

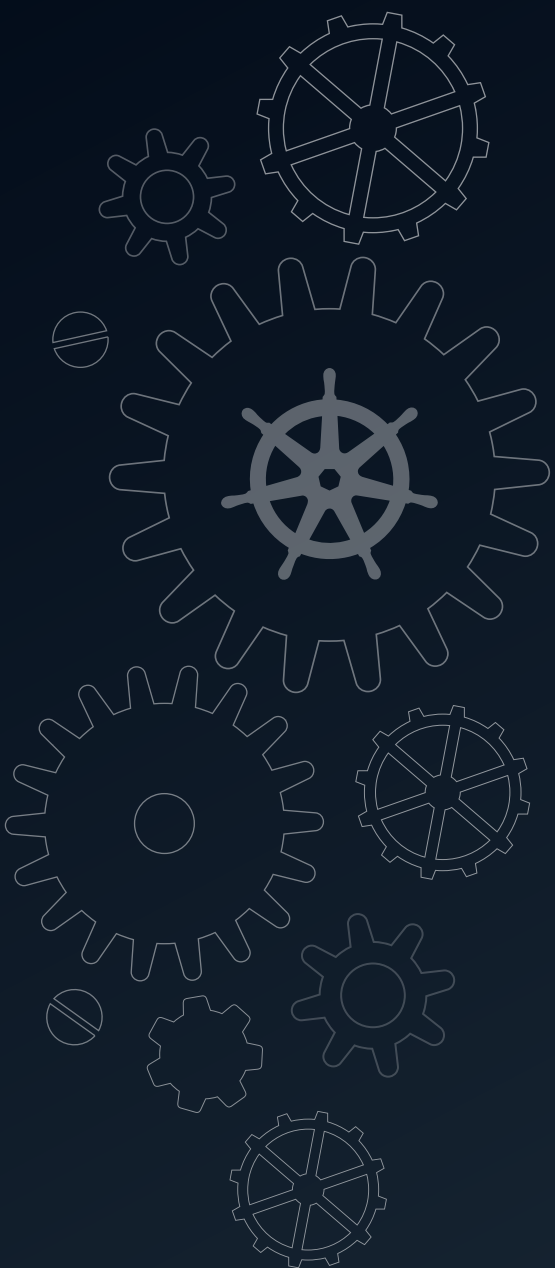


Top 6 Reasons Companies are Choosing Rafay over Rancher OSS

WHITE PAPER

CONTENTS

Introduction	03
Reason #1: A Single Controller for Your Entire Organization	04
Reason #2: Simplified Governance and Drift Detection / Remediation at Scale	05
Reason #3: Centralized Auditing of Administrative and Kube API Activity Across Your Fleet	06
Reason #4: Use Every Single Feature In Your Favorite Managed Kubernetes Service	07
Reason #5: Best-in-Class Customer Success with Kubernetes Experts Available Within Minutes, 24x7	08
Reason #6: Time-to-K8s in Days, Not Months with Low Total Cost of Ownership	09
Leverage the Power of a SaaS Platform for Kubernetes Operations	10



INTRODUCTION

If Kubernetes, as a technology, is inherently complex, then a production-grade Kubernetes infrastructure may seem impossible at first glance. The sheer amount of work involved with building all the necessary features for platform, developer, and operations teams as well as the number of tools and services that must integrate can be overwhelming.

Many enterprises cut their Kubernetes teeth using Rancher OSS. After all, it's free. So, it's a great way to learn Kubernetes in a lab and even support your first few applications. But as the number of workloads and clusters grows across multiple infrastructures, the initial plan to do it yourself (DIY) begins to show cracks that may dampen the company's ability to scale efficiently and effectively.

The total cost of ownership (TCO) of Kubernetes can be quite hard to quantify given its technical complexity, resource requirements, and the number of available deployment options. And, depending on the approach, enterprises can be surprised by the increasing hidden costs and complexity of operating Kubernetes. While the initial TCO of a Rancher OSS approach may be low, the cost and overhead increase quickly as the company expands usage across departments and grows the number of clusters under management.

This paper details six key technological and financial challenges that enterprises face on day 2 when adopting Rancher as their main Kubernetes operations platform and why many are switching to Rafay.

REASON

1

A Single Controller for Your Entire Organization

With Rancher, enterprises must run multiple controllers to maintain isolation

Rancher's Kubernetes distribution requires that each small set of clusters needing its own access control or isolation boundary has its own controller. Therefore, a separate Rancher controller is required for each and every separate team to ensure appropriate security and isolation boundaries are properly implemented. For even modest Kubernetes implementations 5-10 Rancher controllers will need to be installed and managed.

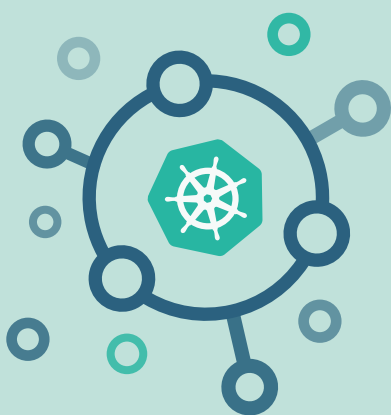
For production environments, it is necessary to deploy each controller with high availability (thus doubling the actual number of controllers required), including the necessary networking infrastructure and load balancers. As a result, the day-2 overhead associated with managing these controllers as well as the hardware portion of the TCO quickly gets out of hand, even with Rancher's hosted model.

THE RAFAY APPROACH

One controller for fleet-wide operations

With Rafay's SaaS approach, only one controller is needed to deploy and manage any number of clusters with boundary isolation through fleet-wide multi-tenancy support. As a result, platform teams easily provide business or engineering organizations completely isolated operating environments without the installation, configuration, and ongoing maintenance of dedicated controllers/servers.

This approach simplifies day-2 operations significantly since multi-cluster management is now possible from a single, unified console across all of the on-prem, bare metal, public cloud, and remote edge environments.



REASON

2

Simplified Governance and Drift Detection / Remediation at Scale

With Rancher, customers need to manage policies for each cluster, leading to fleet-wide inconsistencies

Rancher OSS's lack of native tools for drift detection and consistency enforcement allows for clusters to be built with configurations that can differ and inadvertently generate issues with authentication, outdated K8s versions and software add-ons, exposed Kube API ports to insecure networks, inconsistent RBAC profiles, and audit logging nightmares.

The impact on an enterprise's MTTR and support costs can't be overstated. In addition, potential Kubernetes security risks can severely compromise applications and IT budgets due to recurring debugging and rework or financial loss due to unscheduled downtimes.

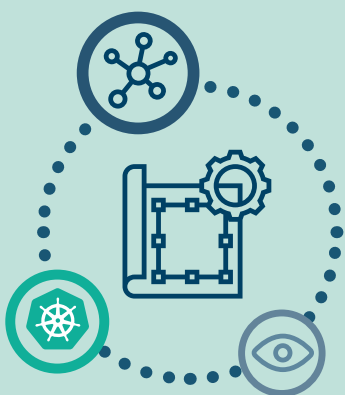
THE RAFAY APPROACH

Cluster standardization and governance built-in

Rafay's Cluster Blueprint and Drift Detection features reduce cluster sprawl and ensure cluster maintain compliance with internal policies and external regulations. With Cluster Blueprints, enterprises centrally specify and manage configurations for clusters encompassing security policy and software add-ons such as service mesh, ingress controllers, monitoring, logging, and backup and restore solutions. Enterprises typically securely manage these version-controlled cluster configurations in Git repositories.

Rafay's Drift Detection feature will detect, report, and block manual, out-of-band changes (inadvertent or malicious) to the configuration of the add-ons deployed to clusters as part of a Cluster Blueprint.

With Rafay, enterprises ensure that their fleet of clusters is consistent and standardized upon provisioning and over the lifespan of the cluster. As a result, they reduce operational and support overhead as well as business risks.



REASON

3

Centralized Auditing of Administrative and Kube API Activity Across Your Fleet

With Rancher, customers end up implementing bespoke solutions and custom code for auditing

Kubernetes clusters are critical operating infrastructure. And by default, kubectl doesn't provide any role based access control (RBAC), and executed commands are not logged by user account. As a result, security and compliance teams require deep visibility and insight into the following:

- What did a specific operator/developer do?
- When did they do it?
- On what cluster(s) did they perform the action(s)?

With Rancher, enterprises don't record or access this data by default. Typically 3rd-party tools have to be deployed or custom code has to be written in order to have a centralized view and audit log of the Kubernetes environment.

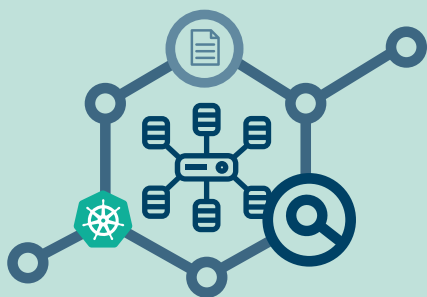
As a result, the building of this critical requirement increases the time (and support) needed to achieve an enterprise-grade K8s infrastructure. If not done correctly, this also increases security and business risk. Further, by not having multi-tenancy support, the challenges of integrating audit logs increase in complexity and cost because each set of clusters work independently with their own controller (as described in Reason #1 above).

THE RAFAY APPROACH

Automatic audit logs for all users and kubectl commands

Rafay removes the need and complexity of building a bespoke auditing capability. With Rafay, from day 1, enterprises leverage centralized and immutable audit logs of all user activity on an entire fleet of clusters including zero trust kubectl access. In addition, Rafay provides an intuitive reverse chronological view of audit logs for analytics and can stream audit logs to corporate SIEM platforms such as Splunk™ for long-term log retention and forensics.

Rafay's auditing features help enterprises prove compliance with internal policies and external regulations as well as secure the mission-critical Kubernetes infrastructure to reduce the risk of breaches and fines.



REASON

4

Use Every Single Feature In Your Favorite Managed Kubernetes Service

With Rancher, customers end up compromising EKS/AKS capabilities and services

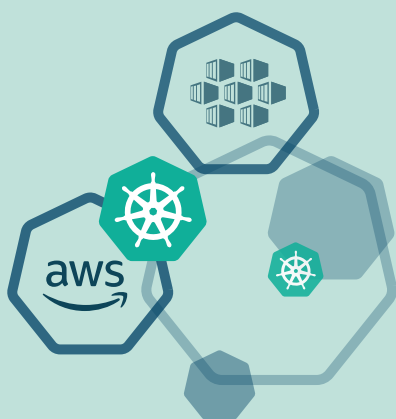
For enterprises using cloud Kubernetes distributions such as Amazon EKS and Microsoft AKS, there are two main issues when using Rancher OSS: 1) Leveraging security best practices documented by the cloud provider and 2) Leveraging all of the features from the managed service provider.

With respect to leveraging security best practices, Rancher needs direct access to the Amazon EKS control plane. So, VPC Peering (which adds ongoing costs for data transfer) has to be configured and managed for every Amazon EKS cluster under management. This can become operationally cumbersome especially if clusters are in multiple AWS regions. A separate IAM user credential has to be created and managed for Amazon EKS clusters in each AWS region which dramatically increases the operational and security complexity for enterprises.

THE RAFAY APPROACH

Leverage the best features Amazon EKS and Microsoft AKS have to offer

Rafay's deep integration with Amazon EKS/EKS-D/EKS-A and Microsoft AKS ensures zero loss of Amazon EKS & Microsoft AKS features or capabilities with the platform. This allows for full integration and comprehensive lifecycle management from leading public cloud Kubernetes distributions and products such as Amazon Fargate, Snowball, and Wavelength, and eliminates the security risks that arise from having to indirectly or separately manage access to Kubernetes environments.



REASON

5

Best-in-Class Customer Success with Kubernetes Experts Available within Minutes, 24x7

With Rancher, customers face significant support challenges, risking project delays and unhappy internal users

The modern applications that leverage Kubernetes for orchestration are mission-critical. Thus, the Kubernetes infrastructure is also mission-critical. Downtime, among other issues, can mean loss of revenue, customers, and market share.

For most businesses, the biggest source of competitive advantage is the pace of innovation. It's no secret that the speed at which an organization can improve its products and services by capturing the needs of constantly evolving markets is critical to success. With release cycles accelerating towards daily, or even multiple times a day, and as the average number of clusters continues to grow, a variety of common challenges cross-functional platform teams & operations practices struggle to solve day-in and day-out. With Rancher, customers face significant support challenges, risking project delays and unhappy internal users.

THE RAFAY APPROACH

Talk to and gain from a relationship with real K8s experts

By partnering with Rafay, enterprises have access to a Customer Success plan with deep bench of certified Kubernetes experts to jump-start & customize your Kubernetes and application modernization journey. For Rafay, it's not just about having the best product, it's about having an amazing team that supports our customers.

Stop struggling to find and retain the expertise to manage and maintain Kubernetes distributions, tools, and infrastructures. Leverage Rafay as an extension of your team, available within minutes, 24x7 with experience running Kubernetes at scale across dozens of enterprise deployments.



REASON

6

Time-to-K8s in Days, Not Months with Low Total Cost of Ownership

With Rancher, even a basic K8s infrastructure is 6-9 months away with a high TCO

Enterprises that have switched to Rafay from Rancher have stated that building a Rancher K8s infrastructure from scratch with approximately 3 engineers can take anywhere between 9 to 12 months just to launch. This is perhaps the largest hidden cost that has a negative impact on an enterprise's business. This means the enterprise cannot take advantage of the efficiencies K8s has to offer for about a year. And this directly translates into real negative business impact in the form of slower deployments, higher MTTR, and less IT agility and scalability until a fully functional K8s environment can be leveraged.

Another important aspect, as mentioned before, is that Rancher's K8s distribution requires that each small set of clusters needing its own access control or isolation boundary has its own Controller. For production environments, it is necessary to deploy Controllers with high availability (HA), including the necessary networking infrastructure and load balancers. The cost and overhead associated with managing these controllers and hardware increase TCO.

THE RAFAY APPROACH

Solve the K8s day 2 problem within hours with a low TCO

With Rafay's SaaS approach, enterprises obtain all the benefits of SaaS including a fast time-to-value. Enterprises begin utilizing a fully functional K8s infrastructure within the average of 2 to 4 weeks (with customizations and automation configured) compared to an average of 9+ months with a DIY Rancher K8s.

This is possible with Rafay because Rafay's SaaS control plane includes dozens of pre-existing features that replace all of the manual work required to build, integrate, and deploy K8s with a solution that works out of the box – including pre-built, one-click integrations with popular K8s add-ons.





Leverage the Power of a SaaS Platform for Kubernetes Operations

As enterprises modernize their applications, they are quickly realizing the significant increase in the cost and resources required to operationally manage Kubernetes clusters and application lifecycles with a DIY approach.

As stated in the introduction, Rancher OSS is a great way to learn Kubernetes in a lab and even support your first few applications. But as the number of workloads and clusters grow across multiple infrastructures, the growing complexity, work involved, and TCO limit an enterprise's ability to scale efficiently and effectively.

Rafay's SaaS-first approach enables companies to gain efficiencies from Kubernetes almost immediately, thus speeding digital transformation initiatives while keeping operating costs low. Benefits of Rafay's cloud approach include:



Reliability: Rafay's platform has consistently maintained >99.99% uptime



Fast time to K8s: Gain the benefits of Kubernetes in hours, not months



Operational Scalability: Easily manage hundreds of clusters and apps in software-defined groups with no management needed for administrative clusters



Zero-Trust Security: Cloak your K8s API endpoints so they're never visible on the Internet, and centrally configure role-based access control for easy access to any cluster, anywhere



Deployment Flexibility: Leverage the cloud or deploy the platform in air-gapped environments

Modernize security with integrated zero-trust and role-based access control for your entire fleet with Rafay Systems. **Sign up for a free trial today.**

Learn More About Rafay Systems

