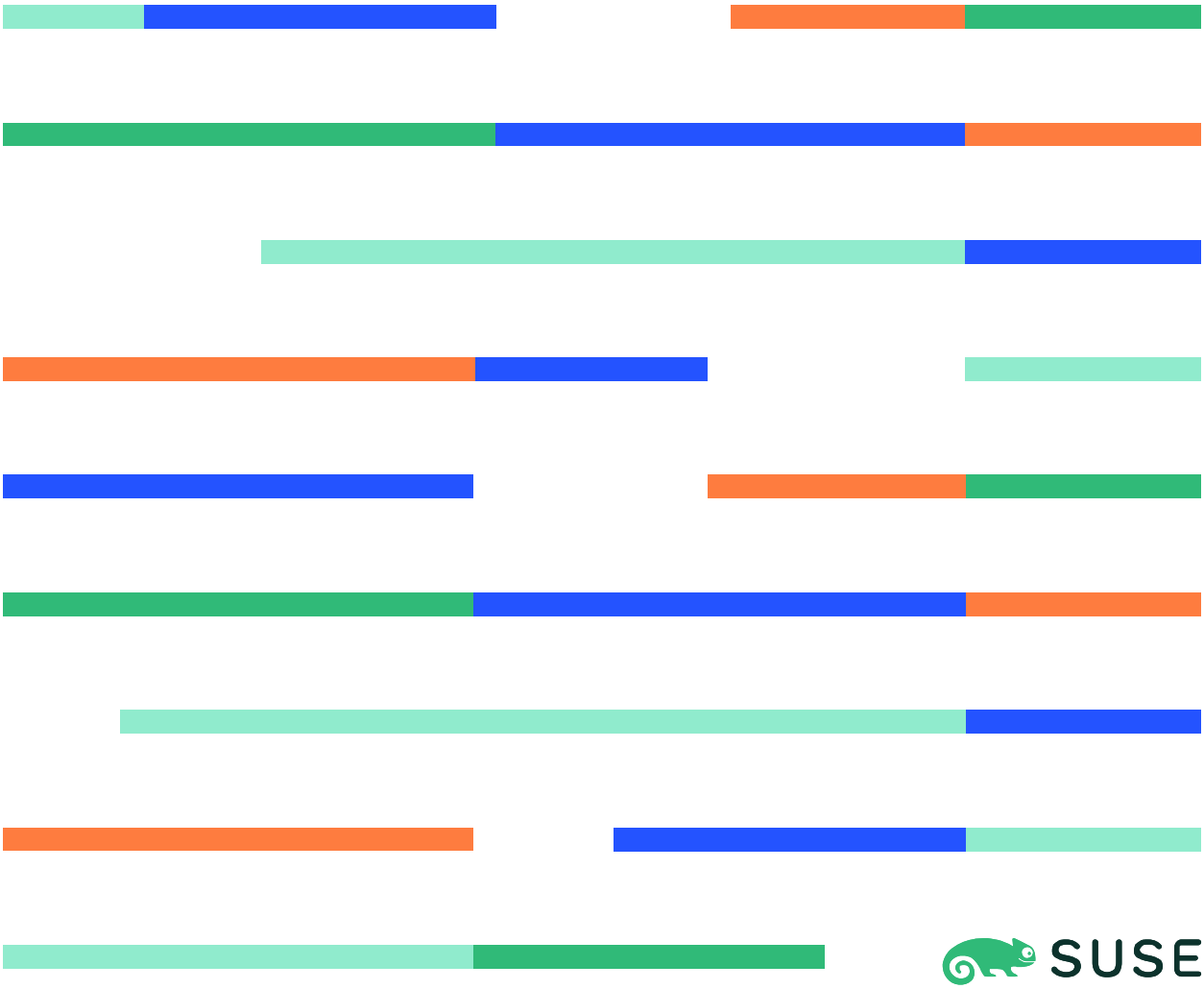
Last Updated: Dec 2022

A Buyer's Guide to Enterprise Kubernetes Management Platforms

Red Hat OpenShift 4.9, VMware Tanzu 1.4, Google Anthos 1.10, and Rancher 2.7



SUSE

Contents

1 Executive Summary

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 potential of containers and Kubernetes was evident when, in 2020, Gartner[2] predicted that more than 75% of worldwide organizations would run containerized applications in production by 2022. Confidence of this prediction demonstrated the value of cloud native technologies for developers, who will always look for solutions to help them build applications quickly without compromising 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

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

In December 2020, open source technology leader SUSE acquired Rancher Labs and its flagship product, Rancher. Rancher remains available as an 100% open source project that anyone can use, with Rancher Prime as the commercially supported and fortified version. With the additional that SUSE has brought, Rancher's growth has accelerated, with downloads now exceeding 102 million.

Commercially, Rancher Prime has extended its success in the enterprise market by maintaining double digit growth year on year. Its latest release, Rancher 2.7 is a continuation of acquisition's success and includes new extension capabilities and performance updates to help users get more out of the platform and strengthen their 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

[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 – Download Report

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

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 to remain competitive in the market.

In the last three years, VMware has acquired several 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 4.9 (OpenShift/OCP4) with Red Hat Advanced Cluster Management for Kubernetes (RHACM), 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 Rancher.

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

2 Capabilities Summary

2.1 Overview

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

- 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.

2.2 Cluster Operations

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

Feature	Rancher	OpenShift	Tanzu	Anthos
Install and Operations	4	3	3	2
Intuitive UI	4	3	3	3
Hosted & Managed Services	3	3	1	2
Multi-Cluster Management	4	3	2	2
Edge Support	4	3	2	1
Integrated Public Cloud Support	4	2	2	2
Bare Metal, OpenStack & vSphere	4	3	2	2
Import Existing Clusters	4	3	3	3
Centralized Audit	4	3	3	2
Cluster Self-Service Provisioning	4	4	4	1
Private Registry & Image Management	4	4	4	2
Cluster Upgrades & Version Management	4	4	2	2
Storage Support	4	4	4	3
Arm Support	4	2	1	0
Airgap Support	4	3	2	0
Etcd Backup and Restore	4	2	3	1

2.3 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	2
Pod and Network Security Policies	4	3	2	2
Configurable Adherence to CIS	4	3	2	2
Global RBAC Policies	4	2	3	2

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

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 Installation and Operations

- Rancher: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 2

3.1.1.1 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 SLE Micro 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.

3.1.1.2 OpenShift

OpenShift Container Platform 4 (OCP4) ships a large installation binary that includes Terraform and a set of scripts to deploy OCP4. 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.

To execute the installation binary, operators can customize the `install-config.yaml` file to access additional customizations for the automated installer. Users can also install OpenShift clusters from RedHat Advanced Cluster Management (RHACM) user interface to install OpenShift clusters and achieve day two operations.

3.1.1.3 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 run on vSphere, Amazon, Microsoft Azure or GCP nodes if operators choose to use the bring your own host feature (BYOH). Tanzu's BYOH feature allows operators to use different platforms and operating systems; however, in doing so, operators will lose access to some features of Tanzu.

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.

3.1.1.4 Anthos

If you're already operating in GKE, installing Anthos is easy. Using Anthos with AWS or Azure is more challenging as they have dependencies on Google Cloud projects. Anthos can also be used on VMware infrastructure or on bare metal servers 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 3 times more expensive per vCPU than if you use AWS, Azure or GCP. On top of this, there is an additional fee for the connectivity service that provides communication among on-premises and cloud.

3.1.2 Intuitive UI

- Rancher: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 3

3.1.2.1 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. Rancher has been designed to make it possible for teams to easily use Kubernetes across an organization without needing extensive training up front.

Rancher also provides an integrated user interface for Harvester, the open and interoperable hyperconverged infrastructure solution from the Rancher by SUSE team. With Rancher and Harvester, operators can manage their virtual machine workloads alongside their container clusters, all within a single platform.

3.1.2.2 OpenShift

OpenShift's user interface provides a curated view for administrators and developers. 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

TKGI does not come with a built-in management interface; instead, VMware offers visual cluster management through an additional SaaS product called Tanzu Mission Control (TMC). TMC is part of VMware Cloud Services and has a well-designed user interface that comes in two versions: Standard and Advanced. Depending on the version of TMC users purchase, they can get access to additional features.

3.1.2.4 Anthos

Anthos and Anthos GKE's user experience is derived from Google's years of building excellent cloud applications. Existing users of Google Cloud will find Anthos to be a familiar, easy-to-use cohesive experience.

3.1.3 Hosted & Managed Services

- Rancher: 3
- OpenShift: 3
- Tanzu: 1
- Anthos: 2

3.1.3.1 Rancher

SUSE also offers Rancher Prime Hosted – a premium 'white-glove' service available to organizations looking to manage scale their Kubernetes environment without needing to manage the operational complexities. Rancher Prime Hosted is a fully managed cloud-hosted service of Rancher that alleviates the operational complexities around Rancher and Kubernetes.

The Rancher Prime Hosted team manages all aspects from uptime, monitoring, logging, and security to backups, restores and upgrades and enables teams to focus on business continuity and reduce their total cost of ownership.

3.1.3.2 OpenShift

Red Hat's offering includes OpenShift managed, including OpenShift dedicated managed by Red Hat, Azure Red Hat OpenShift (ARO) managed by Microsoft running on Azure, Red Hat OpenShift Service on AWS (ROSA) managed by Amazon and running on AWS, and Red Hat OpenShift Kubernetes Service (ROKS) managed by IBM and running on IBM Cloud. However, there is no offering for the multi-cluster management piece RHACM.

3.1.3.3 Tanzu

VMware does not offer TKG or TKGI as a hosted or managed service, although Tanzu Mission Control is a SaaS offering.

3.1.3.4 Anthos

Google offers Anthos and other services as a SaaS offering but GKE or Anthos clusters are not offered as hosted or managed services. By default, users must go through Google's Cloud Services to manage their clusters and integration with Anthos management.

3.1.4 Multi-Cluster Management

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 2

3.1.4.1 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 deployed. Rancher is also platform agnostic when it comes to managing or deploying Kubernetes clusters. It offers full lifecycle management across the major public cloud provider's distributions, including EKS, AKS and GKE as well as RKE, RKE2 and K3s or any CNCF-conformant Kubernetes distribution. All the Rancher features are available for any managed Kubernetes out of the box.

To help manage clusters at scale, Rancher utilizes Fleet, an open source project that enables GitOps at scale. Built by the Rancher team, Fleet is designed to manage both large and small scale cluster deployments.

The Rancher by SUSE team has also built several complementary open source tools that can be integrated with Rancher to help operators achieve better business continuity across their platforms and applications. These include the CNCF Incubation project Longhorn, which enables powerful, highly available persistent block storage to be delivered on any Kubernetes environment and Harvester, the 100% open source modern HCI solution that is built on Kubernetes and designed to help operators unify their container and virtualized workloads.

3.1.4.2 OpenShift

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

With the additional RHACM subscription, OpenShift customers have access to perform full lifecycle management across any OpenShift clusters including the OpenShift managed services and can support the management of hosted Kubernetes services including Amazon EKS, Azure AKS, and Google GKE. It is important to note that full lifecycle management is not currently available for the hosted hyperscaler Kubernetes services.

With RHACM, operators also get access to a policy engine via GitOps help manage clusters at scale. OpenShift clusters will also have full monitoring capabilities with RHACM where as non-OpenShift clusters will get access to limited monitoring features. For extensive RedHat OpenShift environments, RHACM integrates with RedHat OpenShift Data Foundation to provide a business continuity solution for stateful applications on OpenShift.

3.1.4.3 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. To get comprehensive full lifecycle management and full functionality of TKGI Clusters, operators must subscribe to Advanced TMC option. TMC offers the capabilities to manage non-Tanzu clusters; however, they do not have full lifecycle management capabilities.

3.1.4.4 Anthos

Anthos has full lifecycle management for GKE and Anthos clusters that are running on either GCP, AWS, Azure, vSphere, or bare metal. Anthos users will experience differences in features between Anthos on GKE clusters verses clusters on other Kubernetes distributions.

Anthos users can also get GitOps capabilities through Anthos Config Management to manage multiple cluster environments. However, operators looking to deploy Anthos clusters outside of the GCP and/or Anthos environment can expect complexity that they may need to solve.

3.1.5 Edge Support

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 1

3.1.5.1 Rancher

Rancher has extensive capabilities at the edge. Operators can utilize Rancher with distributions like K3s and RKE2 to build a secure and resilient Kubernetes environment that consumes a small blueprint of resources. Users can also install Rancher on a Single Node using Docker requiring minimal resources to operate and run at edge locations.

SUSE Edge, a new bundle offering from SUSE, incorporates enterprise-grade support for Rancher and K3s. It gives operators the confidence to deploy Kubernetes clusters across a large scale of resource-limited and or remote locations.

K3s is a lightweight Kubernetes distribution originally developed by the Rancher team that can run in remote, resource-constrained environments including Raspberry Pi. In August 2020, K3s was accepted as a CNCF Sandbox project.

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 from core to cloud or at the edge.

In December 2021, SUSE announced Harvester, an HCI virtualization platform based on Kubevirt and Longhorn. It offers a flexible and affordable way to put VM workloads in your edge locations. Harvester can be managed with Rancher, giving you a single management platform for Kubernetes and VMs. In combination with RKE2 and K3s, Harvester gives you endless possibilities for your edge strategies.

3.1.5.2 OpenShift

Red Hat's offering in edge and strategy has evolved in the last year. Now with OpenShift 4.9, you have the possibility to run Single Node OpenShift (SNO) clusters. However, the SNO needs are high: the minimum hardware to run SNO is 8 vCPU cores, 32 GB of RAM and 120GB of storage, making it less than ideal for small edge devices, Arm boards or IoT devices. Red Hat recently announced their new project MicroShift, which explores how OpenShift distributions and Kubernetes can be optimized for edge computing using containers.

With RHACM you can manage common OpenShift clusters, SNO and MicroShift.

3.1.5.3 Tanzu

The Tanzu edge story was 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. This solution did not consider resource-constrained environments or a management solution that does not include additional paid VMware services.

In October 2021, VMware announced project Santa Cruz. This solution is a piece of hardware developed by VMware to run containers at the edge and provide secure remote access to these containers. Clusters running on this hardware are then managed by TMC.

As mentioned previously in this guide, VMware has a 'BYOH' feature. This can be incorporated with ESXI-Arm to enable VMware operators to run small footprint clusters remotely. However, this is a complicated approach that can often be too complex to implement and build due the design and over-engineering of the integration.

3.1.5.4 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.

3.1.6 Integrated Public Cloud Support

- Rancher: 4
- OpenShift: 2
- Tanzu: 2
- Anthos: 2

3.1.6.1 Rancher

Rancher offers full lifecycle support for deployment into managed Kubernetes solutions from Amazon (EKS), Google (GKE), and Azure (AKS). Operators can also use Rancher to create clusters from other hosted cloud providers including Alibaba, Baidu, Huawei, DigitalOcean 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.

With EKS, GKE and AKS, Rancher can now import, provision, upgrade, configure and secure clusters across all three environments directly using 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.

3.1.6.2 OpenShift

Red Hat OpenShift is a Kubernetes distribution; as such it does not offer capabilities to manage hosted Kubernetes solutions from any provider. It can be deployed in AWS, Azure, IBM Cloud and GCP. Separately, you can buy a subscription for Red Hat Advanced Cluster Management for Kubernetes (RHACM), which can import and manage pre-built EKS, GKE, AKS or IKS clusters; but it can´t offer full lifecycle management for them.

3.1.6.3 Tanzu

Tanzu Mission Control supports the management of hosted Kubernetes clusters across cloud providers but cannot deploy or delete them. Instead, clusters must be created directly with the hosting provider first and then 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. No full lifecycle management capabilities are available for EKS and AKS clusters in Anthos.

3.1.7 Bare Metal, OpenStack & vSphere

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 2

3.1.7.1 Rancher

Rancher provides the capabilities needed to deploy and manage RKE, RKE2 and K3s clusters across these platforms. Rancher is also able to manage any CNCF compliant Kubernetes distribution running on these environments through the platform's agnostic approach to running Kubernetes anywhere.

3.1.7.2 OpenShift

OpenShift can be deployed in RedHat OpenStack, vSphere and bare metal using the OpenShift installer or from the additional paid RHACM console which offers full lifecycle for the OpenShift clusters deployed on these platforms. However, if operators want to manage other Kubernetes distribution running on these platforms it won't be supported by RedHat which limit choices for users and promotes lock-in to the Red Hat ecosystem.

3.1.7.3 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. Tanzu can also manage non TKG clusters deployed on different platforms through the TMC subscription.

3.1.7.4 Anthos

Anthos supports deployment within a vSphere environment or on bare metal or virtual machines. Anthos also can manage non GKE, or Anthos clusters previously deployed on these infrastructure providers.

3.1.8 Import Existing Clusters

- Rancher: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 3

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 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.

3.1.8.2 OpenShift

Red Hat ACM (an additional paid service) can import existing OpenShift clusters in different substrates and locations. It can also provide operators with the possibility to import and manage AKS, EKS, GKE and managed OpenShift services like ARO, ROSA and OpenShift dedicated. RHACM offers all functionality and lifecycle management capabilities to all OpenShift clusters.

3.1.8.3 Tanzu

Tanzu Mission Control (TMC) can import clusters from external providers. TMC is a SaaS-only solution available with Tanzu Standard or Tanzu Advanced.

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 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 the Rancher by SUSE CNCF-certified Kubernetes distributions, is included in this list.

3.1.9 Centralized Audit

- Rancher: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 2

3.1.9.1 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.

3.1.9.2 OpenShift

OpenShift can log all interactions with the OCP API, including request and response body and metadata. OpenShift collect logs from applications, infrastructure, and audit logs. This information can be queried via the `oc` command or in the Kibana dashboard. OpenShift logging is based in the EFK stack (Elasticsearch, Fluentd and Kibana). The audit logs can be accessed via `oc` commands and can be forwarded to external tools.

3.1.9.3 Tanzu

TKG ships with Fluent Bit for collecting and forwarding logs. Logs can go to an Elasticsearch, Kafka, Splunk, syslog or HTTP endpoint. The deployment and configuration of Fluent Bit is a manual process that must happen on each Kubernetes cluster. With a paid TMC subscription, operators can use it to create reports of audit events. TMC also collects and stores logs and audit events for 60 days.

3.1.9.4 Anthos

Google GKE clusters are GKE clusters running on GCP. GKE clusters running in any other - infra are called Anthos clusters. GKE clusters by default run the GCP Cloud Logging service. At installation you can change this behavior to use a different logging service.

Anthos clusters hosted on VMware or bare metal run Cloud Logging by default. For connected clusters (i.e., clusters that have been imported into Anthos), AWS or Azure clusters, Google provides the possibility to install the Google Cloud's operations suite through an operator.

This allows users to access the 'Cloud Logging Service' by forwarding the logs to the Cloud Logging Service. The operator installation will require prior configurations to provide access to Anthos.

3.1.10 Cluster Self-Service Provisioning

- Rancher: 4
- OpenShift: 4
- Tanzu: 4
- Anthos: 1

3.1.10.1 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.

3.1.10.2 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, RHACM (an additional paid service) can deploy OpenShift clusters in multiple environments using the CLI, API or UI.

3.1.10.3 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). VMware has developed with Terraform a TMC provider which provides a new set of tools to developers to self-provision TGK workload clusters.

3.1.10.4 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.

3.1.11 Private Registry and Image Management

- Rancher: 4
- OpenShift: 4
- Tanzu: 4
- Anthos: 2

3.1.11.1 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.

For organizations that require an extra level of assurance, Rancher Prime provides customers with the option to deploy from a trusted private registry. This capability is available to all customers who consume the Rancher Prime support subscription.

3.1.11.2 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 `oc` CLI to create image pull secrets and optionally attach them to service accounts.

3.1.11.3 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.

3.1.11.4 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 as you must pay for the storage consumed by the images stored.

3.1.12 Cluster Upgrades and Version Management

- Rancher: 4
- OpenShift: 4
- Tanzu: 2
- Anthos: 2

3.1.12.1 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 also enables upgrades in air-gapped environments with Helm template options.

3.1.12.2 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. The upgrade process can be triggered using the CLI or the UI. Once a cluster has been upgraded there is no rollback to previous versions.

Before triggering and upgrade you need to check the release paths to see to which version you can update.

3.1.12.3 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.

3.1.12.4 Anthos

Anthos has different upgrade processes for their clusters depending on where clusters are hosted. Anthos in VMware clusters need to upgrade in the admin workstation first, followed by the user clusters and finally (optionally), the admin cluster. To upgrade Anthos clusters in VMware you'll need to use `gkectl` CLI.

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 upgrade process has improved with the latest release of Anthos. For GKE or Anthos clusters running on Public Cloud, the upgrade can be done with the CLI `gcloud` or via the multi-cloud Anthos API from the Anthos UI. The process starts with the control plane, destroys the node, and spins up a new node with the latest configuration. It then tests the

new node and if the tests pass, it keeps going instance by instance until the upgrade is complete.

The inconsistency across these upgrade procedures increases the cognitive load for cluster administrators of multi-cluster environments that need to use different platforms, which can increase the likelihood of error and outages.

3.1.13 Storage Support

- Rancher: 4
- OpenShift: 4
- Tanzu: 4
- Anthos: 3

3.1.13.1 Rancher

The Rancher by SUSE team created and contributed 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.

3.1.13.2 OpenShift

Red Hat's preferred option for storage is Open Data Foundation, formerly known as OpenShift Container Storage, which is based on Ceph, NooBaa and Rook. OpenShift Container Storage covers different use cases for OpenShift and is a powerful solution. But as it based on Ceph, it requires substantial compute resources to run.

OpenShift offers support for different storages from NFS to public cloud storage, such as EBS or Azure Disk. OpenShift also supports CSI drivers for different types of storage and from different vendors.

3.1.13.3 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.

3.1.13.4 Anthos

Anthos supports in-tree, CSI, AWS, NFS, Azure, vSphere storage drivers and all types of Google Cloud storage.

3.1.14 Arm Support

- Rancher: 4
- OpenShift: 2
- Tanzu: 1
- Anthos: 0

3.1.14.1 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.

3.1.14.2 OpenShift

OpenShift does not currently support deployment on Arm processors. In January 2022 Red Hat announced MicroShift, a new research project that explores how OpenShift

Kubernetes (OKD) can be optimized for small form and edge computing. It is a solution that can run on different Linux systems, including those running on Arm. However, it is currently immature with limited features.

3.1.14.3 Tanzu

Tanzu does not support deployment on Arm processors by default. VMware recently added the possibility to use BYOH in combination with ESXi-Arm to deploy Kubernetes in Arm processor-based systems and manage them with TMC. It is a suboptimal resource-heavy solution.

3.1.14.4 Anthos

Anthos does not support deployment on Arm processors.

3.1.15 Airgap Support

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 0

3.1.15.1 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.

3.1.15.2 OpenShift

OpenShift supports air gapped installations across all platforms where it can be installed. No matter what installation method is used, operators must create a local registry with all the images for OpenShift and need to mirror locally all the images that they would want to use. The images needed to install operators from the OperatorHub must be versioned and mirrored locally to install operators.

3.1.15.3 Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) supports air-gapped 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.

3.1.15.4 Anthos

Anthos has no documentation for deploying into an air-gapped 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.

3.1.16 Etcd Backup and Restore

- Rancher: 4
- OpenShift: 2
- Tanzu: 3

- Anthos: 1

3.1.16.1 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.

3.1.16.2 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.

3.1.16.3 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.

3.1.16.4 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. There are only clear instructions for the backups for Anthos on-premises (VMware) and for Anthos on bare metal.

3.2 Security, Policy & User Management

3.2.1 Active Directory and LDAP Support

- Rancher: 4
- OpenShift: 4
- Tanzu: 4
- Anthos: 2

3.2.1.1 Rancher

Rancher integrates directly with Active Directory, Azure AD, OpenLDAP, FreeIPA, OAuth providers like GitHub and SAML providers like 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.

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

Connect and OAuth and it provides an interface for basic authentication and external authentication systems capable of setting a request header.

3.2.1.3 Tanzu

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

3.2.1.4 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.

3.2.2 Pod and Network Security Policies

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 2

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

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. 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).

RHACM provides a policy engine that can be managed via GitOps and deploys any kind of policy at scale including network policies. It offers basic integration with OPA, Kubernetes Vault and Kyverno.

3.2.2.3 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 Flannel for networking. Antrea has its own advanced network policy extensions but also supports Kubernetes Network Policies.

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.

3.2.2.4 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.

3.2.3 Configurable Adherence to CIS Security Benchmarks

- Rancher: 4
- OpenShift: 3
- Tanzu: 2
- Anthos: 2

3.2.3.1 Rancher

Rancher maintains a hardening guide and self-assessment that references CIS benchmarks with specific user actions to satisfy the requirements. 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 Rancher.

With the acquisition of NeuVector in 2021, Rancher has expanded its security offering since NeuVector assesses and reports on all major security standards including PCI, NIST, GDPR and HIPAA. NeuVector is now 100% open source and can now be integrated alongside the Rancher platform.

3.2.3.2 OpenShift

OpenShift offers Compliance Operator, which offers CIS scanning for clusters and nodes out of the box. It has a cron that runs the scan as often as you want and stores the reports in a PV. It offers additional compliance standards like ACSC, NIST and NERC and offers the possibility to create your own profiles to perform scanning based on your security needs. There is also an additional hardening guide for OpenShift and for RHCOS.

3.2.3.3 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.

3.2.3.4 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, Azure or on bare metal.

However, if you use the Anthos Config Management tool, there are a set of policies to enforce CIS policies in your clusters. This solution enforces the policies, but it doesn't give you a CIS score. Manual steps are required before utilizing it, since the policies need to be installed in the Anthos Config Management tool.

3.2.4 RBAC Policies

- Rancher: 4
- OpenShift: 2
- Tanzu: 3
- Anthos: 2

3.2.4.1 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.

Rancher users can also integrate CNCF sandbox project 'Kubewarden' to help manage their policy requirements. Kubewarden is a policy engine for Kubernetes that validates incoming requests using policies written in WebAssembly.

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 unless operators use RHACM, which can provide basic policies for certain subsets of clusters or clustersets. With the RHACM policy engine you can manage and deploy at scale individual Kubernetes RBAC policies to the different clusters. RHACM is a separated subscription from OpenShift.

3.2.4.3 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.

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. Google provides an Identity Service that can be used across any platform where GKE or Anthos clusters can run, providing a unified access system for all the clusters. However, the RBAC will be local for each cluster depending on the permissions given by the admins. The Identity Service can be connected to GCP to connect to the clusters using the Google Cloud ID. The Identity Service is compatible with OIDC protocol identity systems in any platform and with LDAP for clusters in VMware or bare
metal.

3.3 Shared Tools & Services

3.3.1 Application Catalog

- Rancher: 4
- OpenShift: 4
- Tanzu: 3
- Anthos: 1

3.3.1.1 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.

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. 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. Through the Developer UI, OpenShift users can also select a git repo to access their code and base image with the programming language needed to deploy a pod.

3.3.1.3 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.

3.3.1.4 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.

3.3.2 Provision with Terraform / Ansible / Others

- Rancher: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 3

3.3.2.1 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, 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.

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. OpenShift users who purchase a RHACM subscription, will get Ansible integration out of the box to perform different kind of operations in cluster lifecycle management, application lifecycle management and policies.

3.3.2.3 Tanzu

VMware has announced in February 2022, a Terraform provider for TMC. This provider allows users to deploy TKG clusters from TMC using Terraform, this new approach allows Tanzu customers to define clusters as code and to be more agile. This new feature is restricted to deploy workload clusters.

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: 3
- OpenShift: 4
- Tanzu: 2
- Anthos: 4

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 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.

3.3.3.2 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.

3.3.3.3 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.

3.3.3.4 Anthos

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

3.3.4 Advanced Monitoring

- Rancher: 4
- OpenShift: 4
- Tanzu: 3
- Anthos: 2

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 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.

3.3.4.2 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. In a multi-cluster level, RHACM offers a single pane of glass view of cluster metrics of OpenShift clusters using popular open source projects like Grafana, Observatorium and Thanos in the background.

3.3.4.3 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.

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 are add-on components with their own pricing and require manual configuration from administrators to implement.

3.3.5 Alerts and Notifications

- Rancher: 4
- OpenShift: 4
- Tanzu: 3
- Anthos: 2

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 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.

3.3.5.3 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.

3.3.5.4 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.

3.3.6 External Log Shipping

- Rancher: 4
- OpenShift: 4
- Tanzu: 2
- Anthos: 3

3.3.6.1 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.

3.3.6.2 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.

3.3.6.3 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.

3.3.6.4 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).

3.3.7 Windows Container Support

- Rancher: 4
- OpenShift: 4
- Tanzu: 1
- Anthos: 2

3.3.7.1 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.

3.3.7.2 OpenShift

OpenShift (OCP4) includes production support for using Windows servers in Kubernetes clusters and deploying Windows containers under management of an OpenShift control plane. In the OperatorHub, you can find the Windows Machine Config Operator (WMCO) that allows you to add Windows workers to any OpenShift cluster running on AWS, Azure, or vSphere.
Windows is also supported via a BYOH approach with the WMCO for OpenShift 4.8+ and WMCO 3.1.0+.

3.3.7.3 Tanzu

Tanzu Kubernetes Grid (TKG) does not support Windows workers or workloads. However, Tanzu Kubernetes Grid Integrated Edition (TKGI) offers the possibility to be deployed in Windows workers. The documentation specifies that it is a beta feature exclusively for vSphere with Flannel network plugin and using NSX-T for networking.

3.3.7.4 Anthos

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

3.3.8 Integrated Service Mesh Support

- Rancher: 4
- OpenShift: 3
- Tanzu: 1
- Anthos: 4

3.3.8.1 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.

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

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

3.3.8.4 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.

3.3.9 Enterprise SLA

- Rancher: 4
- OpenShift: 4
- Tanzu: 4
- Anthos: 2

3.3.9.1 Rancher

The Rancher by SUSE team provides a comprehensive subscription known as 'Rancher Prime'. The support package aims to help operators get more value and an exceptional experience out of their Kubernetes implementation with Rancher. Backed by a world-class 24x7x365 team of experts, Rancher Prime support covers Rancher, Docker, Kubernetes and other cloud native technology software (see support matrix for more information). Rancher Prime comes with a fortified edition of Rancher, plus access to our team of professional services experts, IP assurance and indemnification all in in configurable packages to help teams scale with the confidence they need across their unique use case.

The Rancher Prime 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 in two levels, 12x5 and 24x7. 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 subscription model is priced by virtual core or per socket in bare metal environments. This means upgrades across environments increase support costs. Red Hat offers additional paid professional services support including Technical Account Managers who can be hired in order to help with requests in addition to subscription support.

3.3.9.3 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.

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: 4
- OpenShift: 3
- Tanzu: 3
- Anthos: 0

3.3.10.1 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.

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

Tanzu's momentum across the community has been driven by VMWare's existing customer base. The entry point for Tanzu Kubernetes Grid has been users with 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. 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.

However, recently VMWare has done extensive work to expanding their community outside the VMware existing customers. In 2021 they released Tanzu Community Edition, giving the open source community the opportunity to test their stack on Tanzu. Alongside this, VMware has also conducted multiple events and community activities to showcase Tanzu and its developer experience. As of December 2022, Tanzu Community Edition will no longer be maintained by VMWare.

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 from their existing GCP customer base.

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.

3.4 Overview of Solutions

3.4.1 Rancher

Rancher is the solution that offers you the most flexible and open solution in the market. It is platform agnostic and integrates well with public cloud-hosted Kubernetes services and is the only solution that offers full lifecycle management for AKS, EKS and GKE. With Rancher you can use popular distributions built by the Rancher by SUSE team including RKE, RKE2 and K3s or alternatively leverage any CNCF compliant distribution that suits your environment.

When using Rancher with one of the Rancher by SUSE built distributions, users can run a large variety of operating systems giving them the flexibility and adaptability they need to implement container and Kubernetes solutions across their infrastructure. Rancher also is 100% open source with a large community backing. SUSE also invest heavily in the open source community with a large number of open source projects in development including Harvester, Epinio and Rancher Desktop.

Rancher also offers integration with popular tools like Terraform, Ansible and Salt that can automate Kubernetes deployments in different platforms to help your operations teams work more efficiently. Rancher remains 100% open source and free to use for users.

For organization's who need additional insight across their growing Kubernetes workloads, the Rancher Prime subscription is available and charges per node and not per vCPU, providing transparent and economical pricing for users. Combined with a flexible and vendor-agnostic approach to Kubernetes, Rancher Prime's fortified platform and exception support and services, it is the perfect holistic package for enterprises looking for a modern, open solution to help scale their container with secured confidence.

3.4.2 OpenShift

OpenShift offers a versatile Kubernetes platform, with a lot of different additional features available for developers included in its price, plus a huge community behind the platform. It can be deployed across a variety of platforms and environments or consumed as managed service.

OpenShift in combination with Red Hat Advanced Cluster Management for Kubernetes (RHACM) gives user a good variety of multi-cluster capabilities which are tailored around the wider OpenShift ecosystem.

Operators looking to implement OpenShift across their environment should consider the following:

- OpenShift needs to be installed on CoreOS or RHEL, which may limit the options available to operators when selecting operating systems. OpenShift can be a very complex distribution to utilize and is not an industry standard.
- Red Hat offers a very well-defined blueprint for their stack; however, it makes you highly dependent on their technology, which increases an organization's risk of lock in.

OpenShift and RHACM are charged per physical socket or vCPU of worker nodes, which when scaled can be a more costly and less flexible solution compared to other solutions available on the market.

3.4.3 Tanzu

For operators with a base built on vSphere infrastructure across their organization, Tanzu may be a good option since it presents a fantastic integration with vSphere.

VMware also offers many different developer tools integrated with Tanzu. However, it does have a very complex portfolio that is composed of multiple products and services. These products and services come as an additional cost on top of Tanzu, which increases an organization's dependency on VMware.

In addition to the lock-in nature of Tanzu, the segmented parts of Tanzu and its additional portfolio and services adds an additional level of complexity to the platform compared to other solutions available on the market which offer a much simpler deployment and operational experience. Enterprises with a large Edge computing requirements may also find Tanzu is limited in terms of its Edge capabilities and support for distributed clusters in remote locations.

For operators that are looking for the top-tier full feature Tanzu experience they would need to subscribe to Tanzu Advanced Edition which incorporates the Tanzu Mission Control (TMC) subscription on top of Tanzu. This can become costly as environments scale and does subject environments to be locked in.

3.4.4 Anthos

Anthos is an excellent solution for existing GCP-heavy infrastructure environments. Organizations with a large investment with Google and not planning to diversify their infrastructure cloud capabilities should use Anthos as it offers a seamless integration with GCP, giving operators and developers and easy transition into the container and Kubernetes space.

However, it presents a few downsides, especially for those with a diversified infrastructure stack. Anthos seems to be designed and built for existing Google stack users and the services and products integrated with Anthos do push users to consume more GCP.

For organizations that require operational support for on-premise environments, Anthos is an expensive solution compared to other alternatives on the market. It also requires operators to utilize their connectivity services, which will raise your costs considerably. Anthos' approach to Edge is also lacking, compared with other platforms in the market, as they do not support Arm or provide a solution for resource-remote environments.

4 About this Guide

This guide is a cumulation of research based on publicly available documentation from each vendor written from the perspective of a team of technical experts from SUSE. The writers found the differences between documentation from each vendor to differ vastly and that it is often complex for operators to source the information they need.

RedHat provided rich and comprehensive technical documentation for those looking to implement OpenShift onto their environment. However, there is a higher level of expected existing Kubernetes and container knowledge required. The documentation could be improved with less complex language used and simpler concepts to help less technical operators onboard easier.

Both Anthos and VMware Tanzu's documentation lacked the technical insights often expected in documentation, making it difficult for any operator looking to extract insights and decipher and troubleshoot the platform's processes. Tanzu did have an easier navigational experience for operators who need to search for specific information compared to Anthos.

Rancher documentation is well structured and makes it easy for any operator to find what they are searching for. It's user friendly and covers most technical information adequately but could be enriched with more information around performing operations with the CLI.

5 About the Author

SUSE is a global leader in innovative, reliable and enterprise-grade open source solutions. SUSE specializes in Enterprise Linux, Kubernetes management and edge solutions, and the company collaborates with partners, system integrators 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, the team now known as 'Rancher by SUSE' remain behind successful open source products including:

- **Rancher** - the world's most popular enterprise-grade Kubernetes management platform. Rancher is available as free, open source software.
- **Rancher Prime** – the commercial version of Rancher, which includes the option to deploy from a trusted private registry, up to 24/7 support + expert consulting and training services.
- **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 Kubernetes clusters at scale
- **K3s** – a lightweight production-grade Kubernetes distribution built for embedded systems and the edge. In August 2020, K3s was donated to the CNCF as a sandbox project.
- **Longhorn** - a powerful cloud-native distributed storage platform for Kubernetes. In October 2019, Longhorn was donated to the CNCF as a sandbox project. In November 2021, Longhorn was promoted to an 'Incubating' project with the CNCF.
- **Harvester** - a modern open source hyperconverged infrastructure solution built on Kubernetes
- **SUSE NeuVector –** an open source Zero Trust Kubernetes-native security platform.
- **Kubewarden** - a policy engine for Kubernetes. In June 2022, Kubewarden was donated to the CNCF as a sandbox project. Kubewarden enforces policy-as-code model allowing you to write policies in your favourite programming language.

All of Rancher's products and projects remain open source after the acquisition, with support from a vibrant, active community. SUSE offers an enterprise support subscription for some solutions, and those are differentiated by the name 'Rancher Prime.'

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 please visit: www.rancher.com

6 Glossary

6.1 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.
- Hosted & managed services
  - Additional professional services provided by vendors on top of their standard product and services to help you manage the operational complexities of Kubernetes clusters.
- Multi-cluster management
  - 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-premises 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.
- Integrated public cloud support
  - Support for popular cloud environments like AWS, Azure and GCP minimizes the commercial and technical risks of being locked into a single cloud provider.
- 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.
- 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.
- Cluster 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.

6.2 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 provide 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.

6.3 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.

7 Legal Statements

7.1 Copyright Notice

7.2 Third-Party Trademark Usage

Please note that Red Hat OpenShift, VMware Tanzu, Google Anthos are the registered trademarks of Red Hat Inc., VMware Inc. And Google LLC. respectively.

7.3 Note from the Authors

The views in this whitepaper are those of SUSE. 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 – suse.com
Contact Us – suse.com/contact
Twitter – @SUSE