

Accelerating Deployment and Management with a K8s-As-A-Service Platform for Siemens



Introduction

This case study delves into our collaboration with a leading technology provider to expand their existing footprints in AWS by building out a multi-tenant Kubernetes-As-A-Service platform in AWS using cloud native services as an offering to various business units within the organization as well as to the external entities.

At the time of collaboration, the customer had 10+ Kubernetes upstream clusters running 1000+ containers across various environments deployed in on-premises environment and they want to move away from self-managed Kubernetes clusters to managed Kubernetes clusters to onboard new delivery teams, reduce operational tasks, enhance scalability and availability, simplify management and to improve the overall security standards.

Customer Challenge

Building out Kubernetes As A Service solution offering requires a holistic approach, encompassing technical expertise and effective implementation strategies. Kubernetes has a steep learning curve, requiring a solid understanding of containerization concepts and distributed systems. This poses a serious challenge for the delivery teams within the organization new to container orchestration. As an organization, there were multiple delivery teams and business units with different use case requirements, it is a big challenge for the customer to build a highly efficient and robust platform that could satisfy all their requirements. The platform should be flexible enough to accommodate new features, tools and services based on requirements.

Another big challenge was setting up and configuring a Kubernetes cluster involves various components, including networking, storage, security, and resource management. Managing and troubleshooting these complex systems can be challenging, particularly for inexperienced teams.

Here are some of the key challenges that we considered during build-out phase:

- AWS Account Strategy aligned with organizational structure
- AWS VPC Network Topology
- Cross account and cross region network connectivity
- Centralized User Access Management
- Multi Tenancy (Dedicated vs Shared Kubernetes Cluster)
- Unified Multi Cluster Management
- Consistent Security Policy and Compliance
- Centralized Observability for simplified logging and monitoring
- Establish a strategy to deploy infrastructure and applications consistently
- Integration with CI/CD tools and ServiceNow workflows

About Siemens



Siemens is a technology company focused on industry, infrastructure, transport, and healthcare. From more resource-efficient factories, resilient supply chains, and smarter buildings and grids, to cleaner and more comfortable transportation as well as advanced healthcare, the company creates technology with purpose adding real value for customers. By combining the real and the digital worlds, Siemens empowers its customers to transform their industries and markets, helping them to transform the everyday for billions of people.



Partner Solution

EKS (Elastic Kubernetes Service) is a fully managed Kubernetes service provided by AWS (Amazon Web Services). EKS allows users to run Kubernetes clusters in the AWS cloud without having to manage the underlying infrastructure. With EKS, users can deploy, manage, and scale containerized applications using Kubernetes, while AWS takes care of the underlying infrastructure, including the control plane, worker nodes, and networking.

EKS provides a highly available and scalable Kubernetes control plane, which is distributed across multiple availability zones to ensure high availability. Kubernetes is the core of the platform and platform leverages other cloud native services in AWS such as Load Balancers, Route53, S3, RDS to support customer application architecture.

The solution was designed and developed through a collaborative process with customer's technical team. This involved conducting multiple workshops that focused based on the five pillars of the well-architected framework (operational excellence, security, reliability, performance efficiency, and cost optimization).

There is a wide range of tooling was used to assist with various aspects of deploying, managing, and monitoring Kubernetes clusters and applications. Here are some commonly used Kubernetes tools:

- **Terraform:** Terraform is an open-source infrastructure as code (IaC) tool developed by HashiCorp. It allows you to define, provision, and manage infrastructure resources in a declarative and version-controlled manner.
- **Rancher:** A Kubernetes management platform that simplifies the deployment, scaling, and monitoring of Kubernetes clusters across multiple environments, including on-premises and cloud.
- **Argo CD:** A continuous delivery tool for Kubernetes that automates the deployment and management of applications, enabling GitOps-style workflows.
- **Helm:** A package manager for Kubernetes that simplifies the deployment and management of applications by using pre-configured templates called charts.
- **Prometheus:** A popular open-source monitoring and alerting tool that collects metrics from Kubernetes clusters and applications, providing insights into performance, resource usage, and more.
- **Grafana:** A visualization and monitoring tool that works well with Prometheus, providing a customizable dashboard to display metrics and monitor the health of Kubernetes clusters and applications.
- **Istio:** A service mesh tool that enhances network communication between services in a Kubernetes cluster, providing features like traffic management, load balancing, observability, and security.
- **Telepresence:** A tool that allows local development and debugging of Kubernetes services by proxying network traffic between a local development environment and a Kubernetes cluster.
- **Velero:** A backup and restore tool for Kubernetes clusters, providing data protection for persistent volumes, resources, and configurations.
- **Calico:** A networking and network security solution for Kubernetes that enables secure and scalable communication between pods and provides network policies for fine-grained access control.
- **HashiCorp Vault:** HashiCorp Vault is an open-source tool that provides secure secrets management, data encryption, and identity-based access control for modern applications and infrastructure.

- **Cert Manager:** Cert Manager is an open-source certificate management tool for Kubernetes. It automates the management and issuance of TLS (Transport Layer Security) certificates within Kubernetes clusters.
- **External DNS:** External DNS is a tool that automates the management of DNS records for services running in cloud environments, such as Kubernetes clusters. It helps synchronize the DNS entries with the dynamically changing IP addresses of resources, making it easier to expose services externally.

Implementation Strategy

Here is the implementation strategy for building out the platform in AWS.

- Created AWS organization structure along with organizational units & accounts.
- Integrated Amazon Identity with customer's identity provider and deployed the core Landing Zone using AWS Control Tower.
- Designed and implemented the EKS cluster architecture considering the factors such as regions, availability zones, networking, and security requirements.
- Hub and Spoke connectivity model using Direct Connect and Transit Gateway.
- All the infrastructure modules are developed and provisioned using Terraform (IAC) including EKS clusters.
- Setup dedicated Rancher clusters in a regional strategy for unified cluster management per continental basis.
- Deployed Argo CD for deploying the application workloads to the downstream clusters.
- Rolled out centralized secrets management solution using Hashi Corp Vault to integrate with EKS cross region clusters.

Results and Impact

After the successful rollout design, the customer observed the following benefits:

- Helped to build highly available and scalable platform using AWS EKS Service.
- Scaled EKS clusters to 90+ clusters with 50000+ containers across multiple AWS regions.
- Expanded the platform to support new AWS operating regions.
- Enhanced the existing solution to meet complex networking needs.
- Implemented cost optimization measures to reduce the overall spending by 15%.
- Streamlined workflows by eliminating the need for multiple disjointed systems.
- Simplified cluster management and maintenance.
- Enhanced collaboration and knowledge sharing.
- Improved visibility and traceability into DevOps processes.

About Intuitive Cloud

Intuitive Cloud is an AWS Advanced Consulting Partner that specializes in providing cloud migration, infrastructure design, and DevOps services to help companies optimize their AWS environment. The company's team of certified AWS experts has extensive experience in designing and deploying AWS solutions for businesses of all sizes and industries. Intuitive Cloud is committed to delivering high-quality services that drive innovation and efficiency while providing exceptional customer satisfaction.



Intuitive.Cloud