

Hybrid Cloud Meets Kubernetes: How to Reduce Ops Complexity with Amazon EKS, EKS-D and Rafay Systems



As organizations move up the cloud computing maturity curve, they increasingly want flexibility in workload

locations. It's not surprising that 87% of enterprises have adopted a hybrid cloud strategy, according to [Flexera's 2020 State of the Cloud Report](#).

There are many advantages to this approach. Workloads that require processing on-premises can be kept in the data center and burst to the cloud during periods of peak activity. Organizations also often find it easier to monitor costs, utilization levels, and user activity on platforms that they own. And many want to get the greatest mileage from their existing investments while they shift workloads gradually to the cloud.

But a hybrid cloud strategy introduces some complexity as well, particularly when workloads shift between platforms. Public cloud providers take a disciplined approach to applying patches and upgrades, but the task of performing such maintenance on private clouds falls to the customer. Between skills shortages and competing priorities, patches and software releases can be overlooked or out of sync.

Hybrid clouds also present new security challenges since access controls should be consistent across platforms if workloads are shifted between them. Finally, it can be difficult for IT organizations to get a unified view of workloads distributed across multiple clouds.

87%
of enterprises have
adopted a hybrid
cloud strategy.

SOURCE: Flexera's 2020 State
of the Cloud Report



RAFAY



SPONSORED CONTENT



Kubernetes Complications

Organizations that are adopting Kubernetes for container orchestration face unique challenges that increase as hybrid cloud implementation expands. The [Cloud Native Computing Foundation](#) [reported](#) that 84% of companies ran containers in production in 2019, up from 23% three years earlier. More than three-quarters of companies that use containers also use Kubernetes.

Kubernetes adopters tend to ramp up their usage rapidly. A [recent survey](#) commissioned by VMware found that one-third of organizations that are running Kubernetes in production operate 26 clusters or more and one-fifth run more than 50 clusters.

However, Kubernetes is a complex environment to set up and operationalize, and complexity grows with scale. Kubernetes "cluster sprawl" across a hybrid infrastructure presents several operational challenges:

- Lack of standards for configuring Kubernetes clusters can create a chaotic mishmash of instances that are difficult to manage and troubleshoot.
- Provisioning Kubernetes clusters is easy but ongoing lifecycle management isn't. Cluster lifecycle management must be unified across public and private cloud infrastructure to enable consistent operations, performance monitoring, and troubleshooting, especially when a small number of clusters grow into fleets.
- Companies can't measure what they can't see but obtaining a single pane of glass view across a hybrid infrastructure spanning global regions is very difficult.
- Controlling access and user rights to all the various components of a Kubernetes infrastructure can be difficult. Access controls should be integrated with an organization's existing directories and identity management platforms, undergirded by role-based policies and audit trails.

Cloud providers deliver some these capabilities in their managed offerings. For example, Amazon Elastic Kubernetes Service (EKS) can be used to create reliable and secure Kubernetes clusters, lifting much of the deployment and operational complexity burden from users' shoulders. EKS also has unique features like [managed node groups](#) that simplify provisioning and maintenance complexity.

Amazon recently extended EKS to on-premises environments with the introduction of Amazon EKS Distro (EKS-D), a Kubernetes distribution based on and used by EKS to create reliable and secure Kubernetes clusters. EKS-D is functionally identical to EKS, fully tested, and comes with long-term AWS support.

That said, taking full advantage of EKS requires some technical skill. For example, organizations have to provision low-cost spot instances manually, and clusters must be managed on a region-by-region basis.

Making the operations of Kubernetes in hybrid infrastructures easy is where the Rafay Kubernetes Operations Platform (KOP) shines. With the Rafay KOP, enterprises can:

- Easily provision clusters from a preapproved set of standardized EKS and EKS-D clusters
- Gain unified visibility and streamline cluster lifecycle management across AWS regions
- Govern access to and audit the operations performed on clusters for security and compliance purposes.

Amazon Elastic Kubernetes Service (EKS) can be used to create reliable and secure Kubernetes clusters, lifting much of the deployment and operational complexity burden from users' shoulders.

With the Rafay KOP, enterprises obtain these benefits across any environment in the cloud or within data centers via a single pane of glass UI, as well as a CLI or API. Exactly how is detailed below.

Standardizing Cluster Blueprints in Hybrid Environments

Customers accustomed to the convenience of the AWS managed EKS service may find the EKS-D environment a bit more work. Cluster provisioning is straightforward using the EKS console but requires more technical dexterity in EKS-D. And, as the number of clusters increase, it becomes increasingly hard to govern and onerous to support the growing variety of cluster configurations across a company's hybrid infrastructure.

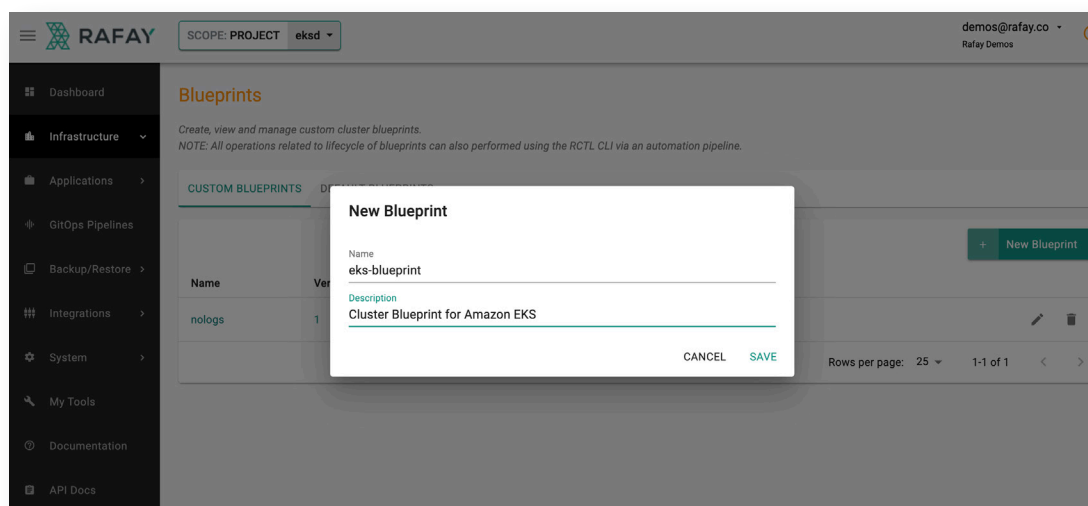
Enterprises with even a small number of Kubernetes clusters need capabilities to ensure that their clusters are compliant and have a certain baseline set of software components as required by the organization. For example, consider a global organization in the financial vertical with 10-20 Kubernetes clusters. They may require some of their clusters to be compliant with the PCI DSS and others with GDPR. Clusters used by their QA teams may require certain specialized software add-ons. Doing this manually is operationally cumbersome, error prone and time-consuming.

The best approach to controlling Kubernetes is to standardize configuration options for elements such as security, storage, and visibility—and apply them consistently. This vastly simplifies administration and makes patching and upgrading easier at scale. Ideally, multiple sets of preapproved cluster configurations can be used by different internal groups and at different development stages. Consistently applying saved specifications eliminates cluster configuration sprawl, and dramatically simplifies support.

Using Rafay Cluster Blueprints to Standardize Amazon EKS and Amazon EKS-D Clusters

With the Rafay KOP, enterprises can create one or more sets of reusable cluster configurations. Each blueprint centrally specifies configurations for clusters encompassing security policy and software add-ons such as service mesh, ingress controllers, and backup and restore solutions.

Creating a blueprint takes just a few clicks:



The best approach to controlling Kubernetes is to standardize configuration options for elements such as security, storage, and visibility—and apply them consistently.

All Rafay KOP cluster blueprints are automatically version-controlled. Customers can also manage versions in their Git repositories. The next step is to configure the blueprint with the appropriate add-ons. See below for an example of a custom blueprint.

The entire history of cluster blueprint versions is maintained on the Rafay KOP.

blueprints > eks-blueprint > New Version

New Version

Create a new version of a cluster blueprint based on the configuration provided below

Version Name *

Pod Security Policies

Add-Ons

Managed System Add-Ons

Name: eks-blueprint

Provide a unique version for the cluster blueprint

Select one or more PSPs from the available list

Select one or more addons and their versions from the available list

The list of default addons that will be part of this cluster blueprint.

Version Name *

Pod Security Policies

Add-Ons

Managed System Add-Ons

amazon-cloudwatch

v1.24

+ ADD DEPENDENCY

alb-ingress-controller

v1.1.8

+ ADD DEPENDENCY

calico

v1.6

+ ADD DEPENDENCY

nginx-ingress-controller-v035

v035

+ ADD DEPENDENCY

+ ADD MORE

Ingress Controller

Log Aggregation

Monitoring & Alerting

Rafay K8s Operator

☐

☐

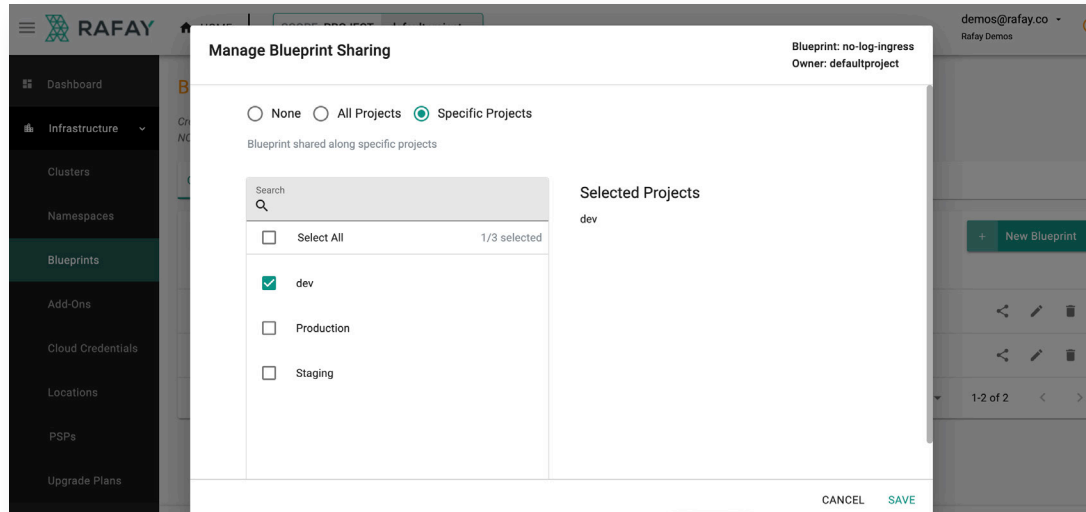
☒

☒

How to Reduce Complexity with Amazon EKS, EKS-D and Rafay Systems

4

Once a custom cluster blueprint has been created, it can be used during initial provisioning or applied to existing clusters. Blueprints can be created centrally and shared across projects ensuring the entire enterprise—across departments and across the globe—is using standardized clusters.



Unified Cluster Visibility & Monitoring

AWS's EKS dashboard provides good management and status reporting on individual clusters but customers with large distributed Kubernetes environments may require finer levels of control. AWS infrastructure is also defined by regions, meaning that customers must log into each region individually to monitor status and perform maintenance.

A hybrid cloud environment presents additional challenges because the EKS dashboard does not extend to EKS-D configurations. Customers must build and maintain their own monitoring tools for on-premises use. Monitoring and maintaining a large, multi-region Kubernetes environment may involve logging into multiple dashboards and consolidating information manually.

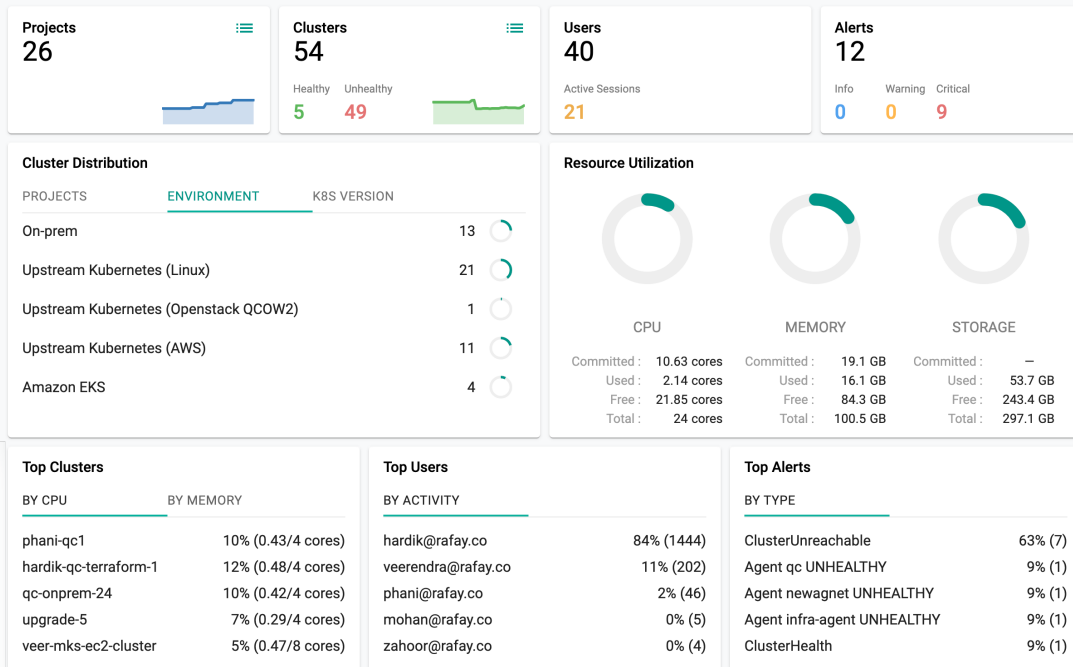
A comprehensive dashboard should provide a single view of all clusters and include information on location, resource utilization, and other factors. Users should be able to drill down by cluster to see utilization details, workload status, and history. Similar details should also be available at the node, pod, and individual container level.

Unified Cluster Visibility of Amazon EKS and Amazon EKS-D with the Rafay KOP

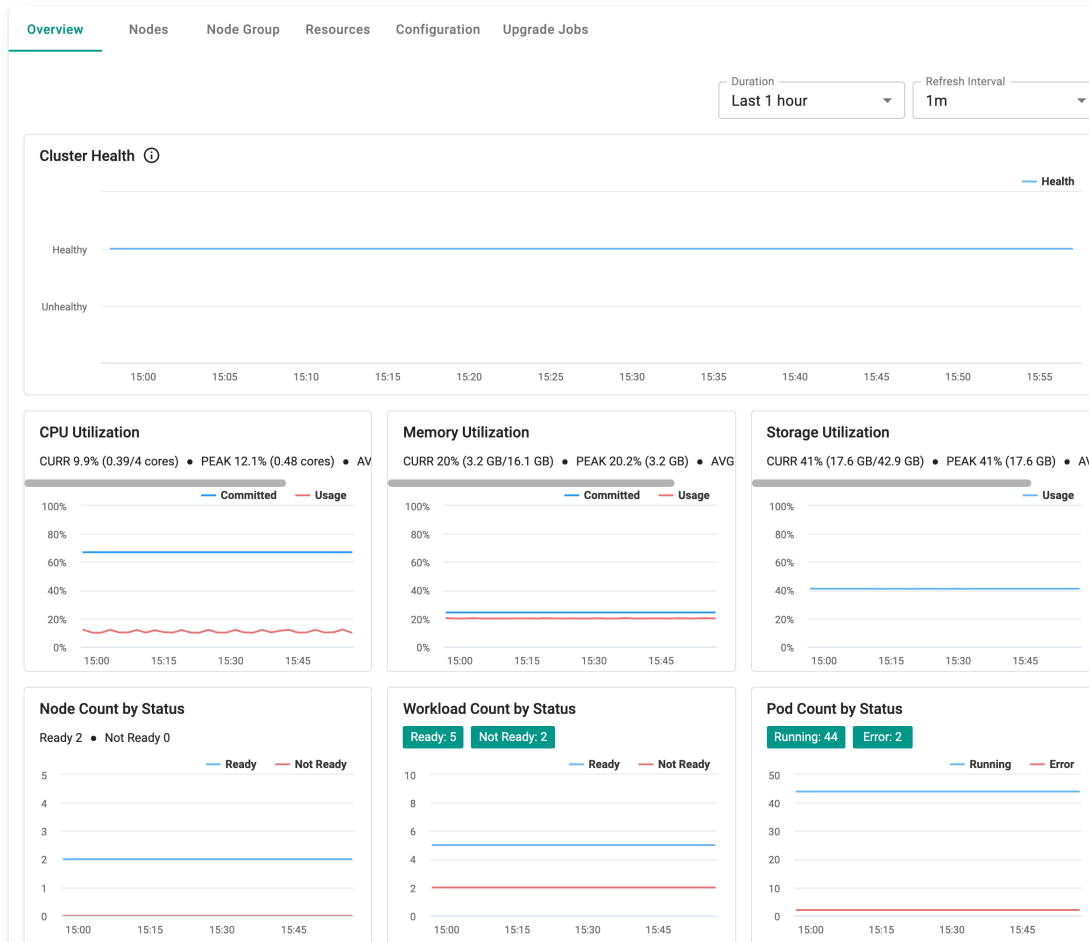
The Rafay KOP's integrated dashboard gives cluster administrators detailed visibility and insight into the Amazon EKS and EKS-D clusters. Additional dashboards help administrators manage resources across the infrastructure and/or on a group or single cluster effectively.

A comprehensive dashboard should provide a single view of all clusters and include information on location, resource utilization, and other factors.

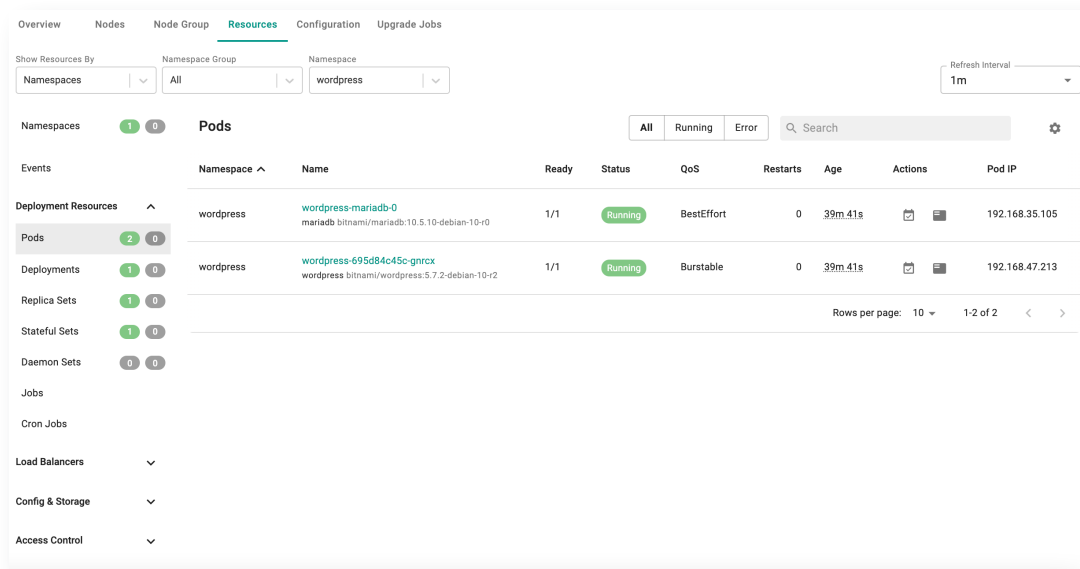
Dashboard



A detailed dashboard is available for every Amazon EKS and Amazon EKS-D cluster. It provides at-a-glance information including health, resource utilization, and pod/workload status.



A built-in Kubernetes dashboard displaying both current and time-series data allows users to view details about every Kubernetes resources on the cluster.



Consolidated Lifecycle Management

Another challenge created by hybrid cloud environments is consistent lifecycle management of clusters across AWS regions and on-premises infrastructure.

As a cloud platform provider, AWS focuses on ensuring platform health and availability; it does not provide comprehensive management capabilities for Kubernetes clusters. For example, upgrading Kubernetes on an Amazon EKS cluster requires many manual steps repeated across AWS regions.

Because the cost of operationally managing Kubernetes grows over time, it's critical for enterprises to streamline day 2 operations wherever possible. This includes:

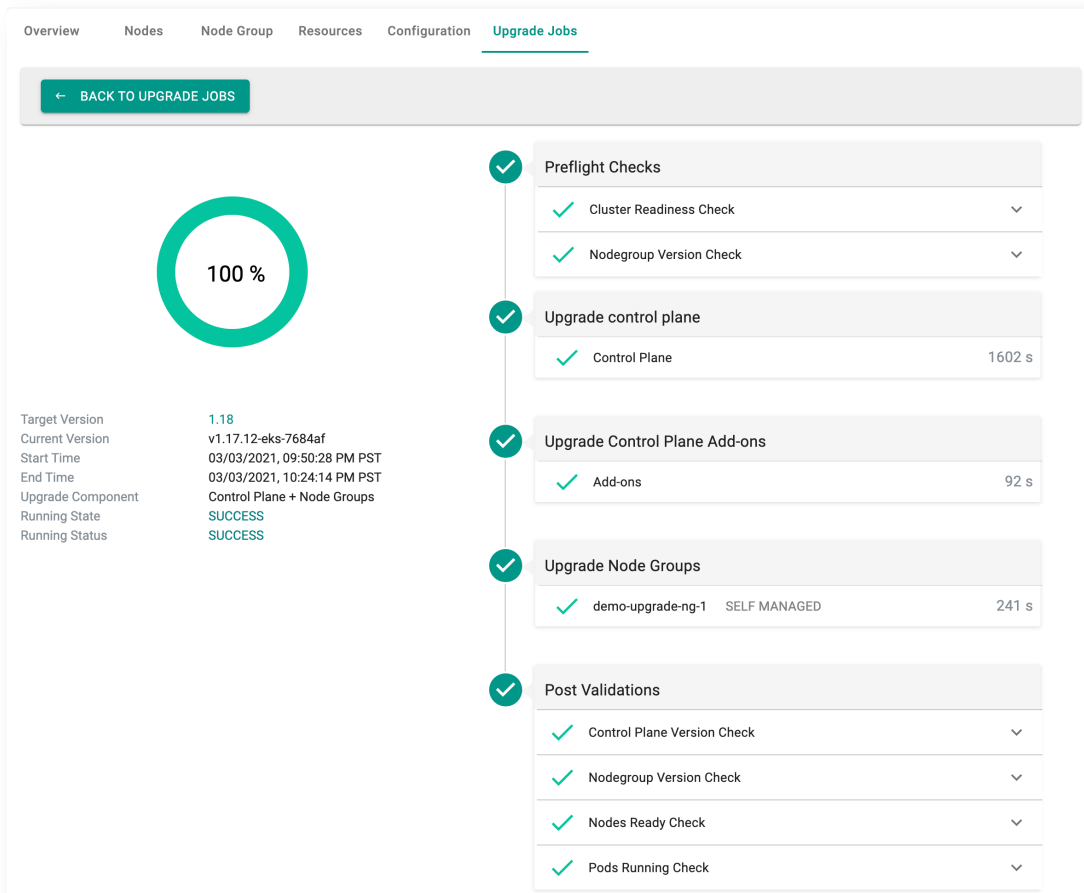
- Provisioning and deprovisioning clusters
- Upgrading the Kubernetes version
- Maintaining and updating Kubernetes nodes
- Upgrading clusters based on new or changes to application requirements

Cluster Lifecycle Management of Amazon EKS and Amazon EKS-D with the Rafay KOP

The Rafay KOP streamlines day 2 operations for Amazon EKS and Amazon EKS-D clusters. It only takes a few clicks to upgrade Amazon AKS or Amazon EKS-D clusters whether administrators require an in-place upgrade or by migration to a new cluster.

The Rafay KOP automatically performs all the preflight checks, upgrades the cluster, and validates results—all in matter of minutes. All of these capabilities are available through the use of a CLI and API as well.

AWS focuses on ensuring platform health and availability; it does not provide comprehensive management capabilities for Kubernetes clusters.



Security and Compliance in Hybrid Environments

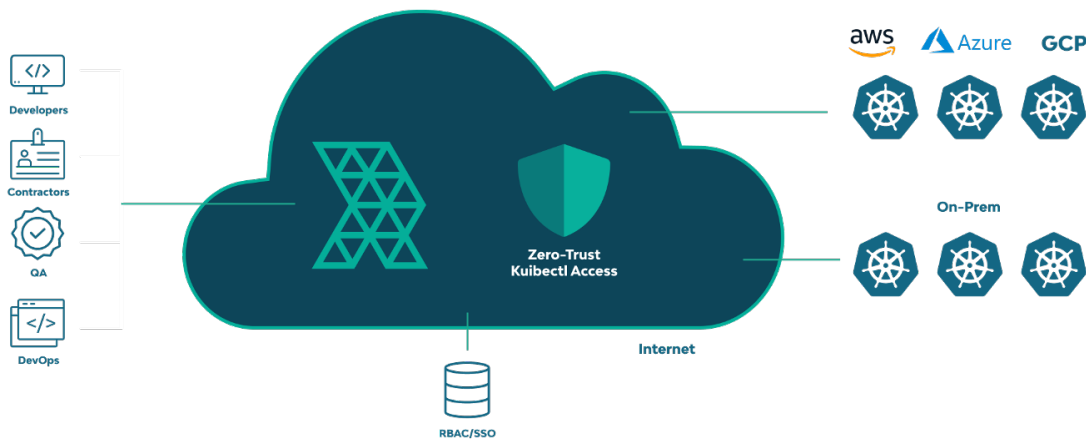
Although AWS provides world-class infrastructure security, securing the operating environment and individual applications is the customer's responsibility. This presents some special considerations for multi-cluster hybrid environments.

While most large organizations use identity management and access control for their business applications, they may group multiple clusters within a single AWS administrator account for the sake of convenience. This can create potential security vulnerabilities, and an attacker who breaches an account can also potentially gain access to all the clusters within it.

A better approach is to use role-based access control (RBAC) governed by policies and integrated with the organization's preferred single sign-on solution. For example, a user in the "developer" group would have access only to clusters allocated to developers, as well as those allocated to that individual account.

Using Rafay's Zero-Trust Kubectl Access to Enable Security and Compliance

An even more effective approach is Zero-Trust Kubectl Access (ZTKA). ZTKA secures access to the Amazon EKS and EKS-D clusters' API server via a proxy for centralized authentication, authorization, and auditing.



A Kubectl-based solution enables users to access clusters from anywhere—even from behind firewalls—while maintaining a full audit trail.

The SaaS Option for Kubernetes Operations

Managing the on-premises deployment of open source software often requires a high level of expertise and many additional tools. Responsibility for updating, patching, and maintaining the software falls to an IT staff already adapting to the complexity and skill demands of large Kubernetes environments.

Choosing a software-as-a-service (SaaS) solution for Kubernetes operations offloads these responsibilities from organizations and ensures that their management toolset is current and secure. A SaaS solution also enables them to integrate other Kubernetes environments, both in the cloud and on-premises, as their needs evolve.

The Bottom Line

As hybrid cloud implementations increase, so does the complexity for Kubernetes environments. The combination of Amazon EKS and EKS-D provides a valuable set of Kubernetes distributions that work in the cloud and on-premises. And, via a UI, CLI or API, the Rafay KOP helps enterprises streamline operations and accelerate devops workflows across that increasingly complex infrastructure.

The combination of Amazon EKS and EKS-D provides a valuable set of Kubernetes distributions that work in the cloud and on-premises.

Learn more about achieving security, integration, and reduced complexity for Kubernetes environments in today's increasingly hybrid IT landscape. Visit: <https://rafay.co>