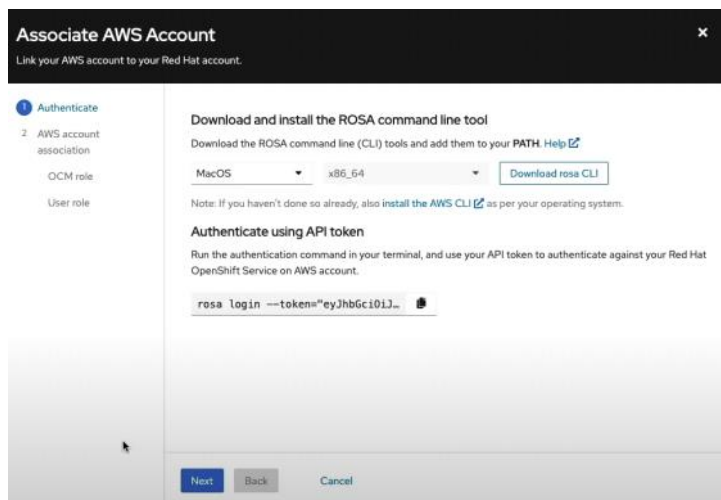
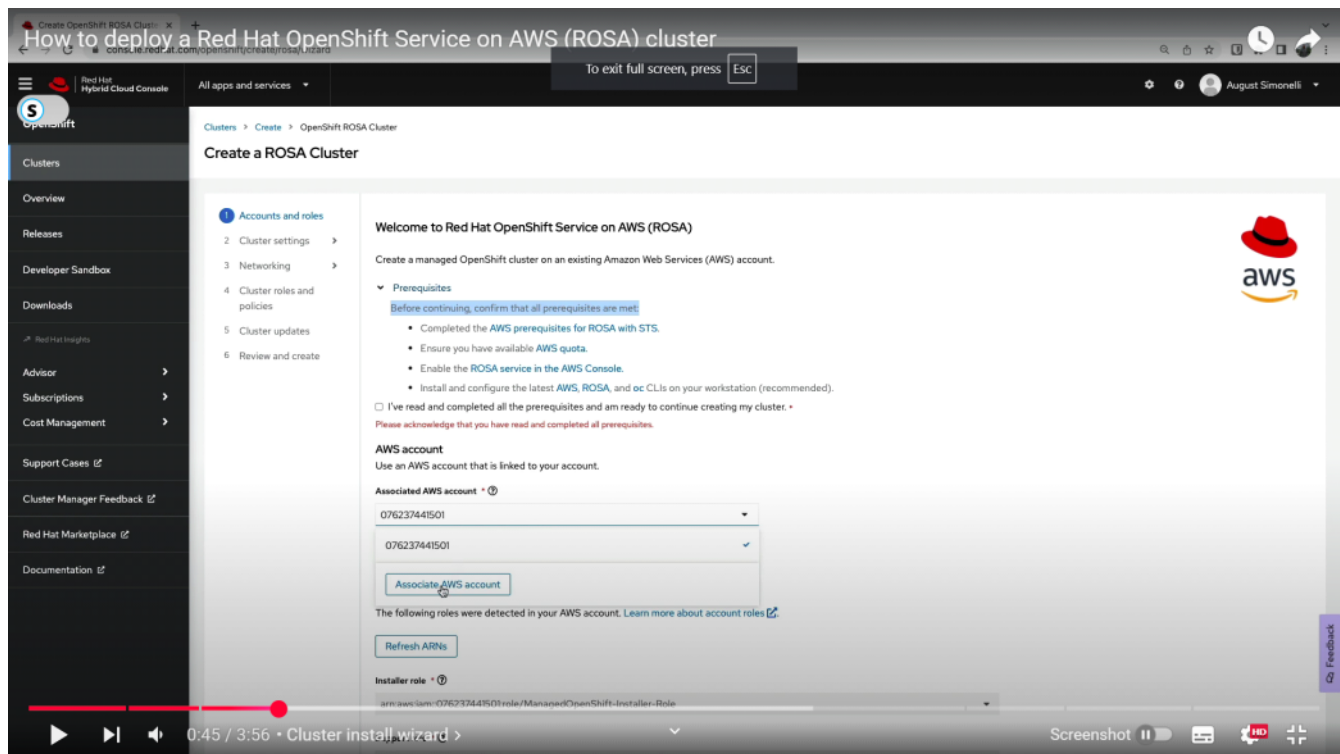
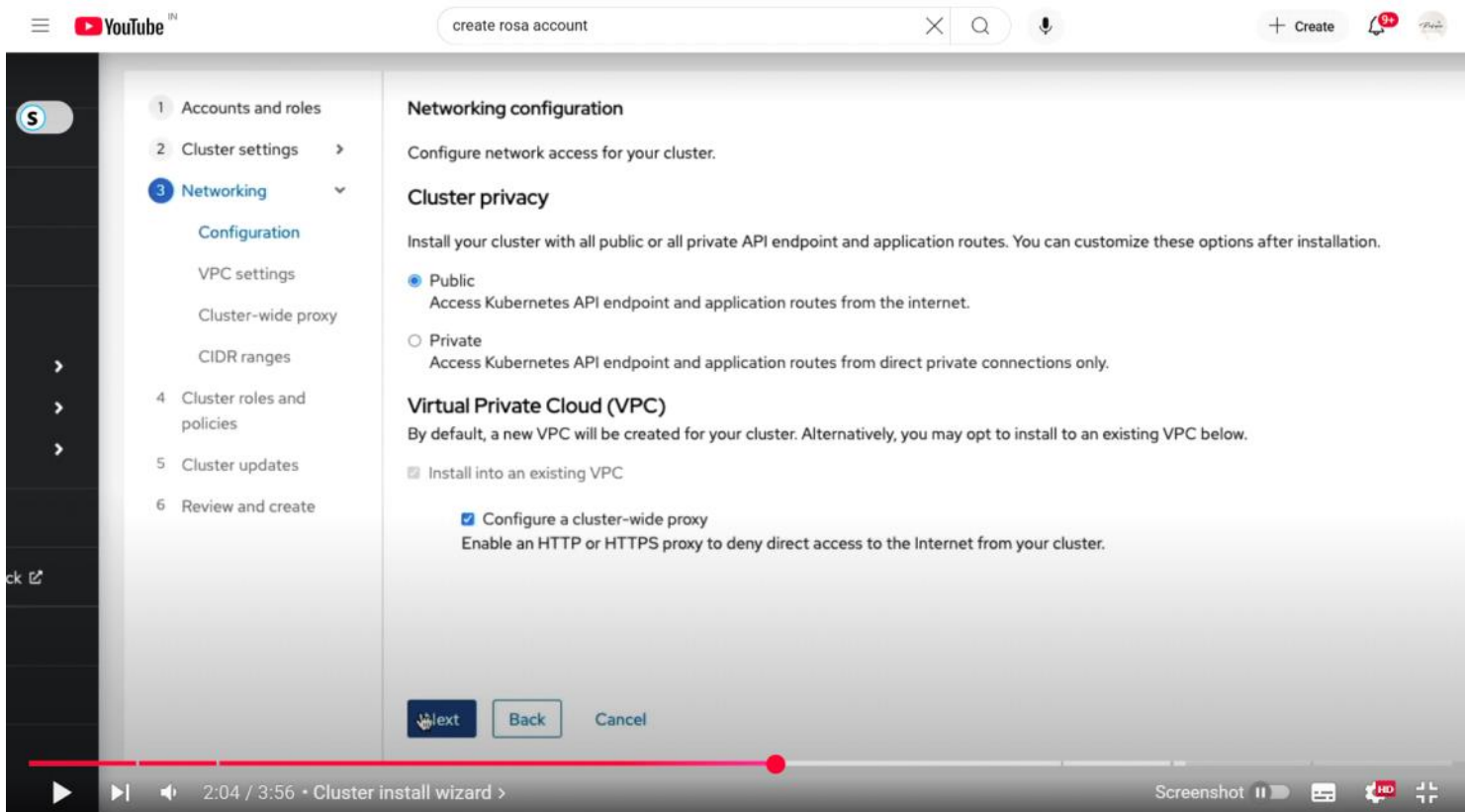
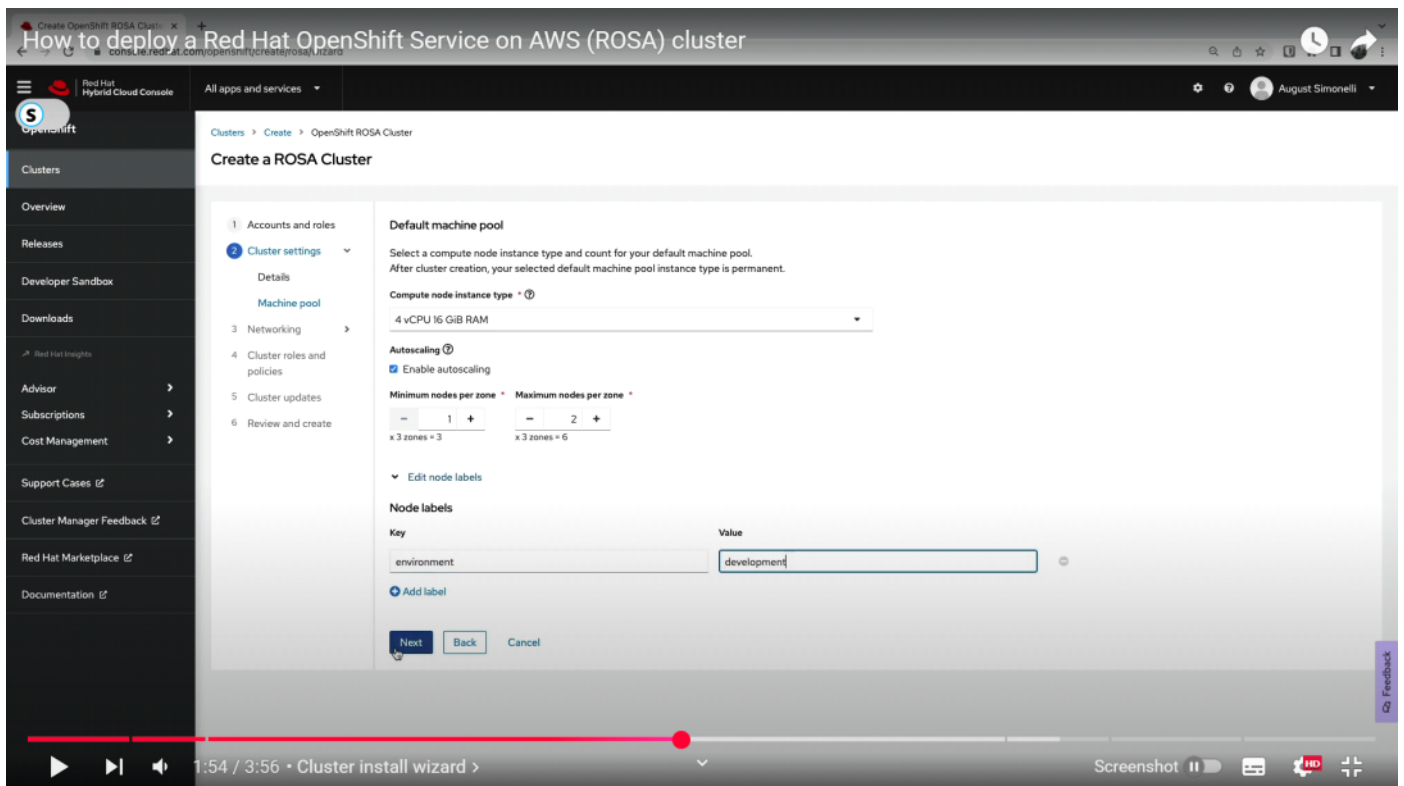


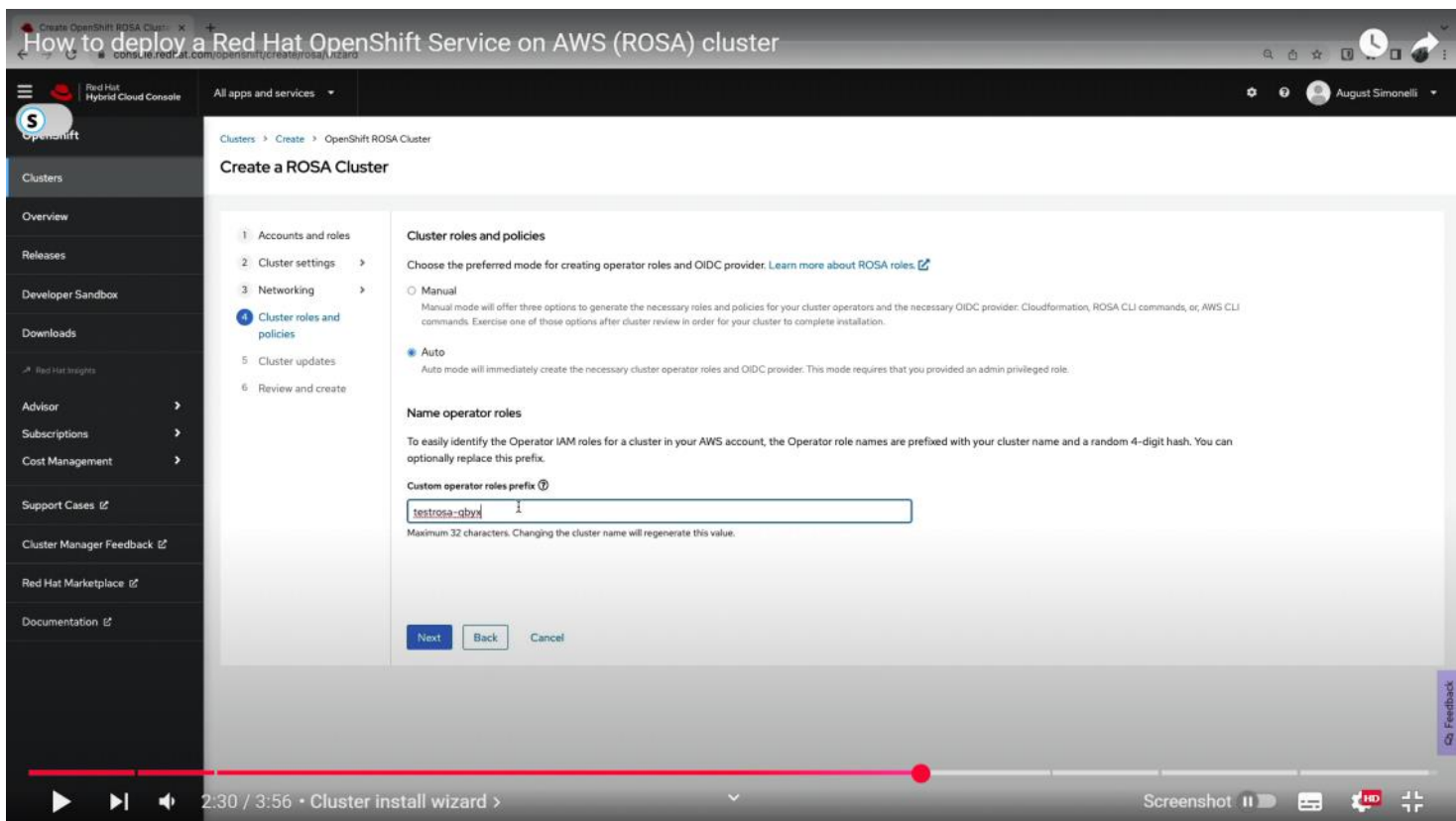
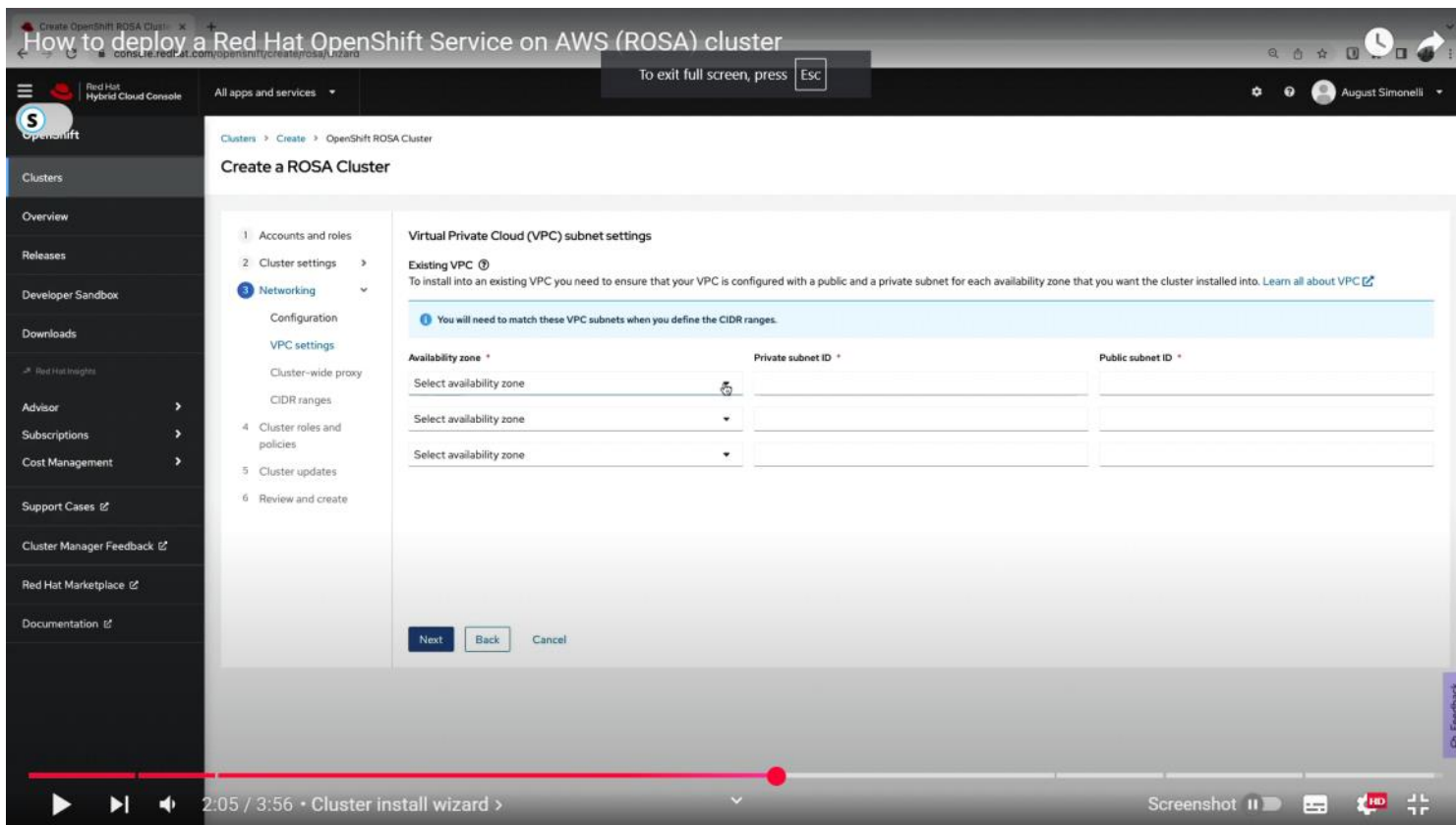
ROSA AWS Setup

Wednesday, April 16, 2025 10:04 AM



- 1) Associate with your AWS account
- 2) Need OCM role and user role to associate with cluster manager





How to deploy a Red Hat OpenShift Service on AWS (ROSA) cluster

OpenShift

Clusters

Overview

Releases

Developer Sandbox

Downloads

Red Hat Insights

Advisor

Subscriptions

Cost Management

Support Cases

Cluster Manager Feedback

Red Hat Marketplace

Documentation

Red Hat Hybrid Cloud Console

All apps and services

Clusters > Create > OpenShift ROSA Cluster

Create a ROSA Cluster

1 Accounts and roles

2 Cluster settings

3 Networking

4 Cluster roles and policies

5 Cluster updates

6 Review and create

Cluster update strategy

Note: In the event of [Critical security concerns](#) (CVEs) that significantly impact the security or stability of the cluster, updates may be automatically scheduled by Red Hat SRE to the latest z-stream version not impacted by the CVE within 48 hours after customer notifications.

☒ Individual updates
Schedule each update individually. Take into consideration end of life dates from the [lifecycle policy](#) when planning updates.

☐ Recurring updates
The cluster will be automatically updated based on your preferred day and start time when new patch updates (z-stream) are available. When a new minor version is available, you'll be notified and must manually allow the cluster to update to the next minor version.

Node draining

You may set a grace period for how long Pod Disruption Budget-protected workloads will be respected during updates. After this grace period, any workloads protected by Pod Disruption Budgets that have not been successfully drained from a node will be forcibly evicted.

Grace period

1 hour

Next

Back

Cancel

2:42 / 3:56 • Cluster install wizard >

Screenshot

How to deploy a Red Hat OpenShift Service on AWS (ROSA) cluster

OpenShift

Clusters

Overview

Releases

Developer Sandbox

Downloads

Red Hat Insights

Advisor

Subscriptions

Cost Management

Support Cases

Cluster Manager Feedback

Red Hat Marketplace

Documentation

Red Hat Hybrid Cloud Console

All apps and services

Clusters > Create > OpenShift ROSA Cluster

Create a ROSA Cluster

Encrypt volumes with customer keys

Disabled

▼ Default machine pool

Node instance type

m5.xlarge

Autoscaling

Enabled

Compute node range

Minimum nodes per zone: 1

Maximum nodes per zone: 2

Node labels

environment = development

▼ Networking

Cluster privacy

Public

Install into Existing VPC

Disabled

Machine CIDR

10.0.0.0/16 (default)

Service CIDR

172.30.0.0/16 (default)

Pod CIDR

10.128.0.0/16 (default)

Host prefix

/23 (default)

▼ Cluster roles and policies

Operator roles and OIDC provider mode

auto

Operator roles prefix

testrosa-qbyx

▼ Updates

Update Strategy

Recurring updates

Recurring update schedule

Every Sunday at 02:00 UTC

Node draining

120 minutes

Create Cluster

Back

Cancel

2:51 / 3:56 • Cluster install wizard >

Screenshot

Missing identity providers

Identity providers determine how users log into the cluster. [Add OAuth configuration](#) to allow others to log in.

Overview **Access control** Add-ons Networking Machine pools Support Settings

OCM Roles and Access

Identity providers

Configure identity providers to allow users to log into the cluster. [Learn more](#).

Cluster Roles and Access

Add identity provider

Identity providers

Overview **Access control** Add-ons Networking Machine pools Support Settings

OCM Roles and Access

Cluster administrative users

Grant permission to manage this cluster

Cluster Roles and Access

Add user

Identity providers

Add cluster user

User ID *

laugust

Group

☒ dedicated-admins

Grants standard administrative privileges for OpenShift Dedicated. Users can perform administrative actions listed in the [documentation](#).

☐ cluster-admins

Gives users full administrative access to the cluster. This is the highest level of privilege available to users. It should be granted with extreme care, because it is possible with this level of access to get the cluster into an unsupportable state.

Add user

Cancel