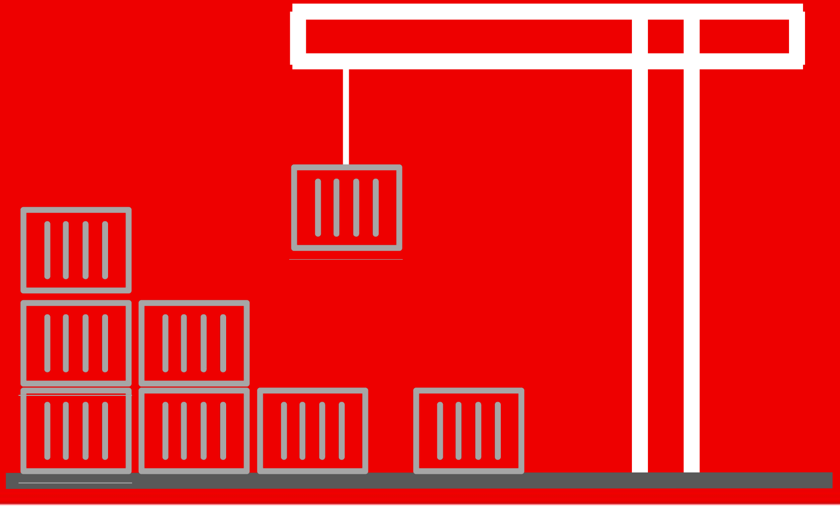
ROSA Workshop
Red Hat OpenShift on AWS

Bern, 29th of August, 2024

Florian Jacquin, EMEA Senior Black Belt, Managed OpenShift

Yury Titov, EMEA Senior Black Belt, Managed OpenShift



ROSA Workshop Schedule 14.00 - 17.00

<u>Getting started</u>

- Walk in
- Intro
- Get your ROSA cluster and get started!
- Break
- Value of cloud services
- Workshop practical exercises

<u>Mini presentations</u>

- Day Two Operations
- Deploy and Expose an Application

- Wrap-up!

Coffee is available at all time outside, you can bring coffee here

Who this Workshop is For.

- Platform engineers looking to build an application platform.
- Developers looking to understand foundations of an application platform.
- DevOps looking to Ops with their Dev.

Knowledge Prerequisites

Skills/Knowledge required to be successful in this workshop.

- Basic understanding of OpenShift or Kubernetes concepts.
- Knowledge of running workloads in a Cloud Provider environment.
- Basic CLI/Linux experience.

What you will learn today!

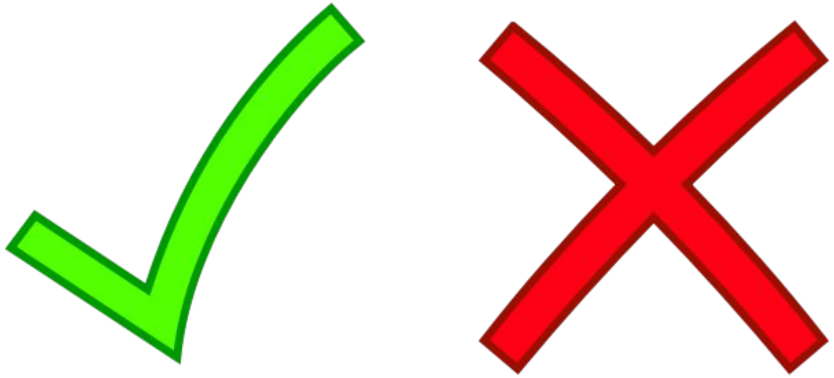
Day Two ROSA Operations:

- Configuring Cluster Authentication
- Managing Cluster Upgrades
- Managing Worker Nodes
- Cluster Autoscaling
- Labeling Nodes
- Logging with AWS CloudWatch

Deploy and Expose an APP:

- Deploy the App
- Make an App Resilient
- Restrict Network Access
- Using OpenShift GitOps
- Automate Deploying the App with Openshift Pipelines

Workshop Guidelines

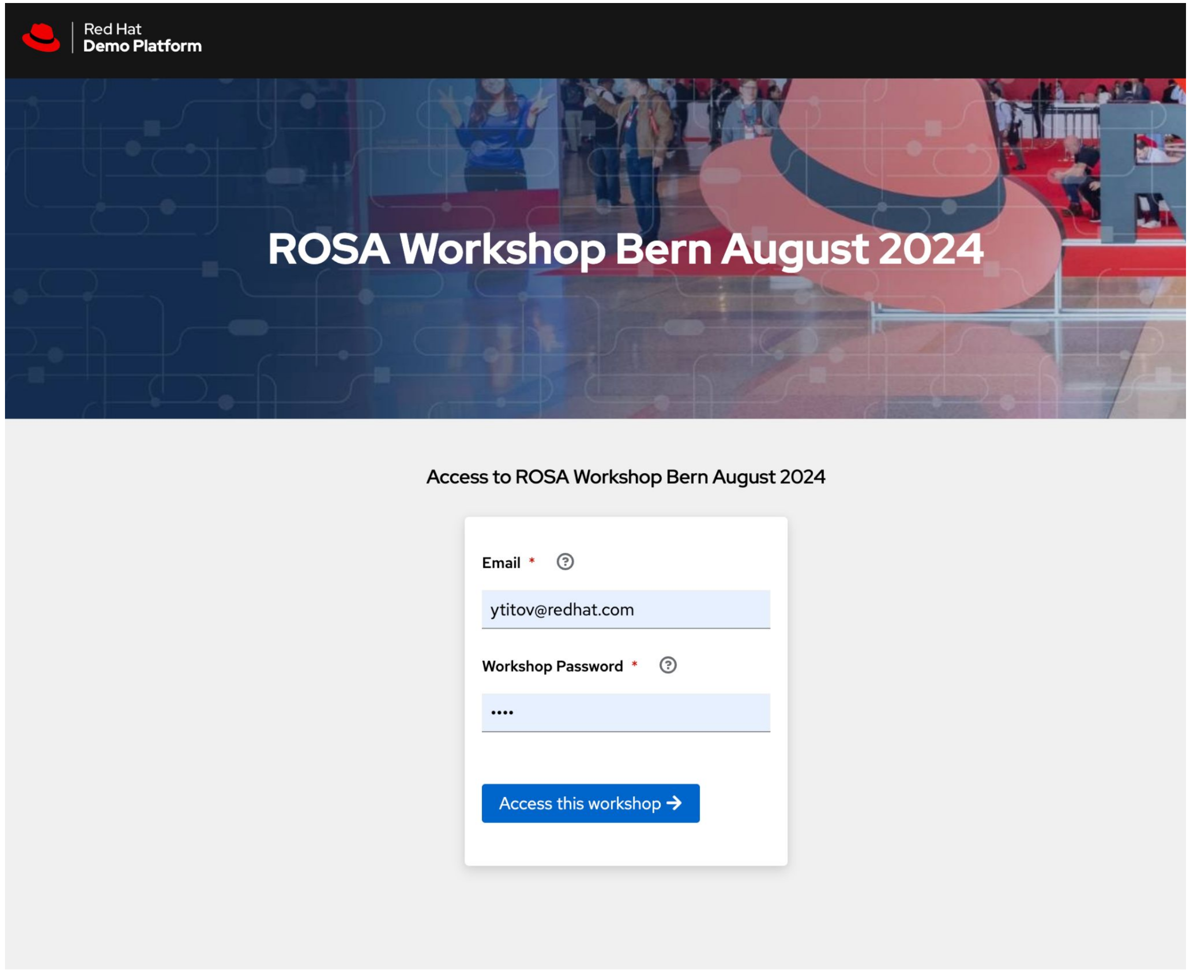


- Be respectful of facilitators, participants, and the compute environments provided.
- Raise your hand or find a facilitator if you need help, have a question, or get stuck.
- Let us know how we did, positive or constructive criticism is welcome!

Accessing the Workshop

Workshop url: red.ht/rosa-bern-aug-2024

Password: **rosa**

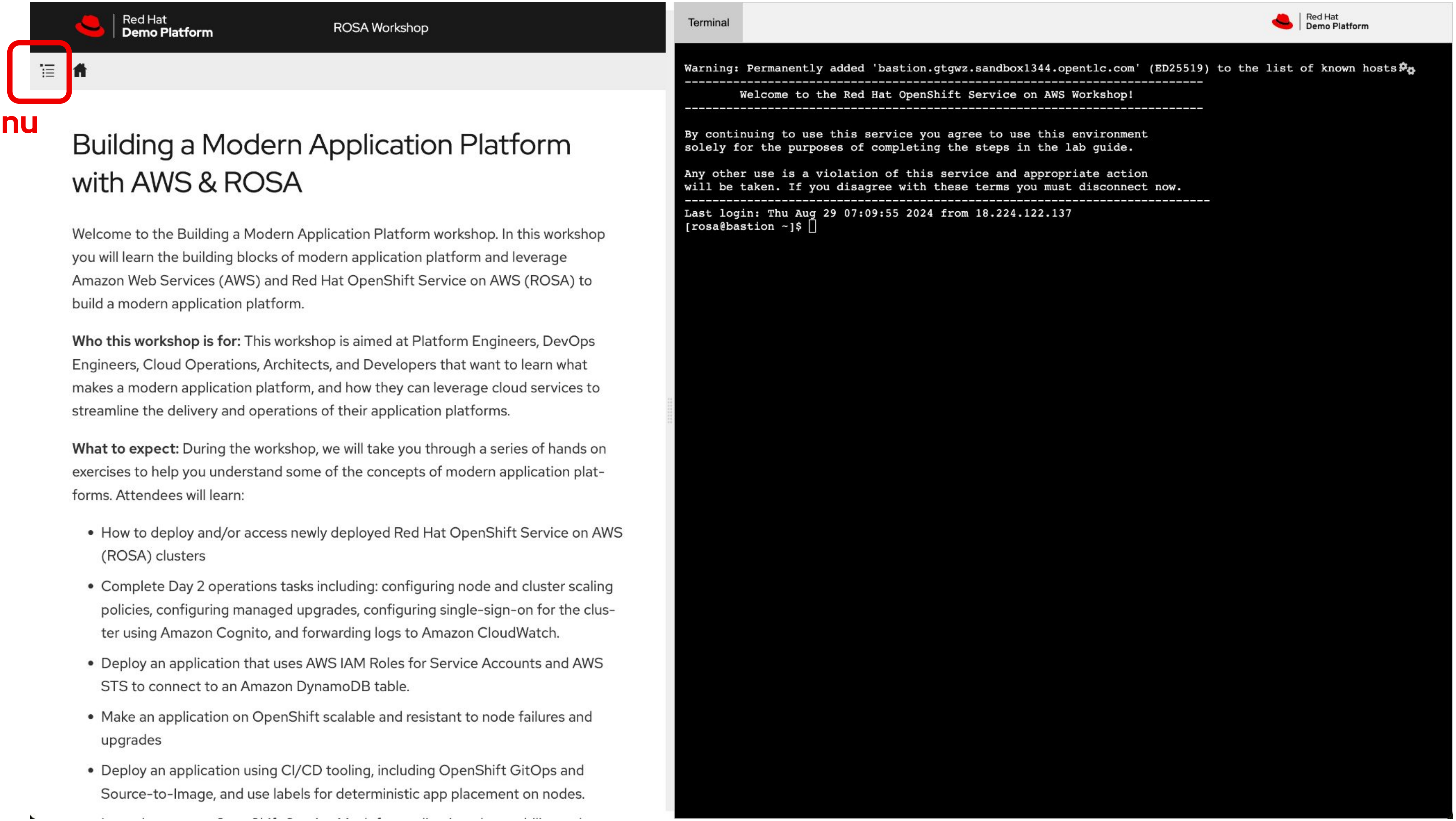


Access to ROSA Workshop Bern August 2024

Email * ytitov@redhat.com

Workshop Password * ••••

Menu



Building a Modern Application Platform with AWS & ROSA

Welcome to the Building a Modern Application Platform workshop. In this workshop you will learn the building blocks of modern application platform and leverage Amazon Web Services (AWS) and Red Hat OpenShift Service on AWS (ROSA) to build a modern application platform.

Who this workshop is for: This workshop is aimed at Platform Engineers, DevOps Engineers, Cloud Operations, Architects, and Developers that want to learn what makes a modern application platform, and how they can leverage cloud services to streamline the delivery and operations of their application platforms.

What to expect: During the workshop, we will take you through a series of hands on exercises to help you understand some of the concepts of modern application platforms. Attendees will learn:

- How to deploy and/or access newly deployed Red Hat OpenShift Service on AWS (ROSA) clusters
- Complete Day 2 operations tasks including: configuring node and cluster scaling policies, configuring managed upgrades, configuring single-sign-on for the cluster using Amazon Cognito, and forwarding logs to Amazon CloudWatch.
- Deploy an application that uses AWS IAM Roles for Service Accounts and AWS STS to connect to an Amazon DynamoDB table.
- Make an application on OpenShift scalable and resistant to node failures and upgrades
- Deploy an application using CI/CD tooling, including OpenShift GitOps and Source-to-Image, and use labels for deterministic app placement on nodes.

```
Warning: Permanently added 'bastion.gtgwz.sandbox1344.opentlc.com' (ED25519) to the list of known hosts.
---------------------------------------------------------------------------
        Welcome to the Red Hat OpenShift Service on AWS Workshop!
---------------------------------------------------------------------------

By continuing to use this service you agree to use this environment
solely for the purposes of completing the steps in the lab guide.

Any other use is a violation of this service and appropriate action
will be taken. If you disagree with these terms you must disconnect now.
----------------------------------------------------------------------------
Last login: Thu Aug 29 07:09:55 2024 from 18.224.122.137
[rosa@bastion ~]$ 
```

Red Hat OpenShift Cloud Services

Red Hat OpenShift cloud services

A turnkey application platform with management and support from Red Hat and leading cloud providers

aws

Azure

IBM Cloud

Google Cloud

Accelerate time to value

Quickly build, deploy, and run applications that scale as needed.

Operational efficiency

Enhance operational consistency, efficiency and security with proactive management and support.

Focus on innovation

Simplify operations so your teams can refocus on innovation, not managing infrastructure.

Hybrid cloud flexibility

Deliver a consistent experience on premises and in the cloud.

Build business value, not a technology platform

DIY Kubernetes-powered platform

Time and resources to integrate 10-20+ individual services

In house or multiple vendors for ongoing maintenance and support

Reliance on one cloud or DIY integration of multi cloud apps

Red Hat OpenShift cloud services

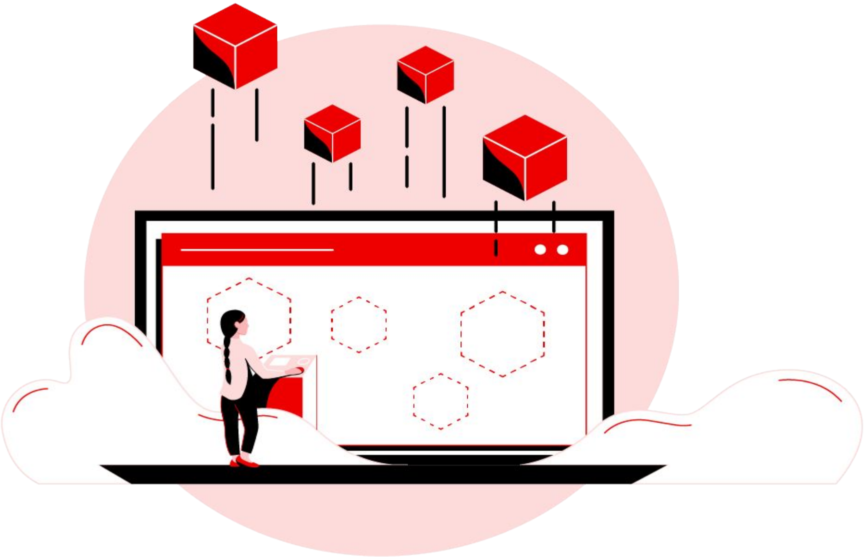
Turnkey application platform with integrated services and tools

Managed Kubernetes AND components to reduce complexity

Consistent hybrid cloud experience and cloud choice

What is an Application Platform?

Used for building, deploying, and running applications through a simple, but flexible experience. An application platform includes the components: runtimes, build tools, CI/CD, and observability (including application logging) and abstracts away technical details such as containers and Kubernetes.



Build, Test, Deploy

Apply the heart of DevSecOps policy & procedure on a consistent infrastructure foundation.

Run and Manage

with consistency and unified security.

Design & Code

using cloud-native dev tools & application technology while benefiting from DevSecOps right at the start.

Building an Application Platform on Public Clouds

The required Parts

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

Kubernetes Cluster Servicess

Kubernetes

Operating System

The AWS Car

CloudWatch | AppMesh | CodeBuild

ECR | CloudWatch | CloudWatch | CodePipeline

VPC, ELB, ALB

EKS

Amazon Linux 2

aws

The Azure Car

Monitoring | Open Service Mesh | Azure Devops

ACR | Azure Monitor | Azure Log Analytics | Azure Devops

VNET, ALB, Frontdoor, App gateway

AKS

Ubuntu

The GCP Car

Cloud Monitoring | Anthos Service Mesh | CodeBuild

GCR | CloudWatch | Cloud Logging | CodePipeline

VPC, CLB

GKE

Ubuntu / Container OS

Google Cloud

3 Different Cars

- Different component versions
- Different life cycles
- Different support models
- Different developer and ops tooling

→ **3 different drivers and pit crews needed**

Red Hat

Build and run a platform *versus* using a turnkey cloud service

The Parts

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

Kubernetes Cluster Services
Basic Networking :: Ingress

Kubernetes

Custom OS

aws | Azure | Google Cloud

xKS + 'native' services

The Assembled Car

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

OpenShift Cluster Services
Networking :: Router :: OLM

Kubernetes

Red Hat Core OS

- Application Platform -
Self-managed Red Hat OpenShift

The Car & Pit Crew

SRE and Customer Success

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

OpenShift Cluster Services
Networking :: Router :: OLM

Kubernetes

Red Hat Core OS

Azure | IBM Cloud | aws | Google Cloud

- Turnkey Application Platform -
Red Hat OpenShift cloud services

"Batteries Included"

... but swappable

Individual components can be swapped out

Eg.

- Using AWS CloudWatch for logging on AWS
- Use specific cloud services or ISV offerings

Red Hat

An opinionated platform for building, deploying and running applications

Red Hat OpenShift

Service Mesh	App-Services	DB-Services
CI/CD	DNS	Authentication
Monitoring	**Kubernetes**	Automation
Logging	Registry	Security
Compute	Storage	Network

- Fully integrated and supported components
- Expert SRE and Customer Success support
- Abstracts away technical details
- Consistent experience across clouds

Move from 24x7 operations to 9-5 innovation

End-to-End support for your entire application platform

- OpenShift cloud services includes full support for worker nodes
  - Zero downtime upgrades,
  - proactive monitoring
  - automated patching
  - Compliance and certifications extend to worker nodes

- 99.95% financially backed SLA
- 24x7 joint support from Red Hat and cloud provider
- Automation and Day 2 Operations by global SREs

[1] “The Total Economic Impact™ of Red Hat OpenShift Cloud Services by Forrester, ”Jan. 2022.

Full Stack management from a global Site Reliability Engineering (SRE) team

Product

Systems

Who are our SREs?

- Developers and systems engineers who know how to handle volume and a diversity of clusters.
- Uniquely offer both an engineering and development mindset.

SRE responsibilities

- Build solutions and features
- Automate at scale
- Day 2 operations: monitor, patch, and upgrade the platform.
- Work hand in hand with cloud providers and open source community.

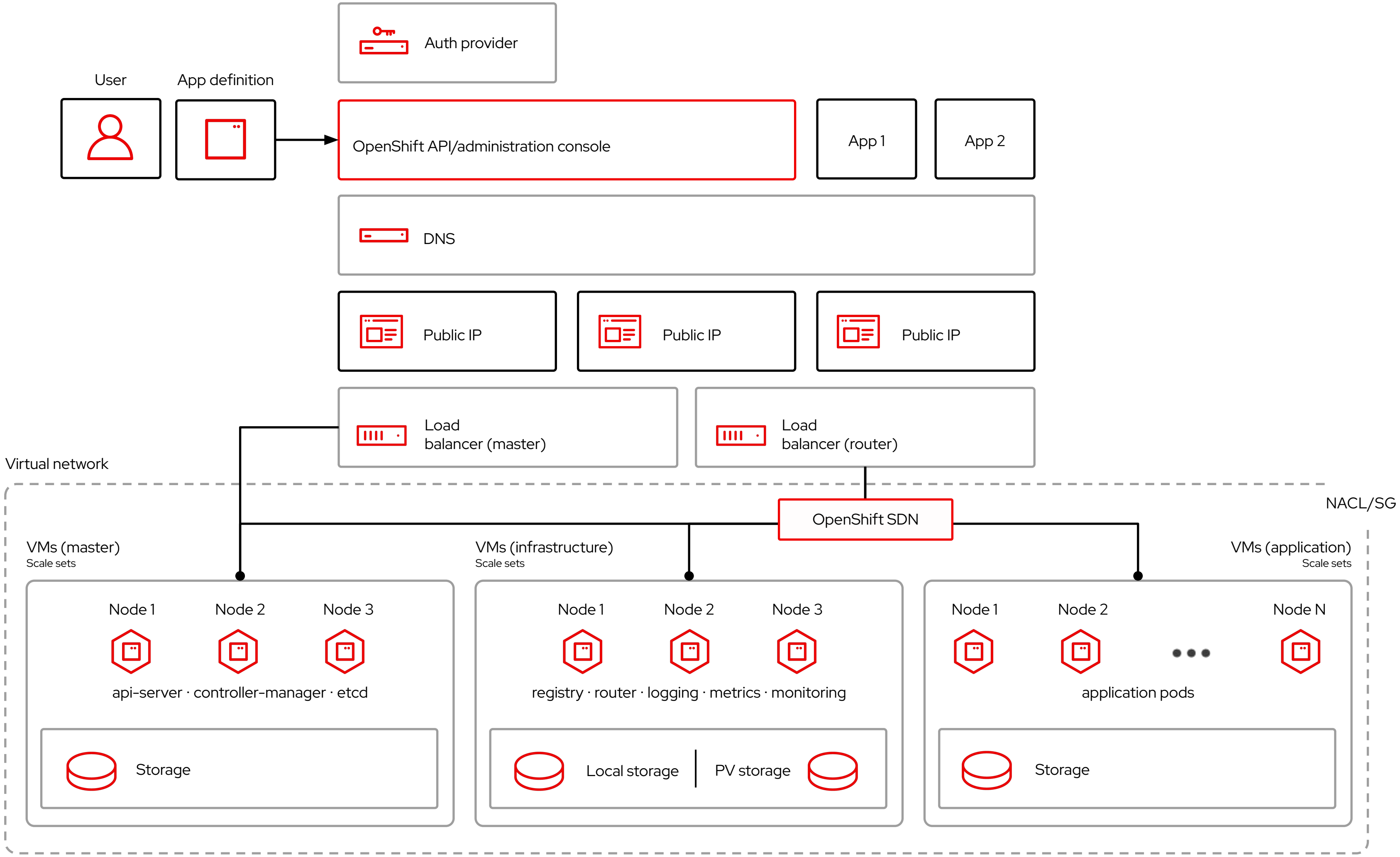
Customer benefits

- Accelerate application development and delivery through automation.
- Improve operational efficiency, security and resiliency.
- Refocus on innovation and core competencies.

Complexity of running your own Kubernetes Cluster

Responsibilities	
User management	⬜
Project and quota management	⬜
Application life cycle	⬜
Cluster creation	⬜
Cluster management	⬜
Monitoring and logging	⬜
Network configuration	⬜
Software and security updates	⬜
Platform support	🟥

⬜ Customer 🟥 Cloud provider & Red Hat

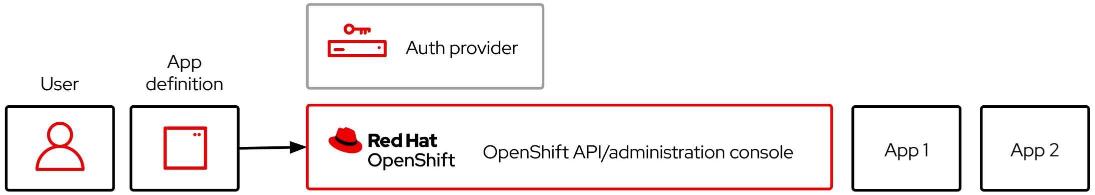


Simplify with fully managed clusters

Red Hat OpenShift cloud services

Responsibilities	
User management	⬜
Project and quota management	⬜
Application life cycle	⬜
Cluster creation	◪
Cluster management	◪
Monitoring and logging	◪
Network configuration	◪
Software and security updates	🟥
Platform support	🟥

⬜ Customer 🟥 Cloud provider and Red Hat



Let Red Hat & AWS...

Manage all your clusters.

Secure your nodes.

Monitor and operate your VMs.

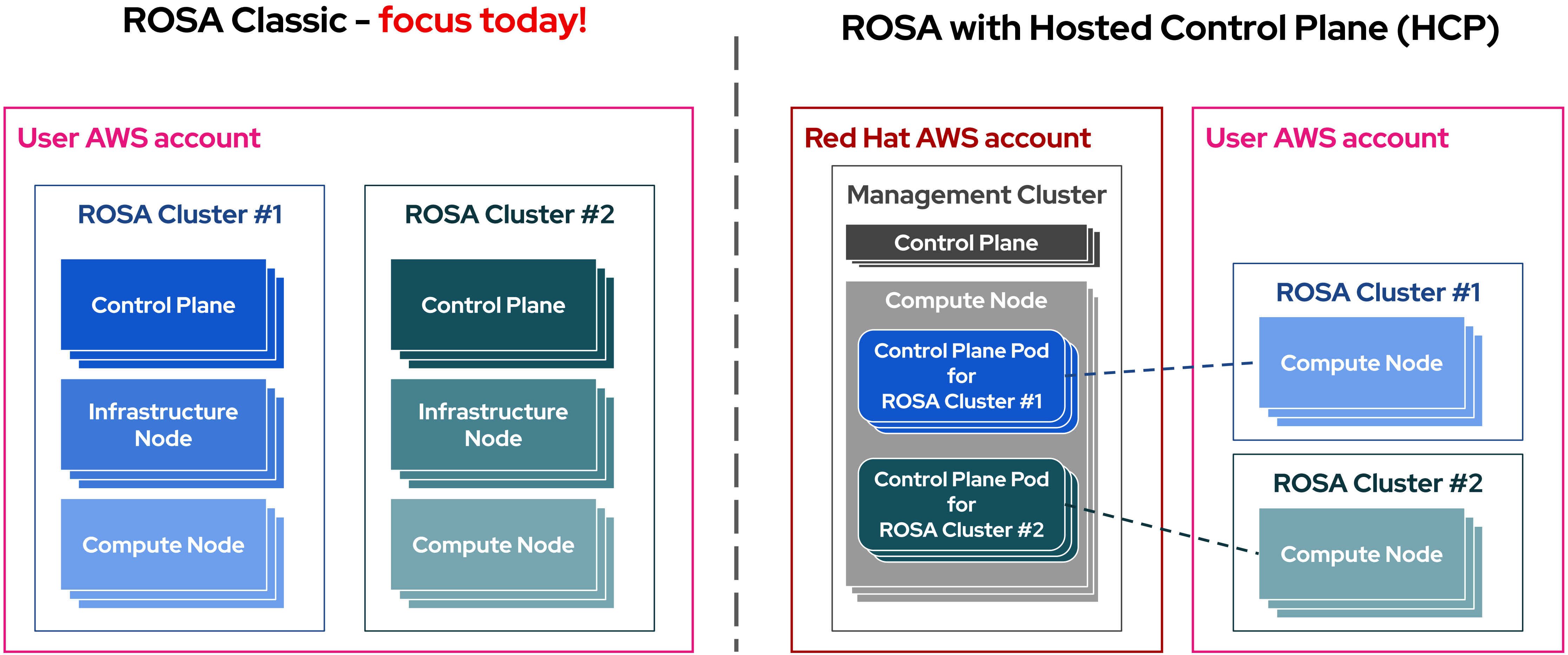
Manage environment patches.

You...

ROSA Classic on AWS Architecture

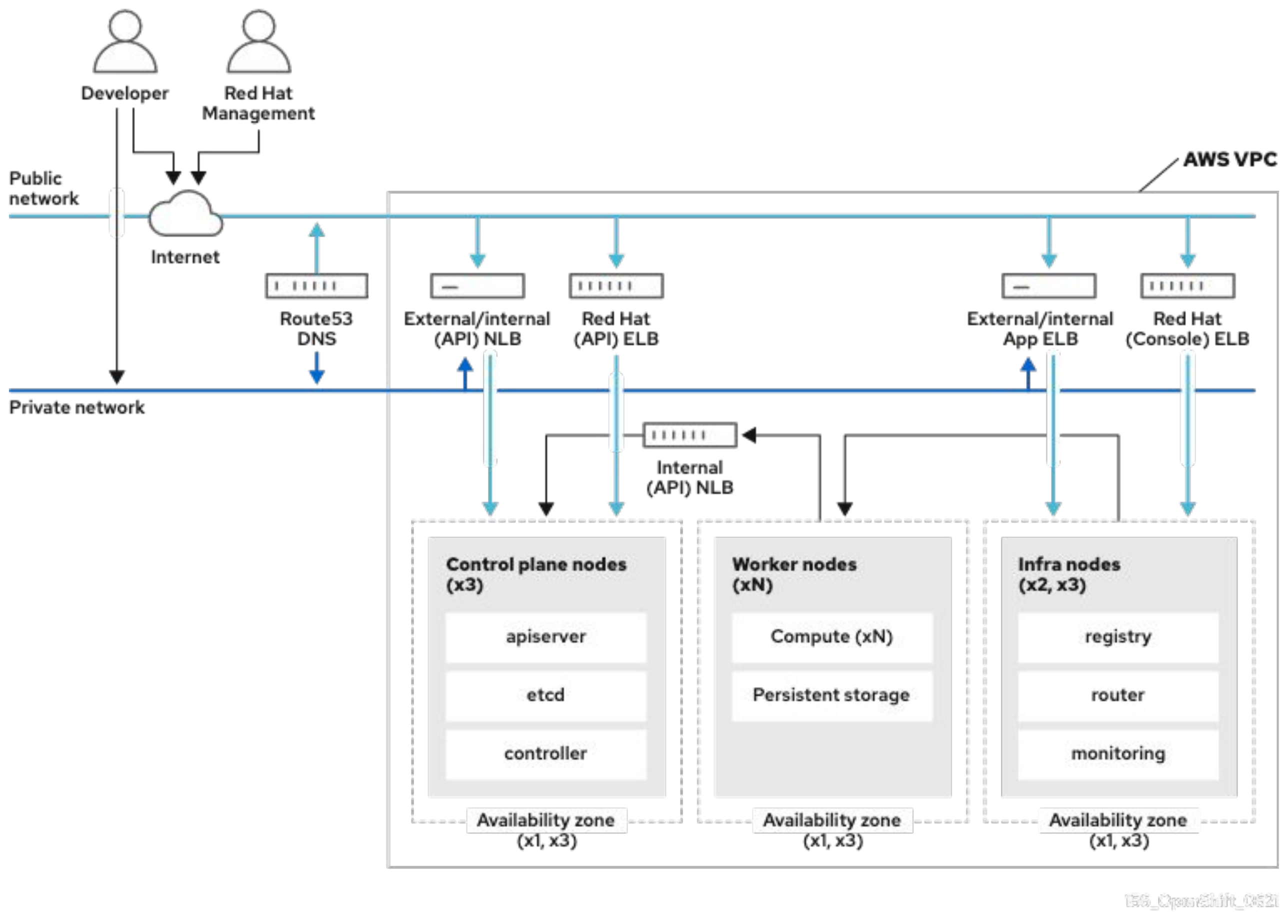
ROSA Variants

Generally Available



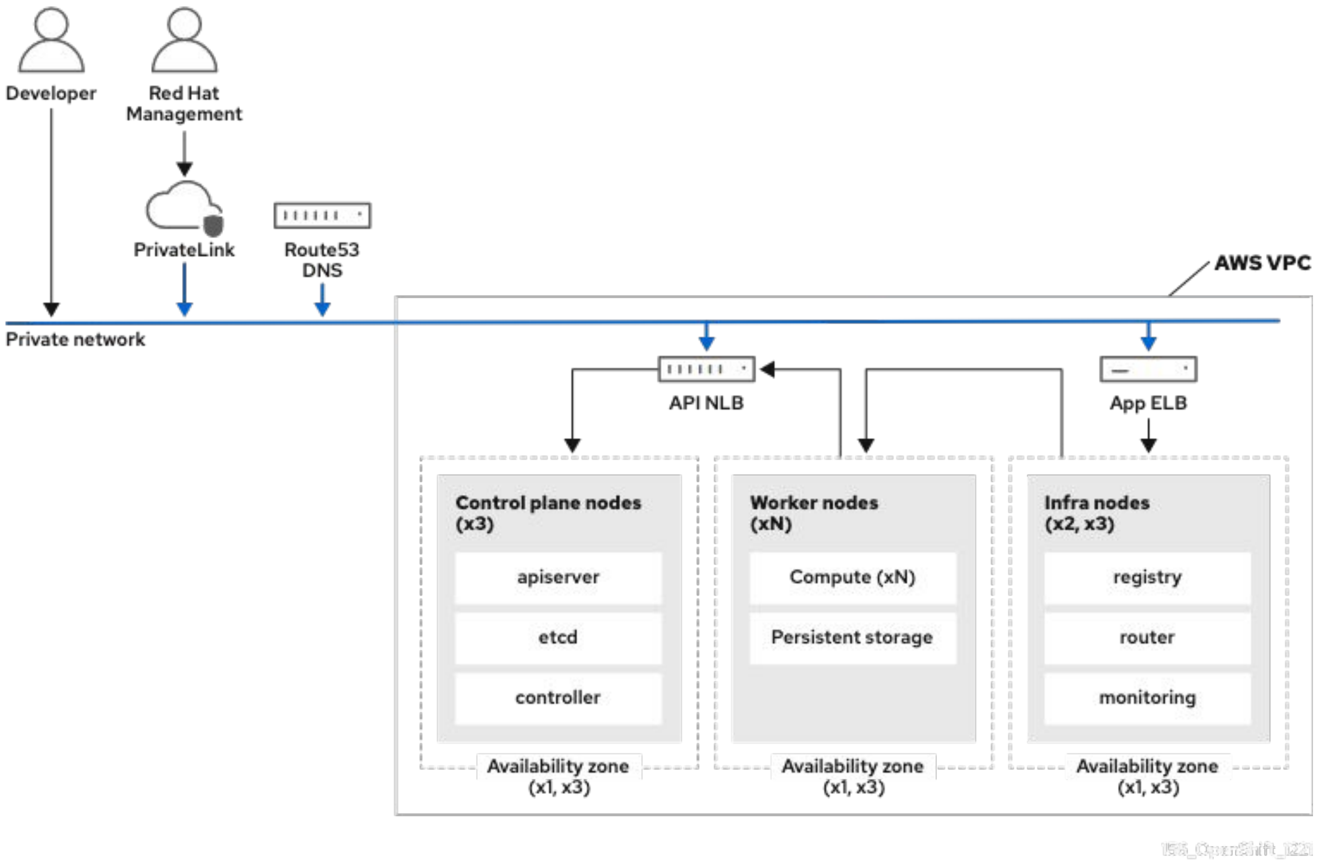
Red Hat

Public / Private Networking



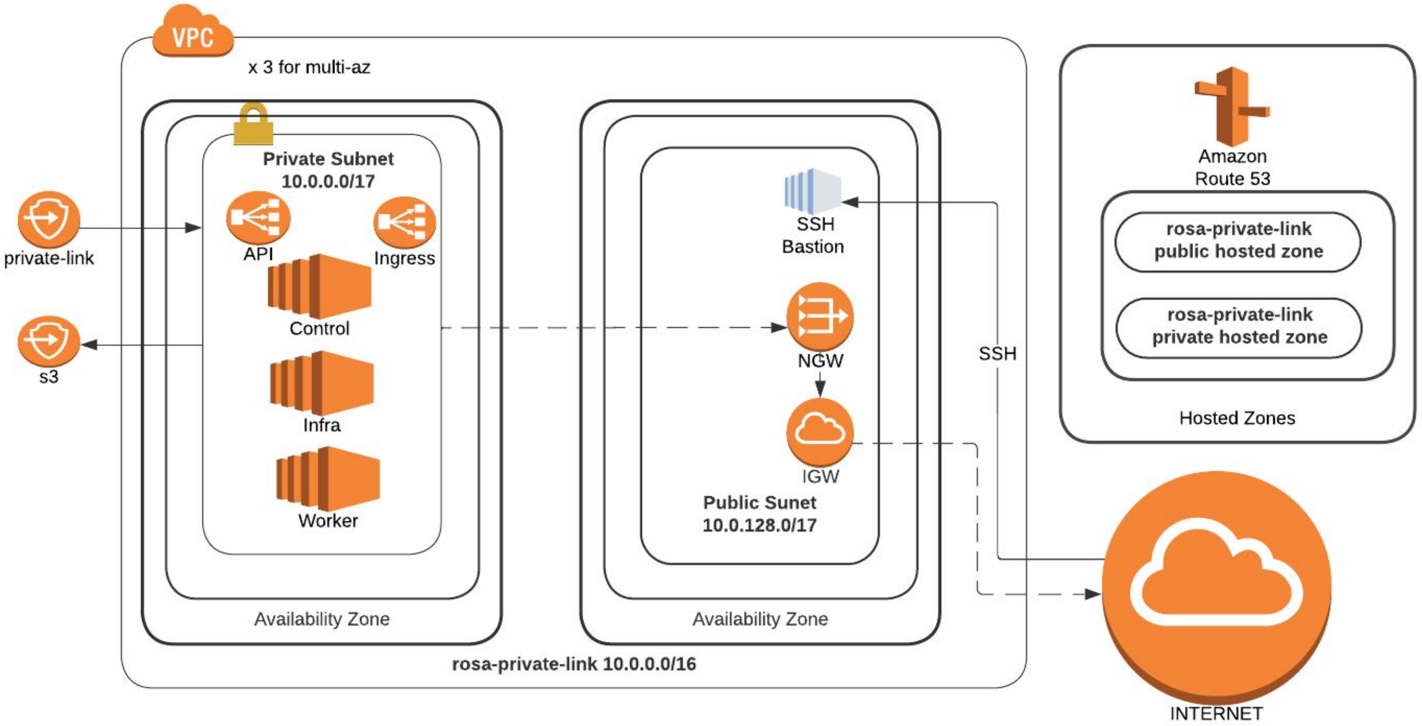
Source: https://docs.openshift.com/rosa/rosa_architecture/rosa_architecture_sub/rosa-architecture-models.html

Private Link Networking



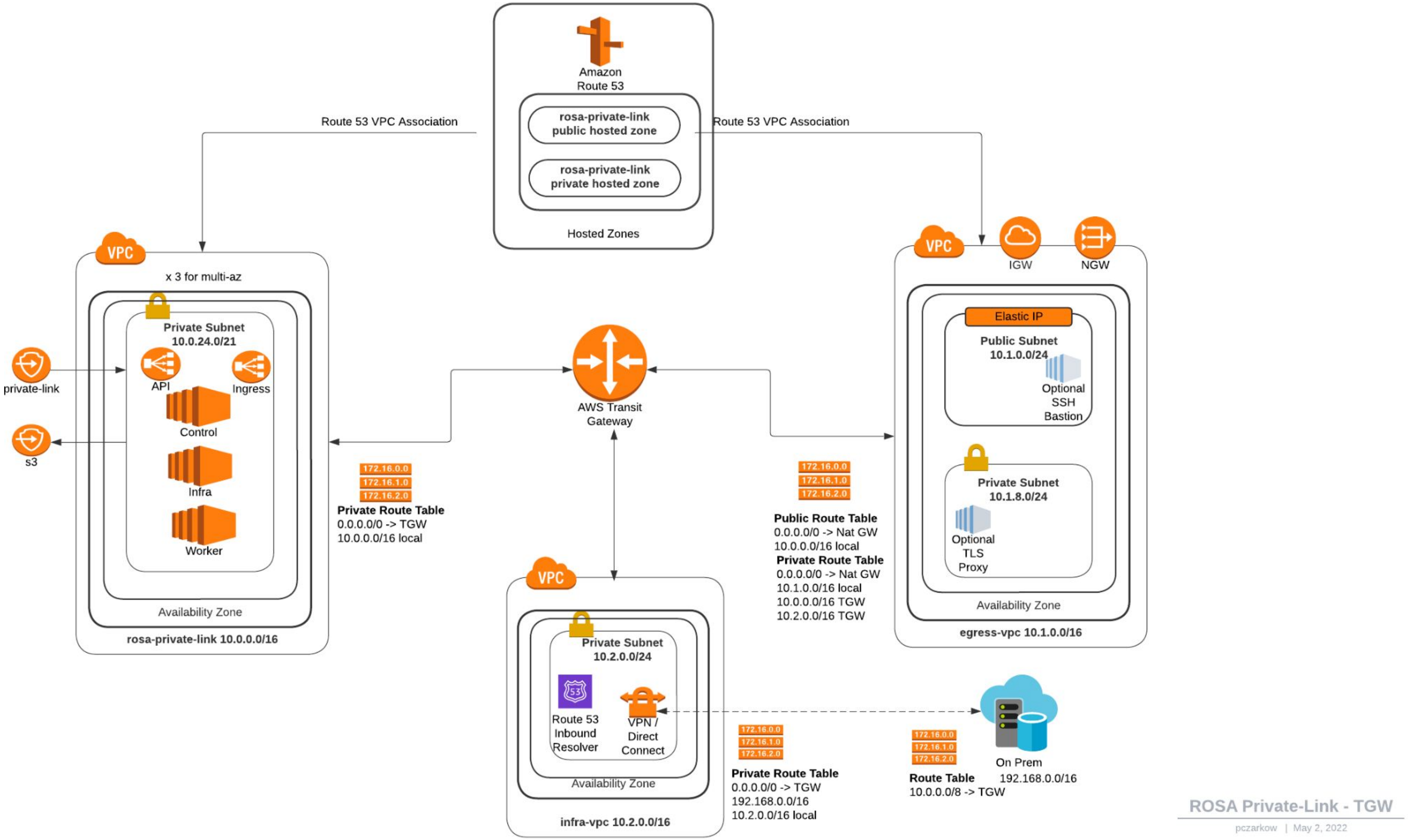
Source: https://docs.openshift.com/rosa/rosa_architecture/rosa_architecture_sub/rosa-architecture-models.html

Private Link Networking



Source: https://mobb.ninja/docs/rosa/private-link/

Private Link Networking (Transit Gateway)



Amazon Route 53

rosa-private-link public hosted zone

rosa-private-link private hosted zone

Hosted Zones

Route 53 VPC Association

Route 53 VPC Association

VPC

x 3 for multi-az

Private Subnet 10.0.24.0/21

API

Ingress

Control

Infra

Worker

private-link

s3

Availability Zone

rosa-private-link 10.0.0.0/16

AWS Transit Gateway

172.16.0.0
172.16.1.0
172.16.2.0

Private Route Table
0.0.0.0/0 -> TGW
10.0.0.0/16 local

VPC

IGW

NGW

Elastic IP

Public Subnet 10.1.0.0/24

Optional SSH Bastion

Private Subnet 10.1.8.0/24

Optional TLS Proxy

Availability Zone

egress-vpc 10.1.0.0/16

172.16.0.0
172.16.1.0
172.16.2.0

Public Route Table
0.0.0.0/0 -> Nat GW
10.0.0.0/16 local

Private Route Table
0.0.0.0/0 -> Nat GW
10.1.0.0/16 local
10.0.0.0/16 TGW
10.2.0.0/16 TGW

VPC

Private Subnet 10.2.0.0/24

Route 53 Inbound Resolver

VPN / Direct Connect

Availability Zone

infra-vpc 10.2.0.0/16

172.16.0.0
172.16.1.0
172.16.2.0

Private Route Table
0.0.0.0/0 -> TGW
192.168.0.0/16
10.2.0.0/16 local

172.16.0.0
172.16.1.0
172.16.2.0

Route Table
10.0.0.0/8 -> TGW

On Prem
192.168.0.0/16

ROSA Private-Link - TGW

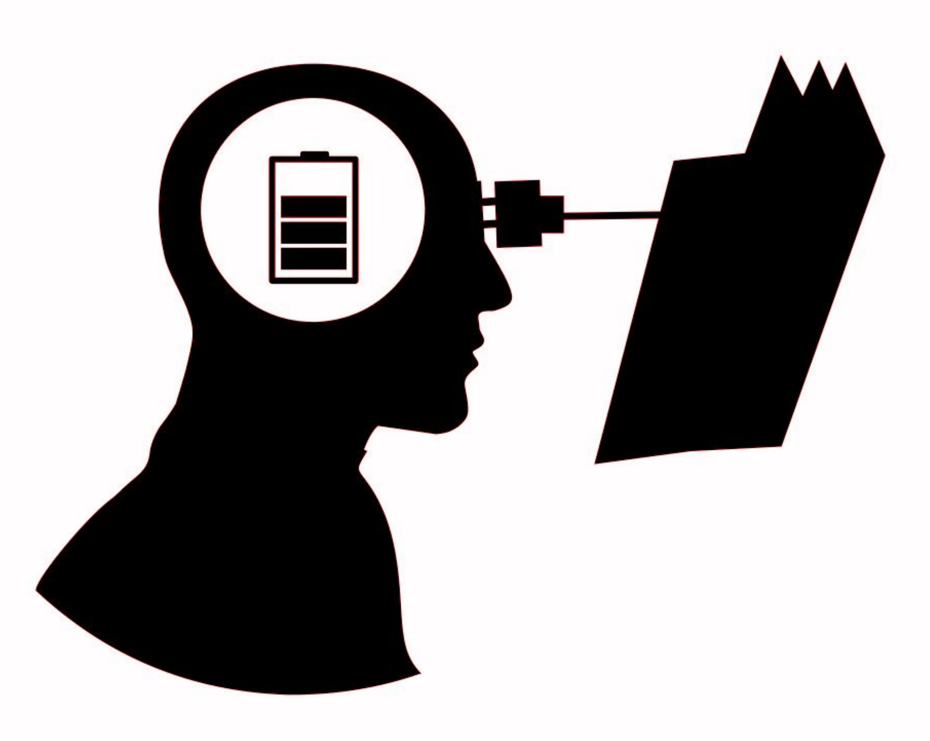
pczarkow | May 2, 2022

Source: https://github.com/rh-mobb/ansible-rosa

Section 1:
Day Two Operations

Day Two Operations

What you'll learn today.

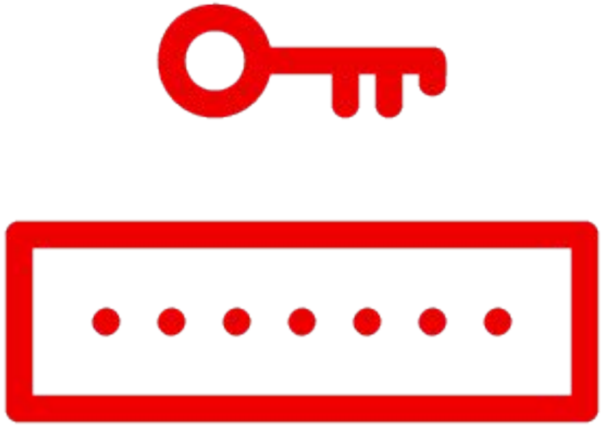


- Integrating with Amazon Cognito for IDP
- Managing Cluster Upgrades
- Managing Worker Nodes
- Cluster Autoscaling
- Labeling Nodes
- Logging with AWS CloudWatch

Day Two Operations

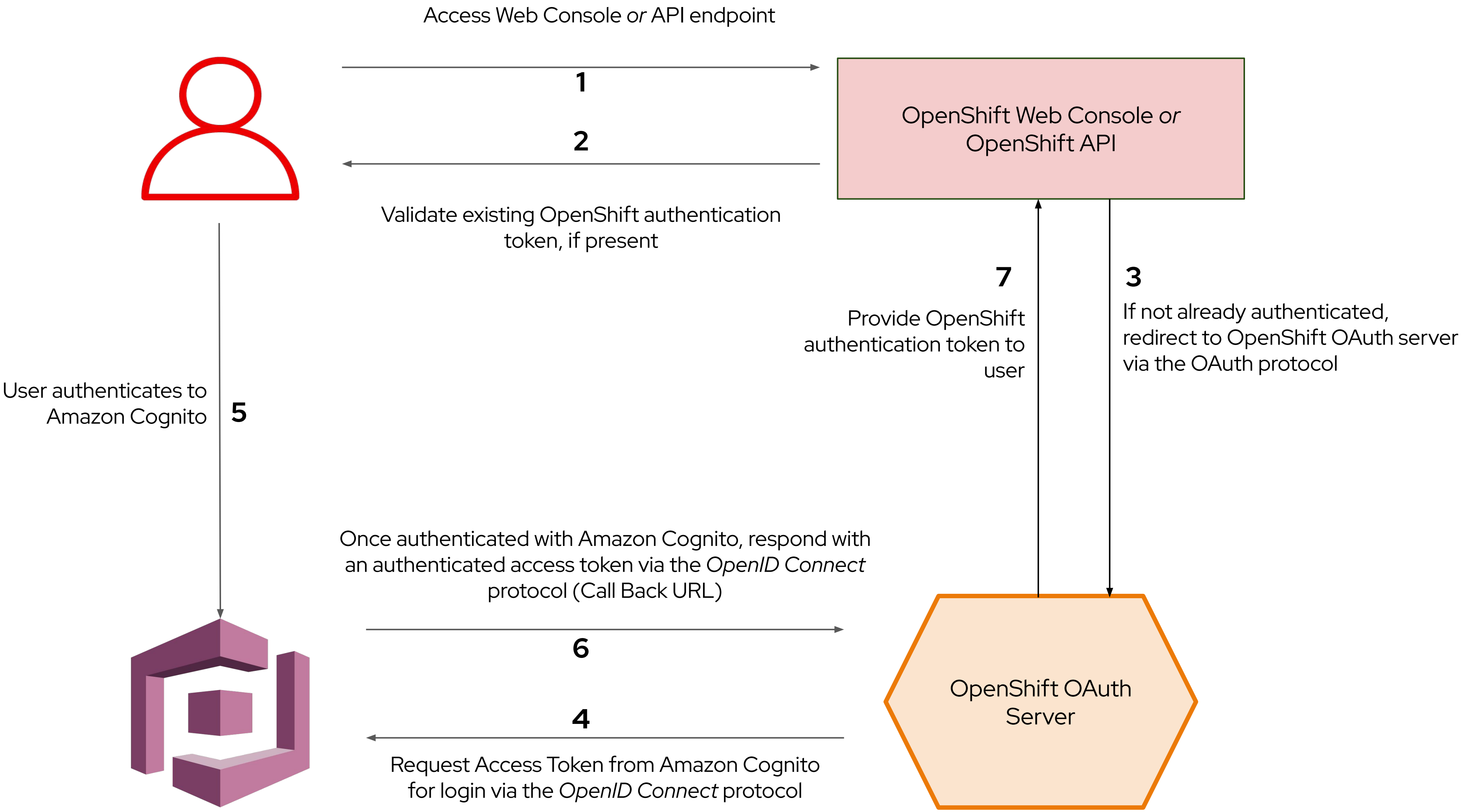
- **Integrating with Amazon Cognito for IDP –** In this module you will learn how to configure ROSA to authenticate against an OpenID Identity Provider such as Amazon Cognito.
- **Managing Cluster Upgrades –** ROSA makes cluster upgrades easy. Manage cluster upgrades – automatically or manually – for major, minor, or patch updates.
- **Managing Worker Nodes –** In this module you'll learn about MachinePools, and how to use them to manage the desired state of worker nodes.
- **Cluster Autoscaling –** In this module we'll cover how to configure a cluster to automatically scale based on the requirements of running (or requested) pods.
- **Labeling Nodes –** Labeling nodes allows for a number of use cases. In this module we will show how to schedule workloads on specific nodes which can be useful to match the application to required hardware (CPU, Memory, GPU).
- **Logging with AWS CloudWatch –** By default cluster logs are stored within the ROSA cluster. This module will show you how to ship logs off the cluster and into your preferred logging destination such as AWS CloudWatch.

Integrating with IDPs



- ROSA supports a number of Identity Providers:
  - GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect.
- In this workshop, we'll use Amazon Cognito via the OpenID Connect integration.

Learn more about Identity Providers here:
https://docs.openshift.com/rosa/rosa_install_access_delete_clusters/rosa-sts-config-identity-providers.html



Access Web Console *or* API endpoint

1

2

OpenShift Web Console *or* OpenShift API

Validate existing OpenShift authentication token, if present

7

Provide OpenShift authentication token to user

3

If not already authenticated, redirect to OpenShift OAuth server via the OAuth protocol

User authenticates to Amazon Cognito

5

Once authenticated with Amazon Cognito, respond with an authenticated access token via the *OpenID Connect* protocol (Call Back URL)

6

OpenShift OAuth Server

4

Request Access Token from Amazon Cognito for login via the *OpenID Connect* protocol

Cluster Upgrades

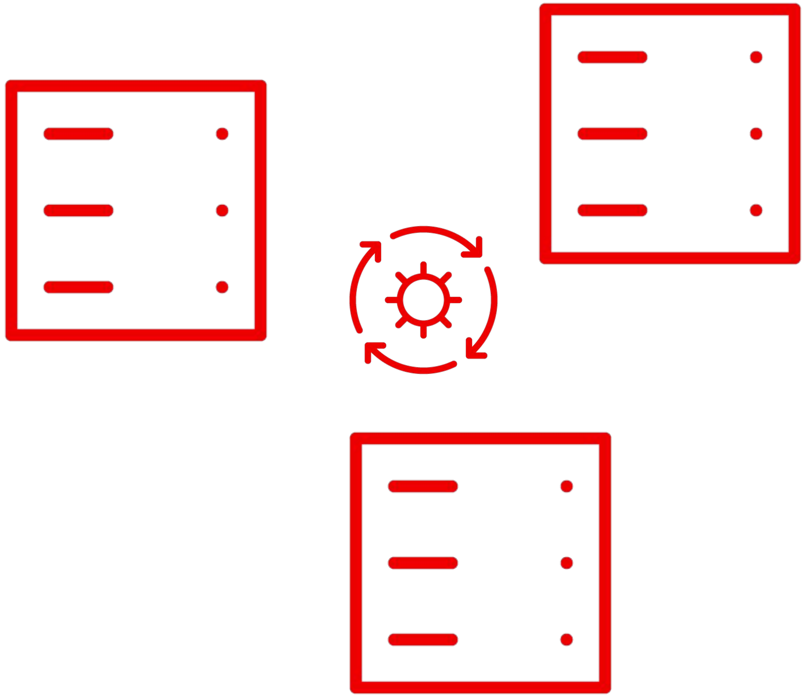
Major.Minor.Patch

- Cluster upgrades can be **manually initiated** or **automatically scheduled**.
- **Critical CVEs** are **automatically patched** within **48 hours** of a Patch release.
  - Impacted Patch releases are deprecated and not supported.
- **Minor versions** are supported for **14 months**.
- **Major versions** are supported for **12 months following** the release of a **new major version**.

Learn more about upgrades here:
https://docs.openshift.com/rosa/rosa_architecture/rosa_policy_service_definition/rosa-life-cycle.html#rosa-life-cycle

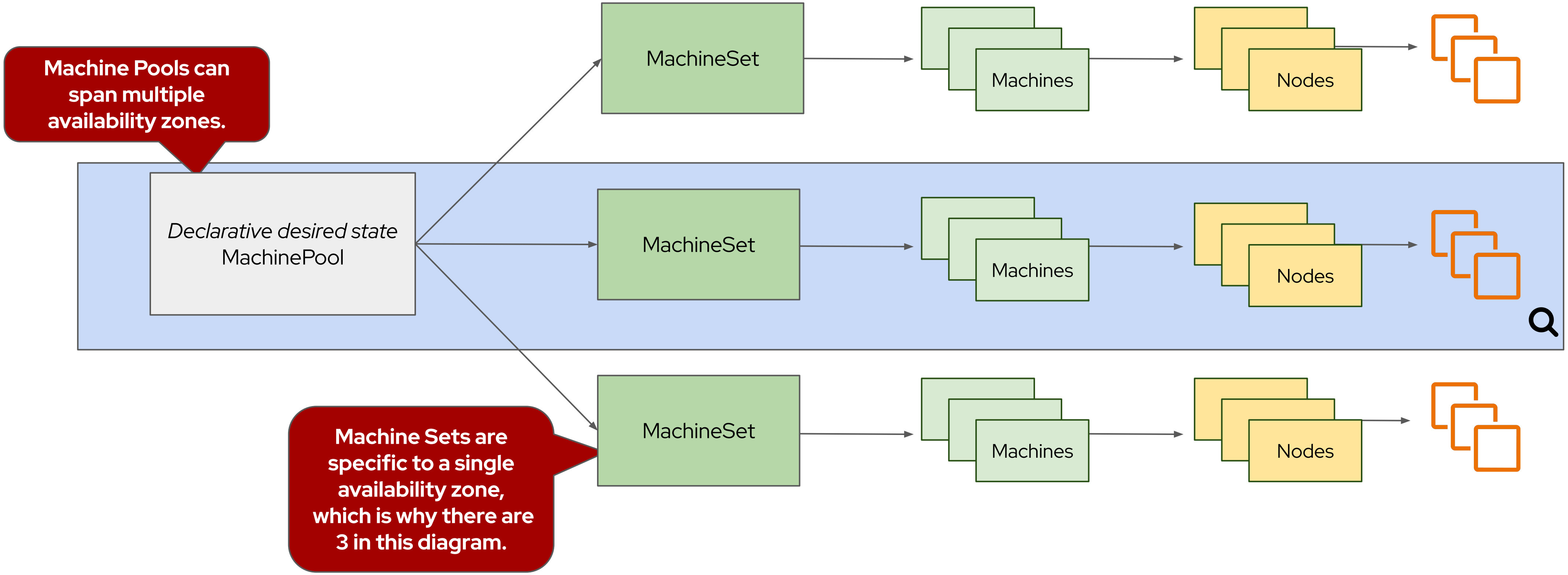
Managing Worker Nodes

Providing highly available compute.



- MachinePools allows for worker nodes that span multiple availability zones (AZs).
- MachinePools provide a declarative desired state for worker nodes to ensure consistency across AZs.
- MachinePools can be scaled up or down manually or automatically.

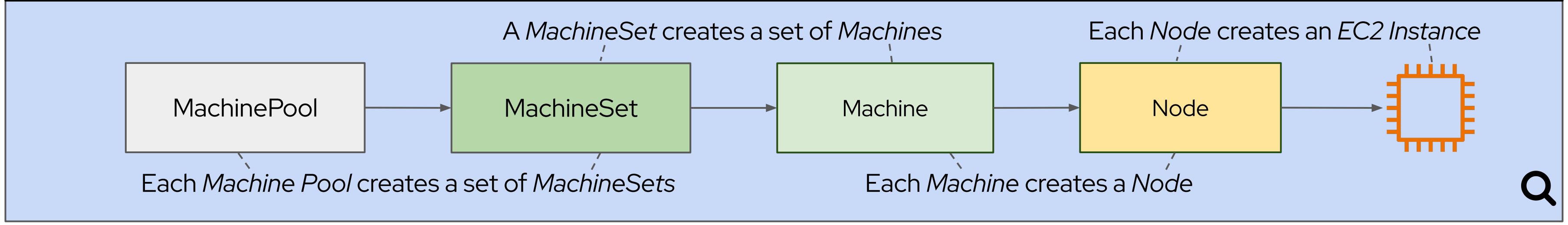
Learn more about Managing Worker Nodes here:
https://docs.openshift.com/rosa/rosa_cluster_admin/rosa_nodes/rosa-managing-worker-nodes.html



Machine Pools can span multiple availability zones.

Machine Sets are specific to a single availability zone, which is why there are 3 in this diagram.

Machine Pools are managed by the *OpenShift Cluster Manager (OCM)*. The rest of the process is managed by the *Machine API Operator*. This operator interacts with the *AWS API* directly to provision *EC2 instances*.



A *MachineSet* creates a set of *Machines*

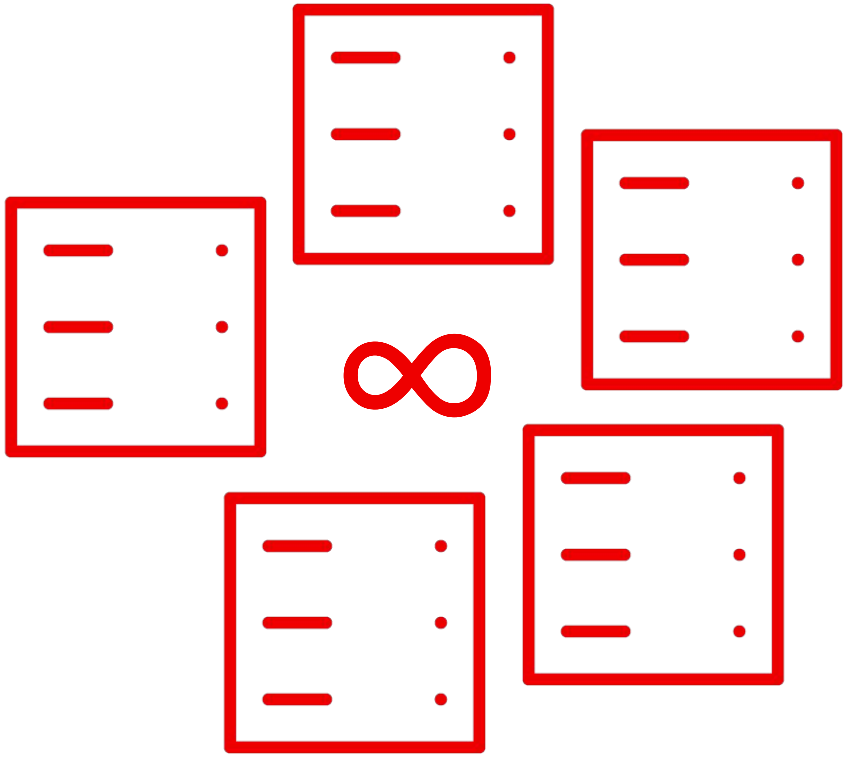
Each *Node* creates an *EC2 Instance*

Each *Machine Pool* creates a set of *MachineSets*

Each *Machine* creates a *Node*

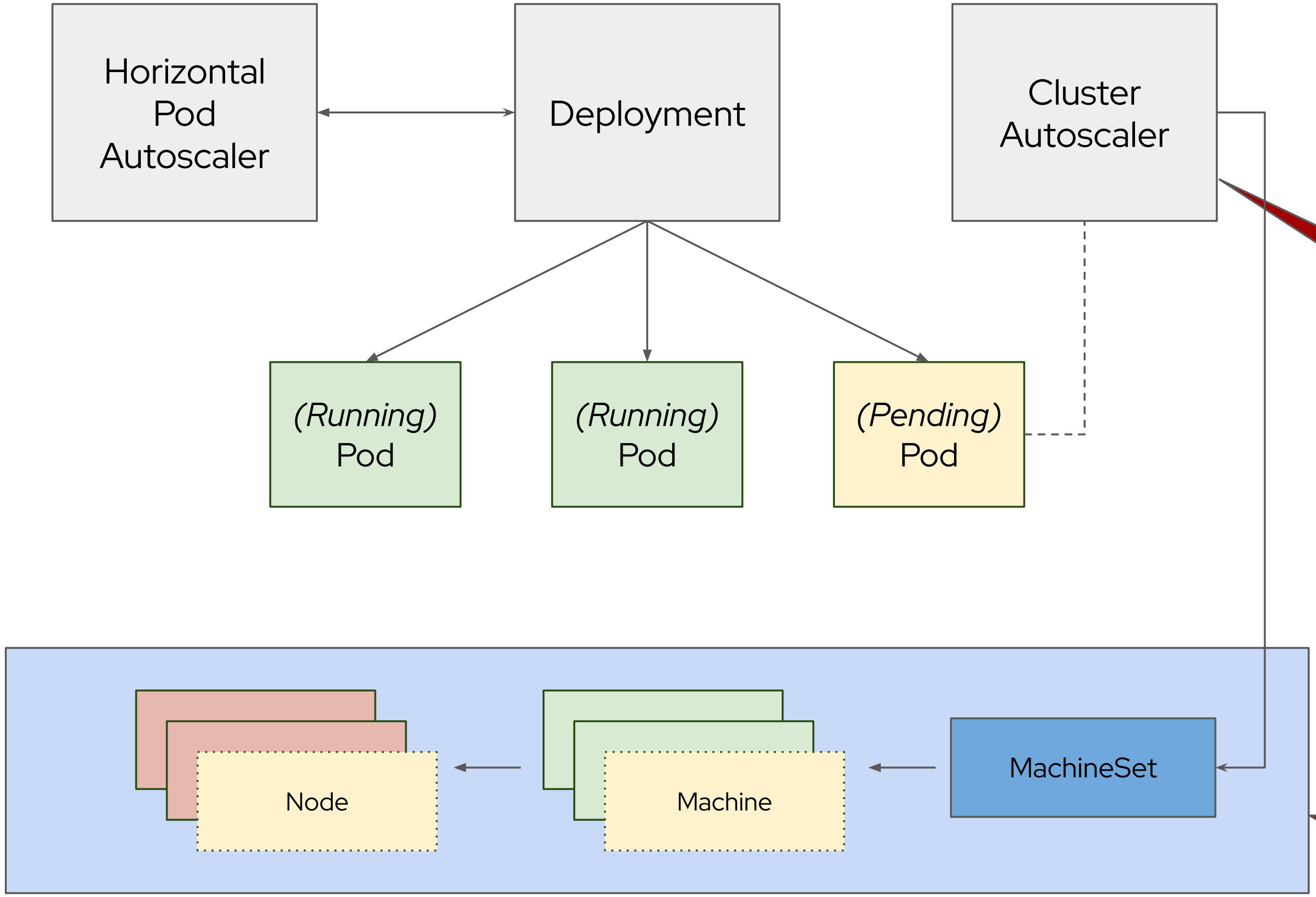
Cluster Autoscaling

Automatically responding to cluster demand.



- MachinePools can be scaled to meet applications demands.
- Cluster AutoScaler will provision additional worker nodes when pods can not be scheduled due to resource constraints.
- Cluster AutoScaler will not scale beyond predefined limits.

Learn more about Cluster Autoscaling here:
https://docs.openshift.com/rosa/rosa_cluster_admin/rosa_nodes/rosa-nodes-about-autoscaling-nodes.html

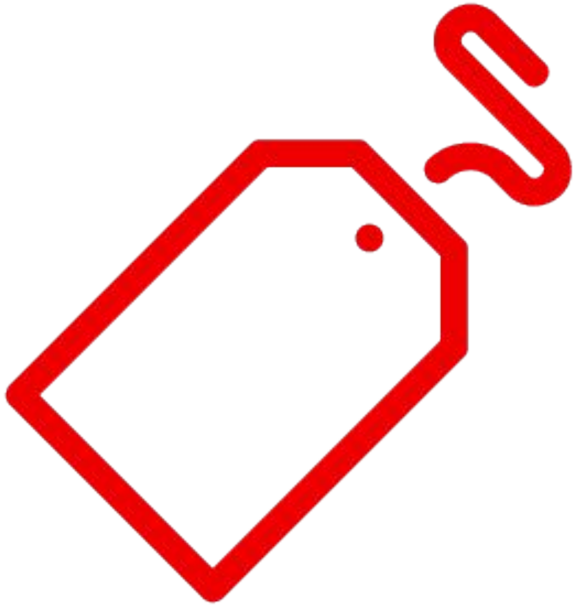


The cluster autoscaler scales the MachineSet up to accommodate the pending pod.

Once the MachineSet scales up, it creates a new machine, which creates a new node.

Labeling Nodes

Deploy the right applications to the right compute resources.



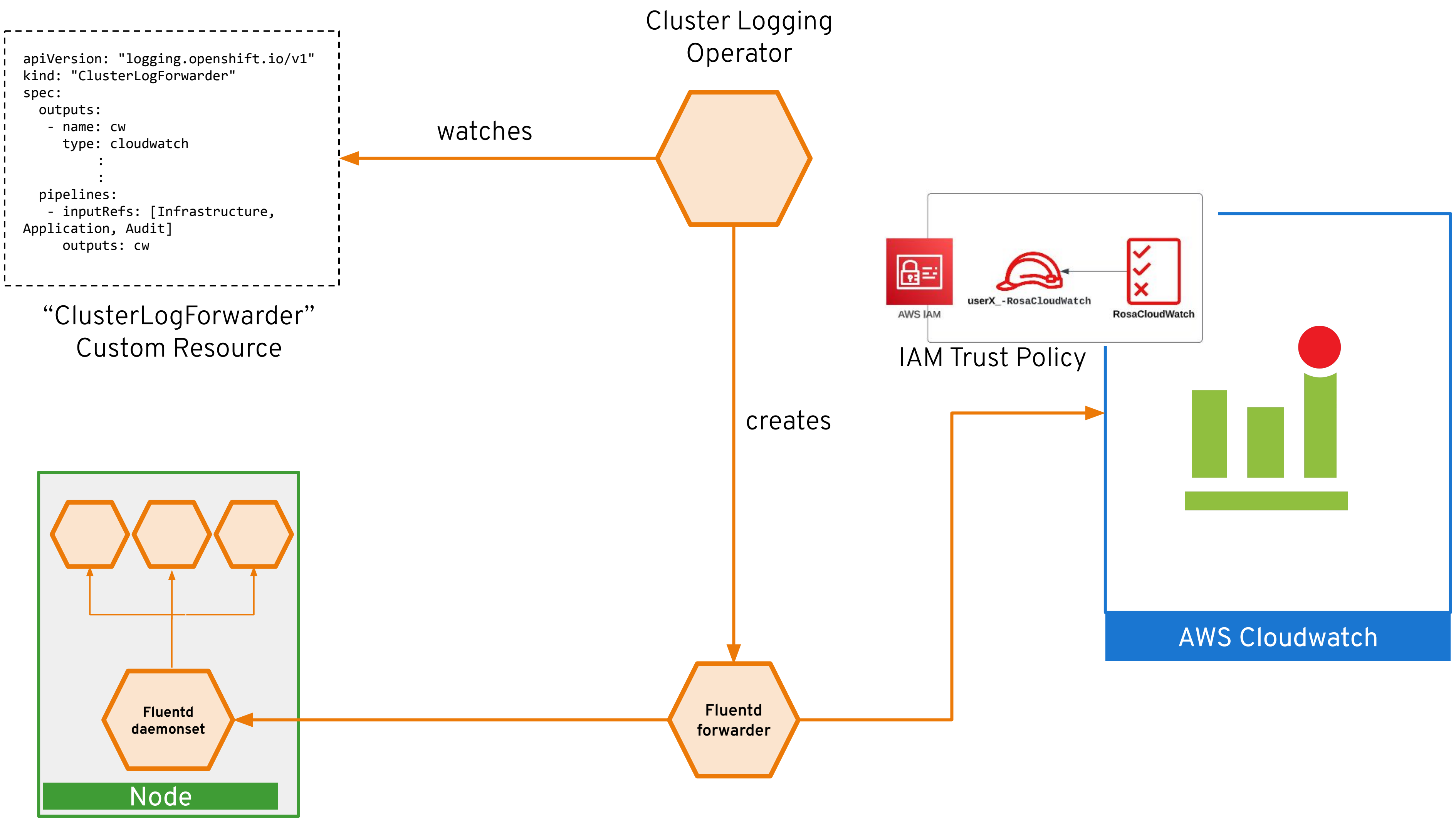
- Labels allow application pods to automatically deploy to the correct compute resources.
- Examples include CPU or Memory intensive workloads, or workloads requiring GPU resources.

Logging with AWS Cloudwatch

Shipping logs to an enterprise-wide log management system.

- **OpenShift Cluster logs** are **stored in cluster** by **default**.
- **Cluster logs** can be **shipped** to a variety of log management systems such as **FluentD, ElasticSearch, Syslog, AWS CloudWatch, Loki, Kafka, and Splunk.**

Secure Log Forwarding to Cloudwatch



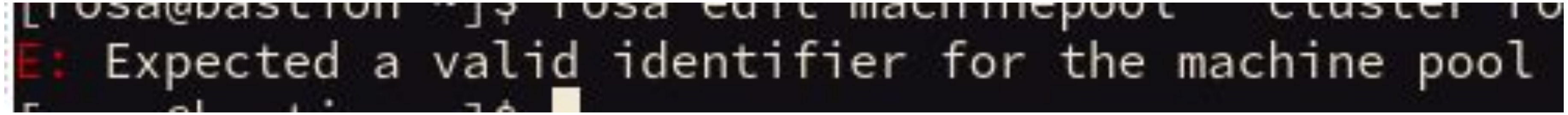
```
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogForwarder"
spec:
  outputs:
   - name: cw
     type: cloudwatch
         :
         :
  pipelines:
   - inputRefs: [Infrastructure,
Application, Audit]
     outputs: cw
```

“ClusterLogForwarder”
Custom Resource

Red Hat

In the section: “*Enable Autoscaling on the Default MachinePool*”

If you see this error message:



```
[rosa@bastion ~]$ rosa edit machinepool --cluster ro
E: Expected a valid identifier for the machine pool
[rosa@bastion ~]$
```

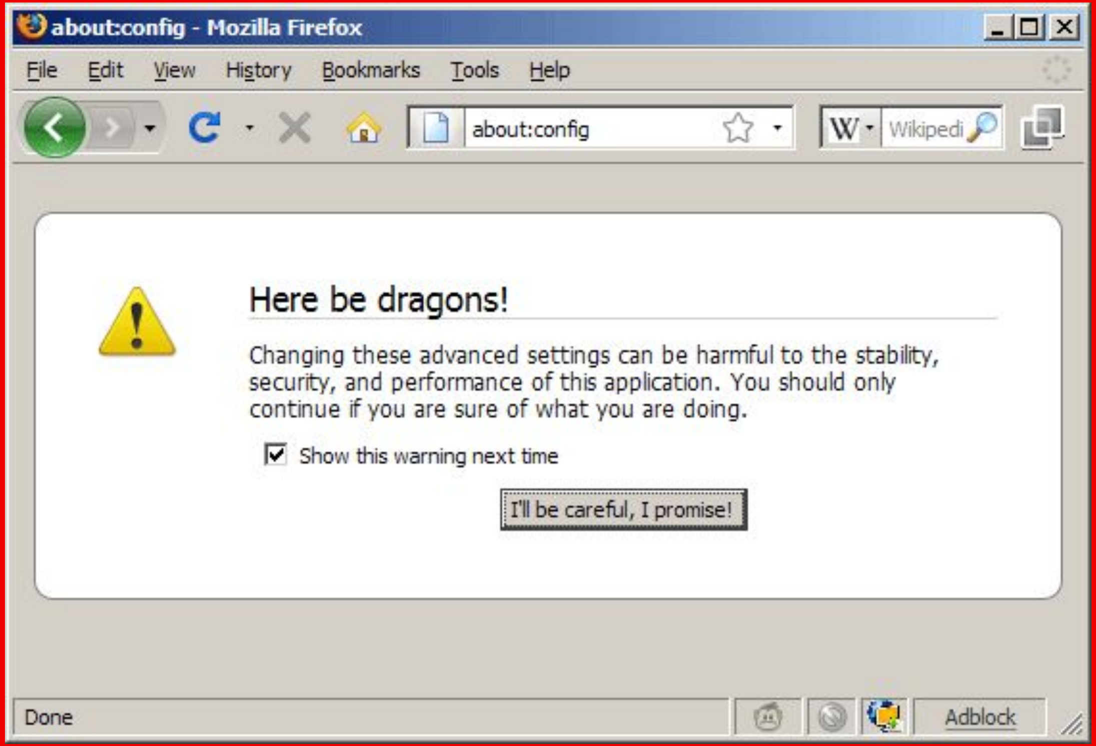
Change the machinepool id from “**Default**” to “**worker**”

Example:
rosa edit machinepool --cluster rosa-${GUID} **Default** --enable-autoscaling --min-replicas=2 --max-replicas=4

->

rosa edit machinepool --cluster rosa-${GUID} **worker** --enable-autoscaling --min-replicas=2 --max-replicas=4

Bonus material



about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
Wikipedi

Here be dragons!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

I'll be careful, I promise!
Done
Adblock

Red Hat - ROSA Workshop

- Deploying an OpenShift cluster with Red Hat OpenShift Service on AWS (ROSA) YouTube Video
- ROSA with STS explained
- Setup an IdP - GitHub
- Obtaining support

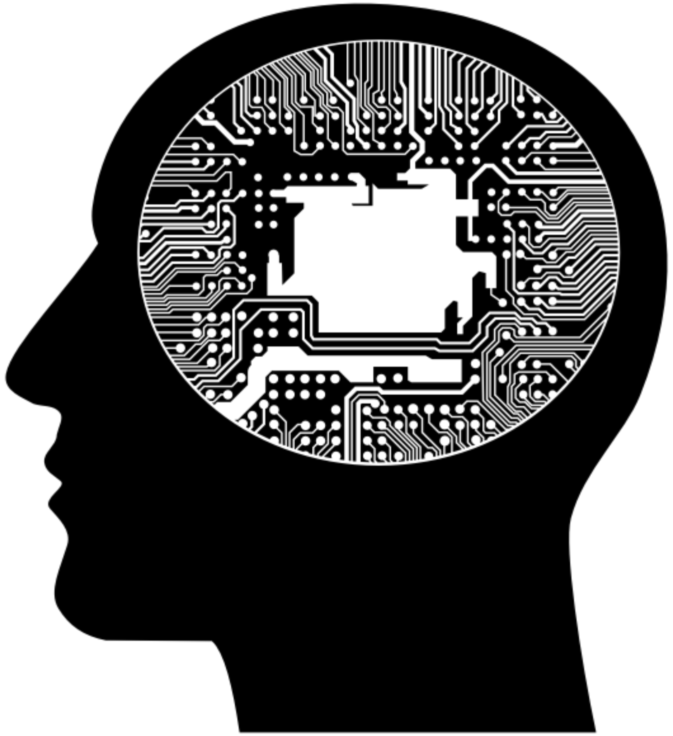
AWS - ROSA Workshop

- Joint Support
- AWS EFS Storage

Section 2:
Deploy and Expose an Application

Deploy and Expose an Application

What you'll learn today.



- Deploying Applications
- Restricting Network Access
- Making Applications Resilient

Deploy and Expose an Application

- **Deploying Applications –** In this module we will deploy an application based on Quarkus that leverages a Amazon DynamoDB database. We will show how to leverage IAM service accounts for DB authentication, as well as how to leverage source-2-image for a true application platform experience.
- **Restricting Network Access –** OpenShift makes it easy to implement zero-trust networking policies. In this module we will restrict network access to our application.
- **Making Applications Resilient –** In this module we will learn how to make an application resilient by leveraging Pod Disruption Budgets, and the Horizontal Pod Autoscaler.

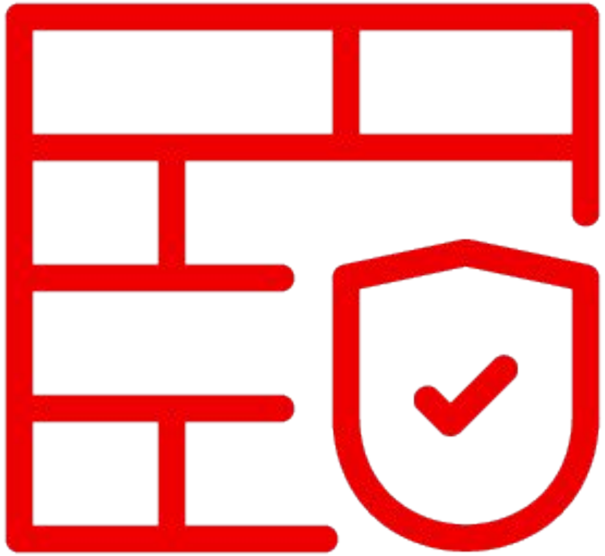
Deploying Applications

Deploy a Java based application using Quarkus and S2I.

- **Source-2-Image** (S2I) takes **application code** and **bundles it into a container** that can be **ran in OpenShift**.
- **Quarkus incorporates S2I** as part of it's build system, and can a**utomatically deploy** an application **to OpenShift** based on the application configuration.
- **Service Accounts** in OpenShift can **map to IAM roles** that **grant access to cloud resources** such as Amazon DynamoDB.

Restricting Network Access

Limit application access using NetworkPolicy.



- **NetworkPolicy allows for** applications to leverage the concepts of **Zero-Trust Networking: Deny by default, explicitly allow ingress/egress.**
- **NetworkPolicy** can **dynamically select** allowed or disallowed **clients** by leveraging **Pod or Namespace labels**.

Making Applications Resilient

- ROSA allows for applications to scale or recover from failure.
- **PodDisruptionBudgets define** the **minAvailable** and **maxUnavailable pods** for a given application (based on labels).
- **HorizontalPodAutoscaler** (HPA) allows for applications to **scale based on resource consumption** such as **CPU or RAM** utilization.

Using OpenShift GitOps

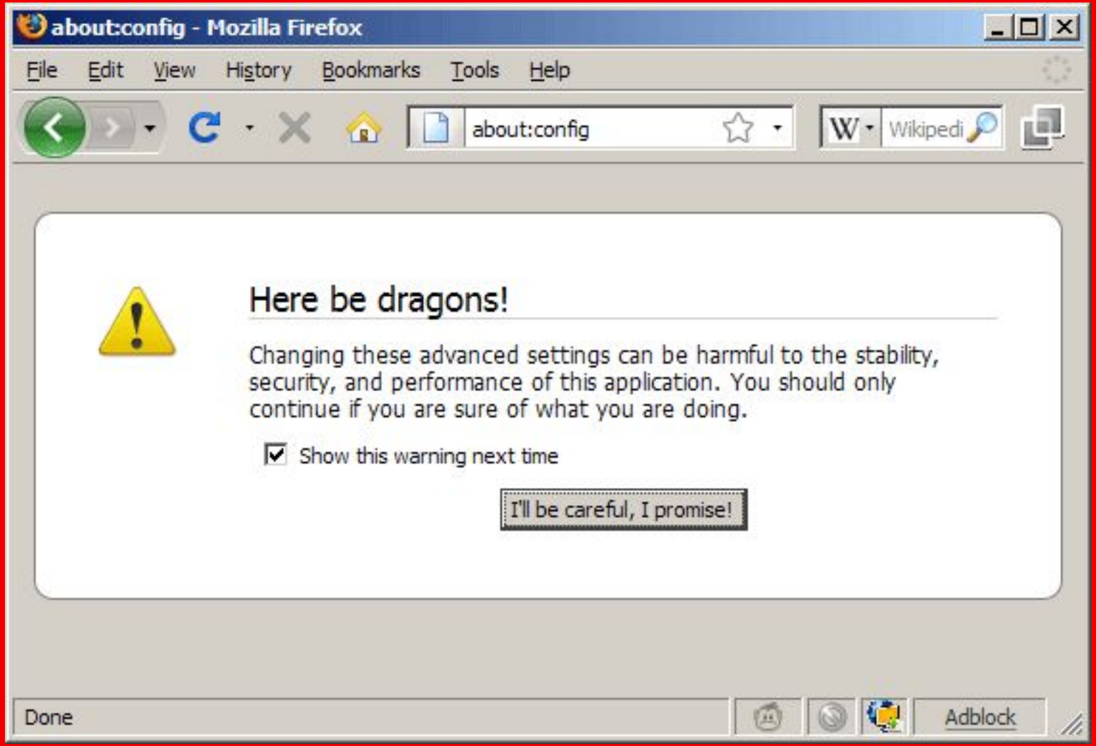
Consistent Code Across Environments

- **Treat everything as code**: Define the state of infrastructure, applications, and configurations with declarative code across environments
- **Single Source of Truth:** Infrastructure and applications are stored and versioned in Git allowing for traceability and visibility into changes that affect their entire state
- **Enhanced security:** Preview changes, detect configuration drifts, and take action
- **Visibility and audit:** Capture and trace any change to clusters through Git history
- **Multi-cluster consistency:** Combine GitOps with Advanced Cluster Manager for Kubernetes to configure multiple clusters and deployments reliably and consistently

Automate Deploying the App with Tekton

- **Cloud-Native Pipelines:** Scalable, portable, and containerized CI/CD workflows aligned with OpenShift's cloud-native architecture
- **Decoupled and Reusable Tasks:** Define and share reusable tasks, reducing duplication and improving maintainability.
- **Kubernetes-Native Custom Resources:** Manage pipelines using familiar Kubernetes tools and concepts.
- **Integration with OpenShift Pipelines:** Higher-level abstractions and tooling for quick setup via web console or CLI.
- **Security and Compliance:** Robust OpenShift security features extend to Tekton pipelines, ensuring protection and compliance.

Bonus material



Here be dragons!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

ROSA Workshop

- Deploy OSToy Application
- Integrating with AWS services - ACK Controller
- S2I Deployments

Wrapping Up!

Building & running a platform *vs* a turnkey Cloud Service

The Parts

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

Kubernetes Cluster Services
Basic Networking :: Ingress

Kubernetes

Custom OS

xKS + 'native' services

The Assembled Car

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

OpenShift Cluster Services
Networking :: Router :: OLM

Kubernetes

Red Hat Core OS

- Application Platform -
Self-managed Red Hat OpenShift

The Car & Pit Crew

SRE and Customer Success

Monitoring | Service Mesh | Dev Tools

Registry | Metrics | Logging | CI/CD

OpenShift Cluster Services
Networking :: Router :: OLM

Kubernetes

Red Hat Core OS

- Turnkey Application Platform -
Red Hat OpenShift cloud services

"Batteries Included"

... but swappable

Individual components can be swapped out

Eg.

- Using AWS CloudWatch for logging on AWS
- Use specific cloud services or ISV offerings

An opinionated platform for building, deploying and running applications

Red Hat OpenShift

Service Mesh	App-Services	DB-Services
CI/CD	DNS	Authentication
Monitoring	**Kubernetes**	Automation
Logging	Registry	Security
Compute	Storage	Network

- Fully integrated and supported components
- Expert SRE and Customer Success support
- Abstracts away technical details
- Consistent experience across clouds

Building blocks of a Modern Application Platform

Red Hat OpenShift

Service Mesh	App-Services	DB-Services
CI/CD	DNS	Authentication
Monitoring	**Kubernetes**	Automation
Logging	Registry	Security
Compute	Storage	Network

Helpful Links

ROSA Documentation

- https://docs.openshift.com/aro/4/welcome/index.html

MOBB.Ninja ROSA Guides

- https://mobb.ninja/#rosa

Introduction to ROSA - Red Hat Training

- https://www.redhat.com/en/services/training/DO120-introduction-to-red-hat-openshift-service-on-aws

ROSA Lightboard Videos

- https://www.redhat.com/en/about/videos/rosa-lightboard

ROSA User Guide - AWS

- https://docs.aws.amazon.com/ROSA/latest/userguide/what-is-rosa.html

Introduction to ROSA - Red Hat Ebook

- https://access.redhat.com/documentation/en-us/red_hat_openshift_service_on_aws/4/pdf/introduction_to_rosa/red_hat_openshift_service_on_aws-4-introduction_to_rosa-en-us.pdf

Thank you!

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat