GoDaddy

Leveraging ROSA to accelerate K8s migration to AWS

Arash Janzadeh   Senior Manager SRE

Sandeep Sidhu   Principal SRE

Yorgensen Vassoodaven Principal SRE

November 2023

At GoDaddy, our goal is to partner with our customers at every point on the **Entrepreneur's Wheel**

Marketplaces & social media

Messaging commerce

Payments

Digital identity

Domain

Logo

Email

Link in Bio

Website

Hosting & security

Ubiquitous presence

Connected commerce

Create posts

Online store

Physical store

Offline point-of-sale

Customer relationship management
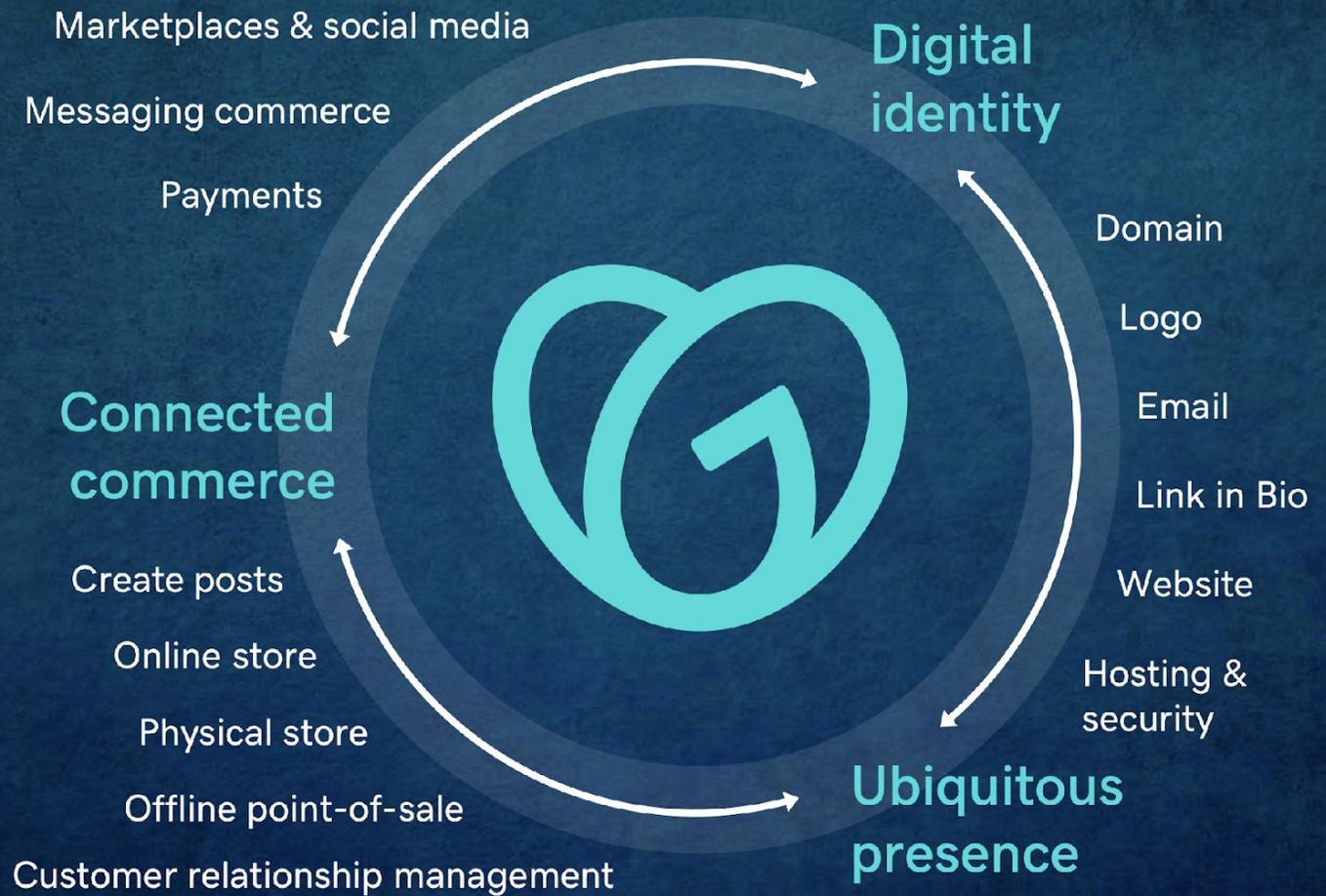
Our customers, Partner Brands, serve uniquely driven customers with differentiated needs

Multi-branded EMEA Commerce

Heart Internet

Heart Internet

TSOHOST

tsoHost

Host Europe

Host Europe

Domain Factory

Domain Factory
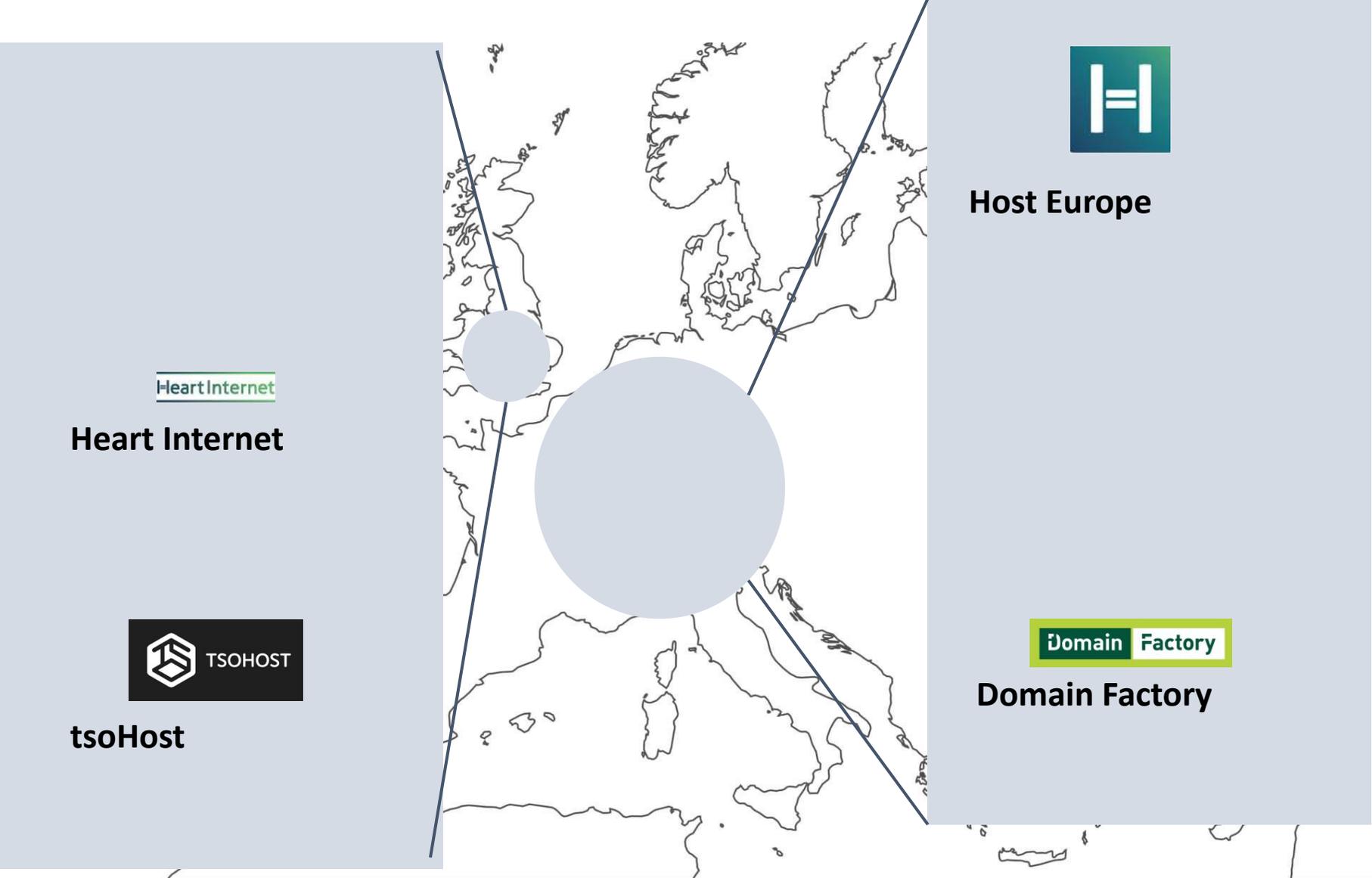
The GoDaddy Reseller Program allows you to sell all GoDaddy products including web hosting, domains and more. Start building your business today.

Resell our products with your brand.

Build your online storefront.

Your store should look like it's yours. Create a storefront that looks like your business.

Set your own prices.

Don't just get a commission, set your own margins and price products your way.

We handle payments.

There's no need to establish your own merchant account. You can use ours to process all payments.

24/7 award-winning support.

IT professionals and all business types welcome.

Contact U

Pre-Migration setup

- Multi Brand EMEA commerce workload on on-prem OpenShift
- The Reseller was on-prem Kubernetes
- Both have shared SRE Teams.

Main requirements

- Use AWS
- Self-service and Multi-tenant solution.
- Cluster Autoscaling and Updates management.
- Authentication using GoDaddy Okta
- Cluster Management API + WebConsole should be internal.
- Secure External Ingress
- Support multiple vanity domains.

What is ROSA

- Managed OpenShift on AWS.

- Built using standard AWS resources.

- Supported by Red Hat and AWS.

- Upgrades are made available by Red Hat, but the scheduling of upgrades is under end-user control.

- For serious critical updates that might affect the security or stability of the cluster, Red Hat can schedule an update after notifying us.

Red Hat OpenShift Service on AWS

Native AWS service

- **Create OpenShift clusters from the AWS console**
- **AWS integrated experience for cluster creation and management**
- **Foundation based on RHEL, providing a stable and secure platform for hybrid deployments**
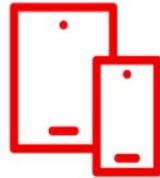
Unified bill

. Leverage your existing AWS commitment to use OpenShift

. Get a single unified bill from AWS for both OpenShift and AWS consumption
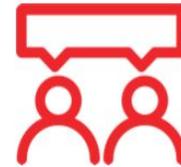
Joint Support

- Integrated support systems
- Contact Red hat or AWS support
- Built on Red Hat and AWS' decades of enterprise IT knowledge and experience
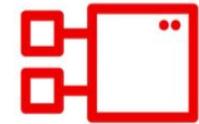
Integration with AWS Services

- Build containerized applications that integrate natively with the > 200 AWS cloud-native services

Red Hat

Managed OpenShift vs Kubernetes stack comparison

Components purposely engineered to work together

Red Hat OpenShift Managed Services

Support and Operations		

Included

Monitoring		Service Mesh	Dev Tools
Registry	Metrics	Logging	CI/CD

Included

OpenShift Cluster Services
Networking :: Router :: OLM

Kubernetes

Red Hat Core OS

aws Azure Google Cloud IBM Cloud

SRE Costs

Services Costs

Subscription Costs

Kubernetes Service Costs

Infra Cost

Infra Cost

$$**   **$$$
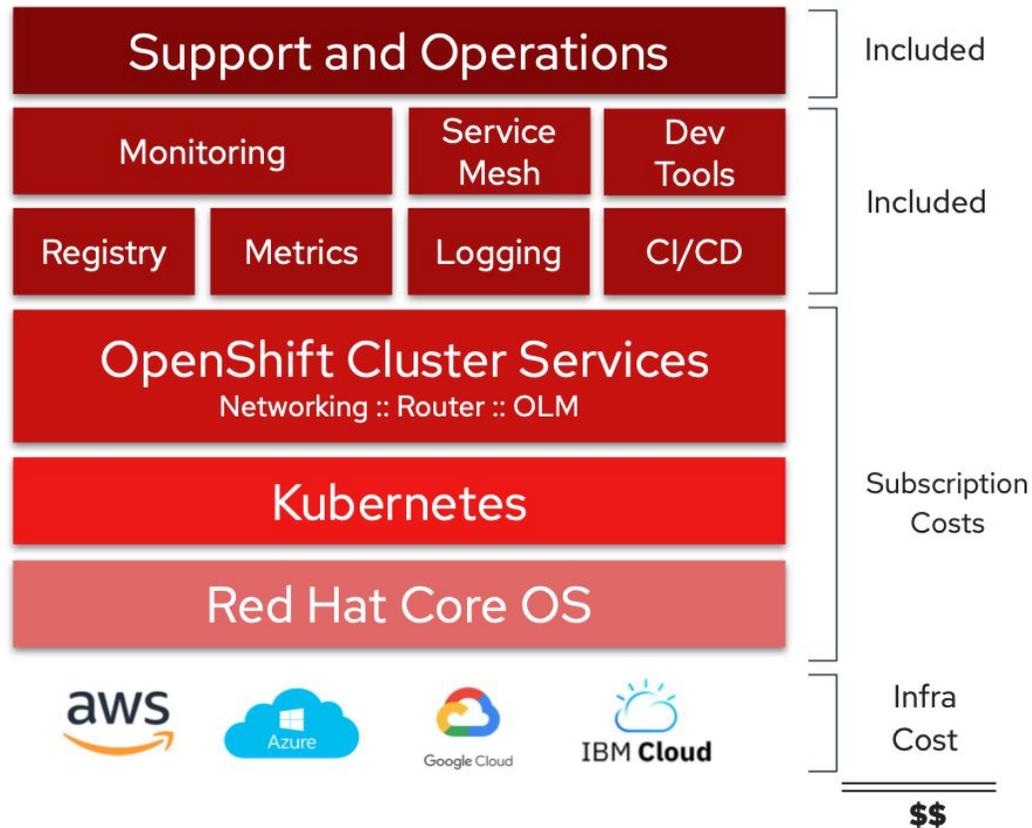
Other Kubernetes Services

Support and Operations		

Ad co co

Monitoring		Service Mesh	Dev Tools
Registry	Metrics	Logging	CI/CD

Kubernetes Cluster Services
Basic Networking :: Ingress

Kubernetes

Custom OS
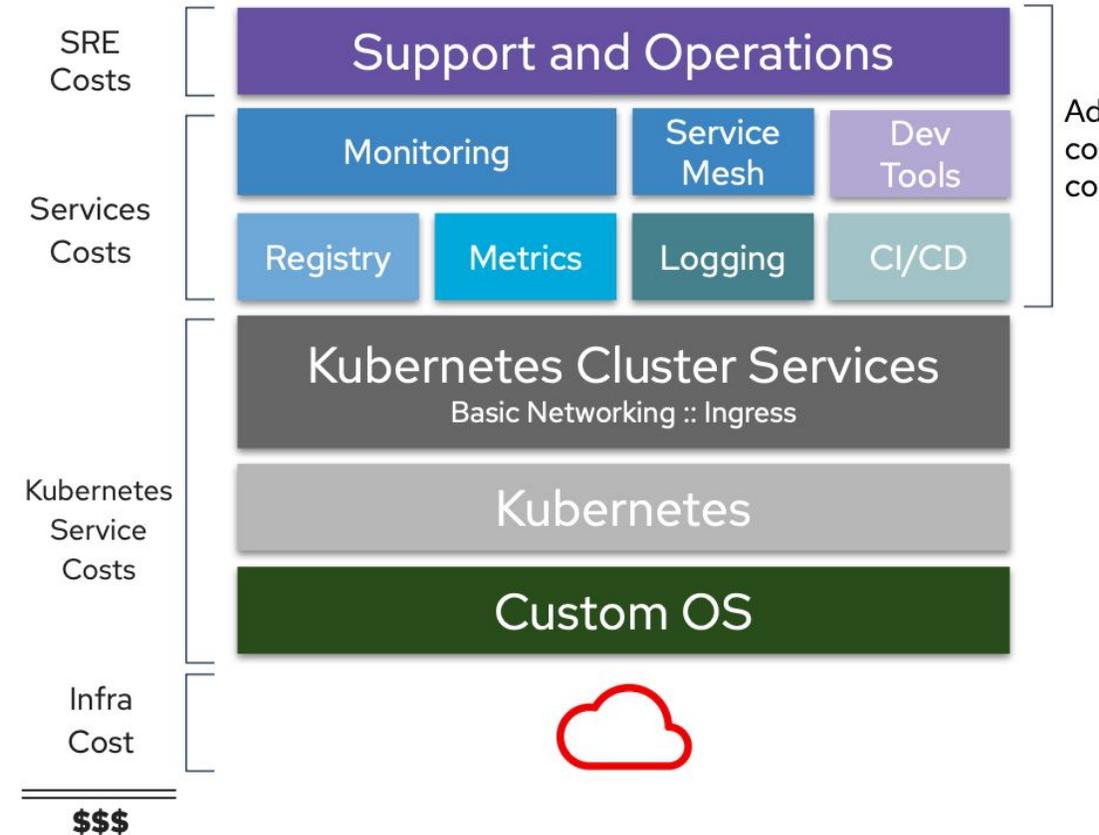
*Operations: Conservative estimate of 0.5 FTE

Red Ha

Fully managed clusters with ROSA

Responsibilities	
User management	⬜
Project and quota management	⬜
Application lifecycle	⬜
Cluster creation	🟧
Cluster management	🟧
Monitoring and logging	🟧
Network configuration	🟧
Software and security updates	🟧
Platform support	🟧

⬜ Customer 🟧 AWS and Red Hat

User App definition

IAM

OpenShift API/administration console

App 1 App 2
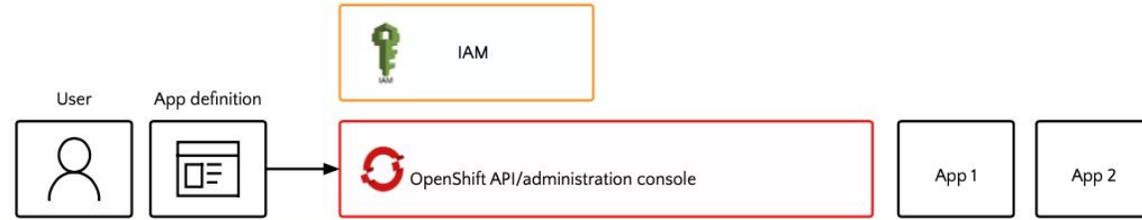
Let AWS and Red Hat...

Manage all your clusters

Secure your nodes

Monitor and operate your VMs

Manage environment patches

13

Why ROSA?

- We already have experience with on-prem OpenShift, allows lift and shift of existing on-prem workloads to AWS.

- Existing pipelines have OpenShift tooling.

- Multi-tenant capabilities out of the box.

- Industry-standard security practices.

- Support Operators.

- RBAC and monitoring come out of the box.

- Red Hat supported updates of the cluster.

Other consideration

- AWS can be complex. Rosa allows developers to focus on writing applications without worrying about managing the underlying infrastructure.

Current Setup

- Authentication by GoDaddy IDP.
- Authorization using OpenShift Groups + k8s RBAC
- Cluster provisioned using AWS STS setup.
- Currently using GitHub actions with self-hosted runners for managing cluster.
- Gatekeeper to enforce policies.
- External Secrets Operator.

GoDaddy Network

Firewall

On Prem Openshift Cluster

CGN Network

VMs

Jenkins OnPrem

Application Clients

Akamai GTM/CDN

AWS Direct Connect

okta

GoDaddy VPN

GoDaddy Developers and SREs

Access to ROSA Dashboard and Kubernetes API (kubectl)

subnet a/b/c

DNS

Internal ELB

AWS Security Groups

External ELB

Red Hat OpenShift Service on AWS

Logs Account

Logs Storage → Dashboards

Logs — Logs/APM

EC2 Compute Nodes

subnet direct connect a//b/c

Aurora DBs

Promethus ← Thanos → Amazon S3

Architecture

14

Self service capabilities.

- Tenants can request a new namespace by making change request. Once approved, the ROSA resources like namespace are created ArgoCD automation.

- Github actions run validation tests that enforces policies the namespaces need to meet, e.g should have a quota, should have a label.

- TLS for routes are automatically provisioned by the Certs Operator which integrates with GoDaddy Cert API.

Observability
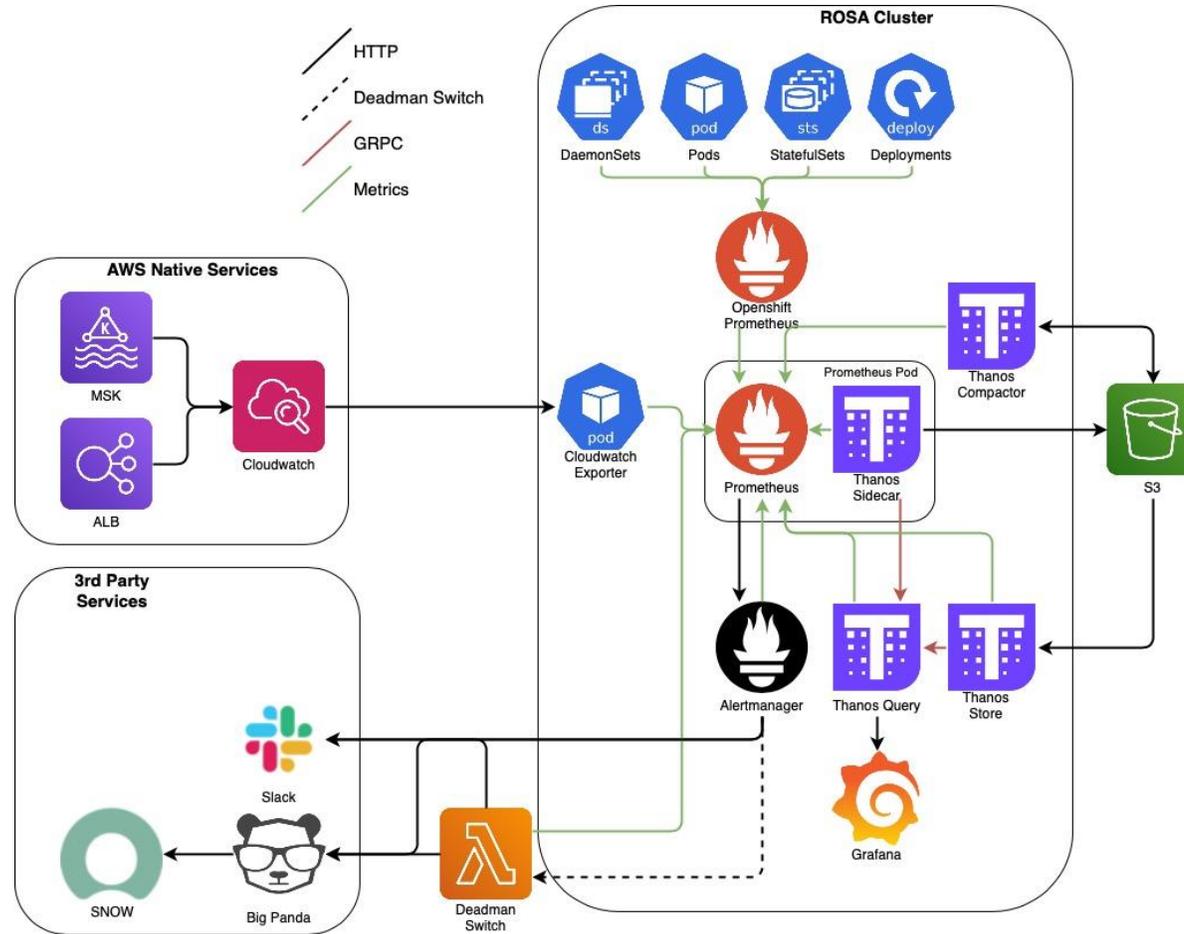
CICD

- tenants currently use existing Jenkins.

- Alternatives:
  - GitHub actions.
  - Redhat Openshift GitOps(aka ArgoCD) for CD.

Challenges

- Like most big tech firms, adding new software to tech radar is a lengthy process and requires multiple departments to sign it off

- The preferred method was provisioning one AWS account per team; ROSA was the first multi-tenanted solution.

Summary

- The self-service platform, supported by automation lets developers create their namespaces by creating a simple GitHub pull request.

- ROSA RBAC (Role-based access control) config as code allows each team to manage their team-level access.

- Check all criteria have been met before developer changes are merged.

- To simplify migration, we support multiple CI/CD pipelines

Thank You

GoDaddy