluster version in the bmctl utility used to manage clusters.

The inconsistency in these upgrade procedures increases the cognitive load for admins of multi-cluster environments that use different platforms, and as a result, mistakes are more likely to occur.

_03.1.15 Storage Support

Rancher	4
OpenShift	3
Tanzu	4
Anthos	3

_03.1.15.1 Rancher

Rancher created and contributes to 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.

_03.1.15.2 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, and NooBaa, a multi-cloud software-defined storage layer that Red Hat acquired in 2018. In addition, Red Hat maintains NooBaa, Ceph, and GlusterFS and can therefore implement OpenShift-specific extensions for these solutions.

_03.1.15.3 Tanzu

VMware vSphere with Tanzu workloads can use storage from vSphere. Tanzu Kubernetes Grid clusters ship with storage classes for Amazon EBS, Azure Disk, or vSphere Cloud Native Storage (CNS), along with NFS and iSCSI. TKG supports any CSI-compliant storage driver.

_03.1.15.4 Anthos

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

_03.1.16 Arm Support

Rancher	4
OpenShift	0
Tanzu	0
Anthos	0

_03.1.16.1 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.

_03.1.16.2 OpenShift

OpenShift does not support deployment on Arm processors.

_03.1.16.3 Tanzu

Tanzu does not support deployment on Arm processors.

_03.1.16.4 Anthos

Anthos does not support deployment on Arm processors.

_03.1.17 Airgap Support

Rancher	4
OpenShift	3
Tanzu	3
Anthos	0

_03.1.17.1 Rancher

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

_03.1.17.2 OpenShift

OpenShift supports air gap installations on user-provisioned infrastructure only. It does not support air gap installations on automatically deployed cloud infrastructure.

_03.1.17.3 Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) supports airgap installations. Before performing the installation, an internet-connected workstation must run a script to pull images from the Internet and populate a private registry server within the air-gapped environment. Once this step is complete, the operator can disconnect the Internet connection and deploy the cluster.

_03.1.17.4 Anthos

Anthos has no documentation for deploying into an airgap environment. The closest they come to a traditional airgap deployment is a guide for deploying GKE Private Clusters that use private address space and don't have Internet routing enabled. All non-GKE Anthos clusters must connect back to Google Cloud, which means they must have Internet connectivity.

_03.1.18 Etcd Backup and Restore

Rancher	4
OpenShift	2
Tanzu	3
Anthos	2

_03.1.18.1 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 performing a new Rancher installation. Upon completion, all remote Kubernetes clusters will reconnect to the new cluster.

_03.1.18.2 OpenShift

Backup of an OCP4 cluster requires manually logging into a control plane node 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.

_03.1.18.3 Tanzu

Tanzu recommends Velero, an open source backup solution maintained by VMware. Operators can install Velero and back up cluster metadata, workload configuration, and workload data. These backups can be restored into a new cluster. For example, Velero can back up user workloads and data on a TKG management cluster, but it cannot back up the cluster state itself.

_03.1.18.4 Anthos

Google provides limited support for backing up and restoring a cluster's etcd datastore and encourages users to 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 as part of standard operating procedures.

_03.2 Security, Policy & User Management

_03.2.1 Active Directory and LDAP Support

Rancher	4
OpenShift	4
Tanzu	4
Anthos	3

_03.2.1.1 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 occurs at the Global level, after which users and groups from the provider are available for assignment to RBAC roles and downstream clusters.

_03.2.1.2 OpenShift

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

_03.2.1.3 Tanzu

Tanzu Kubernetes Grid includes the open source project Pinniped, which enables authentication against providers that support LDAP and OIDC.

_03.2.1.4 Anthos

Anthos supports OpenID Connect (OIDC) in all Anthos cluster types. This can perform authentication against any OIDC provider, with guides provided for Active Directory Federation Services and Google. Headless systems are unsupported. Users must use a browser-based workflow to perform authentication.

_03.2.2 Pod and Security Policies

Rancher	4
OpenShift	3
Tanzu	2
Anthos	2

_03.2.2.1 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. Rancher also ships with OPA Gatekeeper as the industry standard open source solution for policy based management for Kubernetes clusters.

_03.2.2.2 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. OpenShift includes support for network policies and multiple pod networks for traffic isolation. It also provides operators with compliance (via the open source project OpenSCAP) and file integrity (via the open source project AIDE).

_03.2.2.3 Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) requires native PodSecurityPolicies (PSP) to deploy workloads in a Kubernetes cluster. However, this can adversely affect deployments from Helm or operators that either do not have a PSP configured or ask for a greater level of access than a default PSP provides. In addition, Pods running in vSphere are described as "non-conformant" and do not appear to support PodSecurityPolicies.

TKGI uses Antrea (default) or Calico for networking. Both support Kubernetes native NetworkPolicies, and both also have their own advanced network policy extensions.

Tanzu Mission Control (TMC) supports both PSPs and security policies enforced by the Open Policy Agent (OPA) Gatekeeper. Despite being open source, VMware only includes OPA Gatekeeper with the Advanced and higher editions of TMC.

_03.2.2.4 Anthos

Anthos supports Kubernetes NetworkPolicy resources. Clusters that run in GKE can use the Dataplane v2, which supports eBPF with Cilium and exposes the CiliumNetworkPolicy for additional control. Anthos does not directly support PodSecurityPolicies and instead provides a proprietary resource called a Policy Controller that implements similar functionality. Kubernetes network security features differ significantly between GKE, vSphere, bare metal, and AWS.

_03.2.3 Configurable Adherence to CIS Security Benchmarks

Rancher	4
OpenShift	3
Tanzu	2
Anthos	2

_03.2.3.1 Rancher

Rancher maintains a hardening guide and self-assessment that references CIS benchmarks with specific user actions to satisfy the requirements. SUSE Rancher supports CIS scans on any Kubernetes cluster, including hosted Kubernetes providers such as EKS, AKS, and GKE. The CIS scan tool can be easily accessed in the Rancher UI via Cluster Explorer and can be deployed using a Helm chart. Conveniently, it can also be installed independent of SUSE Rancher.

_03.2.3.2 OpenShift

CIS benchmarks are available for OpenShift under the CIS Kubernetes Benchmarks.

_03.2.3.3 Tanzu

Security scanning for adherence to the CIS Benchmarks for Kubernetes is available through Tanzu Mission Control (TMC) or by using the Compliance Scanner for VMware Tanzu (formerly the Pivotal Compliance Scanner). Unfortunately, there is no hardening guide available for Tanzu Kubernetes Grid or clusters managed by Tanzu Mission Control.

_03.2.3.4 Anthos

Google provides documentation on how Anthos scores against CIS benchmarks, but it does not offer a means to perform scans automatically. Instead, they direct users to manual scans using the open source kube-bench utility. Google offers a custom benchmark for GKE derived from the CIS Kubernetes Benchmark and accounts for the shared responsibility of the GKE environment. Google provides guidance for Anthos clusters running under vSphere, but they do not offer any advice or assessment of Anthos clusters running in AWS or on bare metal.

_03.2.4 RBAC Policies

Rancher	4
OpenShift	2
Tanzu	3
Anthos	2

_03.2.4.1 Rancher

Rancher exposes all of Kubernetes RBAC and then enables the configuration and maintenance of RBAC policies at the Global level within the user interface. 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. Furthermore, user templates can inherit from existing templates to create a hierarchy of easily maintained permissions.

_03.2.4.2 OpenShift

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

_03.2.4.3 Tanzu

Tanzu Mission Control (TMC) contains RBAC configuration for the organization, cluster group, and namespace objects, although these don't directly translate to Kubernetes RBAC entities. Clusters deployed by Tanzu (TKG) support the standard Kubernetes entities with extensions that tie back to vCenter Single Sign-On users or the configured OIDC connector for the cluster.

_03.2.4.4 Anthos

Anthos supports Kubernetes RBAC but does not provide a user interface for configuring it or applying it globally across user clusters. Google has a beta implementation of Google Groups for applying group RBAC to clusters, but this proprietary solution has forced some community members to create additional scripts and cluster synchronization workloads to bypass its shortcomings.

_03.3 Shared Tools & Services

_03.3.1 Application Catalog

Rancher	4
OpenShift	4
Tanzu	2
Anthos	1

_03.3.1.1 Rancher

Rancher's Application Catalog extends Helm to provide users with an easily understood form-based installation process for applications. In addition, it integrates with any external Helm repository, giving users the means to install applications from either system. Helm 3.0 is required for inclusion in Rancher's application catalog.

_03.3.1.2 OpenShift

OpenShift integrates with Red Hat's Operator Hub, a curated list of applications that meet Red Hat's requirements for inclusion. OpenShift also includes a developer perspective with resources for interacting with Helm charts. Users can install applications from the Developer Catalog, and administrators can add new Helm repositories to the Developer Catalog via the CLI.

_03.3.1.3 Tanzu

The Tanzu Application Catalog (TAC) is an additional proprietary paid service through which operators can create an application bundle that the TAC monitors, updates, tests, and deploys to a local registry for use by local resources. This service has a basic and an advanced version available as a subscription.

_03.3.1.4 Anthos

Anthos Kubernetes clusters support application deployment via Helm. Google also offers the Google Cloud Marketplace, which has a section for Kubernetes apps. This claims that the apps can be deployed to GKE or to "Kubernetes clusters on-premises or in third-party clouds," but each application lists a different supported environment.

A random sampling showed documentation for deploying to non-GKE environments to consist of "clone the GitHub repository and read the documentation." GKE deployment options appear to make their own new cluster, stating, "Your app will use compute instances managed in a logical grouping called a 'cluster,' which will be configured in a way that's great for getting started with Kubernetes." This information suggests an onerous and manual process for any non-GKE Anthos application deployment.

_03.3.2 Provision with Terraform / Ansible / Others

Rancher	4
OpenShift	2
Tanzu	2
Anthos	4

_03.3.2.1 Rancher

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

_03.3.2.2 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.

_03.3.2.3 Tanzu

It is not possible to deploy a Tanzu Kubernetes Grid (TKG) management cluster through Terraform. However, operators can deploy a TKG guest cluster and connect it to vSphere using the K8s Provider for Terraform. This is different than deploying a management cluster or designating the vSphere supervisor cluster as the TKG management cluster, and although possible, it is not a supported deployment method.

_03.3.2.4 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.

_03.3.3 CI/CD Capabilities

Rancher	4
OpenShift	4
Tanzu	2
Anthos	4

_03.3.3.1 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 leverage Rancher Continuous Delivery (Rancher CD) which incorporates the use of Rancher project Fleet. Rancher CD is a GitOps-based approach that allows users to manage their cluster workflows effectively at scale. Any changes made to clusters go through the centralized Fleet controller, which contains access to the Git repository and the configurations and assignments of clusters. This ensures the correct code is applied to the correct application on the right cluster. Fleet is included with Rancher and can also be installed on any Kubernetes cluster via Helm.

_03.3.3.2 OpenShift

OpenShift will work with any CI/CD system that works with Kubernetes. In addition, it ships with features for building container images within the cluster, a CI/CD system based on the open source project Tekton, and a GitOps workflow based on the open source project Argo CD.

_03.3.3.3 Tanzu

VMware has bundled several open source solutions into the paid Tanzu Build Service that allows developers to use any Kubernetes cluster (including those not from Tanzu) for building container images. They also bundle the open source Concourse CI engine as Concourse for VMware Tanzu. Tanzu Kubernetes clusters will work with any CI/CD system that works with Kubernetes. It does not offer an integrated GitOps solution.

_03.3.3.4 Anthos

GKE includes strong support for CI/CD solutions including GitLab, Knative, Jenkins, and others, although the core solutions they implement are open source and will work in any Kubernetes cluster.

_03.3.4 Advanced Monitoring

Rancher	4
OpenShift	4
Tanzu	2
Anthos	2

_03.3.4.1 Rancher

Rancher ships with basic monitoring activated by default. Cluster admins can enable advanced monitoring with a single click in the SUSE Rancher UI. This deploys Prometheus and Grafana at the project and cluster levels and installs pre-configured 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.

_03.3.4.2 OpenShift

OpenShift ships with Prometheus and Grafana activated by default, with pre-configured alerts and dashboards. As of v4.7, cluster admins can activate monitoring of user workloads from within the same stack.

_03.3.4.3 Tanzu

Tanzu doesn't include monitoring or visualization by default. VMware's recommended solution for additional monitoring of Tanzu is to deploy VMware Wavefront, an additional paid service. They also provide proprietary extensions for installing a signed binary of the open source projects Prometheus and Grafana.

_03.3.4.4 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 are add-on components with their own pricing.

_03.3.5 Alerts and Notifications

Rancher	4
OpenShift	4
Tanzu	1
Anthos	2

_03.3.5.1 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.

_03.3.5.2 OpenShift

OpenShift allows administrators and privileged users to create and manage alerts for the platform and user workloads. By default, alerts are only visible in the UI, but OpenShift supports sending alerts to PagerDuty, Slack, Email, or Webhook destinations.

_03.3.5.3 Tanzu

Alerts and notifications are available via VMware Wavefront, a separate paid-for monitoring solution, or via manual configuration of the Alert Manager component of Prometheus.

_03.3.5.4 Anthos

Anthos enables alerting for clusters and service mesh via Google Cloud Monitoring. Google Cloud Monitoring is its own paid service. Users can also deploy the open source Prometheus solution with its Alert Manager. This is a standard pattern for Kubernetes.

_03.3.6 External Log Shipping

Rancher	4
OpenShift	4
Tanzu	2
Anthos	3

_03.3.6.1 Rancher

Rancher has updated its logging capabilities and now utilizes Banzai Cloud Logging operator to power logging across the platform. Fluent Bit is used to aggregate logs and Fluentd is used for filtering messages and routing them to outputs. Installing logging for a Rancher managed cluster is fast and easy, requiring only a single click from within Cluster Explorer. Administrators can determine log visibility via the two roles available; logging-admin which gives full access to namespaced flows and outputs or logging-view , which gives *view* access only to namespaced flows, outputs and cluster flows

_03.3.6.2 OpenShift

Administrators can deploy the OpenShift Elasticsearch Operator and the OpenShift Logging Operator. Once installed, logs are collected, stored, and visualized using Fluentd, Elasticsearch, and Kibana. Logs can also be forwarded via Fluentd, syslog, or a proprietary Red Hat API protocol. Log visibility follows RBAC permissions for the viewer.

_03.3.6.3 Tanzu

Tanzu Kubernetes Grid (TKG) clusters support log shipping via Fluent Bit or as a component of VMware Wavefront (a paid add-on). Despite being open source, VMware installs Fluent Bit as a proprietary TKG extension.

_03.3.6.4 Anthos

Anthos Kubernetes clusters can use any logging or monitoring solution that works with Kubernetes, including open source solutions like Fluent Bit and third-party solutions like Elasticsearch, Splunk, and Datadog. Their documentation encourages the use of their paid Cloud Operations Suite (formerly known as Stackdriver).

_03.3.7 Windows Container Support

Rancher	4
OpenShift	4
Tanzu	0
Anthos	3

_03.3.7.1 Rancher

Rancher supports Windows worker nodes as a custom cluster and uses RKE to install Kubernetes on existing nodes. Windows clusters provisioned with Rancher must contain Linux and Windows nodes. The Kubernetes control plane can only run on Linux nodes, and the Windows nodes can only have the worker role. Windows nodes can only be used for deploying workloads and can only be added if Windows support is enabled when the cluster is created.

_03.3.7.2 OpenShift

OpenShift (OCP4) includes production support for using Windows servers in Kubernetes clusters and deploying Windows containers under management of an OpenShift control plane.

_03.3.7.3 Tanzu

Tanzu Kubernetes Grid (TKG) is the rebranded name for VMware Enterprise PKS (Pivotal Container Service). Although Windows container support on PKS was in beta in Dec 2019, there is no information in the TKG documentation about deploying Windows workers or Windows container workloads. In addition, references to beta support in TKGI v1.8 documentation have been removed from the v1.11 documentation. There are no other references or indications found to support Windows containers in the v1.11 documentation.

_03.3.7.4 Anthos

GKE and GKE on-prem (VMware) support Windows container workloads, but Anthos on AWS does not. Anthos Migrate includes support for migrating Windows VMs into containers running on Windows node pools.

_03.3.8 Integrated Service Mesh Support

Rancher	4
OpenShift	3
Tanzu	1
Anthos	4

_03.3.8.1 Rancher

Rancher delivers upstream Istio as a single component, Istiod, which combines Pilot, Citadel, Galley, and the sidecar injector. Node Agent functionality has been merged into istio-agent.

_03.3.8.2 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.

_03.3.8.3 Tanzu

VMware sells Tanzu Service Mesh (TSM), a proprietary mesh built on top of NSX and available through their VMware Cloud Services platform.

_03.3.8.4 Anthos

Anthos includes Google Service Mesh (GSM), which is a modified version of Istio. While it may experience challenges similar to those faced by OpenShift in their modified version, Google currently controls Istio development and is unlikely to fall behind.

_03.3.9 Enterprise SLA

Rancher	4
OpenShift	2
Tanzu	2
Anthos	2

_03.3.9.1 Rancher

Rancher provides an enterprise subscription covering 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 hours or 24x7 support. In addition, Rancher's subscription is priced by node, independent of the number of cores.

_03.3.9.2 OpenShift

Red Hat provides support for OpenShift and the Red Hat software stack. However, many of the OpenShift components cannot be modified or used outside Red Hat's parameters without invalidating support. In addition, Red Hat's support model is priced by virtual core, making every upgrade of the customer's environment increase support costs.

_03.3.9.3 Tanzu

VMware offers community support (unpaid), Premium Support (included with a subscription or license), and a higher tier that consists of a dedicated Technical Account Manager (TAM) for "faster resolution and technical guidance." Premium Support includes 24x7 access for Severity 1 issues.

_03.3.9.4 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.

_03.3.10 Community Traction

Rancher	4
OpenShift	3
Tanzu	0
Anthos	1

_03.3.10.1 Rancher

Rancher has a thriving community of users and contributors across all its products and projects. With more than 100 million downloads and over 47,000 deployments, it is the most popular open source solution for deploying and managing Kubernetes clusters.

_03.3.10.2 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.

_03.3.10.3 Tanzu

It isn't easy to measure the community traction of Tanzu because its value largely applies to existing VMware customers. The entry point for Tanzu Kubernetes Grid is a vSphere or VMware Cloud deployment. The origins of TKG are Pivotal Container Service (PKS), whose origins, in turn, are from Cloud Foundry, a platform originally developed and spun off by VMware. VMware re-acquired Pivotal in 2019 after Pivotal was unable to sell PKS on its own. Only after rebranding it to Tanzu Kubernetes Grid and connecting it directly to vSphere were they able to find an audience for it. In addition, its structure and disparate product lines make it a solution designed to take existing VMware customers and lock them even more tightly to VMware's products.

_03.3.10.4 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. Google hopes the support for bare metal and edge deployments will expand their market share, but it's not clear if the community will value paying for the privilege of connecting large numbers of edge deployments to Google Cloud Console.

04 About the Author

Rancher Government Solutions and their parent company SUSE are global leaders in innovative, reliable, and enterprise-grade open source solutions. RGS, Rancher and SUSE specialize in Enterprise Linux, Kubernetes management, and edge solutions, and the companies collaborate with partners and communities around the globe, empowering them to innovate everywhere – from the data center, to the cloud, to the edge and beyond.

In 2020, SUSE acquired Rancher Labs and Rancher Government Solutions, the team behind successful open source products including:

- Rancher - the world's most popular enterprise-grade Kubernetes management platform.
- RKE - a simple, lightning-fast Kubernetes installer that works everywhere;
- RKE2 – is a fully conformant Kubernetes distribution focused on security and compliance
- Fleet – an open source project built to help manage millions of Kubernetes clusters at scale
- K3s – a lightweight production-grade Kubernetes distribution built for embedded systems and the edge. Rancher invented K3s and donated it to the CNCF in August, 2020.
- Longhorn - a powerful cloud-native distributed storage platform for Kubernetes that can run anywhere. Rancher invented Longhorn and donated it to the CNCF in October, 2019.

All of SUSE and Rancher's solutions remain open source after the acquisition, with support from a vibrant, active community.

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.

Rancher Government Solutions was specifically created to address the unique security and operational needs of the Federal Government and US Military. Most of our employees hold security clearances are currently supporting programs across the Department of Defense, Intelligence Community and Civilian Agencies.

RGS is dedicated to helping the US Government run Kubernetes securely everywhere.

To learn more about Rancher Government Solutions please visit:

www.rancher government.com or call: (844) RGS-7779

05 Glossary

_05.1 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 of 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 essential 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. Therefore, 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, collecting statistics, or creating monitoring alerts for unwanted API calls.
- **Self-service Provisioning**
  - Developers must have self-service access to one or more Kubernetes clusters with the correct levels of isolation in place so only members with the correct 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. Therefore, a Kubernetes management platform should support rolling upgrades of clusters, such that the cluster and the cluster API are always available even while the cluster is being upgraded. Additionally, it will provide the ability to roll back to the 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 critical 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.

_05.2 Security Policy & User Management

- **Active Directory and LDAP Support**
  - Out of the box, Kubernetes authentication is not very user-friendly for end-users. Therefore, 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 specifies 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 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.

_05.3 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 be continually monitored to detect issues that might affect cluster and application availability for users. Therefore, 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 into 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 parsing the log data is more challenging without a central point of aggregation. 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**
  - Windows remains one of the most popular operating systems in datacenters, with countless workloads running on its many versions. Whether the requirement is to quickly create and tear down dev or test environments or lift and shift legacy applications to the cloud, support for Windows containers within your Kubernetes management platform is required 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. Instead, 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.

06 Legal Statements

_06.1 Copyright Notice

_06.2 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.

_06.3 Note from the Authors

The views in this whitepaper are those of Rancher Government Solutions. 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:

info@ranchergovernment.com

visit us at www.ranchergovernmnet.com

or call us at (844) RGS-7779.