

A Buyer's Guide to Enterprise Kubernetes Management Platforms

Red Hat OpenShift 4.12, VMware Tanzu 2.1, Google Anthos, and Rancher 2.7



Contents

1	Executive Summary	3
2	Understanding the Portfolios	5
3	Capabilities Summary	7
4	Feature Analysis	10
5	About this Guide	40
6	About the Author	41
7	Glossary	42
8	Legal Statements	46

1 Executive Summary

This document aims to provide an in-depth analysis of the leading Kubernetes management platforms and the market situation. It covers the most successful solutions, including Rancher Prime, Red Hat OpenShift, VMware Tanzu and Google Anthos.

Organizations modernizing their infrastructure continue to choose cloud-based technologies to power their digital transformation. As they move from their legacy environments to hybrid, multi-cloud stacks, enterprises create new opportunities to unify their IT operations with containers and Kubernetes.

The potential of containers and Kubernetes was evident when, in 2020, Gartner¹ predicted that more than 75% of worldwide organizations would run containerized applications in production by 2022. In 2023, the 2022 CNCF survey¹ shows that 79% of the participants already use containers in production, and another 9% actively evaluate the technology.

The CNCF survey¹ has revealed interesting data on Kubernetes adoption, identifying the main barriers as lack of training and security. However, the right partner and tools can significantly overcome these barriers. SUSE offers training and certification services to assist with Kubernetes training needs. Additionally, Rancher Prime simplifies Kubernetes management and improves security through its monitoring and logging capabilities, CIS scans, admission controllers (Kubewarden), and others. Furthermore, the integration of SUSE NeuVector and Rancher Prime enables operators and developers to implement a DevSecOps culture in their organization and secure Kubernetes clusters with minimal investment in training. Lastly, Rancher Prime Hosted offers the same capabilities as Rancher Prime, freeing operations teams from platform and infrastructure maintenance tasks such as scaling, monitoring, and upgrading making Kubernetes adoption easier and faster.

The main adopters of cloud native technologies are developers and IT operators, who always look for solutions to help them build more scalable applications quickly without compromising reliability, agility, and security.

Relying on upstream Kubernetes isn't enough for teams deploying Kubernetes into production. A lack of central visibility, inconsistent security practices, and complex management processes plague basic Kubernetes installations.

Therefore, Kubernetes management platforms need to deliver confidently:

- **Simplified Cluster Operations:** improved DevOps and DevSecOps efficiencies with simplified cluster operations.
- **Consistent Security Policy and User Management:** best-practice security policy enforcement and advanced user management on any infrastructure. Kubernetes security is key in a cloud native world.
- **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.

¹ "CNCF 2022 Annual Survey – [Key Findings](#)"



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

Commercially, Rancher Prime has extended its success in the enterprise market by maintaining double digit growth year over 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 with OpenShift. As of now, Red Hat is the market leader in Kubernetes platform sales.

Since launching 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.

VMware acquired several companies in the past to expand its experience in the cloud native space and maintain a market share that was threatened by the absence of a Kubernetes 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. This was the foundation for Tanzu, which got traction in the market thanks to the huge base of VMware's Virtualization Platform and after a huge investment. Now after the announcement of the Broadcom acquisition, the future of Tanzu is compromised if we consider what Broadcom did in the past with the companies acquired.

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 (OpenShift/OCP4) with Red Hat Advanced Cluster Management for Kubernetes (RHACM) –collectively referred to as OpenShift in this guide–, VMware Tanzu Mission Control with Tanzu Kubernetes Grid –collectively referred to as Tanzu in this guide–, Google Anthos with Anthos GKE –collectively referred to as Anthos in this guide– and Rancher Prime and its ecosystem.

Readers of this guide will gain a comprehensive understanding of the leading Kubernetes Management Platforms on the market, their strengths and weaknesses and the technologies involved on each one of the solutions.



2 Understanding the Portfolios

To understand the different proposals properly is important to present the stacks and how they are built. At this point, you will find four diagrams presenting the components and what area they cover to provide perspective to the readers.

Rancher by SUSE

Registry	Kubernetes Security
3rd party	SUSE NeuVector
Cloud Native Storage	Multicloud management and Platform Services
	
Longhorn	Kubernetes
	RKE, RKE2, K3s, AKS, EKS, GKE
	OS
	SUSE Enterprise Linux, RHEL, Ubuntu, Amazon Linux ...

Red Hat

Registry	Kubernetes Security
Quay	Advanced Cluster Security
Cloud Native Storage	Multicloud management
	Advanced Cluster Management
	Additional Platform Services
	OpenShift Container Platform
	Basic Kubernetes & OS
	OpenShift Kubernetes Engine (Red Hat CoreOS)

VMware

Registry	Kubernetes Security
Harbor	Carbon Black Container
Cloud Native Storage	Multicloud management
	Tanzu Mission Control
	Additional Platform Services
	TAP * TOW ** TSM ***
	Kubernetes
	TKG, TKGm
	OS
	Photon OS, Ubuntu, Amazon Linux

- * Tanzu Application Platform
 ** Tanzu Observability by Wavefront
 *** Tanzu Service Mesh

Google

Registry	Kubernetes Security
GCP Registry	Anthos Policy Controller
Cloud Native Storage	Multicloud management
	Anthos
	Additional Platform Services
	Google Cloud Marketplace Anthos Service Mesh
	Kubernetes
	GKE, Anthos Clusters
	OS
	Ubuntu

2.1 Overview of Solutions

2.1.1 Rancher Prime

Rancher Prime is a powerful Kubernetes management platform that provides users with flexibility and openness, making it one of the most comprehensive solutions in the market. It is platform agnostic and integrates well with public cloud-hosted Kubernetes services, providing full lifecycle management for AKS, EKS, and GKE. With Rancher Prime, users can use popular distributions built by the Rancher by the SUSE team, including RKE, RKE2, and K3s, or leverage any CNCF-compliant distribution that suits their environment.

One of the key benefits of Rancher Prime is its ability to run a large variety of operating systems, providing users with the adaptability and flexibility they need to implement container and Kubernetes solutions across their infrastructure. Rancher Prime is also 100% open source with significant backing from the Rancher community. SUSE invests heavily in the open source community with many open source projects in development, including openSUSE, Harvester, Epinio, Rancher, K3s, Longhorn, and Rancher Desktop.

Rancher Prime also integrates out of the box with Terraform but can be also integrated with popular tools like Ansible, and Salt, enabling users to automate Kubernetes deployments in different platforms and help their operations teams work more efficiently.

For organizations that need additional insight across their growing Kubernetes workloads, the Rancher Prime subscription charges per node and not per vCPU or cores, providing transparent and economical pricing for users. Combined with a flexible and vendor-agnostic approach to Kubernetes, Rancher Prime's fortified platform and exceptional support and services make it the perfect holistic package for enterprises looking for a modern, open solution to help scale their container with secured confidence. Overall, Rancher Prime is a flexible, open, and powerful Kubernetes management platform that allows organizations to manage their Kubernetes clusters at scale.

2.1.2 Red Hat OpenShift

OpenShift is a versatile Kubernetes platform with a rich set of features that cater to the needs of developers. It has strong community support and can be deployed on various platforms and environments. Users can also opt for a managed service of OpenShift such as ARO or ROSA. Combined with Red Hat Advanced Cluster Management for Kubernetes (RHACM), OpenShift offers multi-cluster capabilities tailored to the wider OpenShift ecosystem.

However, deploying OpenShift may have some limitations. It requires installation on CoreOS or RHEL, which may restrict operators' choice of operating systems. Additionally, it is a complex distribution and not an industry standard, which can increase the user learning curve. Organizations should also consider the possibility of vendor lock-in, as Red Hat offers a well-defined blueprint for their stack.

OpenShift and RHACM are charged per physical socket or vCPU of worker nodes, which can be a more costly and less flexible solution as organizations scale their workloads.

2.1.3 VMware Tanzu

Tanzu is a comprehensive platform that provides excellent integration with vSphere, making it an attractive option for operators who have built their infrastructure on vSphere.



Additionally, VMware offers various developer tools that integrate with Tanzu, enhancing the platform's developer experience. However, Tanzu's complex portfolio, including multiple products and services, can increase an organization's dependency on VMware and add an additional level of complexity to the platform. This complexity, coupled with the additional cost of Tanzu's products and services, may make other solutions more appealing. Furthermore, Tanzu's Edge capabilities and support for distributed clusters in remote locations are limited. Those looking for the full-feature Tanzu experience must subscribe to Tanzu Advanced Edition (or Tanzu for Kubernetes Operations), which incorporates the Tanzu Mission Control subscription on top of Tanzu. As environments scale, this can become costly, and users may find themselves locked in.

The recent acquisition of Tanzu's parent company, VMware, by Broadcom has raised questions about the future of the Tanzu platform. Customers who have invested significantly in Tanzu should be concerned about potential changes to the platform's development roadmap and support. Additionally, Broadcom's track record with previous acquisitions may add to the uncertainty surrounding Tanzu's future. It's essential for organizations to monitor any developments and assess their options to mitigate any potential risks.

2.1.4 Google Anthos

Anthos serves as Google's robust solution for enabling multi-cluster management within Kubernetes. However, it predominantly caters to users of GKE and GCP. Anthos is a good choice for companies that have invested a lot in GCP and don't plan to change their infrastructure soon. However, there are other options for companies that want a more diverse infrastructure. Anthos' integrations with Google's products and services may lead to vendor lock-in and push users to consume more GCP services. Additionally, organizations that require operational support for on-premises environments may find Anthos an expensive option compared to other alternatives on the market. Anthos' approach to Edge is also lacking, with limited backing for Arm and solutions for resource-remote environments.

Moreover, Anthos is designed primarily for cloud-based environments and can be significantly more expensive and complex to deploy on-premises, making it less suitable for hybrid cloud environments. As a result, organizations looking for a more flexible and cost-effective hybrid cloud solution may need to consider other options that better cater to their needs.

3 Capabilities Summary

3.1 Overview

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

- The full ball (●) is applied to the best-of-breed platform in that category.
- The three-quarters ball (¾) is applied to the runner-up in that category.
- The half ball (½) illustrates acceptable capability in that category.
- The quarter ball (¼) shows weak capability in that category.

- The empty ball (○) indicates the platform has no capability in that category.

2.2 Cluster Operations

Kubernetes Management Platforms seek to simplify cluster management, ease the operations teams' tasks, and improve DevOps efficiencies by simplifying and automating cluster operations.

Feature	Rancher Prime	Red Hat OpenShift	VMware Tanzu	Google Anthos
Install and Operations	●	◐	◐	◐
Intuitive UI	●	◐	◐	◐
Hosted & Managed Services	◐	◐	◐	◐
Multi-Cluster Management	●	◐	◐	◐
Edge Support	●	●	◐	◐
Integrated Public Cloud Support	●	◐	◐	◐
Bare Metal, OpenStack & vSphere	●	◐	◐	◐
Import Existing Clusters	●	◐	◐	◐
Centralized Audit	●	◐	◐	◐
Cluster Self-Service Provisioning	●	●	●	◐
Private Registry & Image Management	◐	●	●	◐
Cluster Upgrades & Version Management	●	●	◐	◐
Storage Support	●	●	●	◐
Arm Support	●	◐	◐	◐
IBM Z and LinuxONE support	◐	◐	◐	○
Airgap Support	●	◐	◐	○
EtcD Backup and Restore	●	◐	◐	◐

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 Prime	Red Hat OpenShift	VMware Tanzu	Google Anthos
Active Directory and LDAP Support	●	●	●	◐



Network & Security Policies	●	◐	◐	◐
Policy as Code	●	◐	◐	◐
Configurable Adherence to CIS	●	◐	◐	◐
Global RBAC Policies	●	◐	◐	◐

2.4 Shared Tools and Services

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

Feature	Rancher Prime	Red Hat OpenShift	VMware Tanzu	Google Anthos
Application Catalog	●	●	●	◐
Provision with Config Management Systems	●	◐	◐	◐
CI/CD & GitOps	◐	●	◐	●
Desktop Kubernetes & Container Management	●	◐	◐	○
Advanced Monitoring	●	●	◐	◐
Alerts and Notifications	●	●	◐	◐
External Log Shipping	●	●	◐	◐
Windows Container Support	●	●	◐	◐
Integrated Service Mesh Support	●	◐	◐	●
Enterprise SLA	●	●	●	◐
Community Traction	●	◐	◐	○

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

4 Feature Analysis

4.1 Cluster Operations

4.1.1 Installation and Operations

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.1.1 Rancher Prime

The enterprise-grade version of Rancher, Rancher Prime, is a powerful platform for managing containers and Kubernetes clusters. It provides a user-friendly interface and powerful management tools that simplify installation and operations.

Rancher Prime offers a straightforward installation via Helm chart. It can be deployed in a Docker container, a single server, or any Kubernetes cluster deployed using an HA configuration. The supported distributions to deploy Rancher Prime are RKE, RKE2, K3s, AKS, EKS, and GKE. Also, for all these distributions, Rancher Prime offers full lifecycle management.

Rancher Prime provides a centralized platform for managing multiple Kubernetes clusters at scale, deploying, and managing applications across multiple environments easily. This simplifies operations and reduces the need for manual configuration.

Rancher Prime integrates perfectly with DevOps tools and methodologies such as Terraform, Fleet, and CI/CD pipelines, and GitOps simplifying the operations tasks enormously.

Rancher Prime provides tools for managing resources, such as CPU, memory, and storage, across multiple Kubernetes clusters. This helps optimize resource utilization and reduce costs.

4.1.1.2 Red Hat OpenShift

RHACM is a multi-cluster manager developed by Red Hat and created by IBM, which comes packaged as an operator that can be easily installed from the OperatorHub within OpenShift. The installation process involves deploying the operator and creating a Custom Resource Definition (CRD) object to trigger RHACM installation.

It's worth noting that RHACM is a separate subscription and is not included with OpenShift. There are two options for accessing RHACM: purchasing a separate RHACM subscription or purchasing the OpenShift Platform Plus, which includes RHACM.

RHACM complements OpenShift's capabilities by providing day 1 and 2 operations for multi-cluster management. RHACM complements OpenShift's capabilities by providing day 1 and 2 operations for multi-cluster management. OpenShift's operation and developer capabilities are primarily focused on the local cluster, so RHACM is needed for managing multiple clusters. It's important to note that RHACM is heavily focused on managing OpenShift, so it may not be a great choice for organizations that don't rely heavily on OpenShift.



4.1.1.3 VMware Tanzu

Tanzu offers a powerful multi-cluster management tool called Tanzu Mission Control (TMC), a Software-as-a-Service (SaaS) tool that doesn't require any installation. TMC is available for the top Tanzu subscriptions, and currently, it's only available as a hosted solution.

To use Tanzu, you need at least one management cluster on each platform where it runs. These management clusters offer limited features, such as deploying and upgrading clusters using the CLI. However, to access the enterprise capabilities of Tanzu, you'll need TMC.

TMC offers seamless integrations with all the pieces of VMware's cloud portfolio and provides features such as global RBAC, centralized management of Kubernetes clusters, automated deployments, monitoring, and logging. However, the operations capabilities for non-TKG clusters are limited compared to TKG. Additionally, as with RHACM, for OpenShift, the focus is their distributions.

4.1.1.4 Google Anthos

Google Anthos is a SaaS service running on Google Cloud Platform, no installation is available as a non-hosted software. The use of Anthos is restricted to a pay-per-use system or hiring it for a certain time.

Google Anthos provides capabilities for modernizing and managing applications across hybrid and multi-cloud environments. Some of the capabilities include centralized management of Kubernetes clusters and configuration management. Anthos offers security features like encryption, identity and access management, and compliance controls.

In addition, Anthos provides integrated observability features, including monitoring, logging, and tracing.

However, it's worth noting that the tools and methods used to manage clusters in Anthos can vary depending on whether they are deployed on-premises or in the cloud, which can make it slightly inconsistent. Additionally, Anthos does not offer the same level of capabilities for imported clusters that are not GKE or Anthos clusters.

4.1.2 Intuitive UI

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.2.1 Rancher Prime

Rancher Prime'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 Prime's design makes possible for teams to easily use Kubernetes across an organization without needing extensive training upfront. Since Rancher 2.7 extensions were added as a feature in Rancher's UI, extensions allow integration with other tools in the Rancher UI, making it more effective as a single management point for your clusters.



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

4.1.2.2 Red Hat 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 unique to OpenShift are readily available. RHACM provides a consolidated view for all your managed clusters with a clean UI.

4.1.2.3 VMware Tanzu

TKG or TKGM has no built-in management interface; VMware offers visual cluster management through Tanzu Mission Control (TMC) or vSphere for TKG. TMC is part of VMware Cloud Services and has a well-designed user interface. Depending on Tanzu's version, the users get different features from TMC and a slightly different interface.

4.1.2.4 Google Anthos

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

4.1.3 Hosted & Managed Services

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ●

4.1.3.1 Rancher Prime

SUSE also offers Rancher Prime Hosted – a premium 'white-glove' service available to organizations looking to manage and scale their Kubernetes environment without managing the operational challenges. Rancher Prime Hosted is a fully managed cloud-hosted service of Rancher Prime that alleviates the operational complexities around Rancher and Kubernetes, freeing your DevOps and Operations teams focus on innovation.

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

4.1.3.2 Red Hat 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.

4.1.3.3 VMware Tanzu

VMware does not offer TKG as a hosted or managed service, although Tanzu Mission Control is a SaaS offering. However, there are VMware Cloud services on AWS, Azure, and

GCP. In these platforms, you can deploy TKG, but TKG deployed in this manner is not a managed service.

4.1.3.4 Google Anthos

Google offers Anthos and GKE as a SaaS offering but Anthos clusters are not offered as managed services. However, Anthos and GKE clusters can use Autopilot, which offers a similar experience to a managed service. By default, users must go through Google's Cloud Services to manage their clusters and integration with Anthos management.

4.1.4 Multi-Cluster Management

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.4.1 Rancher Prime

Rancher Prime makes Kubernetes management 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 Prime is also platform agnostic when managing or deploying Kubernetes clusters. It offers full lifecycle management across the primary public cloud provider's distributions, including EKS, AKS and GKE, RKE, RKE2, and K3s. Rancher Prime leverages cluster API and Fleet to manage clusters at scale and as code. Also, it can import and manage any CNCF-conformant Kubernetes distribution. All the Rancher Prime features are available for any managed Kubernetes out of the box.

To help manage clusters at scale, Rancher Prime utilizes Fleet, an open source project that enables GitOps at scale. Built by the Rancher team, Fleet is designed to manage cluster at scale, but it can be also used to manage as code just a few clusters.

The SUSE team has also built several complementary open source tools that can be integrated with Rancher Prime 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.

4.1.4.2 Red Hat 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's important to know that the hyperscaler's Kubernetes services don't have full lifecycle management yet.

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 Red Hat OpenShift environments, RHACM integrates with Red Hat OpenShift Data Foundation to provide a business continuity solution for stateful applications on OpenShift.

4.1.4.3 VMware Tanzu

Tanzu Kubernetes grid management clusters 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 AWS or Microsoft Azure. To get comprehensive full lifecycle management and full functionality of TKG Clusters, operators must subscribe to TMC, which offers the capabilities to manage non-Tanzu clusters amongst other. However, they do not have full lifecycle management capabilities for anything else than TKG clusters.

4.1.4.4 Google 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 versus 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 a higher complexity that they need to solve to deploy and manage them.

4.1.5 Edge Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ◐
- Google Anthos: ◐

4.1.5.1 Rancher Prime

Rancher Prime offers robust edge capabilities for operators looking to build a secure and resilient Kubernetes environments at the edge. By leveraging distributions like K3s and RKE2, Rancher Prime enables users to create a lightweight blueprint that consumes minimal resources. In addition, it can be easily installed on a single node using Docker, making it an ideal solution for edge locations where resources are often limited. With these features, Rancher Prime provides a flexible and scalable solution for managing Kubernetes clusters at the edge.

K3s, a lightweight Kubernetes certified distribution, was originally developed by the Rancher team to run in remote, resource-constrained environments. It has since become one of the most widely used distributions worldwide, with millions of downloads, and is now 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.

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.

For telco use cases SUSE created the Adaptive Telco Infrastructure Platform (ATIP) which leverages Rancher, Fleet (GitOps), cluster API, metal3 and other solutions to offer an open world class telco platform.

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 Prime, 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.

4.1.5.2 Red Hat OpenShift

Red Hat's offering in edge and strategy has evolved in the last year. From 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, 16 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 edge offering Red Hat Device Edge which leverages the MicroShift project as a low blueprint Kubernetes-like solution on Tiny edge devices. MicroShift is based on Podman running a pod that implements the Kubernetes API, but it is not a Kubernetes distribution. It can't run CNI or CSI plugins like Kubernetes clusters do.

Ansible is also part of this solution, providing configuration management at scale. With RHACM you can manage common OpenShift clusters, SNO and MicroShift leveraging GitOps for management.

4.1.5.3 VMware 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.

All the solutions discussed require ESXi to function, compelling you to purchase additional VMware products while limiting the ability to run workloads on bare metal.

Presently, VMware is enhancing its offerings for edge computing with TKG 2.1. As an experimental feature, it now supports the deployment of single-node TKG clusters with minimal operating systems for vSphere. These clusters utilize a new, optimized runtime designed explicitly for edge computing.

4.1.5.4 Google 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.

4.1.6 Integrated Public Cloud Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.6.1 Rancher Prime

Rancher Prime offers full lifecycle support for deployment into managed Kubernetes solutions from Amazon (EKS), Google (GKE), and Azure (AKS). Operators can also use Rancher Prime to create clusters from other hosted cloud providers including Digital Ocean, Linode, Alibaba, Baidu, Huawei, and Tencent. If a user wishes to deploy a cluster with a new provider, they can import nodes directly from the UI using the Custom option.

With EKS, GKE and AKS, Rancher Prime can now import, provision, upgrade, configure and secure clusters across all three environments directly using Rancher's updated unified, intuitive user interface. 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.

Rancher Prime offers a cloud hosted service that offer the same capabilities than Rancher Prime without the burden to manage and maintain Rancher Prime's infrastructure.

Rancher Prime does not require a specific distribution for the primary public cloud platforms when operating in a public cloud. The installation of Rancher Prime is fully supported on AKS, EKS, and GKE.

4.1.6.2 Red Hat 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 Alibaba, 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. It offers full lifecycle management for OpenShift managed services in Azure (ARO), AWS (ROSA) and IBM Cloud (ROKS).

4.1.6.3 VMware 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 cloud provider first and then imported. Tanzu can deploy TKG clusters on AWS, Azure and GCP.

4.1.6.4 Google Anthos

Like Tanzu, Anthos enables the import and management of existing EKS and AKS clusters, in addition to the direct management of GKE and Anthos clusters. No full lifecycle management capabilities are available for EKS and AKS clusters in Anthos.

4.1.7 Bare Metal, OpenStack & vSphere

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.1.7.1 Rancher Prime

Rancher Prime provides the capabilities needed to deploy and manage RKE, RKE2 and K3s clusters across these platforms. Rancher Prime is also able to manage any CNCF compliant Kubernetes distribution running on these environments through the platform's agnostic approach to running Kubernetes anywhere. It provides fully automated deployment method for OpenStack and vSphere, for Bare Metal the nodes must be provisioned beforehand and then using the custom option you can perform an automated deployment of RKE, RKE2 or K3s. Rancher Prime also is able to manage Harvester HCI solution and to deploy in an automated fashion and manage RKE, RKE2 or K3s on top of Harvester.

4.1.7.2 Red Hat OpenShift

OpenShift can be deployed in Red Hat 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 Red Hat which limit choices for users and promotes lock-in to the Red Hat ecosystem.

4.1.7.3 VMware 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. However, Tanzu can't and won't deploy clusters on Bare Metal or OpenStack since VMware's business relay in Virtualization.

4.1.7.4 Google 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. There's a new feature added to Anthos clusters on Bare Metal which allows customers to deploy VM's using KubeVirt.

4.1.8 Import Existing Clusters

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.8.1 Rancher Prime

Rancher Prime simplifies cluster management by allowing users to import their existing Kubernetes clusters into the Rancher UI. This includes clusters running on cloud providers, hosted platforms, bare metal or virtual machines, and other platforms. If the cluster is running an unmodified version of Kubernetes, importing it into Rancher Prime requires no additional steps. However, for non-standard versions of Kubernetes, such as OpenShift or Tanzu, some configuration may be needed to enable Rancher Prime's management capabilities. Once imported, Rancher Prime offers full management capabilities for any Kubernetes cluster.

4.1.8.2 Red Hat 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, but not for AKS, EKS and GKE. However, RHACM offers fewer features to non-OpenShift clusters.

4.1.8.3 VMware Tanzu

Tanzu Mission Control (TMC) can import clusters from external providers. TMC is a SaaS solution available to the highest Tanzu subscriptions. TMC can import most of the Kubernetes distribution, but it doesn't offer to all of them the same capabilities it does for TKG.

4.1.8.4 Google Anthos

Anthos includes 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.

4.1.9 Centralized Audit

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.9.1 Rancher Prime

Rancher Prime 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 Prime 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 Prime also supports the standard API logging available from Kubernetes.

4.1.9.2 Red Hat 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.

4.1.9.3 VMware 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.

4.1.9.4 Google 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.

4.1.10 Cluster Self-Service Provisioning

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ○

4.1.10.1 Rancher Prime

Rancher Prime uses a granular permissions scheme to grant or deny access to resources at the Global, Cluster, Project, and Namespace levels. Users with access to the Rancher server will only see their own clusters, logs 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 Prime is used with RKE/RKE2/K3s, the admin can also use templates to standardize cluster configurations. Rancher Prime will guarantee that every cluster it provisions from an RKE template is uniform and consistent in the way it is produced.

4.1.10.2 Red Hat OpenShift

OpenShift is a single-cluster solution that must be deployed via the installer binary. It does not contain any means for launching new clusters. However, RHACM can deploy OpenShift clusters in multiple environments using the CLI, API or UI.

4.1.10.3 VMware 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 TKG workload clusters.

4.1.10.4 Google 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.

4.1.11 Private Registry and Image Management

- Rancher Prime: 
- Red Hat OpenShift: 
- VMware Tanzu: 
- Google Anthos: 

4.1.11.1 Rancher Prime

Rancher Prime offers comprehensive support for private registries, allowing users to easily enter their registry credentials through a dedicated tab in the user interface. These credentials are securely stored as Kubernetes Secrets and utilized when accessing private registries. While SUSE does not offer a registry tool on their catalog, Rancher Prime seamlessly integrates with any third-party registry available on the market.

For organizations with heightened security needs, Rancher Prime provides the option to deploy from a trusted private registry. This feature is accessible to all customers who have subscribed to Rancher Prime support. By leveraging Rancher Prime's powerful private registry capabilities, organizations can rest assured that their software deployments are secure and reliable.

4.1.11.2 Red Hat 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. Red Hat offers a registry with Quay which is a separated product with an extra subscription. OpenShift can be used with other third-party registries.

4.1.11.3 VMware Tanzu

vSphere with Tanzu simplifies the process of setting up a centralized Harbor registry for private images. By enabling the registry on the management cluster, downstream clusters can utilize it without additional configuration. VMware leverages the open-source project Harbor as the registry for Tanzu, ensuring a reliable and secure experience.

Tanzu takes advantage of the native features within Kubernetes to access authenticated and private registries. To enable this functionality, users must manually create registry credential objects and associate them with the corresponding workloads.



4.1.11.4 Google Anthos

Anthos also 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 previously known as Google Container Registry –now Artifact Registry– as part of the GCP service offering and encourages its use in Anthos/GKE clusters. This is an additional paid service as you must pay for the storage consumed by the images stored.

4.1.12 Cluster Upgrades and Version Management

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.1.12.1 Rancher Prime

Rancher Prime users can easily upgrade their Kubernetes clusters to the latest versions without downtime or disruptions to their applications.

Rancher Prime allows users to manage multiple Kubernetes clusters from a single control plane, simplifying the upgrade process. Users can easily view the status of each cluster and upgrade them as needed. With Rancher Prime, upgrading Kubernetes is a simple process that involves just a few clicks.

Rancher Prime also allows users to upgrade their Kubernetes clusters at their own pace. Users can choose to upgrade all their clusters at once or one at a time, depending on their needs. This flexibility ensures that users can upgrade their clusters without disrupting their applications.

In addition to upgrading Kubernetes clusters, Rancher Prime also provides users with tools for managing different versions of Kubernetes. This includes the ability to create new clusters with specific versions of Kubernetes and the ability to manage multiple versions of Kubernetes in a single cluster. This allows users to test new versions of Kubernetes before upgrading their production clusters.

Rancher Prime also enables upgrades in air-gapped environments.

4.1.12.2 Red Hat OpenShift

OpenShift is a platform that leverages Kubernetes Operators for deploying and upgrading OpenShift cluster components. This allows for updates to be made without downtime to running workloads, and upgrades can be triggered through the CLI or UI. However, it's important to note that once a cluster has been upgraded, there is no possibility for a rollback to a previous version.

Before triggering an upgrade, it's crucial to check the release paths to determine which versions are available for an upgrade. Additionally, OpenShift is only able to upgrade one cluster at a time. However, with the Red Hat Advanced Cluster Management (RHACM) solution, customers can upgrade multiple OpenShift clusters simultaneously through policies or manually using the UI.

4.1.12.3 VMware Tanzu

TKG clusters support cluster upgrades through the CLI. However, upgrades are tied to the version of the TKG CLI and require users to download and install virtual machines and base image templates before initiating the upgrade process. It's important to note that a cluster upgrade replaces the virtual machines and must be performed on the management cluster first.

The upgrade process for TKG can be a challenge for cluster administrators as multiple prerequisites and post-upgrade re-registration tasks need to be completed.

Unfortunately, the documentation does not clarify if user-deployed self-service clusters require a cluster administrator to perform the upgrade. However, the number of steps needed and the dependency on the management server imply that upgrades may not be very user-friendly.

Alternatively, clusters deployed through Tanzu Mission Control provide an intuitive interface for upgrades, making it a more user-friendly option. Tanzu Mission Control simplifies the upgrade process and eliminates the need for complex command-line operations.

4.1.12.4 Google Anthos

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

For Anthos on bare metal, the admin cluster must be upgraded first, followed by the user clusters. It's important to note that user clusters must be at most one minor version number behind the new version of the admin cluster before upgrading the admin cluster. Unfortunately, the documentation doesn't explain what happens if user clusters deviate from this requirement. Additionally, upgrades are restricted to the single supported cluster version in the bmctl utility used to manage clusters.

The latest release of Anthos has improved the upgrade process. For GKE or Anthos clusters running on public cloud, upgrades can be performed using the gcloud CLI, through the multi-cloud Anthos API, or the Anthos UI. The upgrade process starts with the control plane, spins up a new node with the latest configuration. Then, the process tests the new node, and if the tests pass, it proceeds instance by instance until the upgrade is complete. This simplifies the upgrade process and eliminates the need for manual intervention, improving the user experience for cluster administrators.

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.

4.1.13 Storage Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ◐



4.1.13.1 Rancher Prime

The Rancher team created and contributed to Longhorn (a persistent block storage open source project governed by the CNCF) and maintained 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. All these solutions can be seamlessly deployed from the Rancher Prime Marketplace on any managed cluster. Rancher Prime also supports the storage of the public cloud providers.

4.1.13.2 Red Hat 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 is 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.

4.1.13.3 VMware 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.

4.1.13.4 Google Anthos

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

4.1.14 Arm Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.1.14.1 Rancher Prime

RKE and K3s support installation on Arm64 and Arm7. RKE2 will have support for Arm in 2023. Rancher by SUSE, partners with Arm and works closely with their engineering team on new releases.

4.1.14.2 Red Hat OpenShift

OpenShift can be deployed on Arm processors, but not in any Arm environment there is a list of compatible hardware. Also, OpenShift can be deployed on AWS Arm instances.

In January 2022 Red Hat announced MicroShift, a new research project that explores how OpenShift 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. MicroShift is a GA product and is part of the Red Hat edge solution.

4.1.14.3 VMware 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.

4.1.14.4 Google Anthos

Anthos started supporting the deployment of Anthos clusters on AWS Arm instances not long ago, also GKE running on Google Cloud Platform Arm instances.

4.1.15 IBM Z and LinuxONE support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.1.15.1 Rancher Prime

RKE2 supports installation across any enterprise Linux distribution that is certified for the s390x architecture which are IBM Z and LinuxONE servers. RKE2 can run on the IBM z/VM hypervisor, KVM hypervisor, or in an LPAR. K3s is currently in technical preview for s390x. Rancher 2.6.4 and any new version can run RKE2 across s390x. Currently it can manage downstream RKE2 clusters running on s390x. Additional Rancher Prime for IBM z including logging, monitoring, alerting, and cloud operators are planned for upcoming releases.

4.1.15.2 Red Hat OpenShift

Red Hat added support for IBM Z and LinuxONE in OpenShift 4.2 running as virtual machines on the IBM z/VM hypervisor. Today the latest OpenShift versions support running as virtual machines on the IBM z/VM and RHEL KVM. Red Hat Enterprise Linux CoreOS is the only Linux operating system choice to run OpenShift. .

4.1.15.3 VMware Tanzu

There is no mention of s390x support in official VMware Tanzu documentation.

4.1.15.4 Google Anthos

No mention of s390x support in Anthos documentation.

4.1.16 Airgap Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.1.16.1 Rancher Prime

Rancher Prime offers a solution for managing Kubernetes clusters in air-gapped environments where direct internet connectivity is unavailable. Rancher Prime provides an Air Gap Guide outlining the steps to set up and operate the platform to facilitate this.

To deploy and manage Kubernetes clusters in an air-gapped environment using Rancher Prime, the Rancher server and agent images must be downloaded and pre-loaded onto an internal registry. The Rancher server and clusters must then be configured to use this internal registry. Once this is complete, Rancher Prime can be used to manage Kubernetes clusters without requiring an internet connection.



Overall, Rancher Prime provides an easy-to-implement solution for managing Kubernetes clusters in air-gapped environments. By following the Air Gap Guide and pre-loading the necessary images onto an internal registry, Rancher Prime can be used to simplify cluster management and deployment in environments where internet connectivity is unavailable.

4.1.16.2 Red Hat 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.

4.1.16.3 VMware 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.

4.1.16.4 Google 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.

4.1.17 Etcd Backup and Restore

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.1.17.1 Rancher Prime

All Rancher-deployed 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.

Rancher Prime's backup need the installation of the rancher-backup operator which is available on Rancher Prime's UI. It will install in the Rancher server Kubernetes cluster. Once configured the agent will perform backups automatically of the Rancher server cluster and the managed clusters.

Restoring an HA cluster requires deploying a new Kubernetes cluster, restoring the backup, and performing a new Rancher Prime installation. Upon completion, all remote Kubernetes clusters will reconnect to the new cluster.

4.1.17.2 Red Hat 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. With the launch of RHACM 2.7 the backup and disaster recovery capabilities for RHACM and OpenShift have improved. RH offers different options with the backup and restore operator that runs Velero under the hood.

4.1.17.3 VMware 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.

4.1.17.4 Google 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.

4.2 Security, Policy & User Management

4.2.1 Active Directory and LDAP Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ○

4.2.1.1 Rancher Prime

Rancher Prime 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.

4.2.1.2 Red Hat 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.

4.2.1.3 VMware Tanzu

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

4.2.1.4 Google 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.



4.2.2 Network and Security Policies

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.2.2.1 Rancher Prime

Rancher Prime supports Pod Security Admission (PSA), this replaces the old Pod Security Policies in Kubernetes. Also ships with OPA Gatekeeper, integrates with Kubewarden, and NeuVector (additional subscription required) being one of the solutions in the market offering more alternatives when it comes to security and admission controllers.

Rancher Prime supports standard Kubernetes network policies, and NeuVector provides advanced network policy creation and enforcement capabilities to secure your Kubernetes clusters. By leveraging a cloud-native Layer 7 container firewall and behavioral learning, NeuVector can automatically discover connections and application protocols between services and create whitelist rules to isolate them. This ensures enhanced security and compliance. Additionally, depending on your choice of Container Network Interface (CNI), you may have access to a wider range of network policies to improve your cluster's security posture further.

4.2.2.2 Red Hat OpenShift

OpenShift integrates PSA with Security Context Constraints to enforce access to namespaces and pods. OpenShift Container Platform provides security context constraints (SCC) that control the actions that a pod can perform and what it has the ability to access.

OpenShift includes support for network policies and multiple pod networks for traffic isolation.

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/Gatekeeper, and Kyverno.

Regarding networks policies things get a little more complex in OpenShift, by default Red Hat offer two network plugins for OpenShift OVN and OpenShiftSDN. OpenShift supports standard Kubernetes network policies.

4.2.2.3 VMware Tanzu

Tanzu Kubernetes Grid (TKG) has the ability of using PSA that are present natively in Kubernetes but also can work with OPA Gatekeeper.

TKG uses Antrea (default) or Flannel for networking. Antrea has its own advanced network policy extensions but also supports Kubernetes Network Policies. However, there are more options like Calico or NSX.

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.



4.2.2.4 Google 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.

4.2.3 Policy as code

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.2.3.1 Rancher Prime

Policy as code is defining policies using code and enforcing them consistently across an organization's resources. Rancher Prime provides tools for implementing policy as code, enabling users to codify their governance policies and apply them consistently across their Kubernetes resources.

Rancher Prime offers different tools for implementing policy as code:

- Kubewarden: A policy engine that enables users to define policies using simple, high-level declarative language and enforce them across Kubernetes resources. Kubewarden provides a library of pre-built policies that can be used out of the box or customized to meet specific organizational requirements.
- NeuVector, is a container security platform that provides network inspection, host security, and container process monitoring to protect Kubernetes workloads. NeuVector enables users to define security policies using simple, high-level declarative language and enforce them across Kubernetes resources.
- Open Policy Agent (OPA) is a powerful policy engine that allows users to define policies in a high-level declarative language and enforce them across Kubernetes resources. OPA can be integrated with the managed clusters Kubernetes API server using the Kubernetes Admission Controller, which evaluates policies before a resource is created or updated.
- Gatekeeper is another excellent tool that enables users to define policies as Kubernetes Custom Resource Definitions (CRDs) and enforce them across Kubernetes resources. Gatekeeper uses OPA to evaluate policies and implements them using Kubernetes Admission Control.

Using policy as code with Rancher Prime helps organizations ensure their Kubernetes resources are secure and compliant and operate according to best practices. By defining policies as code, organizations can automate enforcing these policies, reduce the risk of human error, and provide a consistent experience across their Kubernetes resources. Kubewarden and NeuVector are two powerful tools that can help organizations easily achieve these goals.

4.2.3.2 Red Hat OpenShift

Red Hat OpenShift integrates with robust tools for implementing policy as code as any other Kubernetes distribution. These tools are:

- Open Policy Agent (OPA) can be integrated with Red Hat OpenShift's Kubernetes API server using the Kubernetes Admission Controller, which evaluates policies before a resource is created or updated.
- Gatekeeper uses OPA to evaluate policies and implements them using Kubernetes Admission Control.

While these two options are standard and can be implemented in any Kubernetes cluster locally, RHACM provides a policy engine based on GitOps. This enables Red Hat customers to distribute and manage policies at scale from RHACM.

4.2.3.3 VMware Tanzu

Policy as code defines and enforces policies using code, which can be versioned, reviewed, and automated.

Tanzu Mission Control offers two primary tools for implementing policy as code:

- Policy Library: A curated set of policies that can be used out of the box or customized to meet specific organizational requirements. These policies are defined using Open Policy Agent (OPA) language and can be applied to Kubernetes clusters, namespaces, and objects.
- Custom Policies: A user-defined set of policies that users can create and manage. These policies can be written in rego (OPA language), or any other language supported by OPA. Users can define policies that enforce security, compliance, and operational best practices, among others.

.

4.2.3.4 Google Anthos

Google Anthos provides tools for implementing policy as code that enable users to define, manage, and enforce policies across their Kubernetes clusters, hybrid, and multi-cloud environments.

The tools for implementing policy as code in Anthos:

- Anthos Config Management: A tool for managing and enforcing policies across multiple clusters and environments using declarative configuration files. These configuration files are written in Kubernetes-native YAML and can be versioned and audited using Git.
- Policy Controller: A tool for defining and enforcing policies at the Kubernetes API server level using Open Policy Agent (OPA) language. Policy Controller enables users to define policies that enforce security, compliance, and operational best practices.

4.2.4 Configurable Adherence to CIS Security Benchmarks

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.2.4.1 Rancher Prime

Rancher Prime maintains a [hardening guide and self-assessment](#) that references CIS benchmarks with specific user actions to satisfy the requirements. Rancher Prime



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, SUSE 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 Prime platform.

4.2.4.2 Red Hat 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.

4.2.4.3 VMware 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.

4.2.4.4 Google 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.

4.2.5 RBAC Policies

- Rancher Prime: ●
- Red Hat OpenShift: ○
- VMware Tanzu: ○
- Google Anthos: ○

4.2.5.1 Rancher Prime

Rancher Prime 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 Prime 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 Prime provides an authorization proxy which



allows to use the CLI, UI or API to manage not only the Rancher Prime cluster but all the clusters managed by it from a single point.

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.

4.2.5.2 Red Hat OpenShift

OpenShift uses native Kubernetes RBAC, which is managed through the `oc` command or the UI. It doesn't include centralized RBAC management like Rancher Prime does. RHACM, which can provide basic policies for certain subsets of clusters or clustersets can provide an automated manner to manage RBAC for the managed clusters. 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.

4.2.5.3 VMware 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.

4.2.5.4 Google 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.

4.3 Shared Tools & Services

4.3.1 Application Catalog

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ◐

4.3.1.1 Rancher Prime

Rancher Prime'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. The Application catalog in Rancher Prime, comes out of the box with Rancher software helm repository, partners helm repository and the Rancher admins can provide new helm repositories from where the users and developers can install software in one click.



4.3.1.2 Red Hat 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 repository to access their code and base image with the programming language needed to deploy a pod.

4.3.1.3 VMware 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.

4.3.1.4 Google 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 non-GKE Anthos application deployment process.

4.3.2 Integration with configuration management tools

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.3.2.1 Rancher Prime

Rancher maintains the [Terraform provider](#), enabling users to deploy and manage Rancher Prime using Infrastructure as Code (IaC) principles. Although not officially integrated with other solutions, Rancher's open API make it easy to integrate with solutions such as Ansible, Puppet, Chef, AWS autoscaling groups, or any configuration management tool.

4.3.2.2 Red Hat 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.



4.3.2.3 VMware Tanzu

VMware 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.

4.3.2.4 Google 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.

4.3.3 CI/CD Capabilities & GitOps

- Rancher Prime: 🟡
- Red Hat OpenShift: 🟢
- VMware Tanzu: 🟡
- Google Anthos: 🟢

4.3.3.1 Rancher Prime

Rancher Prime 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 Prime and can also be installed on any Kubernetes cluster via Helm.

GitOps and Fleet (Rancher CD) are crucial for SUSE's strategy for multi-cluster management and Edge. In fact, Fleet is part of SUSE Edge 2.0 solution and of the innovative Adaptive Telco Infrastructure Platform or ATIP that has been released in February 2023.

4.3.3.2 Red Hat 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 solution based on the open source project Argo CD (OpenShift GitOps). RHACM provides also a GitOps engine and integration for OpenShift GitOps.

4.3.3.3 VMware 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, also TMC its management piece is not well suited for GitOps.



4.3.3.4 Google 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.

4.3.4 Desktop Kubernetes & Container Management

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ○

4.3.4.1 Rancher Prime

In 2021, Rancher by SUSE introduced Rancher Desktop, an open-source alternative to Docker Desktop that operates on Linux, Mac, and Windows systems. Rancher Desktop has a customizable Kubernetes distribution based on K3s and a user-friendly interface. It also allows you to manage containers by pulling, pushing, and building images, like Docker Desktop, but with the added advantage of Rancher's UI and without the limitations that Docker has been introducing lately.

The Rancher UI functions as a dashboard for the local cluster and enables users to deploy Helm charts, execute kubectl commands, and select either Docker or containerd as a container runtime, all within one interface. It is also adaptable and user-friendly, with a developer-oriented design that allows for automated updates with each new release and the option to upgrade different CLIs as needed.

Furthermore, Rancher Desktop integrates with popular developer tools such as VSCode, Traefik Proxy, and other CI/CD tools, providing users with a complete local developer toolset and environment to build, test, and develop applications. By simplifying the build process, Rancher Desktop aids developers in increasing their efficiency and productivity.

4.3.4.2 Red Hat OpenShift

OpenShift provides code-ready workspaces, which function as a local version of OpenShift on developers' machines, allowing for seamless coding and development. However, this resource-intensive feature may negatively impact the user experience, resulting in suboptimal performance.

Furthermore, the lack of features and subpar usability of OpenShift's code-ready workspaces has significantly impacted community adoption. Developers require tools that are feature-rich and user-friendly and perform optimally, allowing them to focus on their coding and development tasks without unnecessary disruptions.

Red Hat created Podman which is an open source solution to replace docker, now also provides Podman Desktop which also covers the capabilities that Docker desktop provides.

4.3.4.3 VMware Tanzu

VMware has launched an open-source project called Octant, which serves as a web interface for Kubernetes clusters. This interface enables users to inspect Kubernetes objects, applications, and clusters. Although Octant is a useful tool for Kubernetes clusters, it only provides some of the functionalities available in Rancher Desktop. While Octant can

inspect the clusters and applications, it lacks local image and container management tools, a customizable Kubernetes distribution, and integration with popular developer tools. These features are crucial for streamlining the development process and increasing productivity.

Therefore, while Octant is a valuable resource for developers, it is not a complete alternative to Rancher Desktop.

4.3.4.4 Google Anthos

As far as today Google doesn't offer any solution like Podman, Rancher Desktop or Octant.

4.3.5 Advanced Monitoring

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●

4.3.5.1 Rancher Prime

Rancher Prime 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.

4.3.5.2 Red Hat 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.

4.3.5.3 VMware Tanzu

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.

4.3.5.4 Google 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.

4.3.6 Alerts and Notifications

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ●



4.3.6.1 Rancher Prime

Both the default basic monitoring and the optional advanced monitoring configure alerts for critical cluster components. Users need only create notification targets. Rancher Prime 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.

4.3.6.2 Red Hat 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.

4.3.6.3 VMware 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.

4.3.6.4 Google 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.

4.3.7 External Log Shipping

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ●

4.3.7.1 Rancher Prime

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.

4.3.7.2 Red Hat 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.

4.3.7.3 VMware 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.



4.3.7.4 Google 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).

4.3.8 Windows Container Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.3.8.1 Rancher Prime

Rancher Prime supports the use of Windows worker nodes as a custom cluster. To install Kubernetes on existing nodes.

However, it's important to note that the Kubernetes control plane can only run on Linux nodes, while Windows nodes can only be used as worker nodes for running Windows-based workloads. To add Windows nodes to a cluster, Windows support must be enabled during cluster creation.

Windows workers are currently supported on RKE and RKE2 clusters, but support for Windows workers on K3s is on the roadmap for 2023.

You can easily manage and deploy Windows-based container workloads alongside Linux-based workloads by enabling Windows worker nodes in Rancher Prime. This provides a more unified container management experience across different operating systems and simplifies the deployment of hybrid workloads.

4.3.8.2 Red Hat OpenShift

OpenShift (OCP4) offers production support for using Windows servers in Kubernetes clusters. This allows you to deploy Windows containers under the management of an OpenShift control plane.

To add Windows workers to any OpenShift cluster running on AWS, Azure, GCP, or vSphere, you can use the Windows Machine Config Operator (WMCO), which can be found in the OperatorHub. With the WMCO, you can easily add Windows workers to your existing OpenShift cluster, enabling you to run Windows-based container workloads.

For OpenShift 4.8+ and WMCO 3.1.0+, Windows is also supported via a "Bring Your Own Host" (BYOH) approach with the WMCO. This approach allows you to bring your own Windows hosts to an OpenShift cluster and add them as Windows worker nodes.

4.3.8.3 VMware Tanzu

Tanzu Kubernetes Grid (TKG) is a Kubernetes-based platform that currently does not support Windows workers or workloads. However, Tanzu Kubernetes Grid Integrated Edition (TKGI) does support Windows workers. However, it's important to note that this feature is currently in beta and only available for vSphere with the Flannel network plugin, using NSX-T for networking.



While the beta feature has been available in TKGI for some time, it's worth noting that TKGI is no longer a primary focus for VMware, as it comes from the legacy Pivotal Container Service (PKS) offering.

With the addition of support for Windows workers in TKGI, users can take advantage of a multi-platform container management experience that includes both Linux and Windows workloads. Nonetheless, it's essential to carefully review the documentation and consider the limitations of the beta feature before implementing it in a production environment.

4.3.8.4 Google 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.

4.3.9 Integrated Service Mesh Support

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ●

4.3.9.1 Rancher Prime

Rancher Prime 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.

4.3.9.2 Red Hat 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.

4.3.9.3 VMware Tanzu

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

4.3.9.4 Google Anthos

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

4.3.10 Enterprise SLA

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ●
- Google Anthos: ○

4.3.10.1 Rancher Prime

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 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.

4.3.10.2 Red Hat 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 to help with requests in addition to subscription support.

4.3.10.3 VMware Tanzu

VMware offers 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.

4.3.10.4 Google 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.

4.3.11 Community Traction

- Rancher Prime: ●
- Red Hat OpenShift: ●
- VMware Tanzu: ○
- Google Anthos: ○

4.3.11.1 Rancher Prime

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.

4.3.11.2 Red Hat OpenShift

Red Hat OpenShift is a commercial offering, its upstream project, OKD, is available as an open source alternative. Although OKD has an active community around it, the community around OpenShift is smaller and less active compared to other Red Hat communities. This is because OpenShift 4 was not an open source offering from the outset, which limited the level of participation from the broader open source community.

4.3.11.3 VMware Tanzu

VMware Tanzu tried to gain momentum within the community, primarily driven by VMware's existing customer base. Tanzu Kubernetes Grid has been particularly popular

among users with a vSphere or VMware Cloud deployment, but VMware has made extensive efforts to expand the community beyond its existing customer base. In 2021, VMware released Tanzu Community Edition, providing an opportunity for the broader open source community to test their stack on Tanzu. Additionally, VMware organized multiple events and community activities to showcase Tanzu's developer experience. However, it's important to note that as of December 2022, VMware will no longer be maintaining Tanzu Community Edition.

4.3.11.4 Google 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.

However, Google lack of a community behind their products because most of them are not available as OSS that can be installed in any lab. Their code is not open and the only way to test Anthos or GKE is through GCP.

5 About this Guide

Extensive research has been conducted to produce an informative and comprehensive buyers guide for Rancher, Tanzu, OpenShift, and Anthos, which are all complex and feature-rich Kubernetes management platforms. A team has written the guide of technical experts from SUSE, who reviewed publicly available documentation from each vendor, blogs, videos, and technology to compare the strengths and weaknesses of each platform to provide valuable insights to potential buyers.

6 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



7 Glossary

7.1 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.

7.2 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 Security Admission
 - Feature in Kubernetes that allows cluster administrators to define policies that enforce security requirements for pods. PSA uses admission controllers to intercept requests to the Kubernetes API server, evaluate the security posture of pods, and either allow or deny their creation based on pre-defined policies.
- Network policies
 - A network security policy specifies how Kubernetes resources can communicate with each other and other network endpoints.
- 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.

7.3 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.
- Integration with configuration management tools
 - 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.
- GitOps
 - GitOps is a methodology that uses Git as the single source of truth for declarative infrastructure and applications. It involves using Git as the primary interface for managing infrastructure and application deployments. Any changes made to the Git repository automatically trigger automated processes to apply those changes to the target environment. This approach ensures a consistent and auditable deployment process and enables teams to manage their infrastructure and applications as code.
- Desktop Kubernetes & Container Management
 - Developers require a straightforward and efficient method to test and deploy the containers and microservices they design. A Desktop Kubernetes or a local cluster is essential for agile development, as it

facilitates development and testing. Being able to integrate with various tools and manage containers independently for debugging and testing is a crucial aspect of a developer's daily responsibilities.

- **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.

8 Legal Statements

8.1 Copyright Notice

This document and its content are copyright of SUSE © 2022. All rights reserved. Any redistribution or reproduction of part or all the contents in any form is prohibited other than the following:

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

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

8.2 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.

8.3 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

