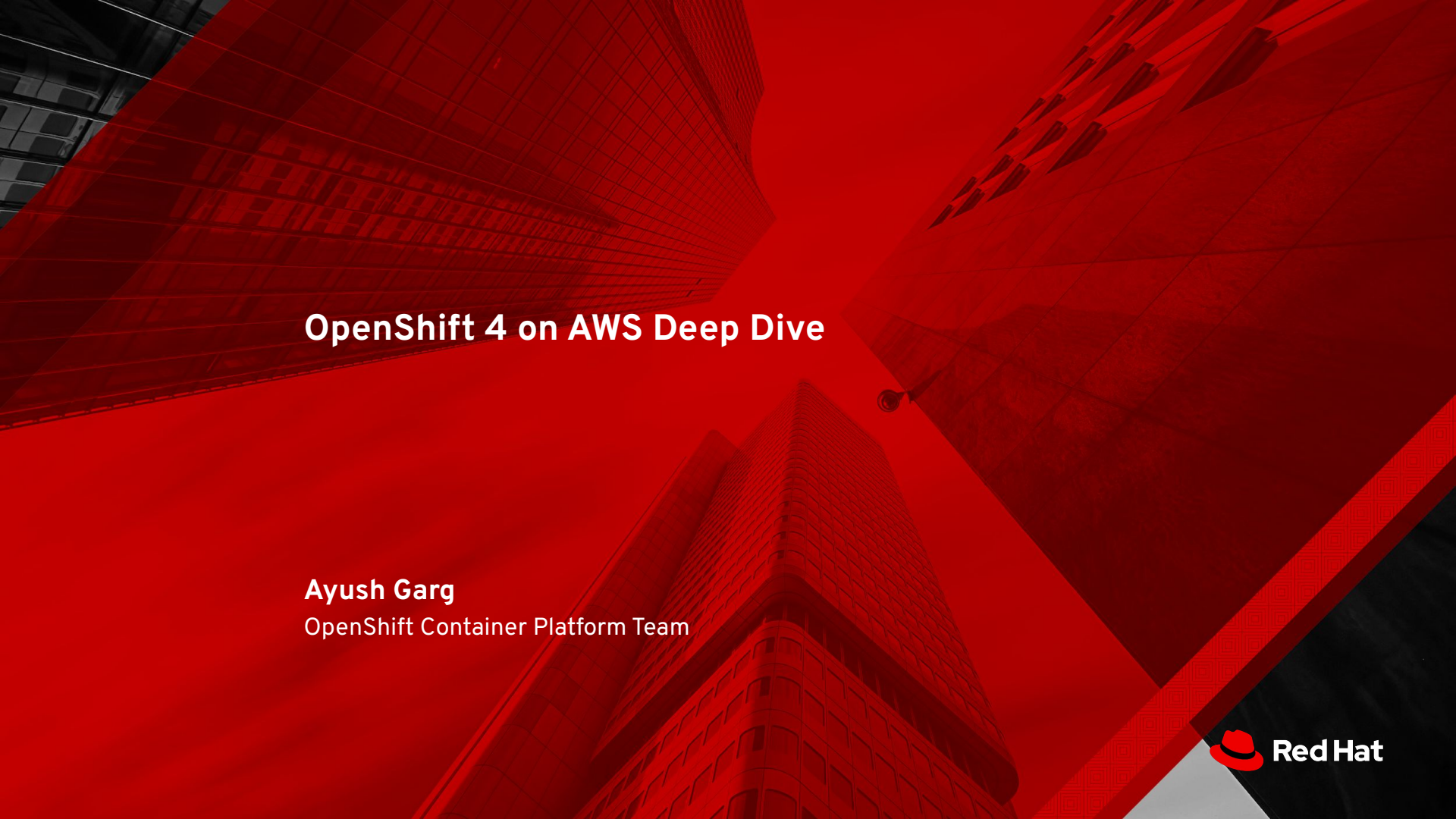

OpenShift 4 on AWS Deep Dive
Ayush Garg
OpenShift Container Platform Team
Red Hat

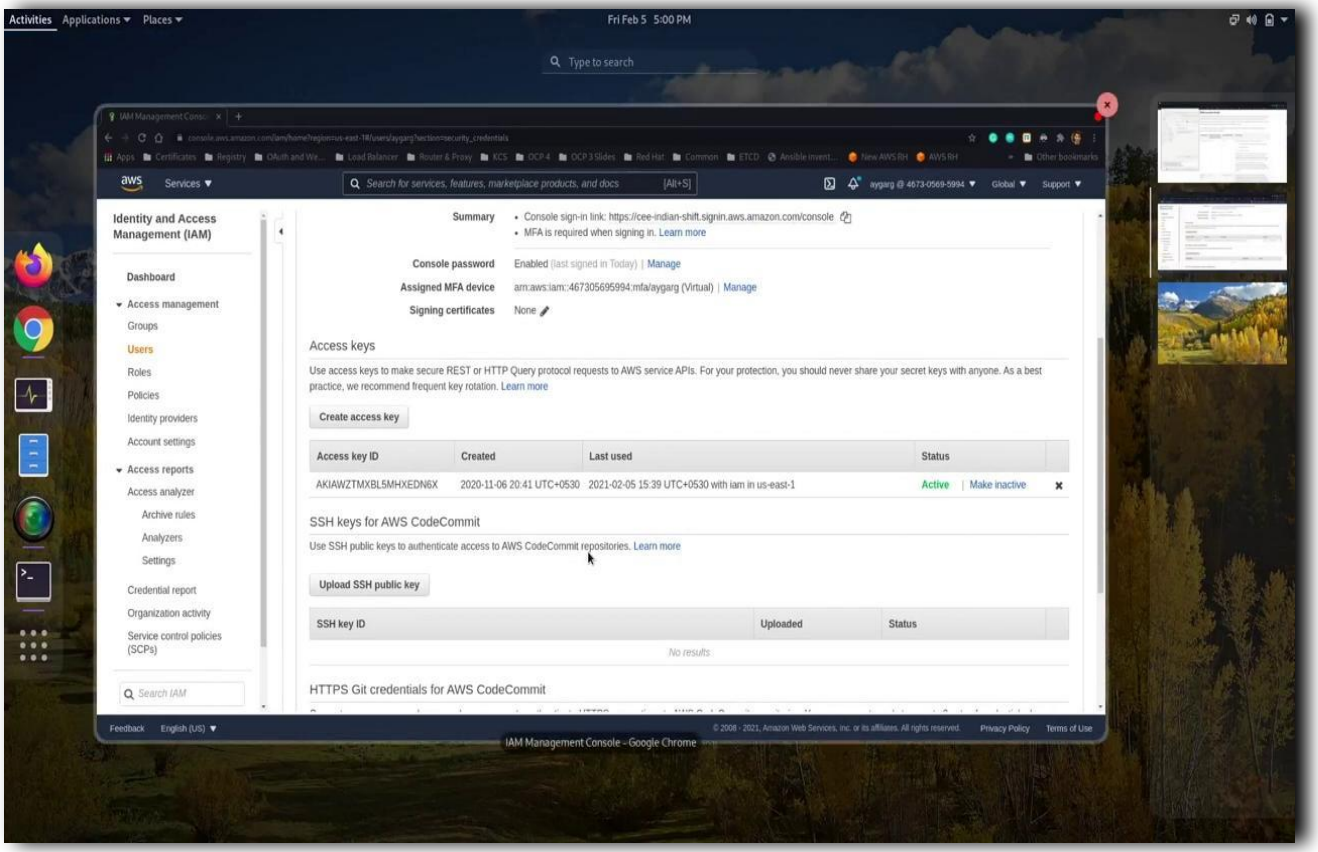
What we'll discuss today

- Prerequisite
- Prerequisite Check
- AWS Services
- VPC Networking Architecture
- Cluster Architecture
- install-config.yaml
- Installation
- AWS Resources Creation and Destruction
- VPC Break-Down
- EC2 Break-Down
- IAM Break-Down
- S3 Break-Down
- Route 53 Break-Down
- AWS specific features
- How OpenShift identifies its resources on AWS?

Prerequisite

- An AWS account with IAM user with `AdministratorAccess` or root account [+]
- Programmatic access keys for user to access the AWS API
- Select a supported AWS region [+]
- Public hosted zone in `Route 53` service
- AWS account limits [+]

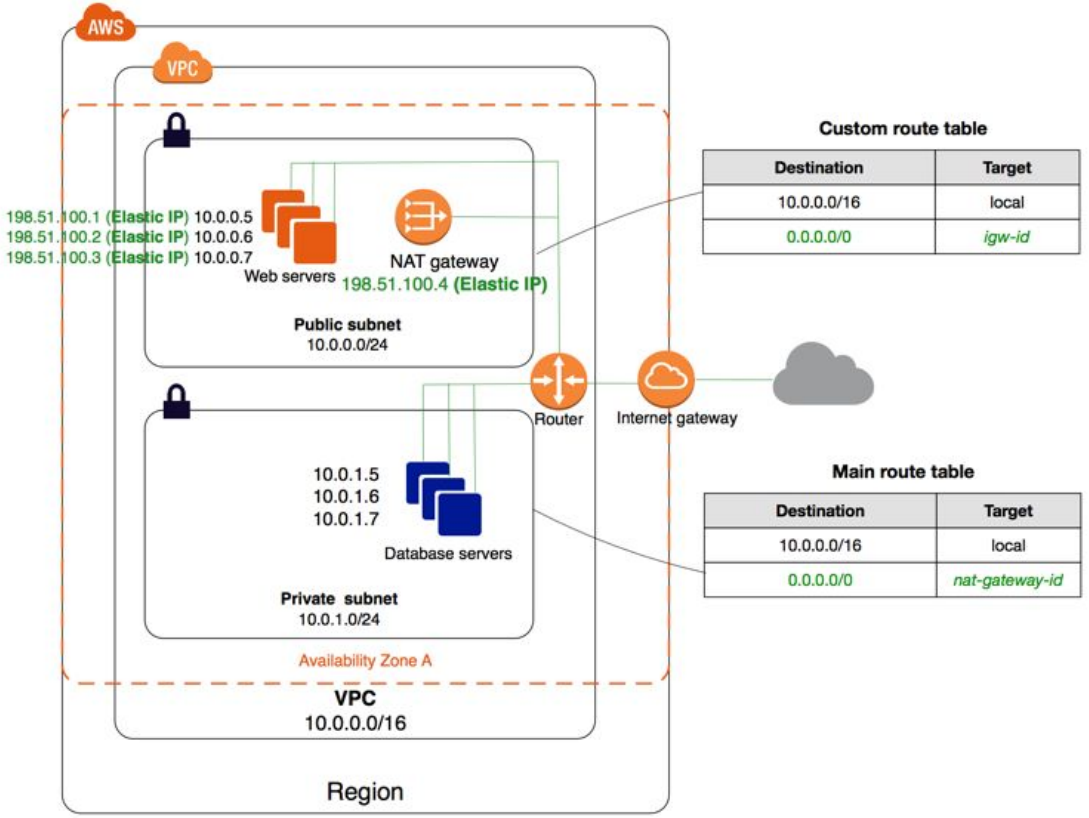
Prerequisite Check



Red Hat

AWS Services

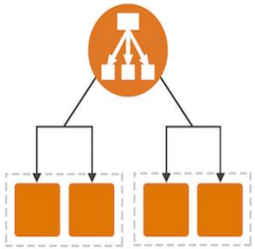
- **Virtual Private Cloud (VPC)**
  - NAT Gateway
  - Internet gateway
  - Subnets
  - Route Table
  - Endpoints

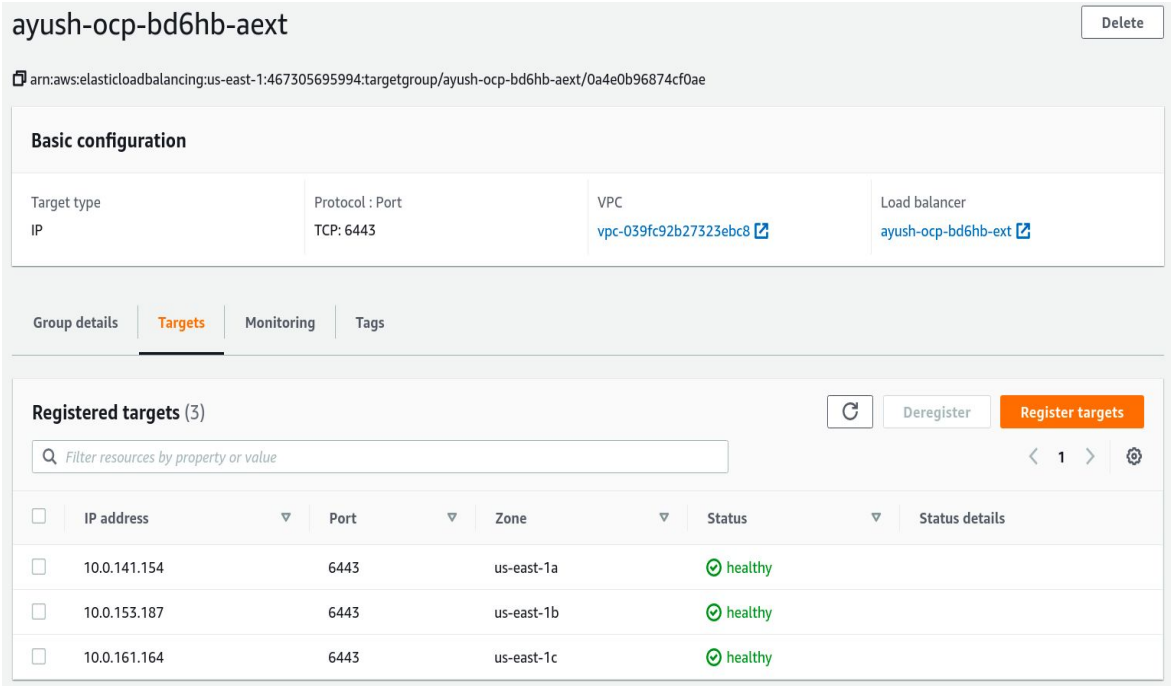


Red Hat

❖ Elastic Compute Cloud (EC2)

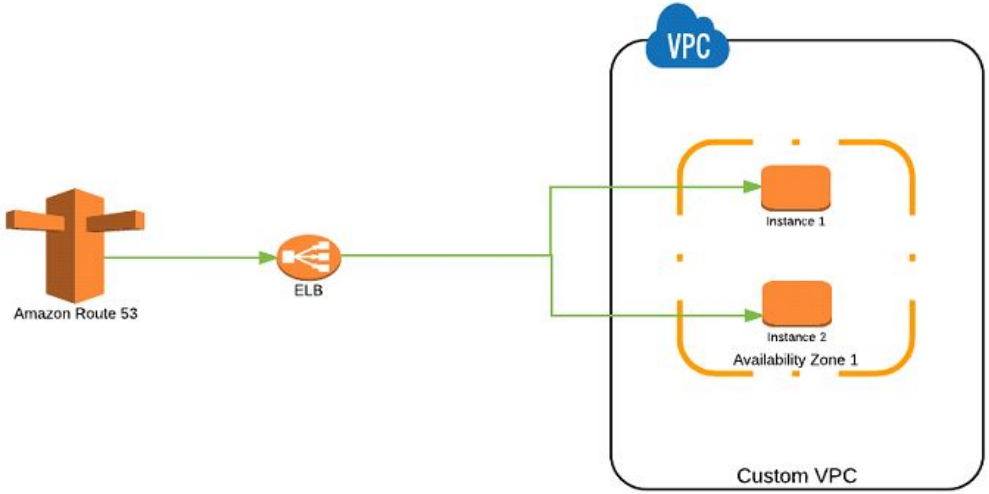
- ➢ Instances
- ➢ AMIs
- ➢ Volumes
- ➢ Security Groups
- ➢ Load Balancers
- ➢ Target Groups



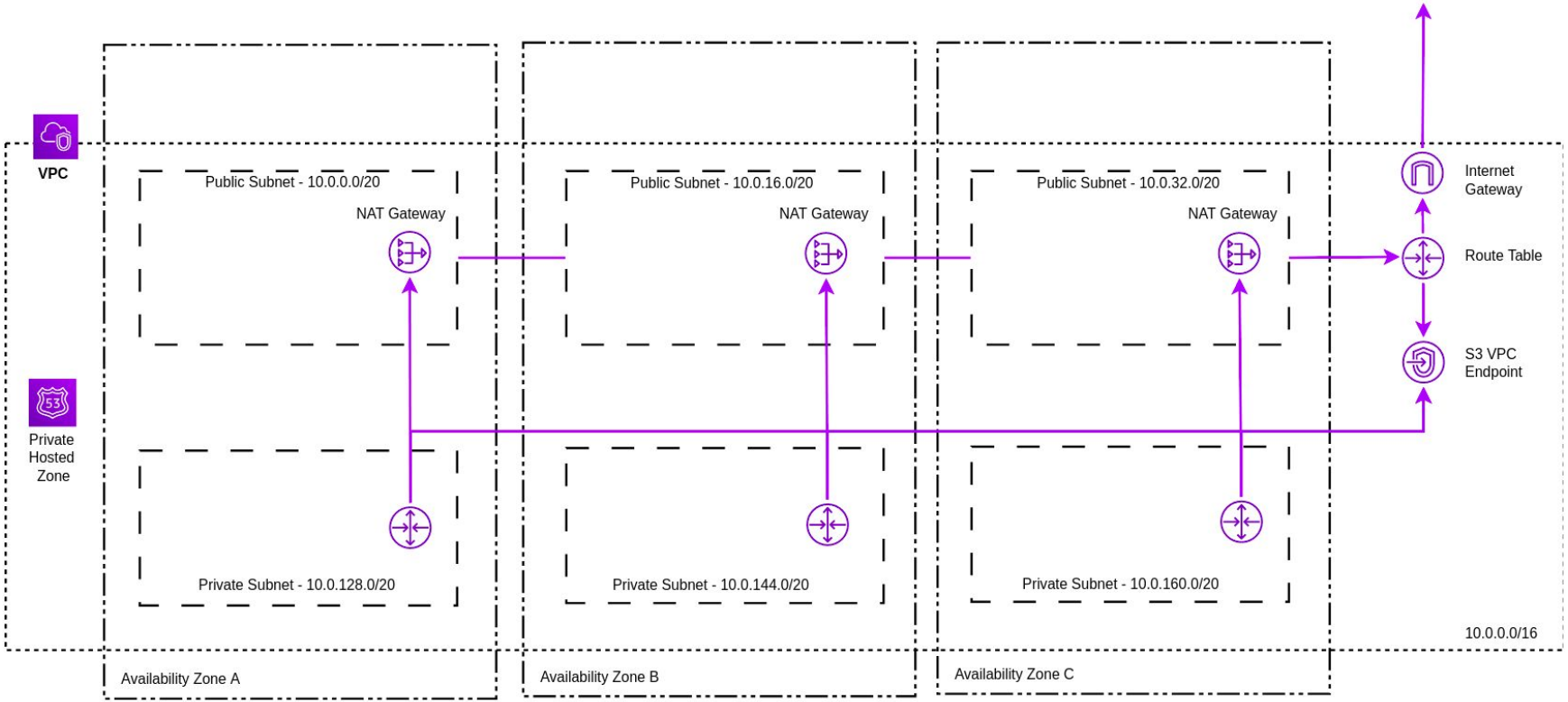


Red Hat

- **Identity and Access Management (IAM)**
  - Users
  - Roles
  - Security Credentials
- **Simple Storage Service (S3)**
  - Buckets (object storage)
- **Route 53 [+]**
  - Public Hosted Zones
  - Private Hosted Zones

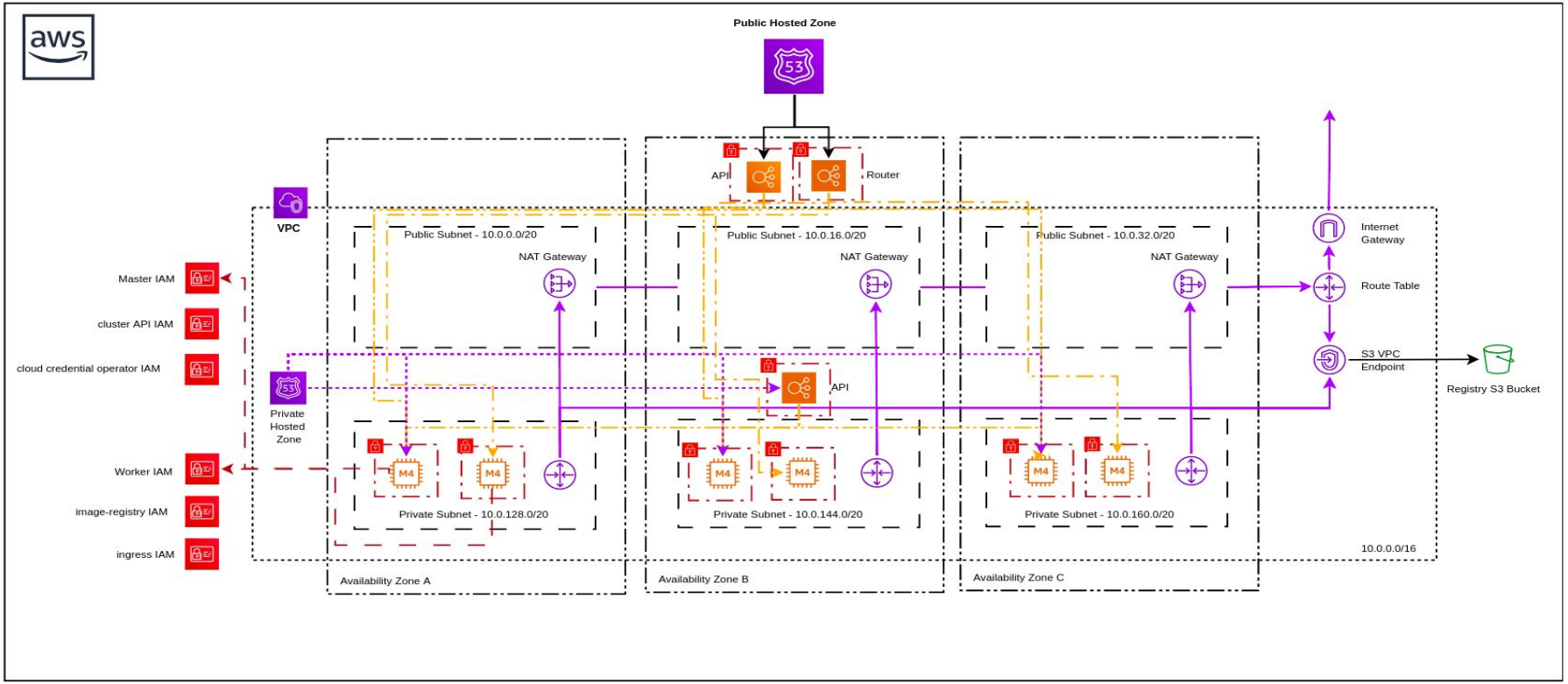


VPC Networking Architecture



Red Hat

Cluster Architecture



Red Hat

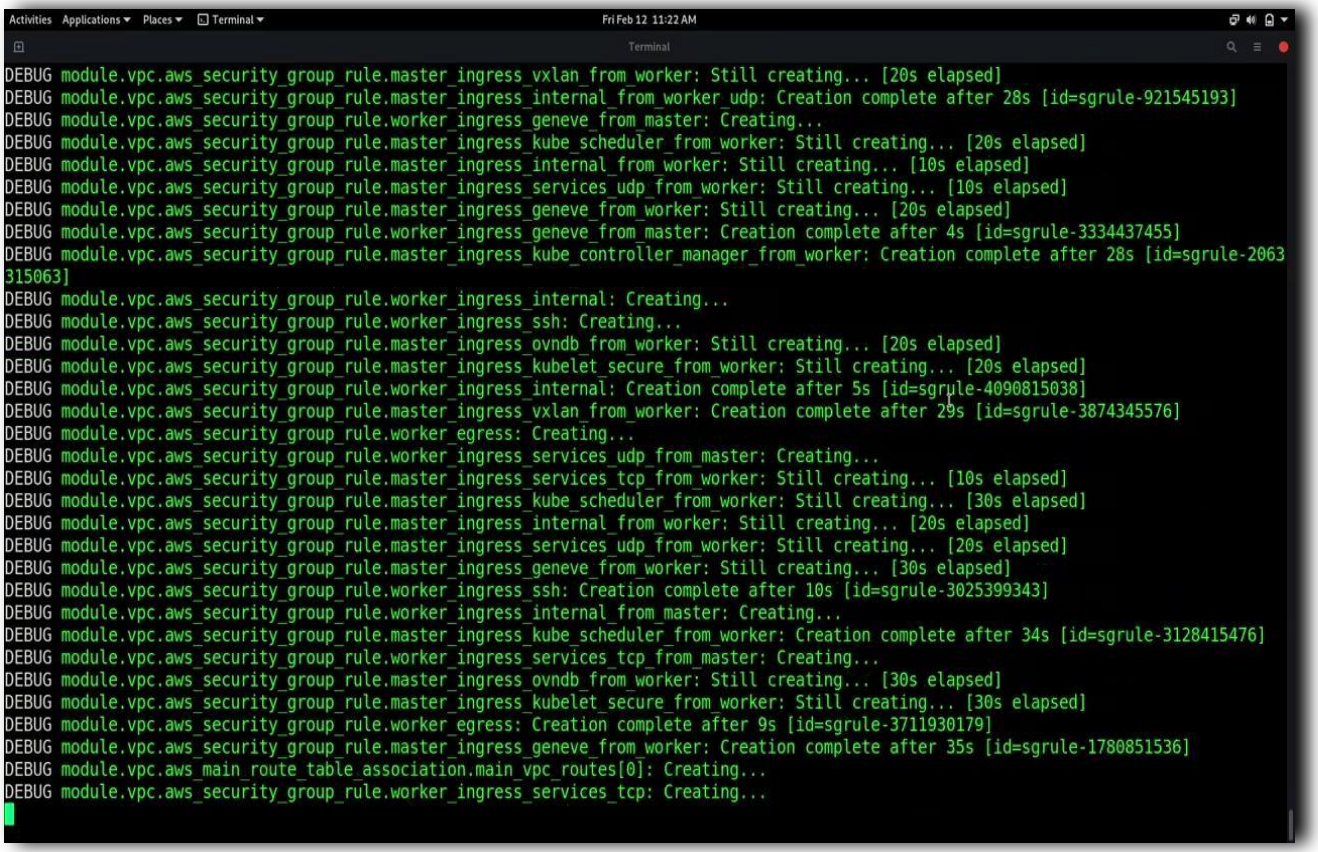
AWS specific options in install-config.yaml

- **baseDomain:** Public Hosted Zone
- **zones:** Availability Zone
- **machineNetwork:** VPC CIDR
- **platform:** AWS and Region
- **publish:** External or Internal

Customization [+]

```
apiVersion: v1
baseDomain: indiashift.support
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    aws:
      zones:
      - us-east-1a
      - us-east-1b
  replicas: 3
...
metadata:
  creationTimestamp: null
  name: ayush
networking:
...
  machineNetwork:
  - cidr: 10.0.0.0/16
...
platform:
  aws:
    region: us-east-1
publish: External
```

Installing on AWS



Red Hat

AWS Resources Creation and Destruction

- **Original Logs [+]:** Proper flow of resource creation, destruction and complete install.
- **Created Resources [+]:** Only the resources created with ID and name.
- **Destroyed Resources [+]:** Destroyed bootstrap resources.

VPC Break-Down

- **VPC:** IPv4 CIDR, DNS hostnames and resolution.
- **Subnets:** IPv4 CIDR for individual subnet per AZ.
- **Route Tables:** A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.
- **Internet Gateways:** To enable access to or from the internet for instances in a subnet in a VPC.
- **NAT Gateways:** To enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- **Endpoints:** A VPC endpoint enables private connections between your VPC and supported AWS services.

EC2 Break-Down

- **Instances:** Virtual machines using RHCOS.
- **Volumes:** Root volume attached to the instances.
- **Security Groups:** A virtual firewall for your EC2 instances to control incoming and outgoing traffic.
- **Load Balancers:** Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances.
- **Target Groups:** Each target group is used to route requests to one or more registered targets. When you create each listener rule, you specify a target group and conditions.
- **AMI:** An Amazon Machine Image (AMI) provides the information required to launch an instance.

IAM Break-Down

- **Instances IAM Roles:** Separate IAM roles attached to master and worker instances to sign the API requests with AWS credentials.
- **IAM Users for Operators:** Several IAM users get created for the operators to manage the internal, registry, machines, ingress, etc.
  - aws-ebs-csi-driver-operator
  - cloud-credential-operator-iam-ro
  - openshift-image-registry
  - openshift-ingress
  - openshift-machine-api-aws

S3 Break-Down

- **S3 Bucket:** Storage for internal registry by default. Images gets stored inside the S3 bucket as image streams get created.

The VPC endpoint for S3 service gets created in the start as the images get pushed to the internal registry. Since the internal registry doesn't need to be accessed directly over the internet that's why endpoint is created so the images can be pushed and pulled to the internal registry over the private AWS network instead of public internet.

Route 53 Break-Down

- **Public Hosted Zone:** This hosted zone contains the “api.<cluster_name>.<base_domain>” and “*.apps.<cluster_name>.<base_domain>” DNS records resolving to NLB (internet-facing) and CLB respectively so the routes and API can be accessed over the public internet.
- **Private Hosted Zone:** It contains the public API and wild-card DNS records as well as the “api-int.<cluster_name>.<base_domain>” DNS record for internal API resolving to NLB (internal). Also, the private hosted zone gets associated with the VPC.

AWS specific features in OpenShift

- **Cloud Credential Operator [+]**

  The Cloud Credential Operator (CCO) manages cloud provider credentials as Kubernetes custom resource definitions (CRDs). The CCO syncs on credentialsRequest custom resources (CRs) to allow OpenShift Container Platform components to request cloud provider credentials with the specific permissions that are required for the cluster to run.

$ oc -n openshift-cloud-credential-operator get credentialsrequest cloud-credential-operator-iam-ro

$ oc -n openshift-cloud-credential-operator get secret cloud-credential-operator-iam-ro-creds -o yaml

Rotate the Cloud Credential Operator Credentials [+]

- **Machine Management**
  - Machine API Operator
  - Machine
  - Machine Sets [+]
  - Scaling a machine set manually [+]
  - Machine set deletion policy [+]

Rotate the Machine API Operator Credentials [+]

Custom machineset with required volumeszie and instance type [+]

- **image-registry**
  - Credentials to access the S3 bucket.

    $ oc -n openshift-image-registry get secret image-registry-private-configuration -o yaml
  - S3 bucket name and its specifications.

    $ oc get configs.imageregistry.operator.openshift.io/cluster -o yaml
  - Cloud credentials for image-registry IAM.

    $ oc -n openshift-image-registry get secret installer-cloud-credentials -o yaml

Rotate the openshift-image-registry operator credentials [+]

- **Ingress**
  - By default, the installer creates an CLB for ingress which is outdated.
  - NLB [+] for ingress is now supported.
  - The load balancer service for ingress is present inside `openshift-ingress` namespace.

    $ oc -n openshift-ingress get svc router-default

Rotate the openshift-ingress operator credentials [+]

❖ **AWS EBS CSI Driver Operator [+]**

- ➢ OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for AWS Elastic Block Store (EBS).
- ➢ To create CSI-provisioned PVs that mount to AWS EBS storage assets, OpenShift Container Platform installs the AWS EBS CSI Driver Operator and the AWS EBS CSI driver by default in the `openshift-cluster-csi-drivers` namespace.
- ➢ The AWS EBS CSI Driver Operator provides a StorageClass by default that you can use to create PVCs.

```
$ oc -n openshift-cloud-credential-operator get credentialsrequest aws-ebs-csi-driver-operator -o yaml
$ oc -n openshift-cluster-csi-drivers get secret ebs-cloud-credentials -o yaml
```

How OpenShift identifies its resources on AWS?

- The OpenShift cluster can be deployed on AWS into an existing VPC.
- Cluster only manages those resources which are created by the installer itself.
- A tag with unique key gets added to the AWS resources which are created by the OpenShift installer. Cluster identifies whether the AWS resource belongs to the cluster or not on the basis of that unique tag.

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat