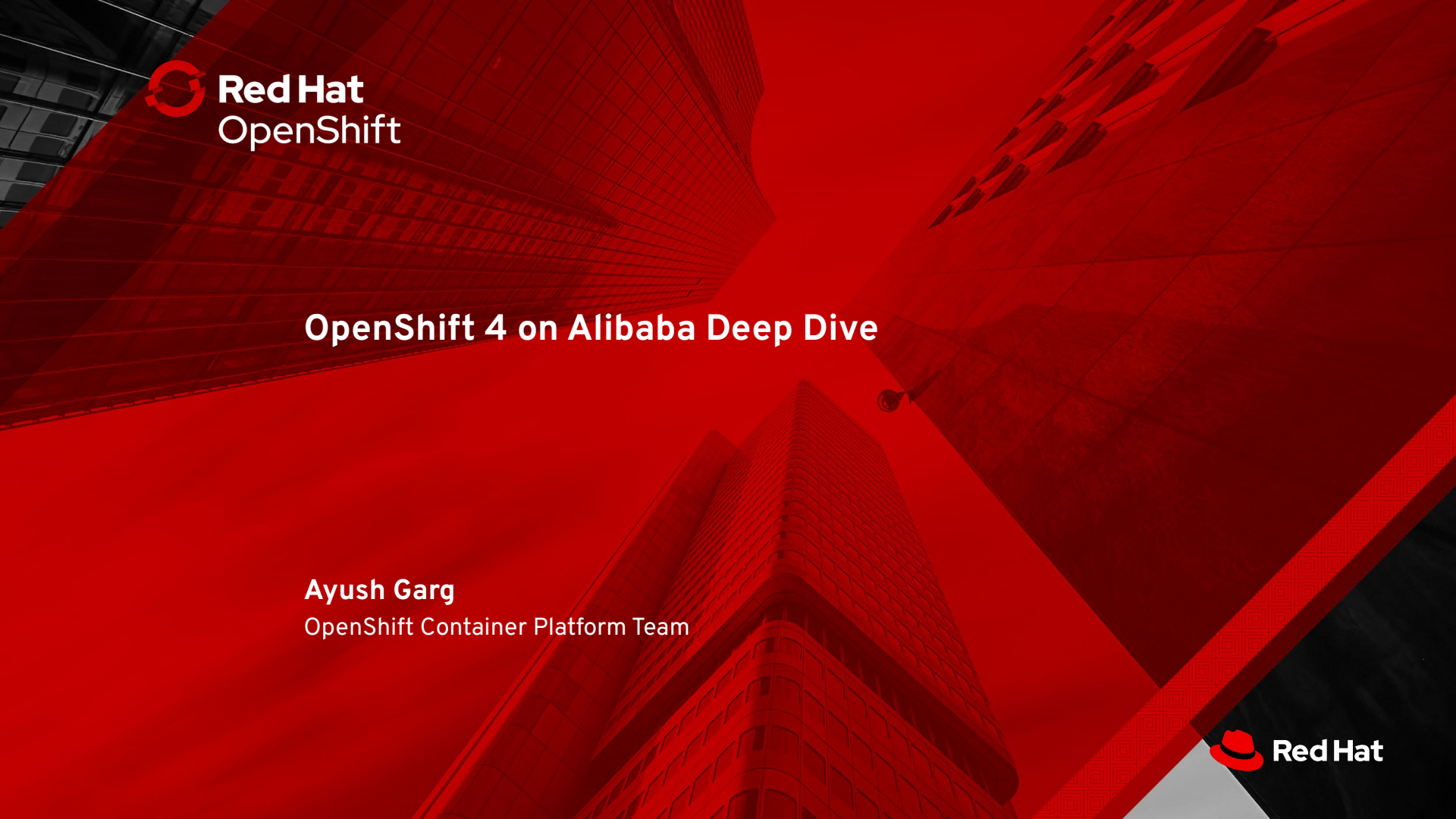


OpenShift 4 on Alibaba Deep Dive

Ayush Garg
OpenShift Container Platform Team

Red Hat

!rhatwho Ayush Garg

- ➔ Works in Red Hat as Technical Support Engineer in the OpenShift domain.
- ➔ Expertise in the installation and architecture of Red Hat OpenShift on various cloud platforms.
- ➔ Conducts sessions on different Red Hat OpenShift topics to share the knowledge with community.
- ➔ You can find me on IRC as ayush.

Agenda

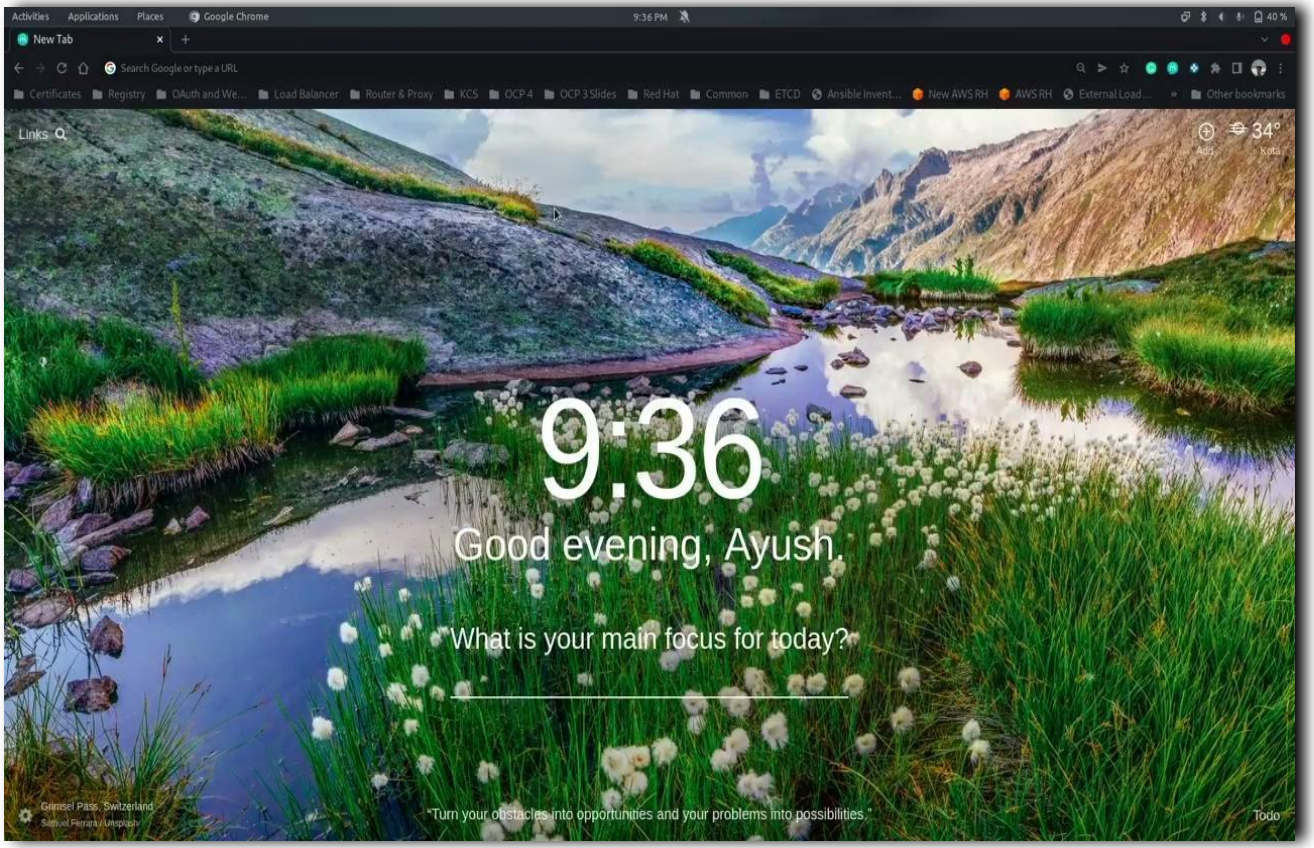
What we'll discuss today

- Prerequisite
- Prerequisite Check
- Alibaba Services
- Architecture
- install-config.yaml
- Creating manifests
- credentialsMode
- CCO Utility for RAM users
- Installation
- VPC Break-Down
- ECS Break-Down
- SLB Break-Down
- RAM Break-Down
- OSS Break-Down
- Cloud DNS Break-Down
- Alibaba specific features
- How OpenShift identifies its resources on AWS?

Prerequisite

- Alibaba account with RAM user with `AdministratorAccess` or root account [+]
- AccessKey pair for user to access the Alibaba API
- Cloud Credential Operator utility [+]
- Select a supported region [+]
- Public hosted zone in `Alibaba Cloud DNS` service [+]

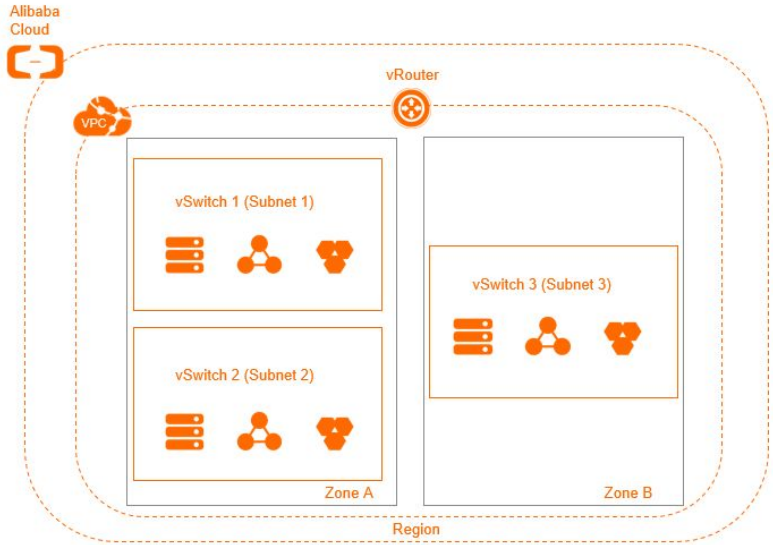
Prerequisite Check

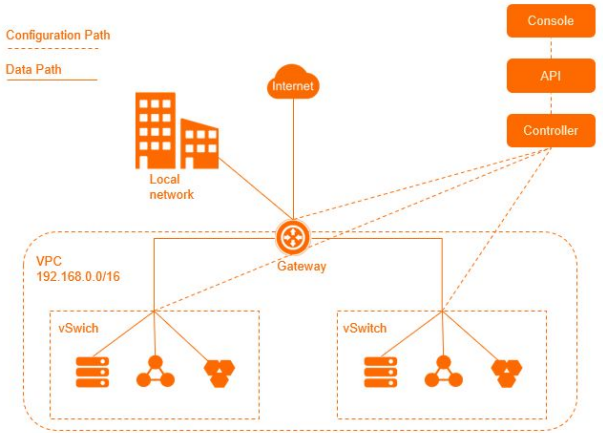


Red Hat

Alibaba Services

- **Virtual Private Cloud (VPC)**
  - Internet NAT Gateway
  - vSwitch
  - Route Tables

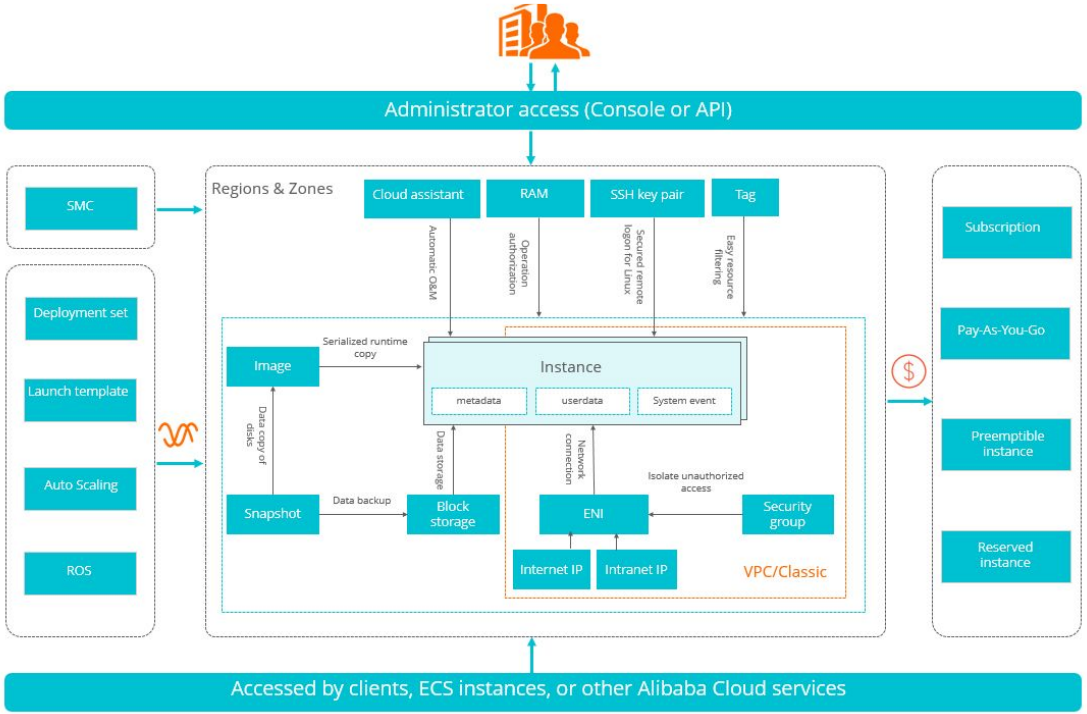




Red Hat

❖ Elastic Compute Service (ECS)

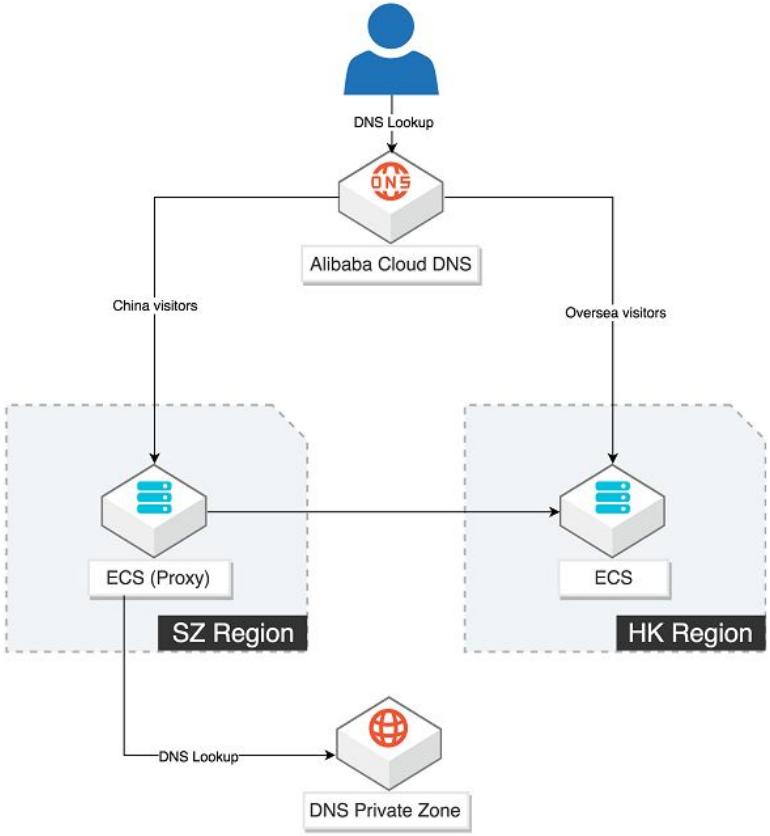
- ➢ Instances
- ➢ Images
- ➢ Disks
- ➢ Security Groups



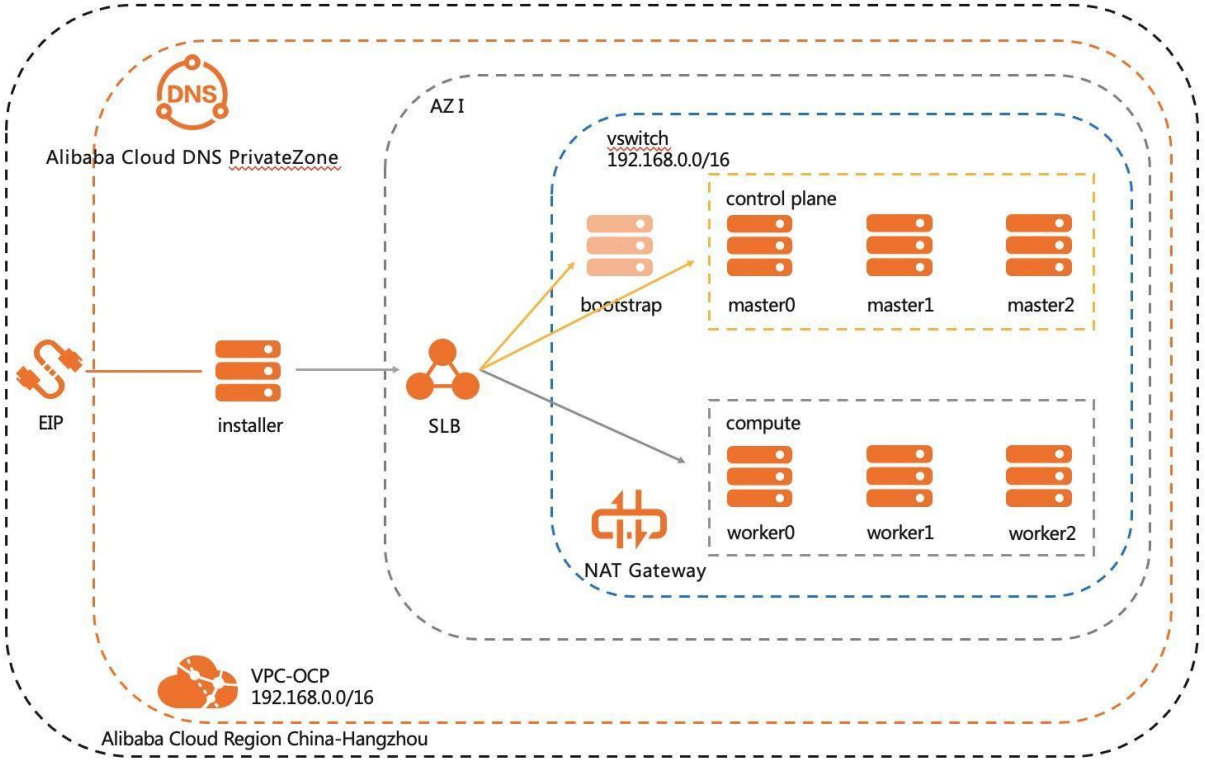
Red Hat

- **Server Load Balancer (SLB)**
  - Instances
  - Listener
  - VServer Groups
  - Default Server Group

- **Resource Access Management (RAM)**
  - Users
  - Roles
  - AccessKeys
- **Object Storage Service (OSS)**
  - Buckets (object storage)
- **Alibaba Cloud DNS**
  - PublicZone
  - PrivateZone



Architecture



Red Hat

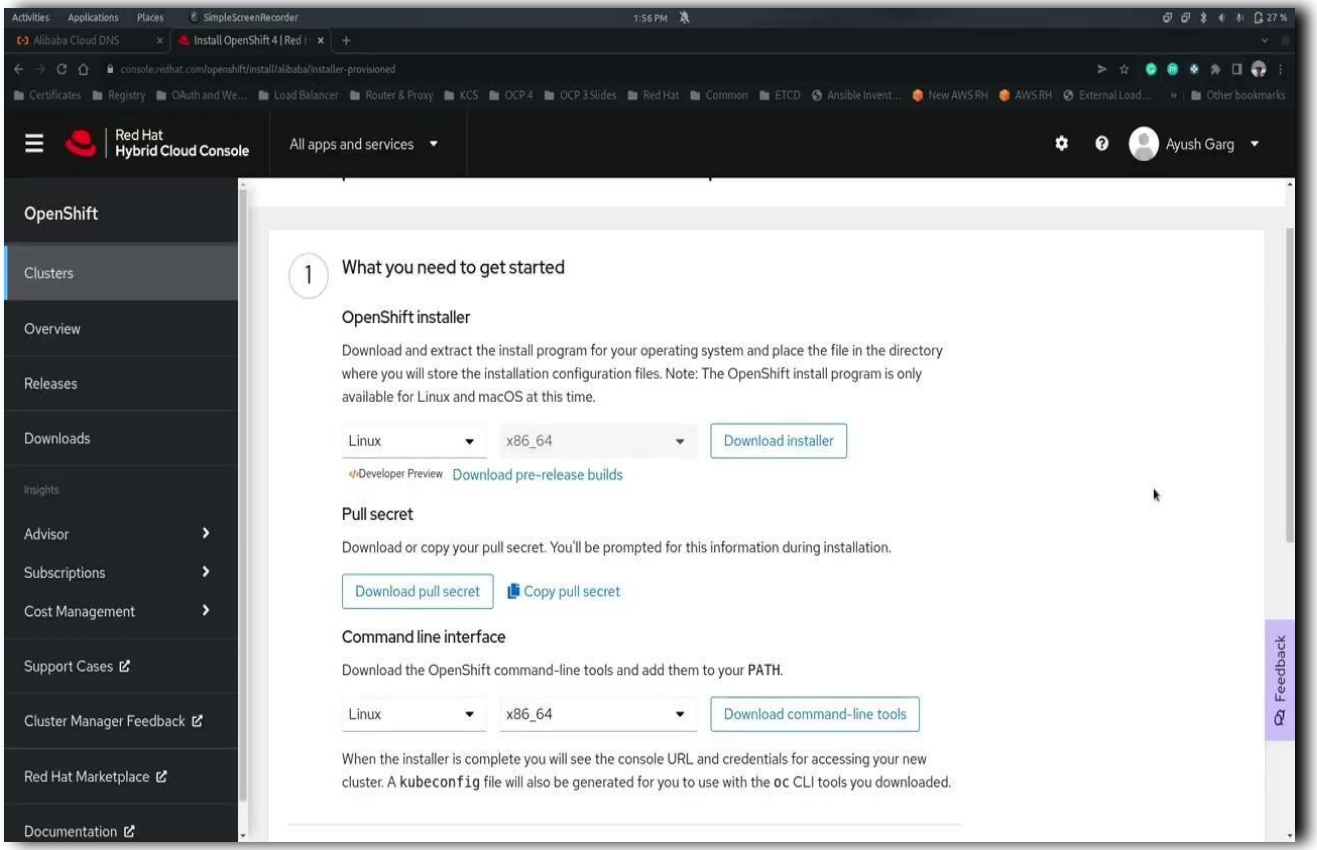
Alibaba specific options in install-config.yaml

- **baseDomain:** PublicZone
- **zones:** Availability Zone
- **machineNetwork:** VPC CIDR
- **platform:** alibabacloud and Region
- **publish:** External or Internal
- **defaultMachinePlatform**

Customization [+]

```
apiVersion: v1
baseDomain: ayushgarg.net
credentialsMode: Manual
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform: {}
---
metadata:
  creationTimestamp: null
  name: aygarg
networking:
---
  machineNetwork:
  - cidr: 10.0.0.0/16
---
platform:
  alibabacloud:
    defaultMachinePlatform:
      instanceType: ecs.g6.xlarge
      systemDiskCategory: cloud_efficiency
      systemDiskSize: 200
    region: ap-southeast-1
publish: External
```

Creating install-config.yaml and manifests



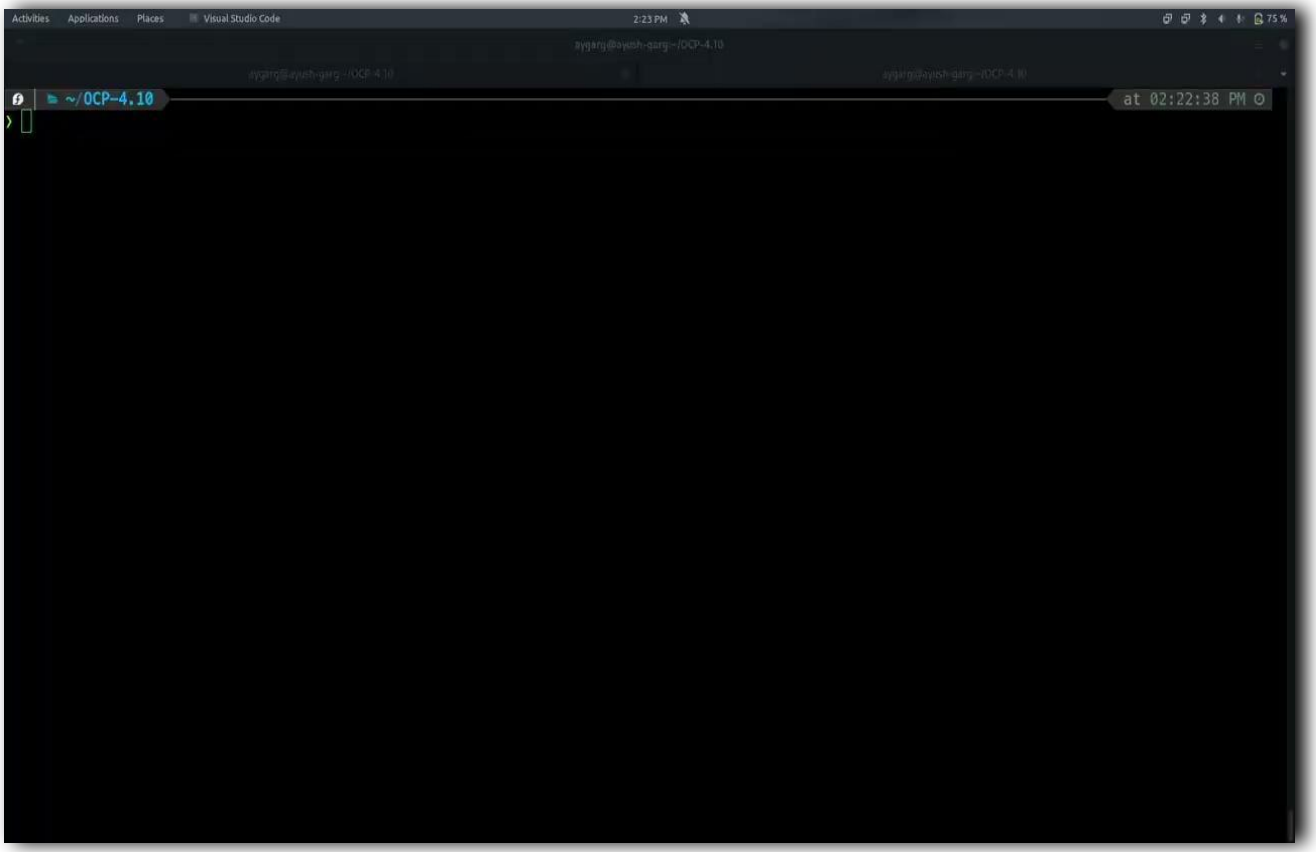
Red Hat

Why credentialsMode set to manual?

If the cloud Resource Access Management (RAM) APIs are not accessible in your environment, or if you do not want to store an administrator-level credential secret in the kube-system namespace, you can manually create and maintain Resource Access Management (RAM) credentials and create credentials with ccoctl tool.

Various operators such as ingress, machine-api requires the RAM user for creating resources such as load-balancer, nodes, etc.

Creating RAM user with CCO utility



Red Hat

Installing on Alibaba

Alibaba 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.
- **vSwitch:** 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 NAT Gateways:** To enable access to or from the internet for instances in a subnet in a VPC.

ECS Break-Down

- **Instances:** Virtual machines using RHCOS.
- **Disks:** Root volume attached to the instances.
- **Security Groups:** A virtual firewall for your ECS instances to control incoming and outgoing traffic.
- **Images:** It provides the information required to launch an instance.

SLB Break-Down

- **Instances:** The load-balancer itself.
- **Listener:** A listener checks for connection requests from clients forward requests to backend servers and performs health checks on backend servers..
- **Default Server and VServer Group:** ECS instances are used as backend servers in Server Load Balancer to receive and process distributed requests. ECS instances can be added to the default server group of a Server Load Balancer instance. You can also add multiple ECS servers to VServer groups or primary/secondary server groups after the corresponding groups are created..

RAM Break-Down

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

OSS Break-Down

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

During the installation, one additional bucket gets created which contains the ignition for bootstrap node. That bucket gets deleted post-installation.

Alibaba Cloud DNS Break-Down

- **PublicZone:** This hosted zone contains the “api.<cluster_name>.<base_domain>” and “*.apps.<cluster_name>.<base_domain>” DNS records resolving to internet-facing load-balancers so the routes and API can be accessed over the public internet.
- **PrivateZone:** 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 internal LB. Also, the private hosted zone gets associated with the VPC.

Alibaba specific features in OpenShift

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

- **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 RAM.

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

❖ Ingress

- ➢ CredentialsRequest for ingress.

  $ oc get CredentialsRequest -n openshift-cloud-credential-operator openshift-ingress

- ➢ Cloud credentials for ingress RAM.

  $ oc get secret cloud-credentials -oyaml -n openshift-ingress-operator

- ➢ The load balancer service for ingress is present inside `openshift-ingress` namespace.

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

❖ **AliCloud Disk CSI Driver Operator [+]**

- ➢ OpenShift Container Platform is capable of provisioning persistent volumes (PVs) using the Container Storage Interface (CSI) driver for Alibaba AliCloud Disk Storage.
- ➢ To create CSI-provisioned PVs that mount to AliCloud Disk storage assets, OpenShift Container Platform installs the AliCloud Disk CSI Driver Operator and the AliCloud Disk CSI driver, by default, in the openshift-cluster-csi-drivers namespace.
- ➢ The AliCloud Disk CSI Driver Operator provides a storage class (alicloud-disk) that you can use to create persistent volume claims (PVCs).

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

How OpenShift identifies its resources on Alibaba?

- Cluster only manages those resources which are created by the installer itself.
- A tag with unique key gets added to the Alibaba resources which are created by the OpenShift installer. Cluster identifies whether the Alibaba resource belongs to the cluster or not on the basis of that unique tag.

Red Hat

RAM Users Deletion

- The additional RAM users that were created using CCO utility for operators ingress, machine-api, image-registry, csi-driver need to be deleted manually. As these RAM users were created manually and not created/managed by the installer/cluster itself.
  - $ ccoctl alibabacloud delete-ram-users --name aygarg

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