IBM® Storage

Red Hat OpenShift on Public Cloud with IBM Block Storage

Contents

Introduction

The purpose of this document is to show how to install RedHat™ OpenShift Container Platform (OCP) on Amazon™ web services (AWS) public cloud with OpenShift installer, a method that is known as Installer-provisioned infrastructure (IPI). We also describe how to validate the installation of IBM container storage interface (CSI) driver on OCP 4.2 that is installed on AWS. This document also describes the installation of OCP 4.x on AWS with customization and OCP 4.x installation on IBM Cloud.

This document discusses how to provision internet small computer system interface (iSCSI) storage that is made available by IBM Spectrum Virtualize for Public Cloud (SVPC) that is deployed on AWS. Finally, the document discusses the use of Red Hat OpenShift command line interface (CLI), OCP web console graphical user interface (GUI), and AWS console.

OpenShift overview

Red Hat OCP provides developers and IT organizations with a hybrid cloud application platform for deploying new and existing applications on secure, scalable resources with minimal configuration and management overhead. OCP supports various programming languages and frameworks, such as Java, JavaScript, Python, Ruby, and PHP.

Built on Red Hat Enterprise Linux and Kubernetes, OpenShift Container Platform provides a more secure and scalable multi-tenant operating system for today's enterprise-class applications, while delivering integrated application run times and libraries. OpenShift Container Platform enables organizations to meet security, privacy, compliance, and governance requirements.

OCP release 4.2 can be installed on AWS, Azure, GCP, Bare Metal, IBM Z, OpenStack, and vSphere platforms.

CSI plug-in and SVPC overview

IBM released its open source CSI driver that allows dynamic provisioning of storage volumes for containers on Kubernetes and OCP that use IBM storage systems.

IBM Spectrum Storage family, SVPC and AWS, support clients in their IT architectural transformation and migration towards the cloud service model. This support enables hybrid cloud strategies or for a cloud-native workload, provides the benefits of familiar and sophisticated storage functions on public cloud data centers, which enhances the existing cloud offering.

For more information about SVPC on Public cloud, see *IBM Spectrum Virtualize for Public Cloud on AWS Implementation Guide*, REDP-5534.

Scope

In this document, we show how to install Red Hat OCP 4.2 on AWS by using the IPI method. For a post-OpenShift installation, we install the IBM CSI driver plug-in and provision storage by using SVPC.

Before this installation is started, ensure that the following requirements are met:

- You have the valid AWS account and rights to log in to AWS console and install or create the infrastructure on AWS.
- With cost estimator available on AWS console, estimate the required cost for the servers and services you use on AWS and get the cost approval per your organization and department policies.
- Valid Red Hat account login so that you can download the required packages, binaries, and pull secrets.
- IBM SPVC is available.
- User account and valid keys in `.ppk` format (for PuTTY login) or `.pem` format (for SSH login) to log in to the Linux node that is created on AWS (AMI image).
- Platform-specific connectivity tools, such as SSH, PuTTY, and WinSCP.

This document does *not* describe installing SVPC on AWS. For more information, see *IBM Spectrum Virtualize for Public Cloud on AWS Implementation Guide*, REDP-5534.

The document also does not cover installing OCP on AWS with any customizations, such as network, restricted network, or Cloud Formation templates.

Steps overview

This demonstration includes the following major steps:

1. Create or get the login credentials for AWS console.
2. Complete all of the installation prerequisites for OCP on AWS.
3. Install SVPC on AWS as described in *IBM Spectrum Virtualize for Public Cloud on AWS Implementation Guide*, REDP-5534.
4. Install the IBM CSI driver plug-in on OCP installed on AWS.
5. Configure storage and SPVC storage volume logical unit number (LUN) on the CoreOS worker nodes.

It is strongly recommended that the user has some basic knowledge of container concepts (for example, Docker and Kubernetes) to run this demonstration.

Infrastructure overview

This section discusses the infrastructure that is used for the demonstration (see Figure 1).

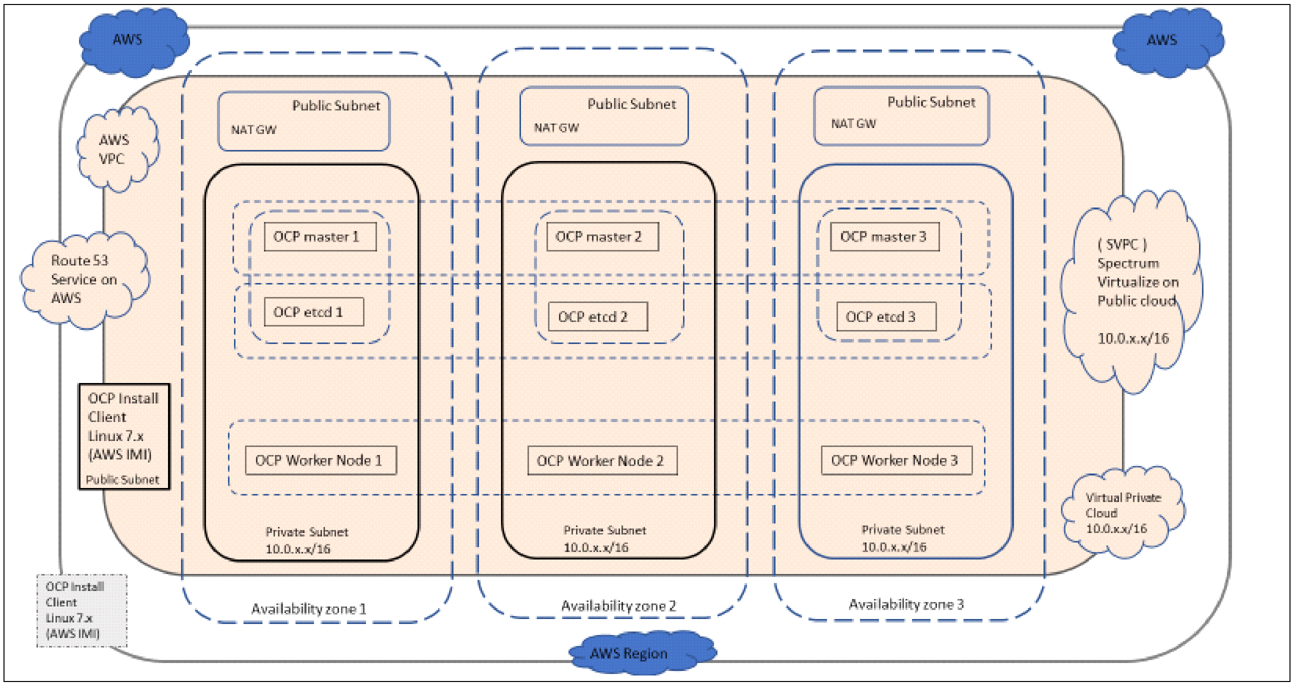


Figure 1 OpenShift Container Platform and SVPC on AWS

The demonstration is composed of eight virtual machines that are hosted on AWS. Table 1 lists the system and operating system requirements.

Table 1 Infrastructure overview

Node role	Type	Operating system	Quantity
Master	m4.xlarge	CoreOS	3
Worker	m4.xlarge	CoreOS	3
Installer node	t2.large	RHEL 7	2
SVCP nodes	2 x c5.9xlarge and 1 x c5.large	N/A	2

Configuring Route 53 Service (created on AWS, public hosted zone)

In this section, we describe configuring Route 53 Service, which was created on AWS with a public hosted zone.

IP addressing and credentials

During the IPI of OCP, all of the required IP addresses, nodes (master and worker), network address translation (NAT) gateway, dynamic host configuration protocol (DHCP), load balancer, and security are automatically provisioned by AWS.

Table 2 lists the components that are created and the required credentials to access them.

Table 2 Infrastructure and credentials overview

Node/Role	Public/Private IP address	User	Password
AWS console	aws.amazon.com/	< your user>	<your password>
OCP Install node rhel 7.x/EC2 instance	• Private IP address by AWS • Public IP provided by AWS	ec2-user <your name>	Key file
Master Nodes	• Private IP address by AWS • Public hostname by AWS	core	ssh key
Worker Nodes			
OpenShift GUI	https://console-openshift-console.apps.ocp42cluster25.ocp42svpc.com	kubeadmin	Password prompted after installation is completed
SVPC	https://3.123.xx.xxx:8443/gui#config-network-iscsi	superuser	<your password>

Demonstration steps

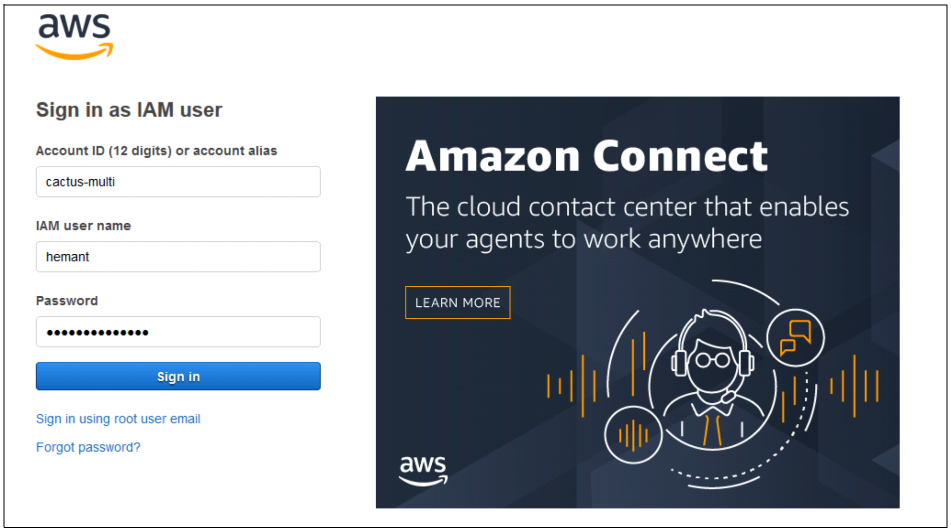
In this section, we describe the steps that are used in the demonstration.

Configuring Route53 Service

For OCP 4.2 installation on AWS, a domain name is needed for the cluster. This name can be an existing or new domain. For our demonstration, we create a domain in AWS.

Complete the following steps:

1. Log in to AWS console (see Figure 2).



Sign in as IAM user

Account ID (12 digits) or account alias: cactus-multi

IAM user name: hemant

Password: ••••••••••••••

Amazon Connect

The cloud contact center that enables your agents to work anywhere

Figure 2 AWS login window

2. Sign on to the AWS console. Under Services, select **Route 53** from the Networking and Content Delivery list (see Figure 3).

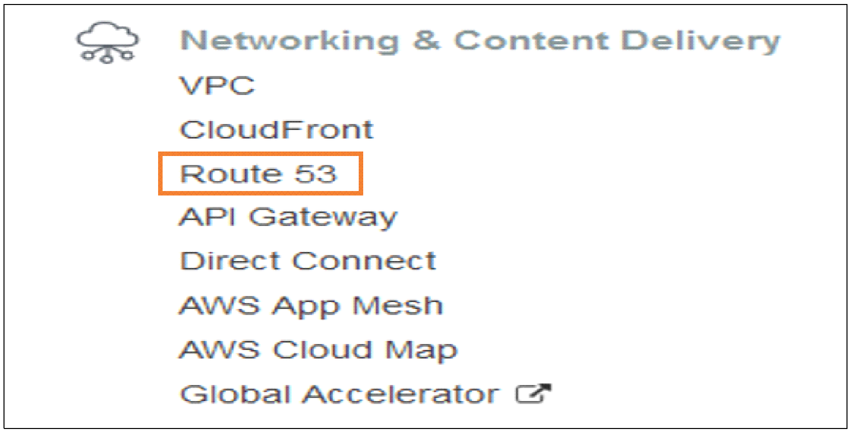
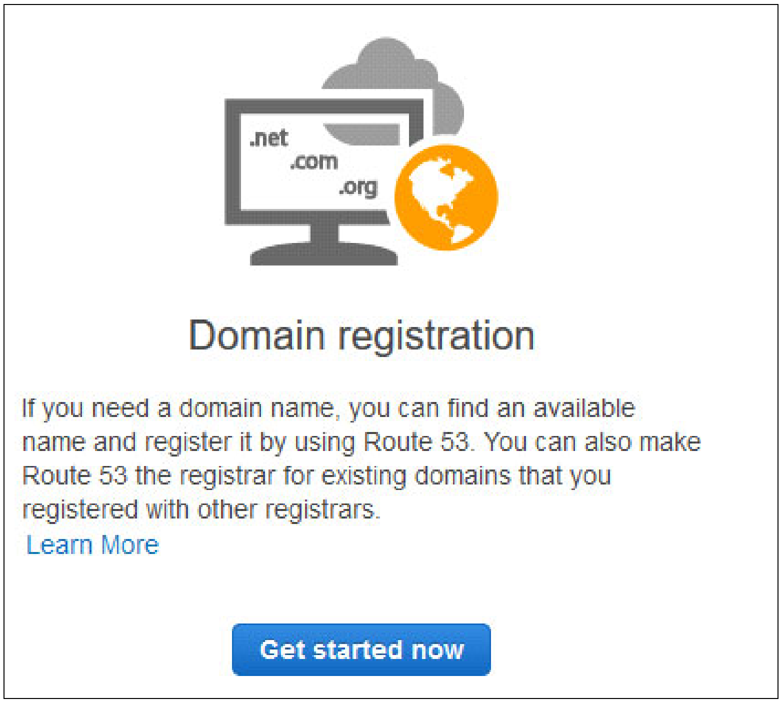


Figure 3 Selecting Route 53

3. Click **Register Domain** (see Figure 4).

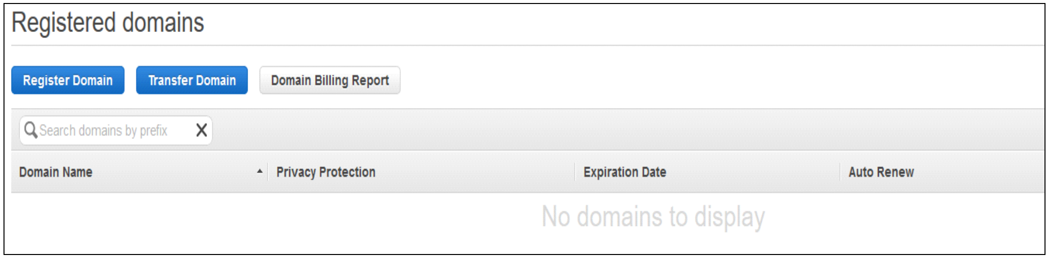


Domain registration

If you need a domain name, you can find an available name and register it by using Route 53. You can also make Route 53 the registrar for existing domains that you registered with other registrars.
Learn More

Figure 4 Domain registration window

The Registered domains window opens (see Figure 5).



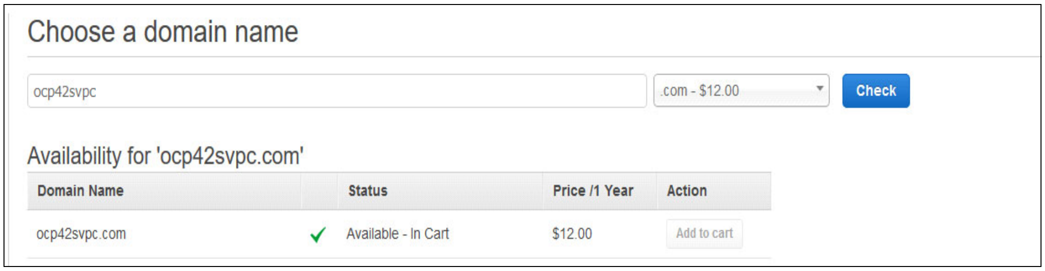
Registered domains

Domain Name	Privacy Protection	Expiration Date	Auto Renew

No domains to display

Figure 5 Registered domains window

4. Enter the domain name and click **Check** (see Figure 6).



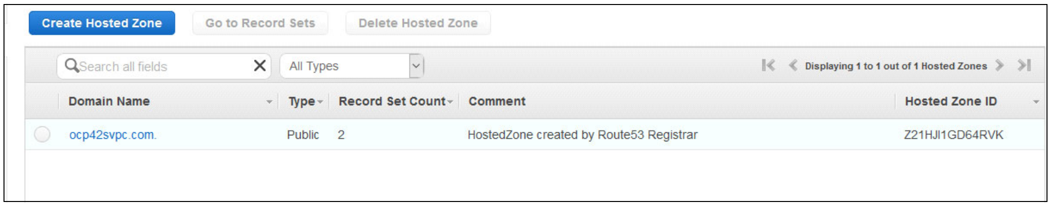
Availability for 'ocp42svpc.com'

Domain Name	Status	Price /1 Year	Action
ocp42svpc.com	✓ Available - In Cart	$12.00	Add to cart

Figure 6 Choose a domain name window

If the wanted domain name is available, click **Add to cart**.

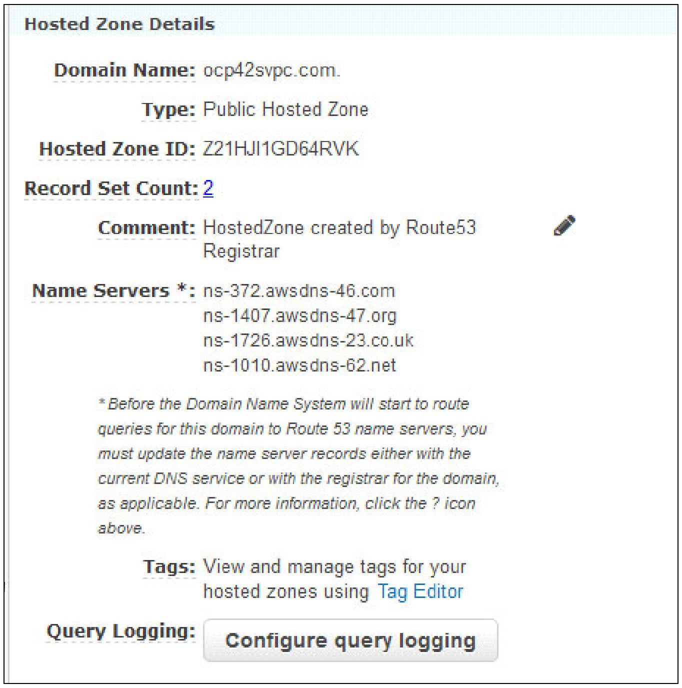
5. Click **Continue** and verify your contact information:
   - Do you want to automatically renew your domain? Select **disable**.
   - Accept the registration agreement and other details.
   - Follow the instruction as prompted.
6. Verify your email address to register the domain with Route 53 service.
7. Check your email and click the link to verify your email for domain registration. A few emails from the Amazon registrar also are sent. Click the links to verify.
8. After the email verification process is completed, go to domains and confirm that your domain is created (see Figure 7).



Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
ocp42svpc.com.	Public	2	HostedZone created by Route53 Registrar	Z21HJI1GD64RVK

Figure 7 Create Hosted Zone window

The details of the hosted zone are shown (see Figure 8 on page 7).



Hosted Zone Details

Domain Name: ocp42svpc.com.

Type: Public Hosted Zone

Hosted Zone ID: Z21HJI1GD64RVK

Record Set Count: 2

Comment: HostedZone created by Route53 Registrar

Name Servers *: ns-372.awsdns-46.com
ns-1407.awsdns-47.org
ns-1726.awsdns-23.co.uk
ns-1010.awsdns-62.net

*Before the Domain Name System will start to route queries for this domain to Route 53 name servers, you must update the name server records either with the current DNS service or with the registrar for the domain, as applicable. For more information, click the ? icon above.

Tags: View and manage tags for your hosted zones using Tag Editor

Query Logging: Configure query logging

Figure 8 Hosted Zone Details window

Creating an AWS user from IAM

In this example, you use your AWS admin user to create the domain. For security reasons, create a user that is used to create a cluster on AWS.

Complete the following steps:

1. In AWS console under Services, select **IAM** from the Security, Identity, and Compliance list (see Figure 9).

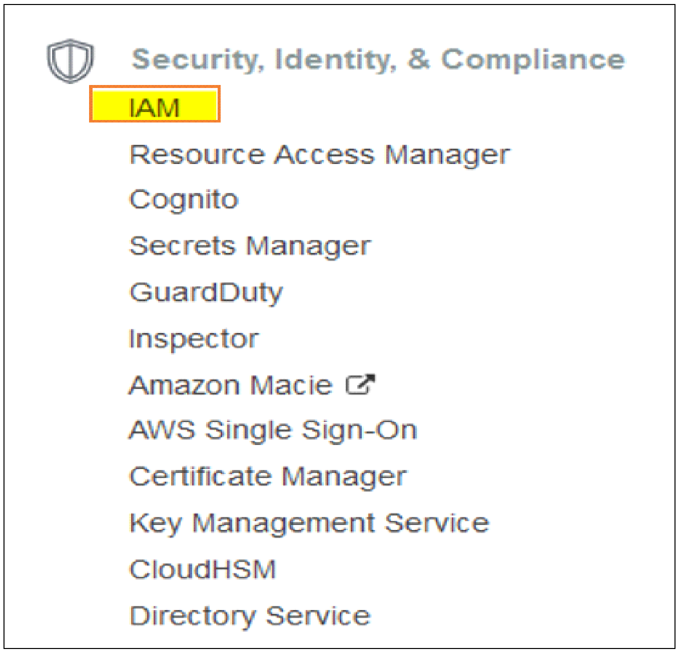
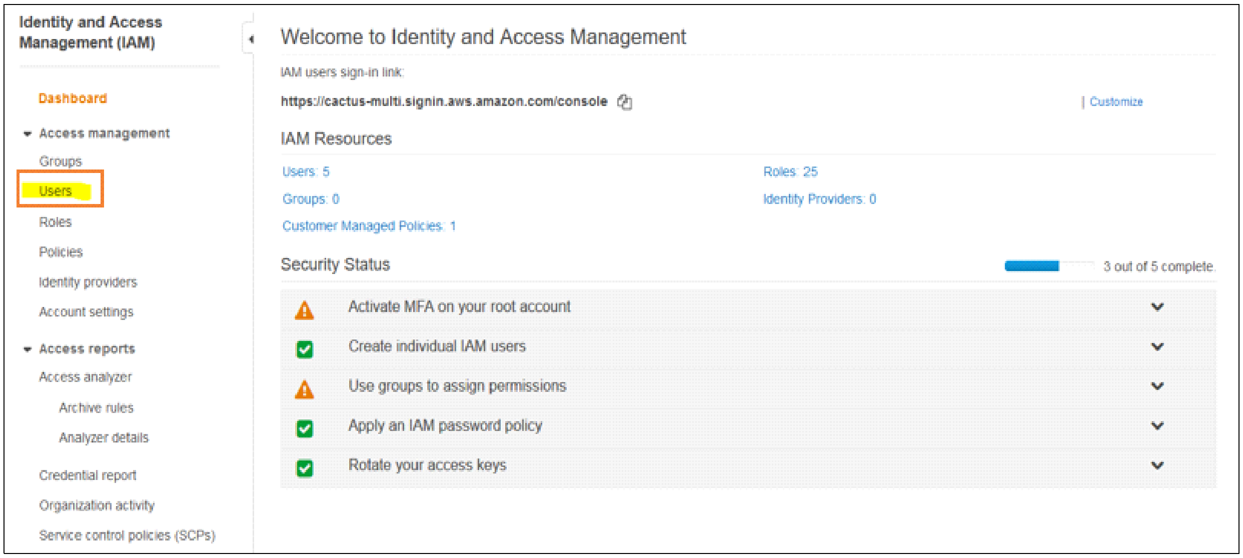


Figure 9 Selecting IAM

2. Click the **Users** option on the left side on the window (see Figure 10).



Welcome to Identity and Access Management

IAM users sign-in link:

https://cactus-multi.signin.aws.amazon.com/console

IAM Resources

Users: 5	Roles: 25
Groups: 0	Identity Providers: 0
Customer Managed Policies: 1	

Security Status — 3 out of 5 complete.

- ⚠ Activate MFA on your root account
- ☑ Create individual IAM users
- ⚠ Use groups to assign permissions
- ☑ Apply an IAM password policy
- ☑ Rotate your access keys

Figure 10 Selecting Users option

3. Click **Add Users** (see Figure 11).

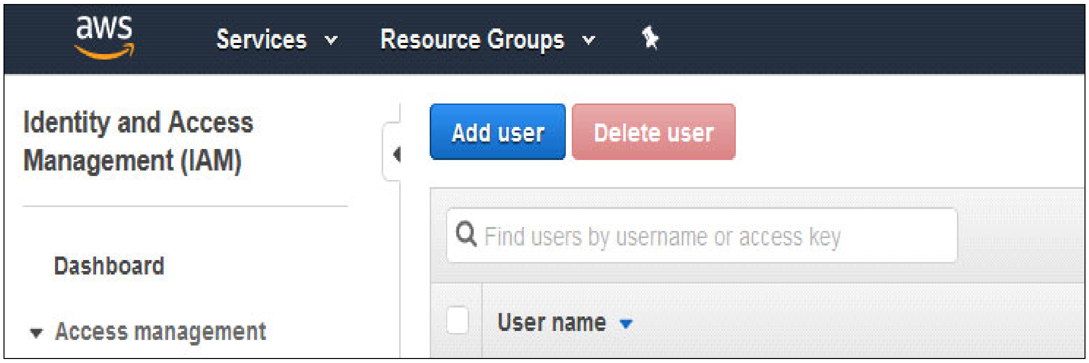
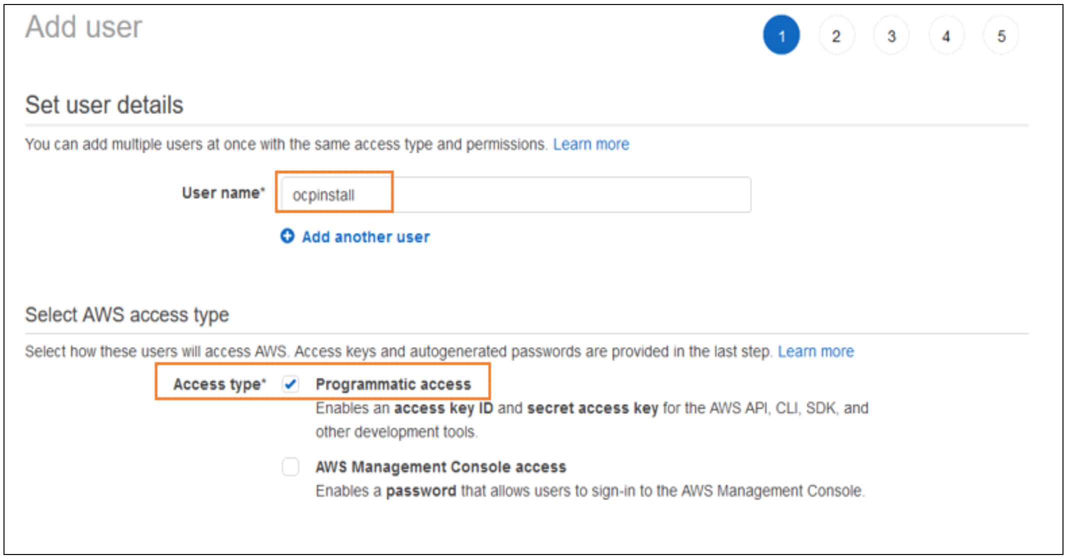


Figure 11 Add user option

4. Enter the wanted username.

5. Select **Access type Programmatic access** (see Figure 12).



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* ocpinstall

Add another user

Select AWS access type

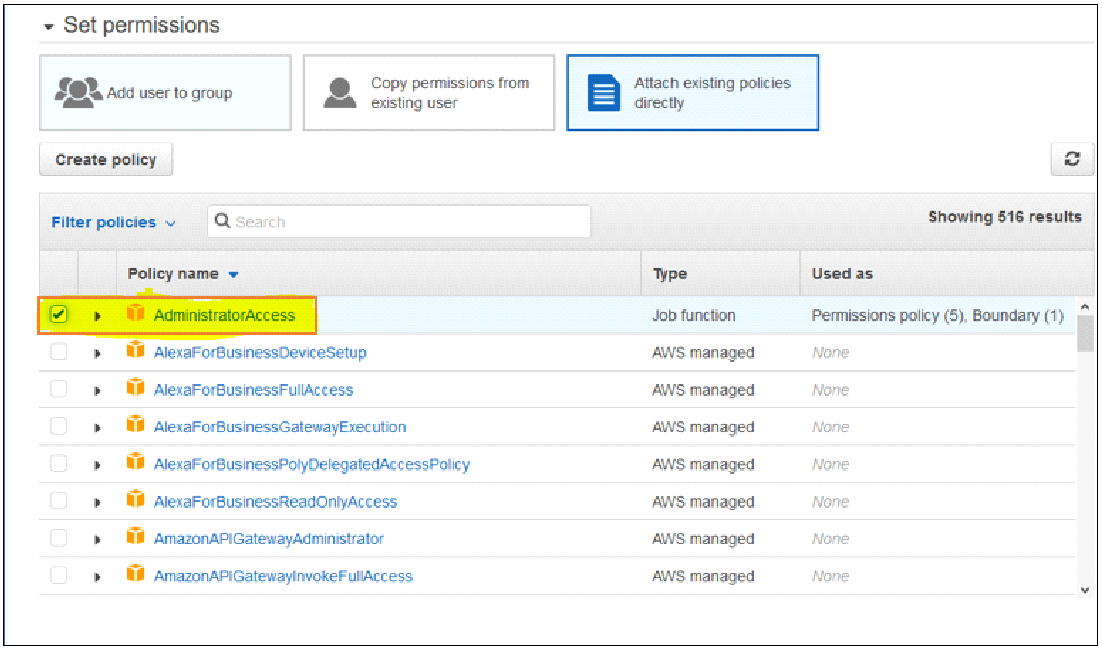
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Figure 12 Selecting Access type

6. Select **Attach existing policies directly**.
7. Select **AdministratorAccess** (see Figure 13).



Set permissions

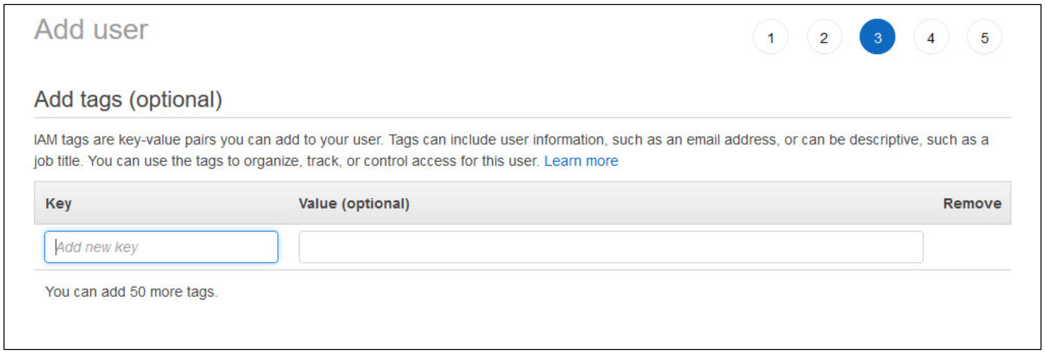
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search

Showing 516 results

	Policy name	Type	Used as
☑	AdministratorAccess	Job function	Permissions policy (5), Boundary (1)
□	AlexaForBusinessDeviceSetup	AWS managed	None
□	AlexaForBusinessFullAccess	AWS managed	None
□	AlexaForBusinessGatewayExecution	AWS managed	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessReadOnlyAccess	AWS managed	None
□	AmazonAPIGatewayAdministrator	AWS managed	None
□	AmazonAPIGatewayInvokeFullAccess	AWS managed	None

Figure 13 Show set permission

8. Click **Next**. Although adding tags is optional, tags can be added in the window that is shown in Figure 14 on page 10.



Add tags (optional)

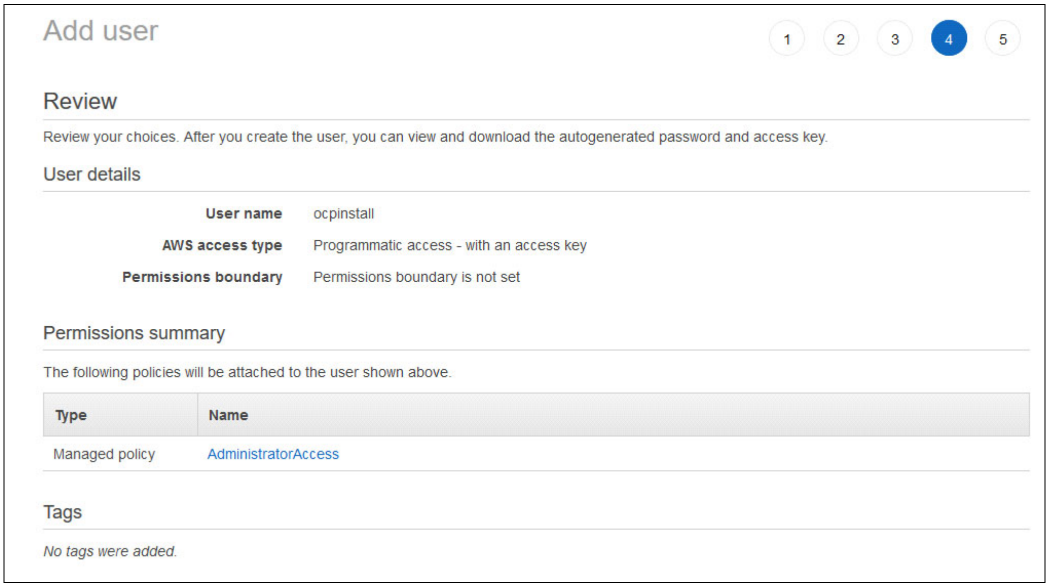
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Figure 14 Add tags (optional) window

9. Click **Next**. The Add user window opens (see Figure 15).



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name ocpinstall

AWS access type Programmatic access - with an access key

Permissions boundary Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

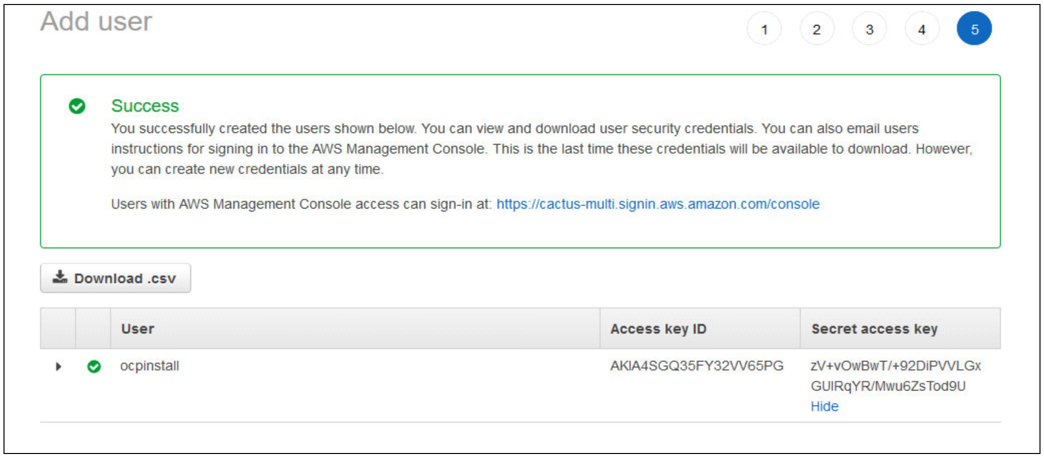
Type	Name
Managed policy	AdministratorAccess

Tags

No tags were added.

Figure 15 Review Add user window

A message that indicates that the user was successfully created is shown (see Figure 16).



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://cactus-multi.signin.aws.amazon.com/console

		User	Access key ID	Secret access key
▸	✓	ocpinstall	AKIA4SGQ35FY32VV65PG	zV+vOwBwT/+92DiPVVLGx GUIRqYR/Mwu6ZsTod9U Hide

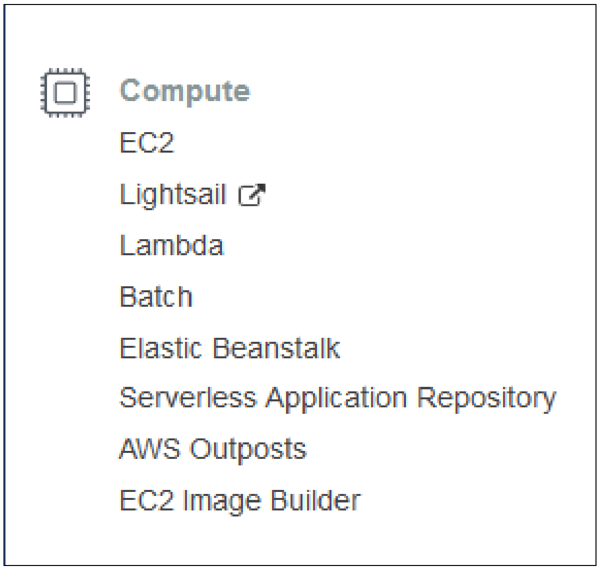
Figure 16 User created successfully message

10. Download the `.csv` file for the important information about the Access key ID and Secret access key for the user. This information is required to install OCP on AWS.

Creating RHEL 7.x node 1 with AMI image

Complete the following steps:

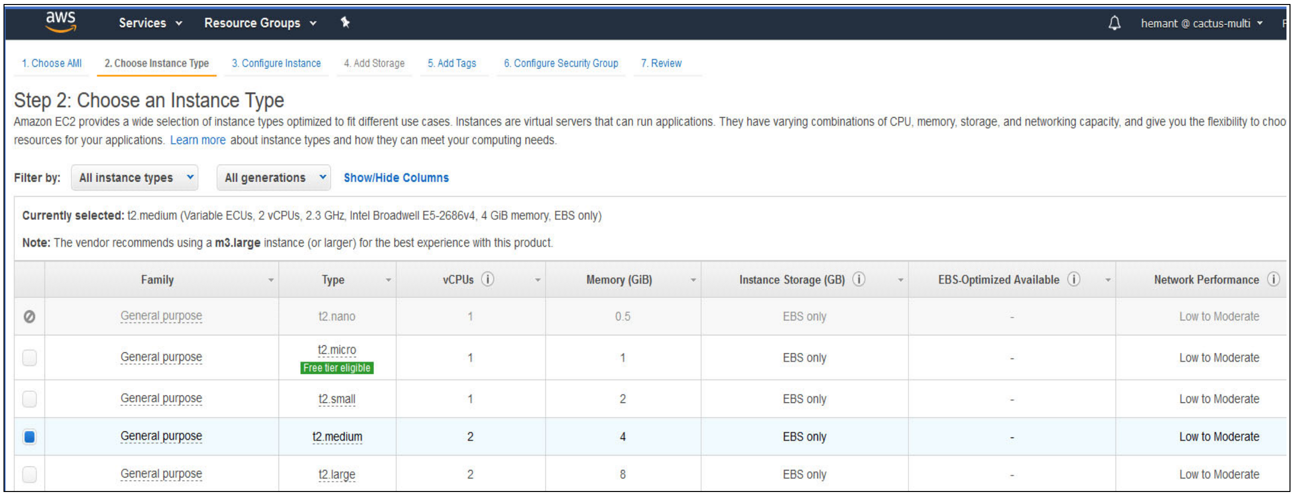
1. Log in to the AWS console by using your AWS admin user. Select **EC2** under Compute (see Figure 17).



Compute

Figure 17 Select EC2 instance

2. Select **Launch Instance**.
3. Search for “Red Hat Enterprise Linux 7 image”. Press Enter.
4. Select **AWS Market Place** and select **(RHEL) 7 (HVM)**.
5. Click **Continue**.
6. Choose the instance type (see Figure 18).



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choo resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types All generations Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

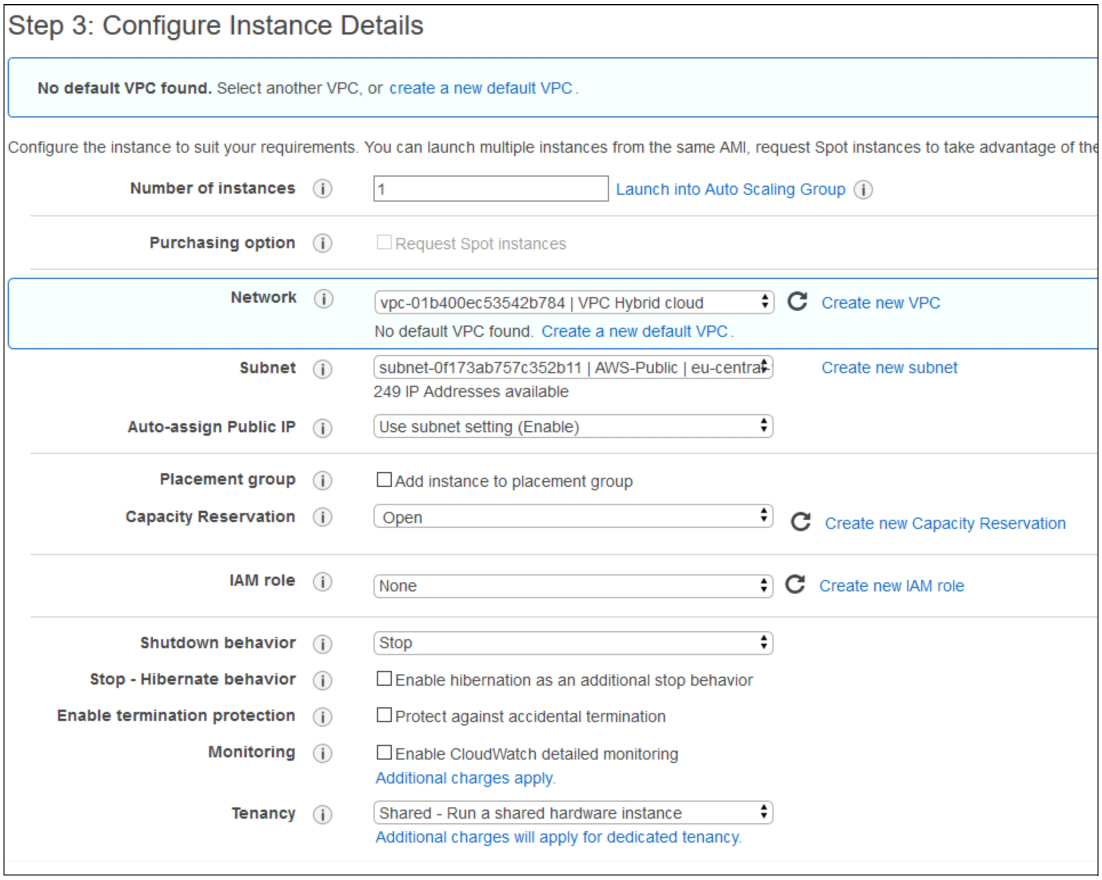
Note: The vendor recommends using a **m3.large** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
⊘	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
■	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate

Figure 18 Choose instance type

7. Configure the instance details (see Figure 19):

   - Auto assign Public IP is set to: Use subnet setting (Enable).
   - The existing VPC is used because it was available. Another VPC can be created if wanted.



Step 3: Configure Instance Details

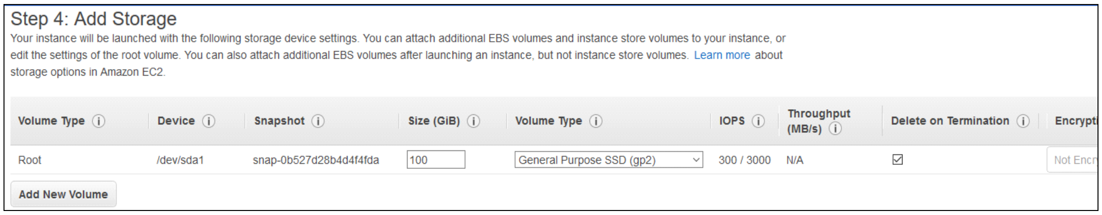
No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances	
Network	vpc-01b400ec53542b784 | VPC Hybrid cloud No default VPC found. Create a new default VPC.	Create new VPC
Subnet	subnet-0f173ab757c352b11 | AWS-Public | eu-central 249 IP Addresses available	Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	□ Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	None	Create new IAM role
Shutdown behavior	Stop	
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior	
Enable termination protection	□ Protect against accidental termination	
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	

Figure 19 Showing details to configure the instance

8. Click **Next** to add Storage (see Figure 20).



Step 4: Add Storage

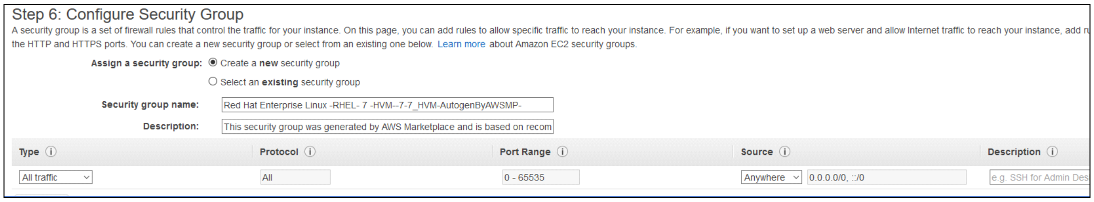
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypti
Root	/dev/sda1	snap-0b527d28b4d4f4fda	100	General Purpose SSD (gp2)	300 / 3000	N/A	☑	Not Encr

Figure 20 Add Storage window

9. (Optional) Click **Next** to add a tag.

10. Click **Next** to configure the security group (see Figure 21 on page 13).



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add ru the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Red Hat Enterprise Linux -RHEL- 7 -HVM--7-7_HVM-AutogenByAWSMP-

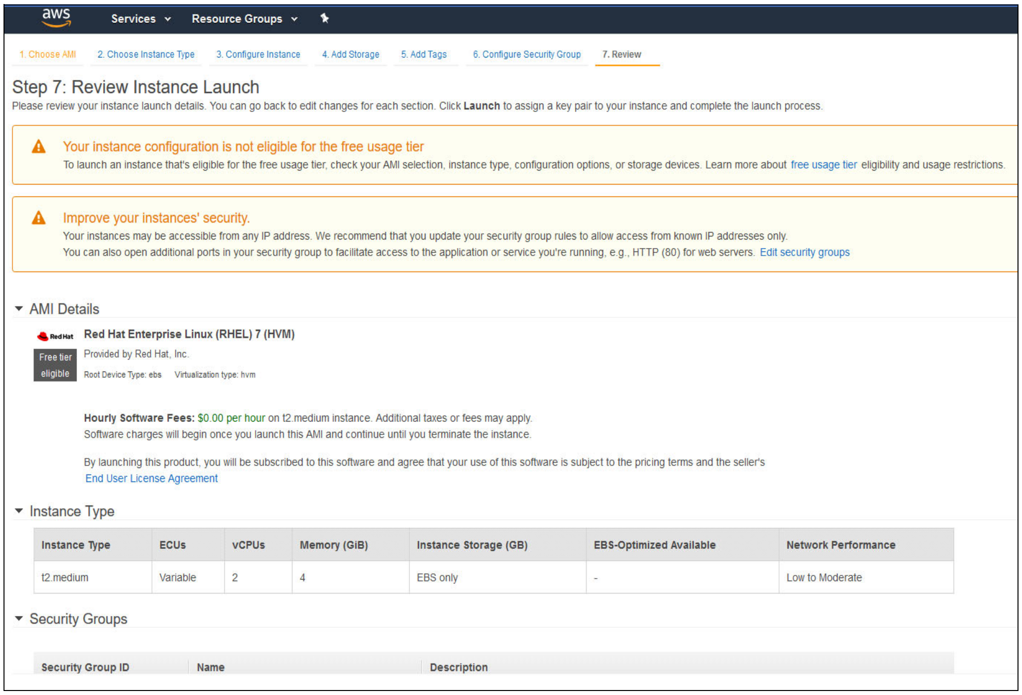
Description: This security group was generated by AWS Marketplace and is based on recom

Type	Protocol	Port Range	Source		Description
All traffic	All	0 - 65535	Anywhere	0.0.0.0/0, ::/0	e.g. SSH for Admin Des

Figure 21 Configure Security Group window

11. For test and demonstration purposes, select **All traffic** for the Type and **Anywhere** as the Source. For other purposes and production, select the suitable security group.

12. Confirm that all settings are accurate in the Review Instance Launch window (see Figure 22).



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.

Improve your instances' security.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

Red Hat Enterprise Linux (RHEL) 7 (HVM)

Free tier eligible

Provided by Red Hat, Inc.

Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: $0.00 per hour on t2.medium instance. Additional taxes or fees may apply.
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

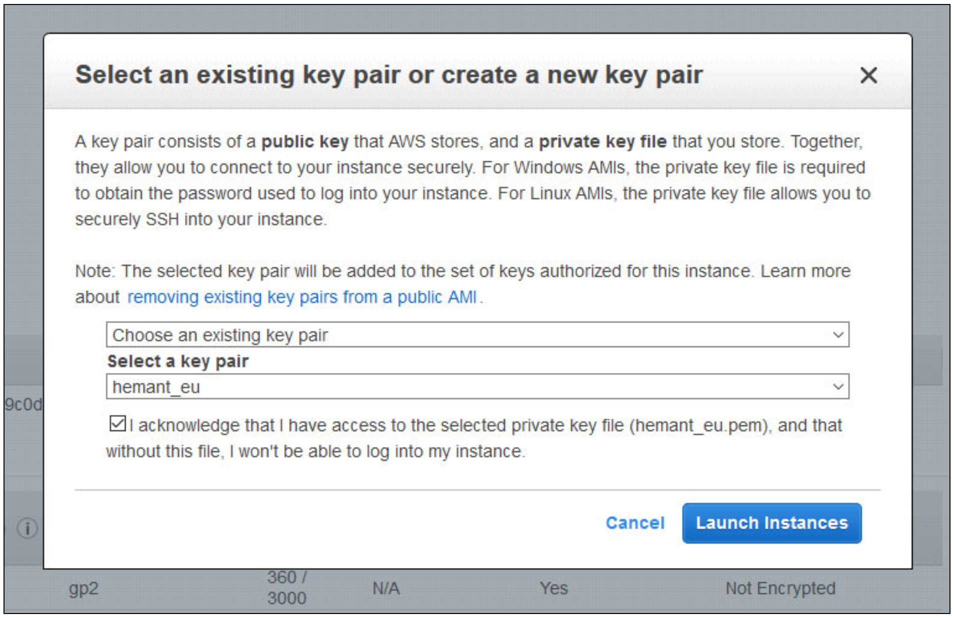
Security Group ID	Name	Description

Figure 22 Review Instance Launch window

13. Use your key pair for the EC2 instance (your name), as described in Table 2 on page 4.

For more information, see this web page.

14. Select an existing key pair or create a key pair (see Figure 23).



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

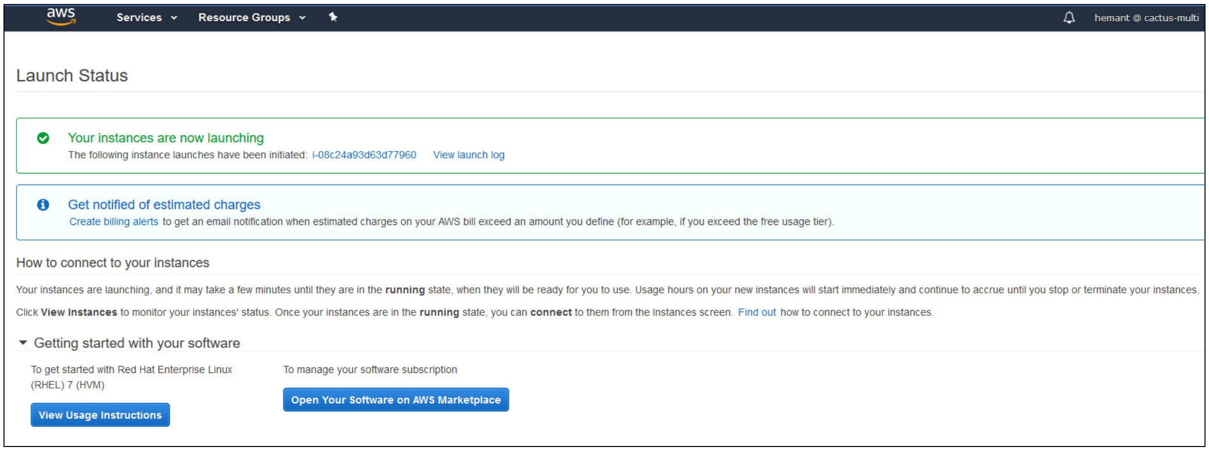
Select a key pair

hemant_eu

☑ I acknowledge that I have access to the selected private key file (hemant_eu.pem), and that without this file, I won't be able to log into my instance.

Figure 23 Select key pair

15. Check the status of your instance (see Figure 24).



Launch Status

Your instances are now launching

The following instance launches have been initiated: i-08c24a93d63d77960 View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Getting started with your software

To get started with Red Hat Enterprise Linux (RHEL) 7 (HVM)

To manage your software subscription

Figure 24 Instance status

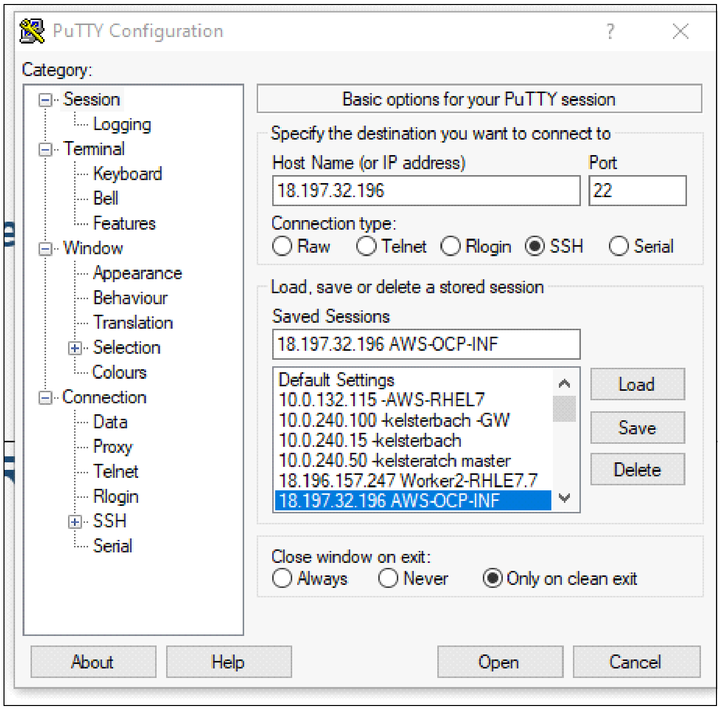
16. Select the **EC2 dashboard**. Your newly created RHEL node 1 instance is in a running state. Enter a name for the instance.

Logging in to the newly created RHEL node 1 by using PuTTY

Complete the following steps:

1. Log in to the AWS console. Select the EC2 instance and your RHEL instance to check the details and public IP address that is assigned to this node.
2. Using your Windows-based notebook, open a PuTTY session and enter the Public IP address of the node. Click **Connection** → **auth** → **browse** and provide the `.ppk` file to log in to the Linux host.

3. Log in by using the username ec2-user. The $ Prompt is shown. The Internal IP address that is assigned for this node is 172.16.2.93 (see Figure 25).



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 18.197.32.196

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: 18.197.32.196 AWS-OCP-INF

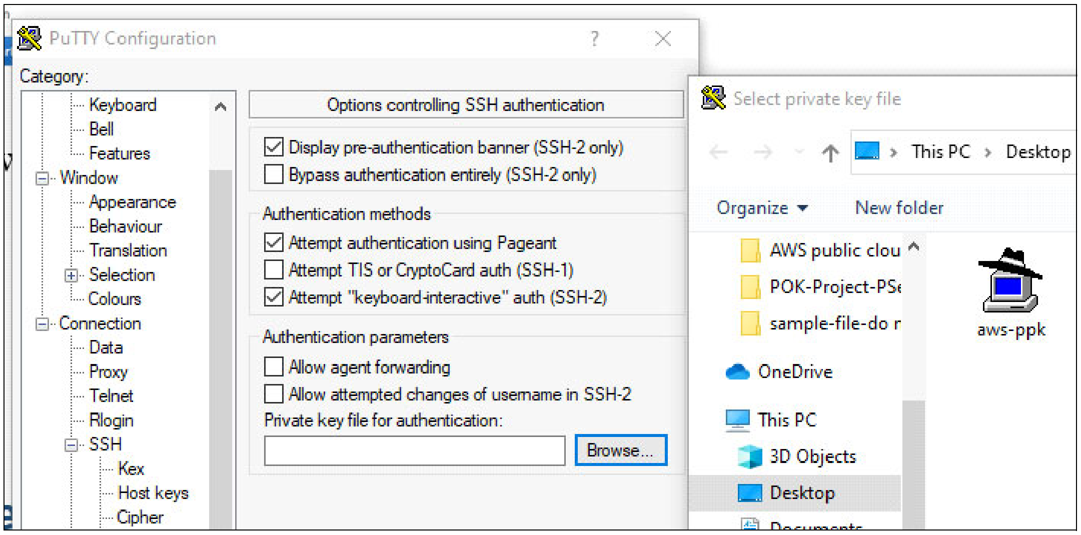
Default Settings
10.0.132.115 -AWS-RHEL7
10.0.240.100 -kelsterbach -GW
10.0.240.15 -kelsterbach
10.0.240.50 -kelsteratch master
18.196.157.247 Worker2-RHLE7.7
18.197.32.196 AWS-OCP-INF

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 25 PuTTY Configuration window

4. Locate the private key (.pem file) for the key pair that you specified when you started the instance. Convert the .pem file to a .ppk file for use with PuTTY (see Figure 26).

For more information, see this web page.



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)

□ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

Figure 26 Configuring PuTTY session

Installing OCP on AWS

In this section, we describe the process that is used to install OCP on AWS.

Preparing the installation

Complete the following steps to prepare for the installation:

1. Log in to you newly created RHEL node 1 by using `ec2-user` and become a superuser.
2. Create a directory that is named `ocp42`.
3. See this Red Hat web page for the OCP 4.2 documentation.
4. Log on to the Red Hat OpenShift Cluster Manager website and browse to the Infrastructure Provider page by using your Red Hat account credentials. Select **AWS** (see Figure 27).

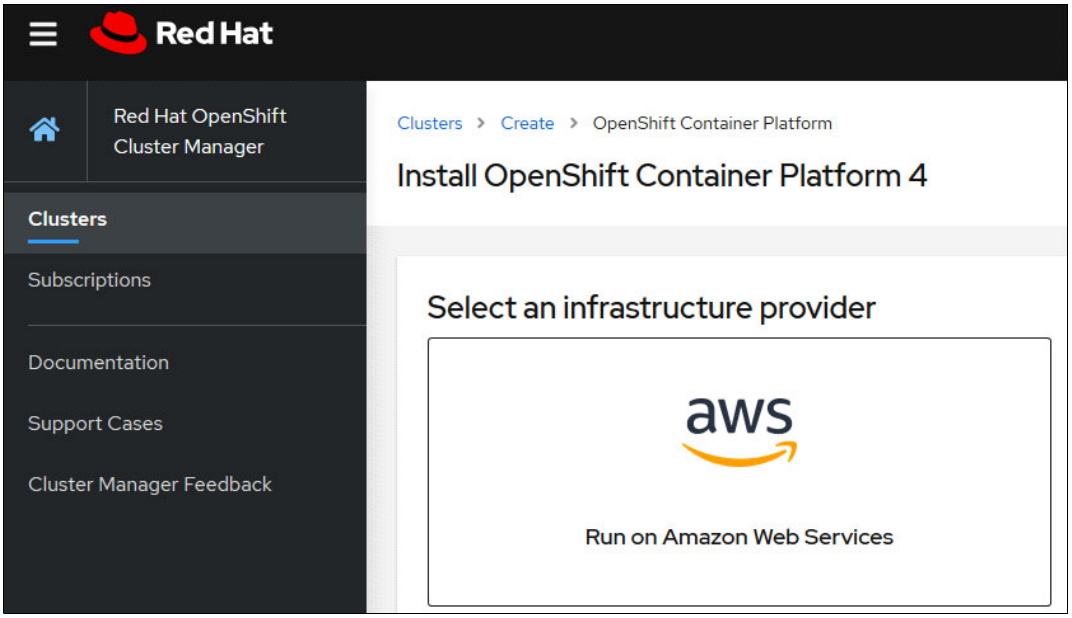
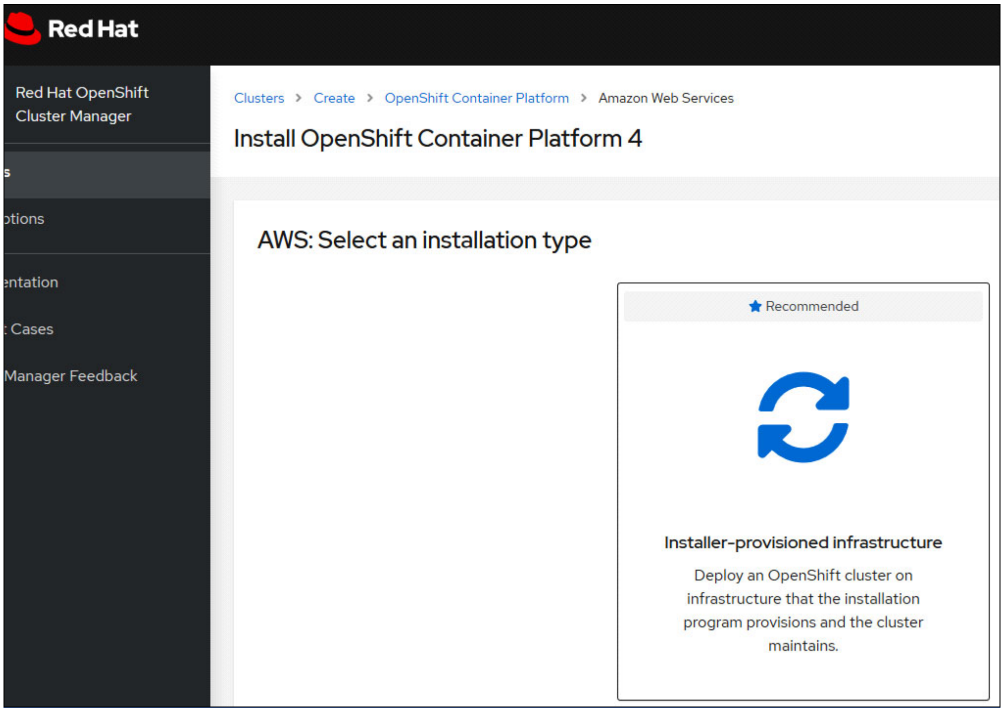

Red Hat
Red Hat OpenShift Cluster Manager
Clusters
Subscriptions
Documentation
Support Cases
Cluster Manager Feedback
Clusters > Create > OpenShift Container Platform
Install OpenShift Container Platform 4
Select an infrastructure provider
aws
Run on Amazon Web Services

Figure 27   Logging in to Red Hat account

5. Select **Installer-provisioned infrastructure** (see Figure 28).


Red Hat
Red Hat OpenShift Cluster Manager
s
ptions
entation
: Cases
Manager Feedback
Clusters > Create > OpenShift Container Platform > Amazon Web Services
Recommended

Install OpenShift Container Platform 4

AWS: Select an installation type

Installer-provisioned infrastructure

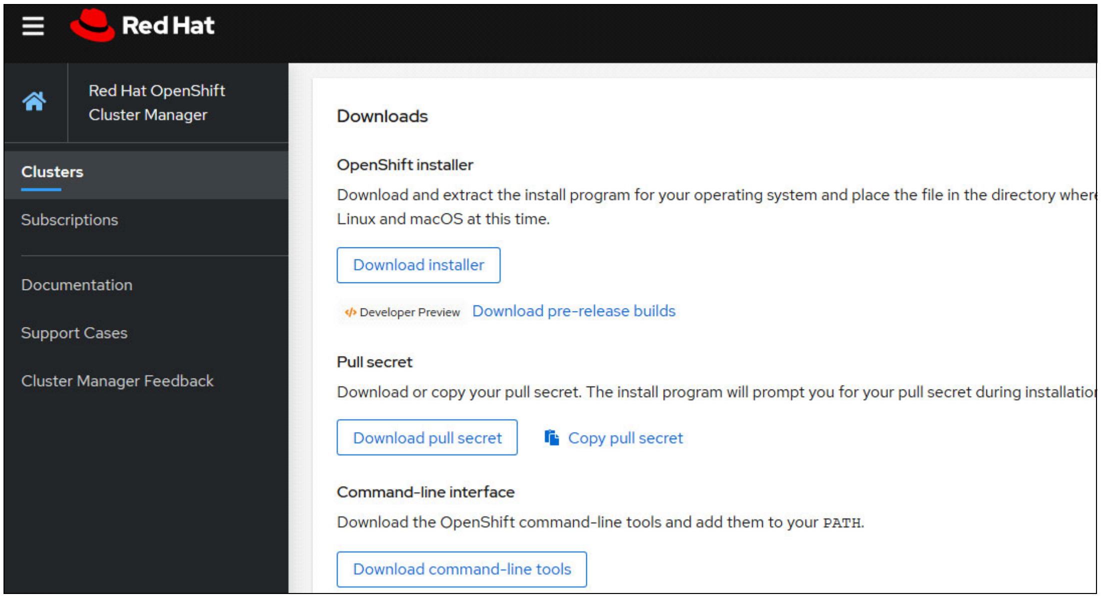
Deploy an OpenShift cluster on infrastructure that the installation program provisions and the cluster maintains.

Figure 28 Selecting installer-provisioned infrastructure

6. Click **Download installer**.
7. Select the required version 4.2 path and right-click to copy the link location to wget the files on the newly created RHEL node.
8. Click **Download command-line tools**. The binary file for OpenShift client is available for download from the following URL:

```
https://mirror.openshift.com/pub/openshift-v4/clients/ocp/4.2.20/openshift-clie
nt-linux-4.2.20.tar.gz
```

9. Click **Download the Pull Secret** and copy the pull secret that is in the `.txt` file (see Figure 29).



Downloads

OpenShift installer

Download and extract the install program for your operating system and place the file in the directory wher
Linux and macOS at this time.

Pull secret

Download or copy your pull secret. The install program will prompt you for your pull secret during installatio

Command-line interface

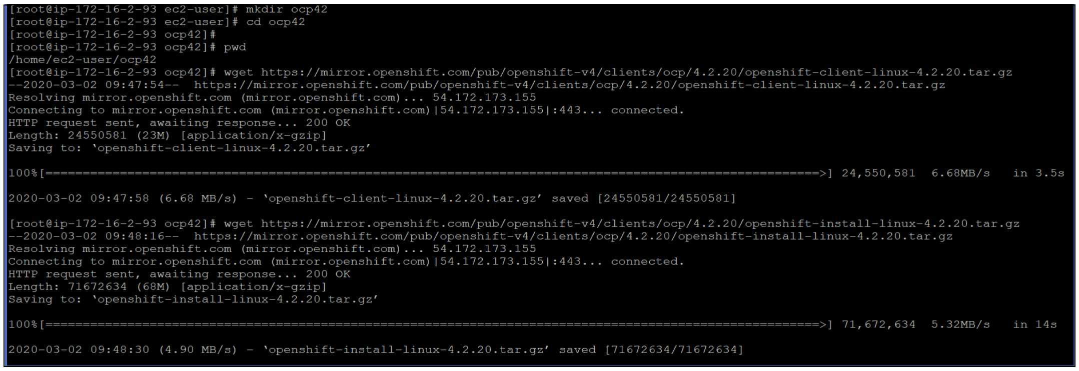
Download the OpenShift command-line tools and add them to your `PATH`.

Figure 29   Download files

Installing OCP 4.2

Complete the following steps:

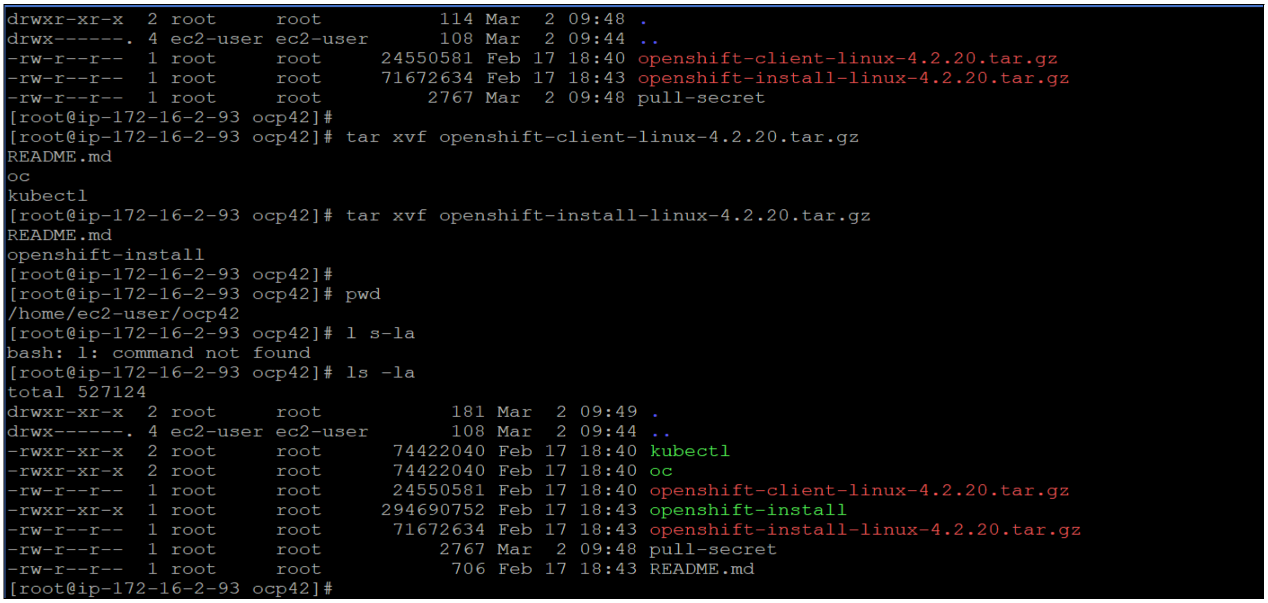
1. Log in to the RHEL node and run wget to download the files from the Red Hat site (see Figure 30).



```
[root@ip-172-16-2-93 ec2-user]# mkdir ocp42
[root@ip-172-16-2-93 ec2-user]# cd ocp42
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# pwd
/home/ec2-user/ocp42
[root@ip-172-16-2-93 ocp42]# wget https://mirror.openshift.com/pub/openshift-v4/clients/ocp/4.2.20/openshift-client-linux-4.2.20.tar.gz
--2020-03-02 09:47:54--  https://mirror.openshift.com/pub/openshift-v4/clients/ocp/4.2.20/openshift-client-linux-4.2.20.tar.gz
Resolving mirror.openshift.com (mirror.openshift.com)... 54.172.173.155
Connecting to mirror.openshift.com (mirror.openshift.com)|54.172.173.155|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24550581 (23M) [application/x-gzip]
Saving to: 'openshift-client-linux-4.2.20.tar.gz'

100%[=========================================================================================================>] 24,550,581  6.68MB/s   in 3.5s

2020-03-02 09:47:58 (6.68 MB/s) - 'openshift-client-linux-4.2.20.tar.gz' saved [24550581/24550581]

[root@ip-172-16-2-93 ocp42]# wget https://mirror.openshift.com/pub/openshift-v4/clients/ocp/4.2.20/openshift-install-linux-4.2.20.tar.gz
--2020-03-02 09:48:16--  https://mirror.openshift.com/pub/openshift-v4/clients/ocp/4.2.20/openshift-install-linux-4.2.20.tar.gz
Resolving mirror.openshift.com (mirror.openshift.com)... 54.172.173.155
Connecting to mirror.openshift.com (mirror.openshift.com)|54.172.173.155|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 71672634 (68M) [application/x-gzip]
Saving to: 'openshift-install-linux-4.2.20.tar.gz'

100%[=========================================================================================================>] 71,672,634  5.32MB/s   in 14s

2020-03-02 09:48:30 (4.90 MB/s) - 'openshift-install-linux-4.2.20.tar.gz' saved [71672634/71672634]
```

Figure 30   Download with wget

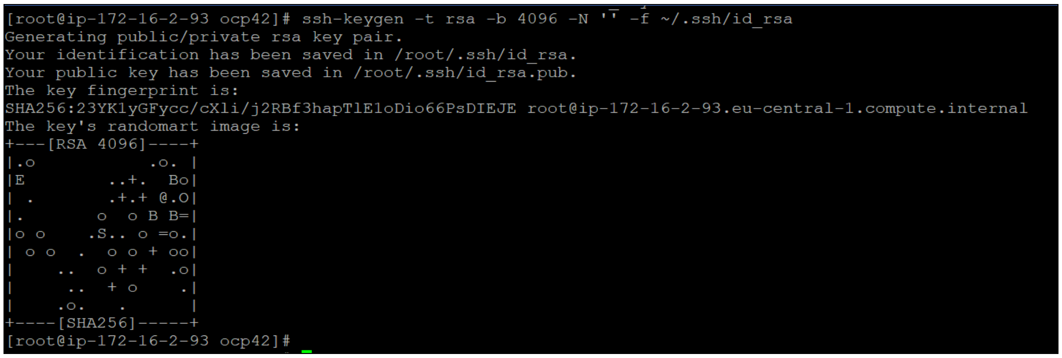
2. Extract OpenShift-client (oc) and OpenShift-install (openshift-installer) from the downloaded files, as shown in Figure 31 on page 19.



```
drwxr-xr-x  2 root     root          114 Mar  2 09:48 .
drwx------. 4 ec2-user ec2-user      108 Mar  2 09:44 ..
-rw-r--r--  1 root     root     24550581 Feb 17 18:40 openshift-client-linux-4.2.20.tar.gz
-rw-r--r--  1 root     root     71672634 Feb 17 18:43 openshift-install-linux-4.2.20.tar.gz
-rw-r--r--  1 root     root         2767 Mar  2 09:48 pull-secret
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# tar xvf openshift-client-linux-4.2.20.tar.gz
README.md
oc
kubectl
[root@ip-172-16-2-93 ocp42]# tar xvf openshift-install-linux-4.2.20.tar.gz
README.md
openshift-install
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# pwd
/home/ec2-user/ocp42
[root@ip-172-16-2-93 ocp42]# l s-la
bash: l: command not found
[root@ip-172-16-2-93 ocp42]# ls -la
total 527124
drwxr-xr-x  2 root     root           181 Mar  2 09:49 .
drwx------. 4 ec2-user ec2-user       108 Mar  2 09:44 ..
-rwxr-xr-x  2 root     root      74422040 Feb 17 18:40 kubectl
-rwxr-xr-x  2 root     root      74422040 Feb 17 18:40 oc
-rw-r--r--  1 root     root      24550581 Feb 17 18:40 openshift-client-linux-4.2.20.tar.gz
-rwxr-xr-x  1 root     root     294690752 Feb 17 18:43 openshift-install
-rw-r--r--  1 root     root      71672634 Feb 17 18:43 openshift-install-linux-4.2.20.tar.gz
-rw-r--r--  1 root     root          2767 Mar  2 09:48 pull-secret
-rw-r--r--  1 root     root           706 Feb 17 18:43 README.md
[root@ip-172-16-2-93 ocp42]#
```

Figure 31   Extract files

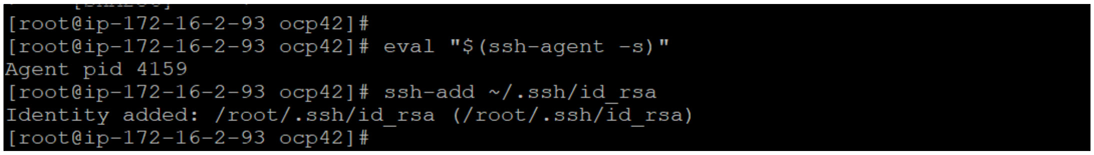
3. Generate the public and private key pairs with ssh-keygen (see Figure 32).



```
[root@ip-172-16-2-93 ocp42]# ssh-keygen -t rsa -b 4096 -N '' -f ~/.ssh/id_rsa
Generating public/private rsa key pair.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:23YKlyGFycc/cXli/j2RBf3hapTlEloDio66PsDIEJE root@ip-172-16-2-93.eu-central-1.compute.internal
The key's randomart image is:
+---[RSA 4096]----+
|.o          .o. |
|E        ..+.  Bo|
| .       .+.+ @.O|
|.       o  o B B=|
|o o    .S.. o =o.|
| o o  .  o o + oo|
|    ..  o + +  .o|
|     ..  + o    .|
|    .o.   .      |
+----[SHA256]-----+
[root@ip-172-16-2-93 ocp42]#
```

Figure 32   Configure ssh-key generation

4. Start the ssh-agent process as a background task (see Figure 33).

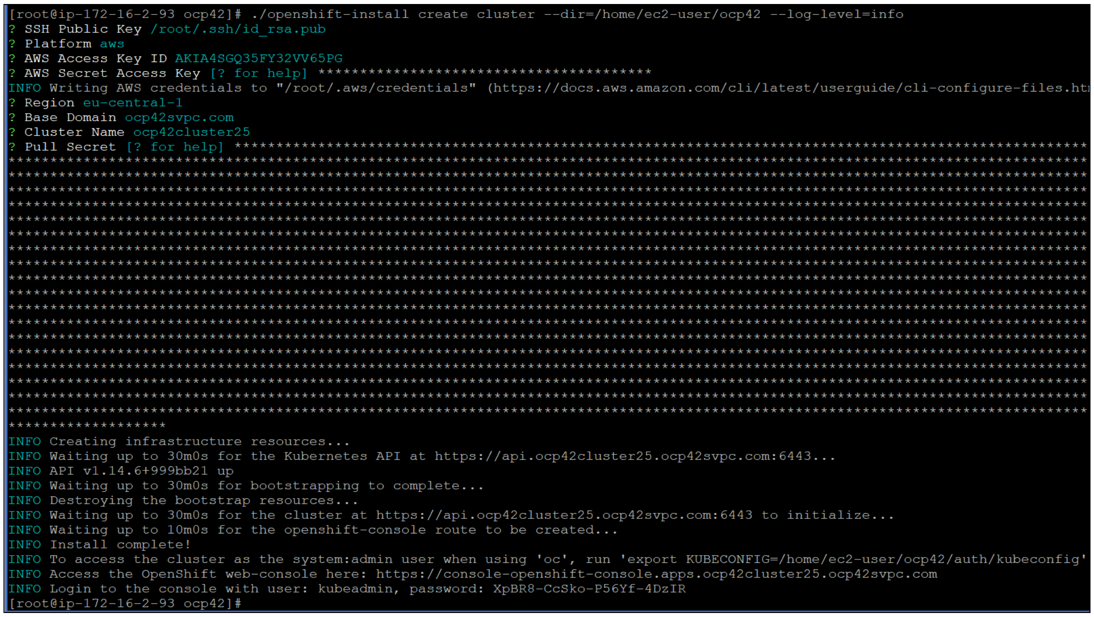


```
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# eval "$(ssh-agent -s)"
Agent pid 4159
[root@ip-172-16-2-93 ocp42]# ssh-add ~/.ssh/id_rsa
Identity added: /root/.ssh/id_rsa (/root/.ssh/id_rsa)
[root@ip-172-16-2-93 ocp42]#
```

Figure 33   Configure ssh agent

5. Run the **`openshift-install`** command to create the cluster (see Figure 34 on page 20). This command prompts you for the following required values:

   – SSH public key: `/root/.ssh/id_rsa.pub`
   – Platform: `aws`
   – AWS access key ID: Paste this key the ID from the `.csv` file that you downloaded.
   – AWS secret access key: Paste the ID from the `.csv` file that you downloaded.
   – Region: This value is shown on your AWS console when you log in.
   – Base Domain: This domain is created by using the Route 53 service.
   – Pull secret: Copy the pull secret that you downloaded from the Red Hat website.



```
[root@ip-172-16-2-93 ocp42]# ./openshift-install create cluster --dir=/home/ec2-user/ocp42 --log-level=info
? SSH Public Key /root/.ssh/id_rsa.pub
? Platform aws
? AWS Access Key ID AKIA4SGQ35FY32VV65PG
? AWS Secret Access Key [? for help] ****************************************
INFO Writing AWS credentials to "/root/.aws/credentials" (https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.ht
? Region eu-central-1
? Base Domain ocp42svpc.com
? Cluster Name ocp42cluster25
? Pull Secret [? for help] *******************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
**********************************************************************************************************************************
*******************
INFO Creating infrastructure resources...
INFO Waiting up to 30m0s for the Kubernetes API at https://api.ocp42cluster25.ocp42svpc.com:6443...
INFO API v1.14.6+999bb21 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO Destroying the bootstrap resources...
INFO Waiting up to 30m0s for the cluster at https://api.ocp42cluster25.ocp42svpc.com:6443 to initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export KUBECONFIG=/home/ec2-user/ocp42/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-console.apps.ocp42cluster25.ocp42svpc.com
INFO Login to the console with user: kubeadmin, password: XpBR8-CcSko-P56Yf-4DzIR
[root@ip-172-16-2-93 ocp42]#
```

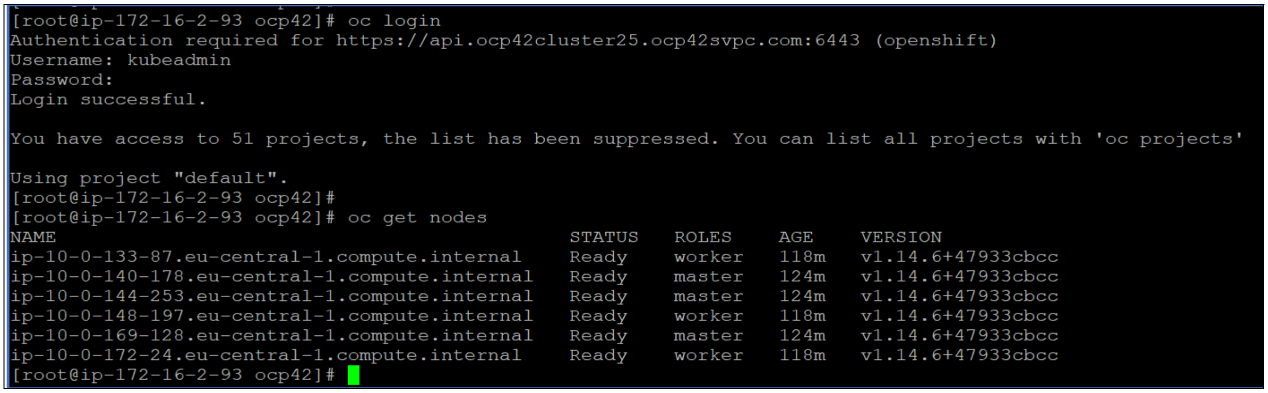
Figure 34 Creating the OpenShift cluster

The **openShift-install create** command completes and provides the username, password, and console login URL information.

6. Set the KUBECONFIG environment variable to point to the kubeconfig file:

```
# export KUBECONFIG=/home/ec2-user/ocp42/auth/kubeconfig
```

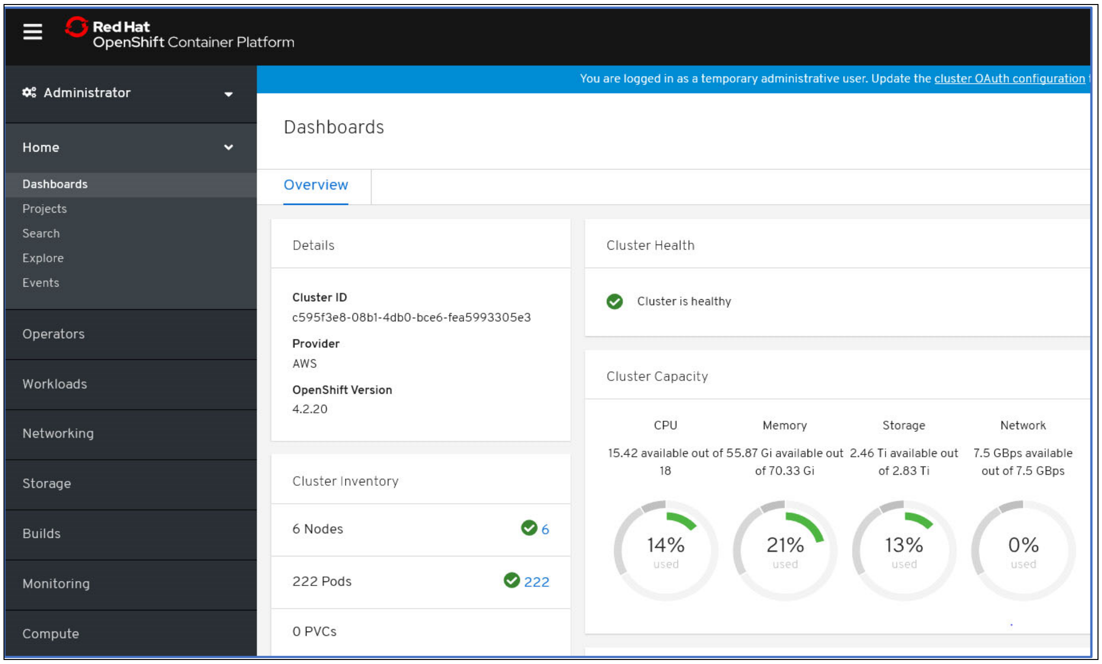
7. Check the status of the cluster and the nodes (see Figure 35).



```
[root@ip-172-16-2-93 ocp42]# oc login
Authentication required for https://api.ocp42cluster25.ocp42svpc.com:6443 (openshift)
Username: kubeadmin
Password:
Login successful.

You have access to 51 projects, the list has been suppressed. You can list all projects with 'oc projects'

Using project "default".
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# oc get nodes
NAME                                         STATUS   ROLES    AGE    VERSION
ip-10-0-133-87.eu-central-1.compute.internal    Ready    worker   118m   v1.14.6+47933cbcc
ip-10-0-140-178.eu-central-1.compute.internal   Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-144-253.eu-central-1.compute.internal   Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-148-197.eu-central-1.compute.internal   Ready    worker   118m   v1.14.6+47933cbcc
ip-10-0-169-128.eu-central-1.compute.internal   Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-172-24.eu-central-1.compute.internal    Ready    worker   118m   v1.14.6+47933cbcc
[root@ip-172-16-2-93 ocp42]#
```

Figure 35 Check cluster status

8. Log in to the console URL and check the status (see Figure 36).



You are logged in as a temporary administrative user. Update the cluster OAuth configuration

Cluster ID
c595f3e8-08b1-4db0-bce6-fea5993305e3

Provider
AWS

OpenShift Version
4.2.20

Cluster is healthy

15.42 available out of 18 | 55.87 Gi available out of 70.33 Gi | 2.46 Ti available out of 2.83 Ti | 7.5 GBps available out of 7.5 GBps

6 Nodes ✓ 6

222 Pods ✓ 222

0 PVCs

Figure 36 OpenShift dashboard

Creating RHEL 7.x node 2 with an AMI image

Complete the following steps:

1. Create an RHEL node as described in “Creating RHEL 7.x node 1 with AMI image” on page 11. Ensure to select the VPC that was created for this OCP cluster so that the new RHEL node includes the similar private IP range per the Master and Worker nodes; for example, 10.0.x.x range (10.0.3.25).

   The Internal IP address that is assigned for this node is (10.0.3.25)

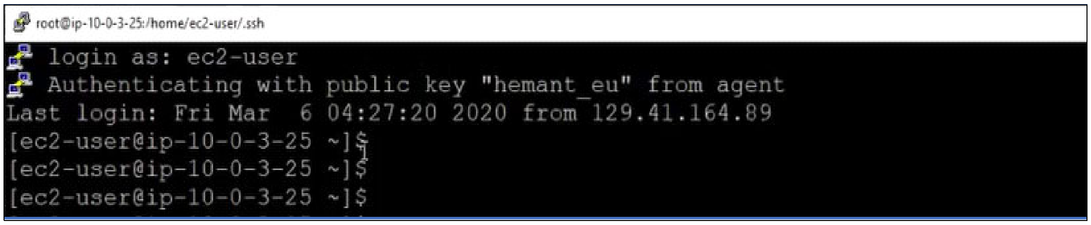
2. Copy all the cluster configuration files and directory from node 1 to node 2:

   a. Log in to RHEL node 1:

      - `scp -r /home/ec2-user/ocp42 ec2-user@node2:/home/ec2-user/`
      - `scp /root/.ssh/ id_rsa ec2-user@node2:/home/ec2-user/id_rsa_node1`

      You also can paste the contents of `id_rsa` file from node1 to create the `id_rsa_node1` file on node 2.

   b. Log in to RHEL node 2 (see Figure 37).



```
login as: ec2-user
Authenticating with public key "hemant_eu" from agent
Last login: Fri Mar  6 04:27:20 2020 from 129.41.164.89
[ec2-user@ip-10-0-3-25 ~]$
[ec2-user@ip-10-0-3-25 ~]$
[ec2-user@ip-10-0-3-25 ~]$
```

Figure 37 Log in to RHEL node

The following code is code is displayed when the cluster installation is complete:

```
# export KUBECONFIG=/home/ec2-user/ocp42/auth/kubeconfig
# oc get node
```

Now, the status of the cluster nodes should be available.

By using this procedure, you created RHEL node 2 in OCP VPC with the similar private IP range of master and worker nodes so that you can log in to cluster nodes from this RHEL node.

Installing CSI driver plug-in

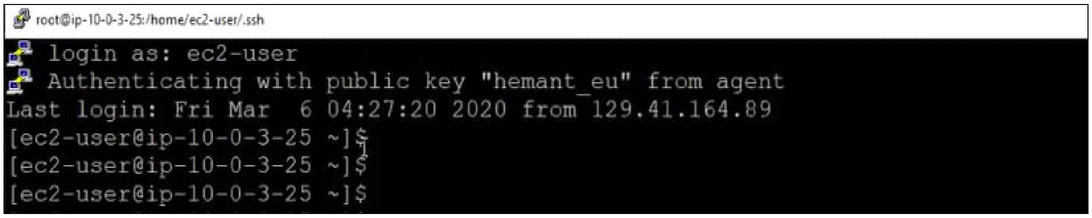
In this section, the process for installing the CSI driver plug-in is described.

Prerequisites for driver installation

For more information about the IBM CSI driver installation procedure, see this web page.

The following prerequisites for driver installation must be met:

- Worker nodes are prepared.
- You logged in to the RHEL node 2 by using your PuTTY session and sudo su (see Figure 38).



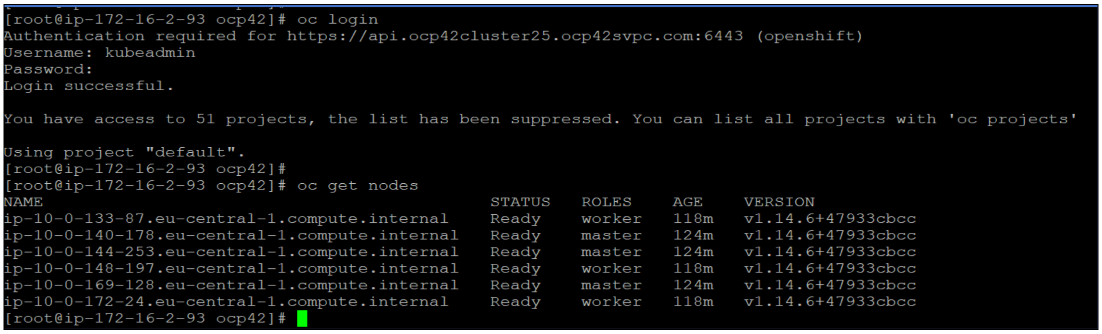
root@ip-10-0-3-25:/home/ec2-user/.ssh

```
login as: ec2-user
Authenticating with public key "hemant_eu" from agent
Last login: Fri Mar  6 04:27:20 2020 from 129.41.164.89
[ec2-user@ip-10-0-3-25 ~]$
[ec2-user@ip-10-0-3-25 ~]$
[ec2-user@ip-10-0-3-25 ~]$
```

Figure 38   Log in to RHEL node

The following code is code is displayed when the cluster installation is complete (see Figure 39):

```
# export KUBECONFIG=/home/ec2-user/ocp42/auth/kubeconfig
# oc get nodes (sample output)
```



```
[root@ip-172-16-2-93 ocp42]# oc login
Authentication required for https://api.ocp42cluster25.ocp42svpc.com:6443 (openshift)
Username: kubeadmin
Password:
Login successful.

You have access to 51 projects, the list has been suppressed. You can list all projects with 'oc projects'

Using project "default".
[root@ip-172-16-2-93 ocp42]#
[root@ip-172-16-2-93 ocp42]# oc get nodes
NAME                                          STATUS   ROLES    AGE    VERSION
ip-10-0-133-87.eu-central-1.compute.internal  Ready    worker   118m   v1.14.6+47933cbcc
ip-10-0-140-178.eu-central-1.compute.internal Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-144-253.eu-central-1.compute.internal Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-148-197.eu-central-1.compute.internal Ready    worker   118m   v1.14.6+47933cbcc
ip-10-0-169-128.eu-central-1.compute.internal Ready    master   124m   v1.14.6+47933cbcc
ip-10-0-172-24.eu-central-1.compute.internal  Ready    worker   118m   v1.14.6+47933cbcc
[root@ip-172-16-2-93 ocp42]#
```

Figure 39   Show cluster node status

Use the `id_rsa_node1` file that you created to log in to the cluster’s worker nodes:

```
[ec2-user2@ip-10-0-3-25]#  ssh -i id_rsa_node1
core@ip-10-0-172-24.eu-central-1.compute.internal
```

Or

```
[ec2-user2@ip-10-0-3-25]#  ssh -i id_rsa_node1 core@10.0.172.24
```

- Install Linux packages to ensure iSCSI connectivity:

  ```
  # yum -y install iscsi-initiator-utils
  ```

  (Preinstalled with RHCOS; needed for RHEL node only.)

- Configure Linux multipath devices on the host by using one of the following procedures:
  - Configuring for OpenShift Container Platform users (RHEL and RHCOS)

    The yaml file that is shown in Example 1 can be used for Fibre Channel and iSCSI configurations. To support iSCSI, uncomment the last two lines in the file.

Example 1   99-ibm-attach.yaml

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-ibm-attach
spec:
  config:
    ignition:
      version: 2.2.0
    storage:
      files:
        - path: /etc/multipath.conf
          mode: 384
          filesystem: root
          contents:
            source:
data:,defaults%20%7B%0A%20%20%20%20path_checker%20tur%0A%20%20%20%20
path_selector%20%22round-robin%200%22%0A%20%20%20%20rr_weight%20unif
orm%0A%20%20%20%20prio%20const%0A%20%20%20%20rr_min_io_rq%201%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%0A%20%20%20%20polling_interva
l%2030%0A%20%20%20%20path_grouping_policy%20multibus%0A%20%20%20%20f
ind_multipaths%20yes%0A%20%20%20%20no_path_retry%20fail%0A%20%20%20%
20user_friendly_names%20yes%0A%20%20%20%20failback%20immediate%0A%20
%20%20%20checker_timeout%2010%0A%20%20%20%20fast_io_fail_tmo%20off%0
A%7D%0A%0Adevices%20%7B%0A%20%20%20%20device%20%7B%0A%20%20%20%20%20
%20%20%20path_checker%20tur%0A%20%20%20%20%20%20%20%20product%20%22F
lashSystem%22%0A%20%20%20%20%20%20%20%20vendor%20%22IBM%22%0A%20%20%
20%20%20%20%20%20rr_weight%20uniform%0A%20%20%20%20%20%20%20%20rr_mi
n_io_rq%204%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%0A%20%20%20
%20%20%20%20%20path_grouping_policy%20multibus%0A%20%20%20%20%20%20%
20%20path_selector%20%22round-robin%200%22%0A%20%20%20%20%20%20%20%2
0no_path_retry%20fail%0A%20%20%20%20%20%20%20%20failback%20immediate
%0A%20%20%20%20%7D%0A%20%20%20%20device%20%7B%0A%20%20%20%20%20%20%2
0%20path_checker%20tur%0A%20%20%20%20%20%20%20%20product%20%22FlashS
ystem-9840%22%0A%20%20%20%20%20%20%20%20vendor%20%22IBM%22%0A%20%20%
```

```
20%20%20%20%20%20fast_io_fail_tmo%20off%0A%20%20%20%20%20%20%20%20rr
_weight%20uniform%0A%20%20%20%20%20%20%20%20rr_min_io_rq%201000%20%2
0%20%20%20%20%20%20%20%20%20%20%0A%20%20%20%20%20%20%20%20path_group
ing_policy%20multibus%0A%2020%20%20%20%20%20%20%20path_selector%20%2
2round-robin%200%22%0A%20%20%20%20%20%20%20%20no_path_retry%20fail%0
A%20%20%20%20%20%20%20%20failback%20immediate%0A%20%20%20%20%7D%0A%2
0%20%20%20device%20%7B%0A%20%20%20%20%20%20%20%20vendor%20%22IBM%22%
0A%20%20%20%20%20%20%20%20product%20%222145%22%0A%20%20%20%20%20%20%
20%20path_checker%20tur%0A%20%20%20%20%20%20%20%20features%20%221%20
queue_if_no_path%22%0A%20%20%20%20%20%20%20%20path_grouping_policy%2
0group_by_prio%0A%20%20%20%20%20%20%20%20path_selector%20%22service-
time%200%22%20%23%20Used%20by%20Red%20Hat%207.x%0A%20%20%20%20%20%20
%20%20prio%20alua%0A%20%20%20%20%20%20%20%20rr_min_io_rq%201%0A%20%2
0%20%20%20%20%20%20rr_weight%20uniform%20%0A%20%20%20%20%20%20%20%20
no_path_retry%20%225%22%0A%20%20%20%20%20%20%20%20dev_loss_tmo%20120
%0A%20%20%20%20%20%20%20%20failback%20immediate%0A%20%20%20%7D%0A%7D
%0A
            verification: {}
        - path: /etc/udev/rules.d/99-ibm-2145.rules
          mode: 420
          filesystem: root
          contents:
            source:
data:,%23%20Set%20SCSI%20command%20timeout%20to%20120s%20%28default%
20%3D%3D%2030%20or%2060%29%20for%20IBM%202145%20devices%0ASUBSYSTEM%
3D%3D%22block%22%2C%20ACTION%3D%3D%22add%22%2C%20ENV%7BID_VENDOR%7D%
3D%3D%22IBM%22%2CENV%7BID_MODEL%7D%3D%3D%222145%22%2C%20RUN%2B%3D%22
/bin/sh%20-c%20%27echo%20120%20%3E/sys/block/%25k/device/timeout%27%
22%0A
            verification: {}
    systemd:
      units:
      - name: multipathd.service
        enabled: true
      # Uncomment the following lines if this MachineConfig will be
used with iSCSI connectivity
      #- name: iscsid.service
      #  enabled: true
```

Save the 99-ibm-attach.yaml file.

Apply the yaml file:

```
oc apply -f 99-ibm-attach.yaml
```

RHEL users should verify that the systemctl status multipathd output indicates that the multipath status is active and error-free:

```
yum install device-mapper-multipath
sudo modprobe dm-multipath
systemctl enable multipathd
systemctl start multipathd
systemctl status multipathd
multipath -ll
```

- Configuring for Kubernetes users (RHEL)

  Create and set the relevant storage system parameters in the `/etc/multipath.conf` file. You can also use the default `multipath.conf` file, which is in the following directory:

  ```
  /usr/share/doc/device-mapper-multipath-*
  ```

  Verify that the `systemctl status multipathd` output indicates that the multipath status is active and error-free:

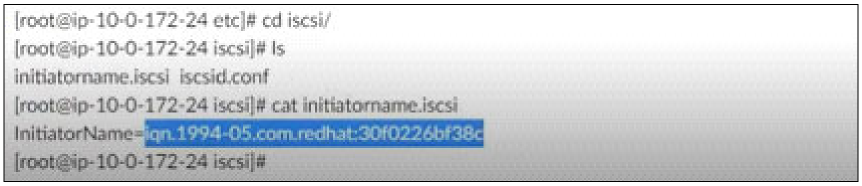
  ```
  yum install device-mapper-multipath
  sudo modprobe dm-multipath
  systemctl enable multipathd
  systemctl start multipathd
  systemctl status multipathd
  multipath -ll
  ```

- Configuring storage system (SVPC) connectivity

  Define the host name of each worker node on the svpc storage with a valid IQN (for iSCSI).

  Log in to the worker node and identify the `initiatorname`:

  ```
  # cat /etc/iscsi/initiatorname.iscsi  à copy the iqn
  ```



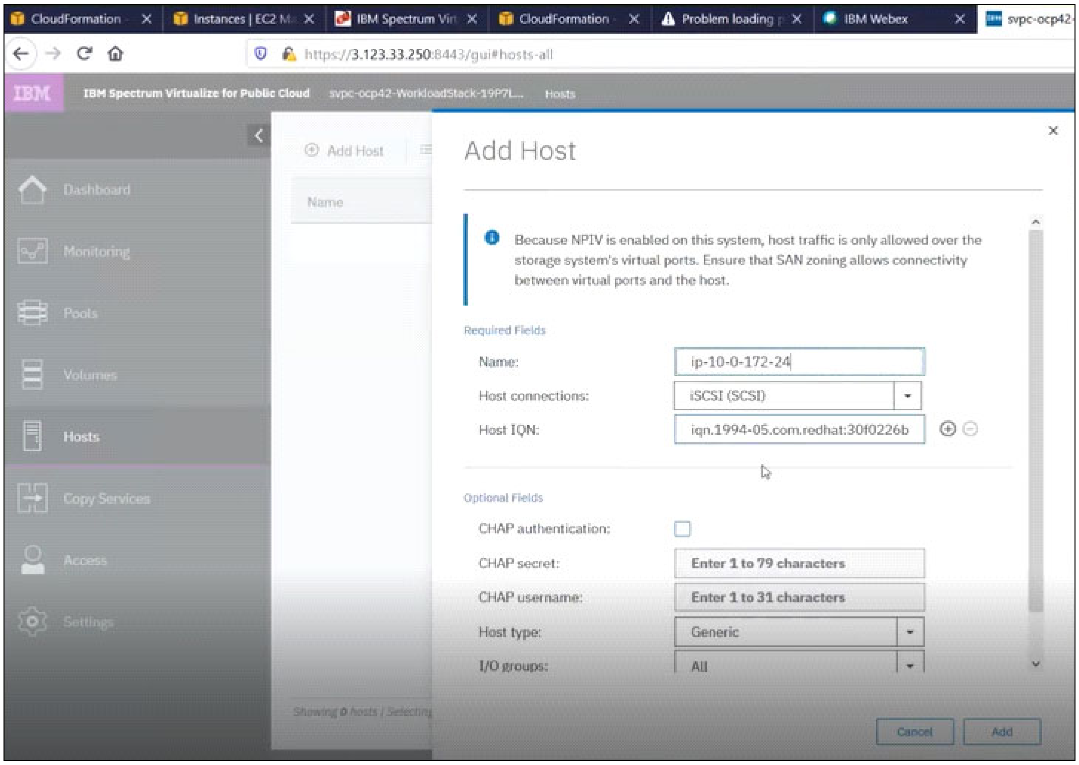
```
[root@ip-10-0-172-24 etc]# cd iscsi/
[root@ip-10-0-172-24 iscsi]# ls
initiatorname.iscsi  iscsid.conf
[root@ip-10-0-172-24 iscsi]# cat initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:30f0226bf38c
[root@ip-10-0-172-24 iscsi]#
```

Figure 40 Check iSCSI IQN

- Log in to the SVPC storage GUI:

  ```
  https://3.123.33.250:8443/gui#hosts-all
  ```

- Click **Hosts** → **Add hosts** and enter the required information (see Figure 40).



Add Host

Because NPIV is enabled on this system, host traffic is only allowed over the storage system's virtual ports. Ensure that SAN zoning allows connectivity between virtual ports and the host.

Required Fields

Name: ip-10-0-172-24

Host connections: iSCSI (SCSI)

Host IQN: iqn.1994-05.com.redhat:30f0226b

Optional Fields

CHAP authentication: □

CHAP secret: Enter 1 to 79 characters

CHAP username: Enter 1 to 31 characters

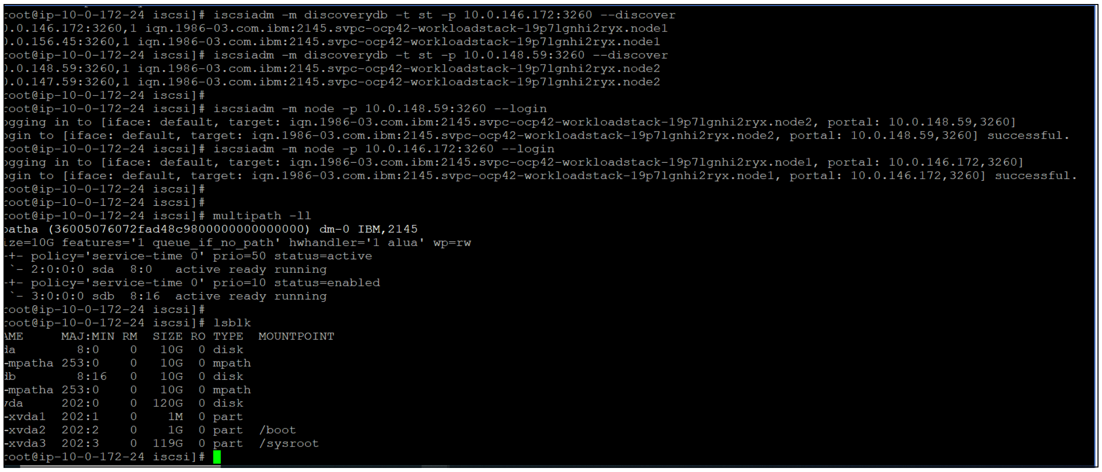
Host type: Generic

I/O groups: All

Figure 41   Configure hosts

- Add a test LUN to this host and check the status.
- Log in to the worker node and run the following **`iscsiadm`** command to discover the new LUN on worker node:

```
[ec2-user2@ip-10-0-3-25]#  ssh -i id_rsa_node1 core@10.0.172.24
```



```
oot@ip-10-0-172-24 iscsi]# iscsiadm -m discoverydb -t st -p 10.0.146.172:3260 --discover
.0.146.172:3260,1 iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node1
.0.156.45:3260,1 iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node1
oot@ip-10-0-172-24 iscsi]# iscsiadm -m discoverydb -t st -p 10.0.148.59:3260 --discover
.0.148.59:3260,1 iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node2
.0.147.59:3260,1 iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node2
oot@ip-10-0-172-24 iscsi]#
oot@ip-10-0-172-24 iscsi]# iscsiadm -m node -p 10.0.148.59:3260 --login
ogging in to [iface: default, target: iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node2, portal: 10.0.148.59,3260]
ogin to [iface: default, target: iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node2, portal: 10.0.148.59,3260] successful.
oot@ip-10-0-172-24 iscsi]# iscsiadm -m node -p 10.0.146.172:3260 --login
ogging in to [iface: default, target: iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node1, portal: 10.0.146.172,3260]
ogin to [iface: default, target: iqn.1986-03.com.ibm:2145.svpc-ocp42-workloadstack-19p7lgnhi2ryx.node1, portal: 10.0.146.172,3260] successful.
oot@ip-10-0-172-24 iscsi]#
oot@ip-10-0-172-24 iscsi]#
oot@ip-10-0-172-24 iscsi]# multipath -ll
atha (36005076072fad48c9800000000000000) dm-0 IBM,2145
ze=10G features='1 queue_if_no_path' hwhandler='1 alua' wp=rw
+- policy='service-time 0' prio=50 status=active
 `- 2:0:0:0 sda  8:0   active ready running
+- policy='service-time 0' prio=10 status=enabled
 `- 3:0:0:0 sdb  8:16  active ready running
oot@ip-10-0-172-24 iscsi]#
oot@ip-10-0-172-24 iscsi]# lsblk
ME      MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
a         8:0    0   10G  0 disk
-mpatha 253:0    0   10G  0 mpath
b         8:16   0   10G  0 disk
-mpatha 253:0    0   10G  0 mpath
da      202:0    0  120G  0 disk
-xvda1  202:1    0    1M  0 part
-xvda2  202:2    0    1G  0 part  /boot
-xvda3  202:3    0  119G  0 part  /sysroot
oot@ip-10-0-172-24 iscsi]#
```

Figure 42   Configure iSCSI

Deploying the CSI driver on OCP

For more information about deploying the IBM Block Storage CSI driver, see *IBM Storage for Red Hat OpenShift Blueprint Version 1 Release 4*, hREDP-5565.

Log in to the RHEL node 2 and check the status of IBM block CSI driver. Verify that the driver is running.

For more information about the use of the CSI driver that uses the secret and storage class, see the OpenShift documentation.

Sample file

A sample /etc/multipath.conf file is shown in Example 2.

Example 2 Sample /etc/multipath.conf file

```
defaults {
    path_checker tur
    path_selector "round-robin 0"
    rr_weight uniform
    prio const
    rr_min_io_rq 1
    polling_interval 30
    path_grouping_policy multibus
    find_multipaths yes
    no_path_retry fail
    user_friendly_names yes
    failback immediate
    checker_timeout 10
    fast_io_fail_tmo off
}
devices {
    device {
        path_checker tur
        product "FlashSystem"
        vendor "IBM"
        rr_weight uniform
        rr_min_io_rq 4
        path_grouping_policy multibus
        path_selector "round-robin 0"
        no_path_retry fail
        failback immediate
    }
    device {
        path_checker tur
        product "FlashSystem-9840"
        vendor "IBM"
        fast_io_fail_tmo off
        rr_weight uniform
        rr_min_io_rq 1000
        path_grouping_policy multibus
        path_selector "round-robin 0"
        no_path_retry fail
```

```
            failback immediate
        }
        device {
            vendor "IBM"
            product "2145"
            path_checker tur
            features "1 queue_if_no_path"
            path_grouping_policy group_by_prio
            path_selector "service-time 0" # Used by Red Hat 7.x
            prio alua
            rr_min_io_rq 1
            no_path_retry "5"
            dev_loss_tmo 120
            failback immediate
       }
}
```

Installing OpenShift 4.x on AWS with customization

In this section, installing customized OpenShift 4.x on AWS is described.

OCP4.3 on AWS with IPI

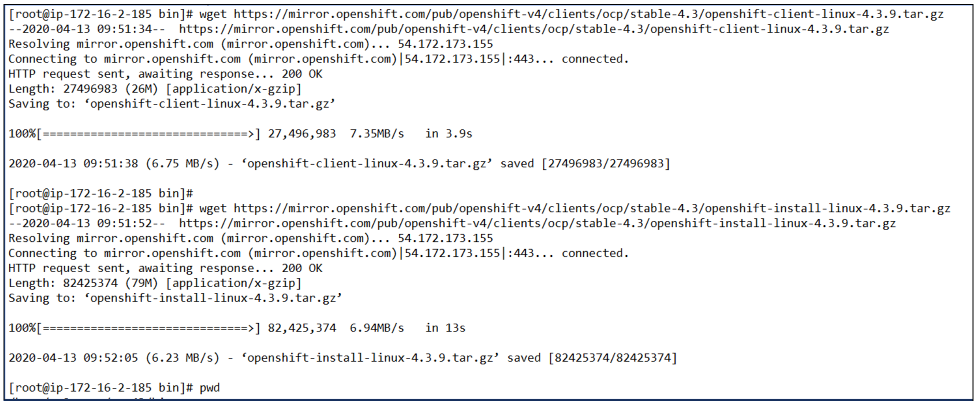
In this section, Red Hat OpenShift installation and configuration by using the OCP4.3 on AWS with IPI (Installer-Provisioned Infrastructure) method is described.

For more information, see this web page.

> **Note:** With OCP version 4.3, installing OpenShift can be done on existing VPCs on AWS. Be sure to complete the VPC prerequisites for installation.

Complete the following steps:

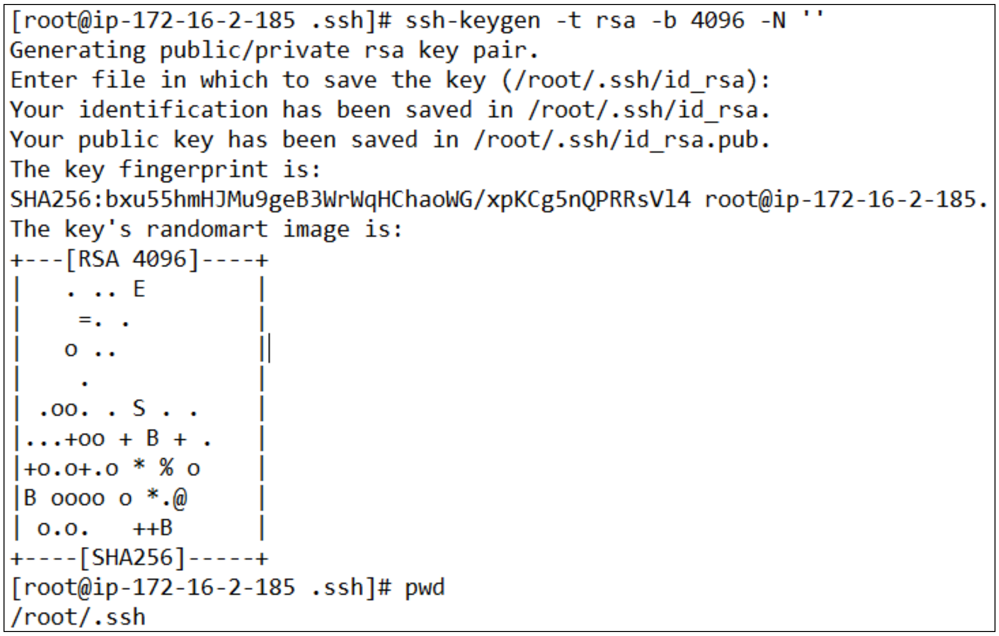
1. Create an RHEL 7.x Linux node with public IP from AWS marketplace from the AWS console and wget the required files for installation (see Figure 43). Ensure that you create this Linux node in the VPC network.



```
[root@ip-172-16-2-185 bin]# wget https://mirror.openshift.com/pub/openshift-v4/clients/ocp/stable-4.3/openshift-client-linux-4.3.9.tar.gz
--2020-04-13 09:51:34--  https://mirror.openshift.com/pub/openshift-v4/clients/ocp/stable-4.3/openshift-client-linux-4.3.9.tar.gz
Resolving mirror.openshift.com (mirror.openshift.com)... 54.172.173.155
Connecting to mirror.openshift.com (mirror.openshift.com)|54.172.173.155|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27496983 (26M) [application/x-gzip]
Saving to: ‘openshift-client-linux-4.3.9.tar.gz’

100%[=============================>] 27,496,983  7.35MB/s   in 3.9s

2020-04-13 09:51:38 (6.75 MB/s) - ‘openshift-client-linux-4.3.9.tar.gz’ saved [27496983/27496983]

[root@ip-172-16-2-185 bin]#
[root@ip-172-16-2-185 bin]# wget https://mirror.openshift.com/pub/openshift-v4/clients/ocp/stable-4.3/openshift-install-linux-4.3.9.tar.gz
--2020-04-13 09:51:52--  https://mirror.openshift.com/pub/openshift-v4/clients/ocp/stable-4.3/openshift-install-linux-4.3.9.tar.gz
Resolving mirror.openshift.com (mirror.openshift.com)... 54.172.173.155
Connecting to mirror.openshift.com (mirror.openshift.com)|54.172.173.155|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82425374 (79M) [application/x-gzip]
Saving to: ‘openshift-install-linux-4.3.9.tar.gz’

100%[=============================>] 82,425,374  6.94MB/s   in 13s

2020-04-13 09:52:05 (6.23 MB/s) - ‘openshift-install-linux-4.3.9.tar.gz’ saved [82425374/82425374]

[root@ip-172-16-2-185 bin]# pwd
```

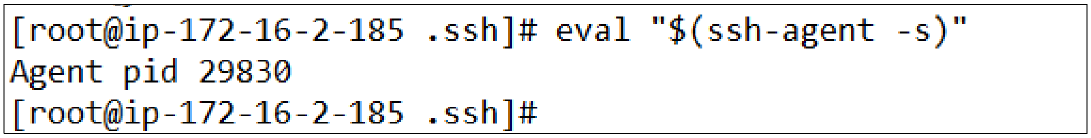
Figure 43   Downloading the required files for installation

For more information. see this web page.



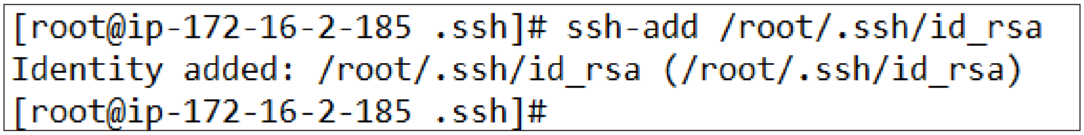
```
[root@ip-172-16-2-185 .ssh]# ssh-keygen -t rsa -b 4096 -N ''
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:bxu55hmHJMu9geB3WrWqHChaoWG/xpKCg5nQPRRsVl4 root@ip-172-16-2-185.
The key's randomart image is:
+---[RSA 4096]----+
|   . .. E        |
|    =. .         |
|   o ..          ||
|    .            |
| .oo. . S . .    |
|...+oo + B + .   |
|+o.o+.o * % o    |
|B oooo o *.@     |
| o.o.   ++B      |
+----[SHA256]-----+
[root@ip-172-16-2-185 .ssh]# pwd
/root/.ssh
```

Figure 44   Configuring SSH



```
[root@ip-172-16-2-185 .ssh]# eval "$(ssh-agent -s)"
Agent pid 29830
[root@ip-172-16-2-185 .ssh]#
```

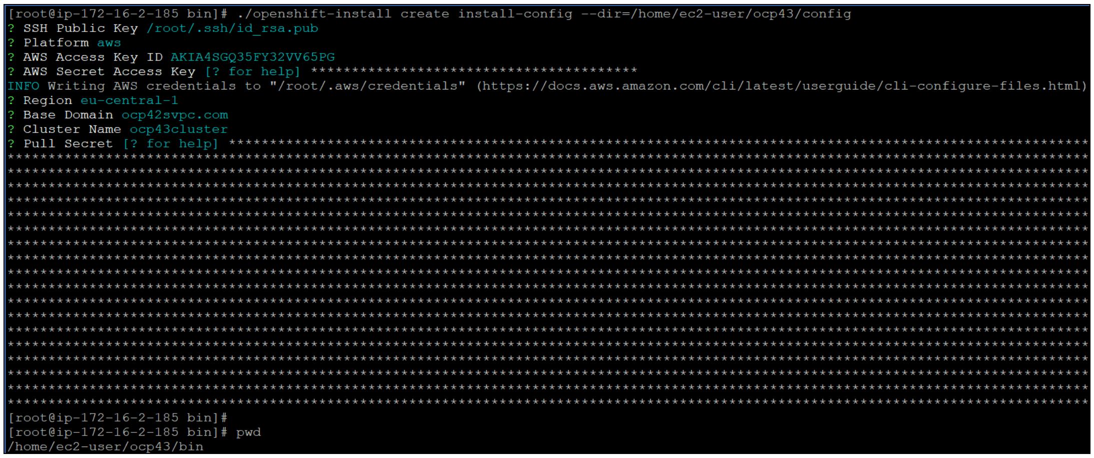
Figure 45   Configuring ssh-agent



```
[root@ip-172-16-2-185 .ssh]# ssh-add /root/.ssh/id_rsa
Identity added: /root/.ssh/id_rsa (/root/.ssh/id_rsa)
[root@ip-172-16-2-185 .ssh]#
```

Figure 46   Configuring SSH

2. Create the installation configuration file and customize the file for installation. The customized cluster is created on the VPC of AWS. A sample `install-config.yaml` file is shown in Figure 47.



```
[root@ip-172-16-2-185 bin]# ./openshift-install create install-config --dir=/home/ec2-user/ocp43/config
? SSH Public Key /root/.ssh/id_rsa.pub
? Platform aws
? AWS Access Key ID AKIA4SGQ35FY32VV65PG
? AWS Secret Access Key [? for help] ****************************************
INFO Writing AWS credentials to "/root/.aws/credentials" (https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html)
? Region eu-central-1
? Base Domain ocp42svpc.com
? Cluster Name ocp43cluster
? Pull Secret [? for help] ********************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
***********************************************************************************************************************************
[root@ip-172-16-2-185 bin]#
[root@ip-172-16-2-185 bin]# pwd
/home/ec2-user/ocp43/bin
```

Figure 47 Custom create install-config.yaml

Consider the following points:

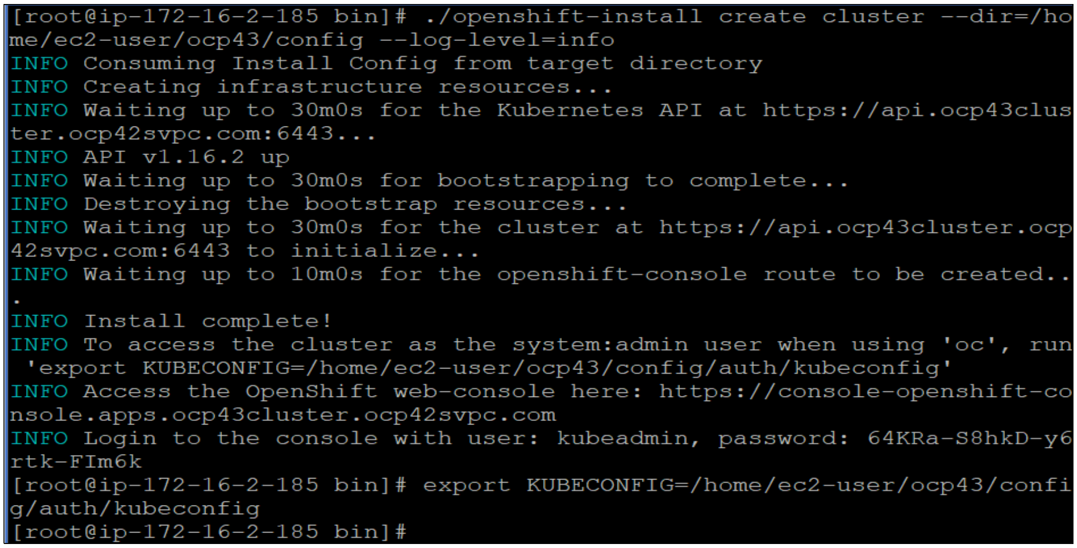
- This sample `install-config.yaml` file is modified per your environment. Ensure that the pull secret and ssh-key is added correctly in the `install-config.yaml` file.
- Use m4.xlarge configuration for worker and master nodes. In this sample, you can use the machine type per your requirement.
- Ensure a suitable subnet ID of the existing VPC for public and private network is included in your `install-config.yaml` file.

The custom configuration file is shown in Figure 48.

```
apiVersion: v1
baseDomain: ocp42svpc.com
controlPlane:
  hyperthreading: Enabled
  name: master
  platform:
    aws:
      zones:
      - eu-central-1a
      rootVolume:
        iops: 2000
        size: 500
        type: io1
      type: m4.xlarge
  replicas: 3
compute:
- hyperthreading: Enabled
  name: worker
  platform:
    aws:
      rootVolume:
        iops: 2000
        size: 500
        type: io1
      type: m4.large
      zones:
      - eu-central-1a
replicas: 3
metadata:
  name: ocp43cluster
networking:
  machineCIDR: 172.16.0.0/16
platform:
  aws:
    region: eu-central-1
    subnets:
    - subnet-0aa84476708f32710
    - subnet-0f173ab757c352b11
pullSecret:
sshKey:
```

Figure 48 Custom configuration file

3. Create the cluster by using the modified `install-config.yaml` file (see Figure 49 on page 32). This cluster is created in your VPC. For more information about VPC requirements, see this web page.

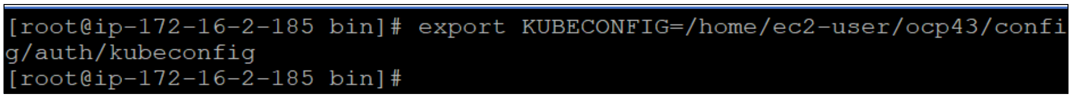


```
[root@ip-172-16-2-185 bin]# ./openshift-install create cluster --dir=/ho
me/ec2-user/ocp43/config --log-level=info
INFO Consuming Install Config from target directory
INFO Creating infrastructure resources...
INFO Waiting up to 30m0s for the Kubernetes API at https://api.ocp43clus
ter.ocp42svpc.com:6443...
INFO API v1.16.2 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO Destroying the bootstrap resources...
INFO Waiting up to 30m0s for the cluster at https://api.ocp43cluster.ocp
42svpc.com:6443 to initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created..
.
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run
 'export KUBECONFIG=/home/ec2-user/ocp43/config/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-co
nsole.apps.ocp43cluster.ocp42svpc.com
INFO Login to the console with user: kubeadmin, password: 64KRa-S8hkD-y6
rtk-FIm6k
[root@ip-172-16-2-185 bin]# export KUBECONFIG=/home/ec2-user/ocp43/confi
g/auth/kubeconfig
[root@ip-172-16-2-185 bin]#
```

Figure 49 Creation of OCP cluster on AWS

4. Check the status of the nodes and cluster with the login and password information that was provided in the command (see Figure 50):

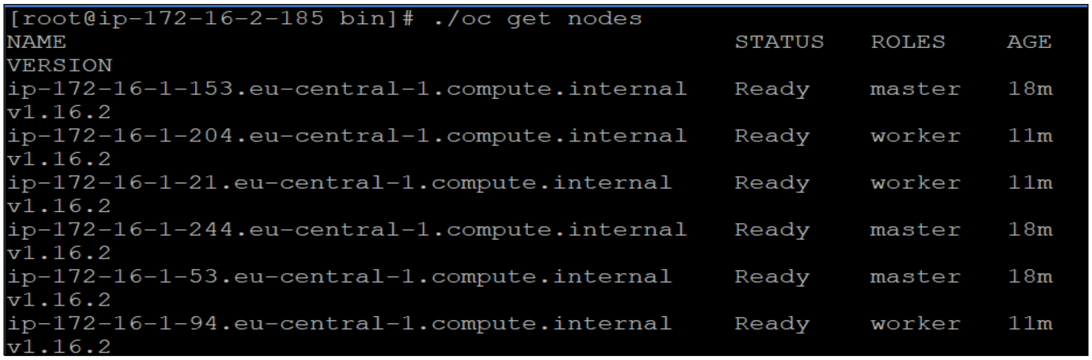
   ```
   Export KUBECONFIG=/home/ec2-user/ocp43/config/ auth/kubeconfig
   ```



```
[root@ip-172-16-2-185 bin]# export KUBECONFIG=/home/ec2-user/ocp43/confi
g/auth/kubeconfig
[root@ip-172-16-2-185 bin]#
```

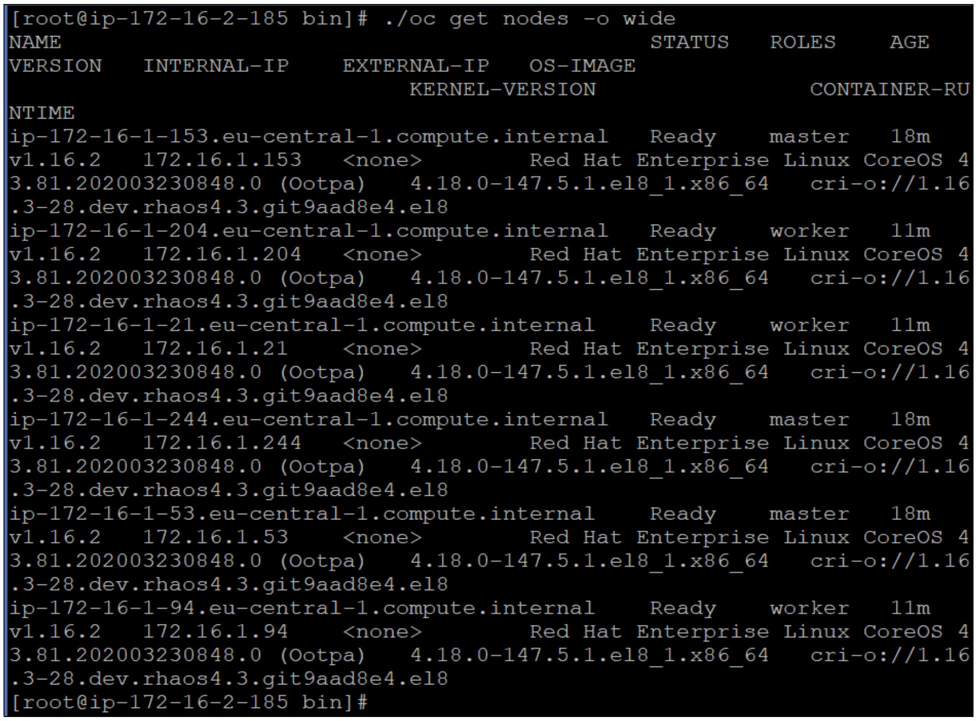
Figure 50 Export kubeconfig

5. Check the status of nodes and cluster (see Figure 51 and Figure 52 on page 33).



```
[root@ip-172-16-2-185 bin]# ./oc get nodes
NAME                                              STATUS    ROLES     AGE
VERSION
ip-172-16-1-153.eu-central-1.compute.internal     Ready     master    18m
v1.16.2
ip-172-16-1-204.eu-central-1.compute.internal     Ready     worker    11m
v1.16.2
ip-172-16-1-21.eu-central-1.compute.internal      Ready     worker    11m
v1.16.2
ip-172-16-1-244.eu-central-1.compute.internal     Ready     master    18m
v1.16.2
ip-172-16-1-53.eu-central-1.compute.internal      Ready     master    18m
v1.16.2
ip-172-16-1-94.eu-central-1.compute.internal      Ready     worker    11m
v1.16.2
```

Figure 51 Nodes status, Part 1



```
[root@ip-172-16-2-185 bin]# ./oc get nodes -o wide
NAME                                            STATUS   ROLES    AGE
VERSION   INTERNAL-IP    EXTERNAL-IP   OS-IMAGE
                              KERNEL-VERSION                CONTAINER-RU
NTIME
ip-172-16-1-153.eu-central-1.compute.internal   Ready    master   18m
v1.16.2   172.16.1.153   <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
ip-172-16-1-204.eu-central-1.compute.internal   Ready    worker   11m
v1.16.2   172.16.1.204   <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
ip-172-16-1-21.eu-central-1.compute.internal    Ready    worker   11m
v1.16.2   172.16.1.21    <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
ip-172-16-1-244.eu-central-1.compute.internal   Ready    master   18m
v1.16.2   172.16.1.244   <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
ip-172-16-1-53.eu-central-1.compute.internal    Ready    master   18m
v1.16.2   172.16.1.53    <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
ip-172-16-1-94.eu-central-1.compute.internal    Ready    worker   11m
v1.16.2   172.16.1.94    <none>        Red Hat Enterprise Linux CoreOS 4
3.81.202003230848.0 (Ootpa)   4.18.0-147.5.1.el8_1.x86_64   cri-o://1.16
.3-28.dev.rhaos4.3.git9aad8e4.el8
[root@ip-172-16-2-185 bin]#
```

Figure 52   Nodes status, Part 2

Installing Red Hat OpenShift 4.x on IBM Cloud

In this section, we describe the process to install Red Hat OpenShift 4.x on IBM Cloud.

Installing Red Hat OpenShift 4.3 on IBM cloud

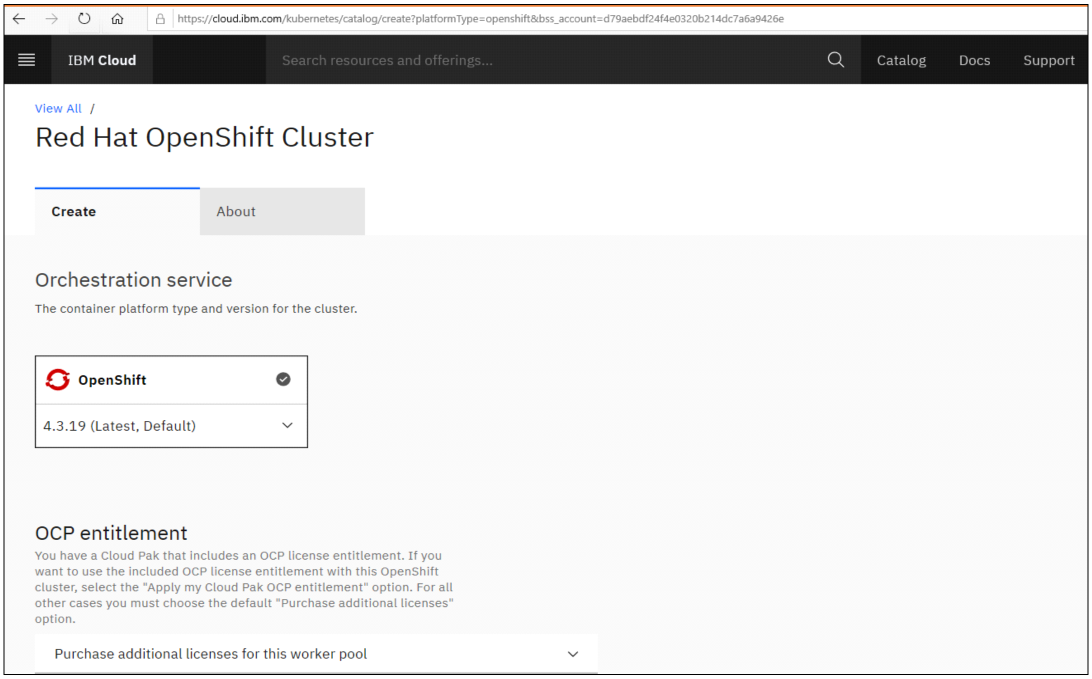
In this demonstration, we use IBM internal paid account process for the deployment of Red Hat OpenShift 4.3 on IBM Cloud.

As a prerequisite, you need the IBM ID for creating the infrastructure components on IBM cloud. If an IBM ID is not available, create an IBM ID.

Log in to the IBM cloud console and create OpenShift cluster on IBM Cloud. For more information about the various options to select during the process of creating OpenShift on IBM cloud, see the IBM Cloud website (login required).

Complete the following steps:

1. Log in with your login ID and search the catalog for OpenShift on IBM Cloud (see Figure 53.



https://cloud.ibm.com/kubernetes/catalog/create?platformType=openshift&bss_account=d79aebdf24f4e0320b214dc7a6a9426e
IBM Cloud
Search resources and offerings...
Catalog
Docs
Support
View All /

Red Hat OpenShift Cluster

Create | About

Orchestration service

The container platform type and version for the cluster.

OpenShift

4.3.19 (Latest, Default)

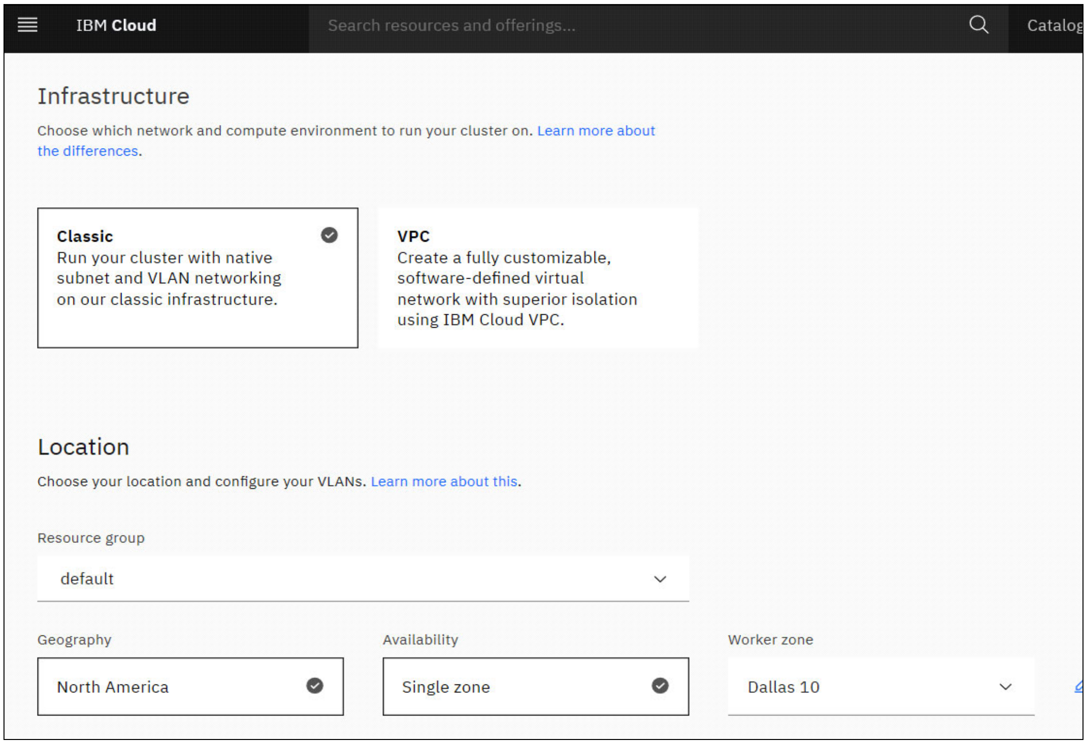
OCP entitlement

You have a Cloud Pak that includes an OCP license entitlement. If you want to use the included OCP license entitlement with this OpenShift cluster, select the "Apply my Cloud Pak OCP entitlement" option. For all other cases you must choose the default "Purchase additional licenses" option.

Purchase additional licenses for this worker pool

Figure 53 Log in to IBM Cloud

2. Select **Classic** infrastructure and select the Geography and Worker zone per your requirement (see Figure 54).



Infrastructure

Choose which network and compute environment to run your cluster on. Learn more about the differences.

Classic ● Run your cluster with native subnet and VLAN networking on our classic infrastructure.

VPC Create a fully customizable, software-defined virtual network with superior isolation using IBM Cloud VPC.

Location

Choose your location and configure your VLANs. Learn more about this.

Resource group: default

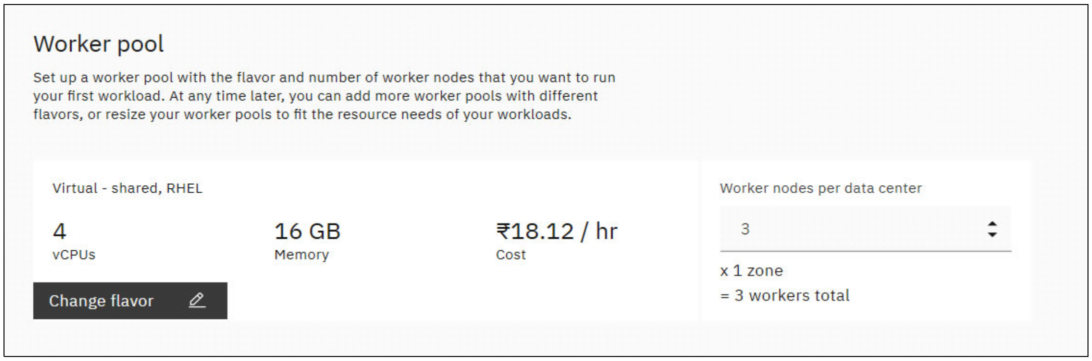
Geography: North America

Availability: Single zone

Worker zone: Dallas 10

Figure 54 Select geography and zone

3. Select the number of workers (see Figure 55).



Worker pool

Set up a worker pool with the flavor and number of worker nodes that you want to run your first workload. At any time later, you can add more worker pools with different flavors, or resize your worker pools to fit the resource needs of your workloads.

Virtual - shared, RHEL

4 vCPUs

16 GB Memory

₹18.12 / hr Cost

Worker nodes per data center: 3

x 1 zone

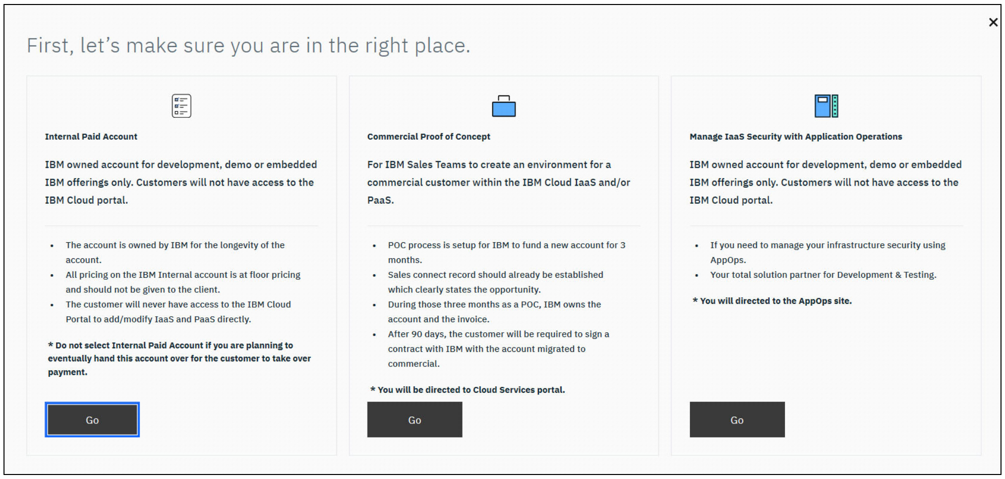
= 3 workers total

Figure 55 Select the number of workers

4. Select **Upgrade** to create the cluster.

   This cluster is your first cluster. Resources that are created on IBM Cloud in the next window display the type “Internal paid account, commercial proof of concept, Manage IAAS security with application operations”.

5. Select **Go** under Internal Paid Account (see Figure 56).



First, let’s make sure you are in the right place.

Internal Paid Account

IBM owned account for development, demo or embedded IBM offerings only. Customers will not have access to the IBM Cloud portal.

- The account is owned by IBM for the longevity of the account.
- All pricing on the IBM Internal account is at floor pricing and should not be given to the client.
- The customer will never have access to the IBM Cloud Portal to add/modify IaaS and PaaS directly.

*** Do not select Internal Paid Account if you are planning to eventually hand this account over for the customer to take over payment.**

Commercial Proof of Concept

For IBM Sales Teams to create an environment for a commercial customer within the IBM Cloud IaaS and/or PaaS.

- POC process is setup for IBM to fund a new account for 3 months.
- Sales connect record should already be established which clearly states the opportunity.
- During those three months as a POC, IBM owns the account and the invoice.
- After 90 days, the customer will be required to sign a contract with IBM with the account migrated to commercial.

*** You will be directed to Cloud Services portal.**

Manage IaaS Security with Application Operations

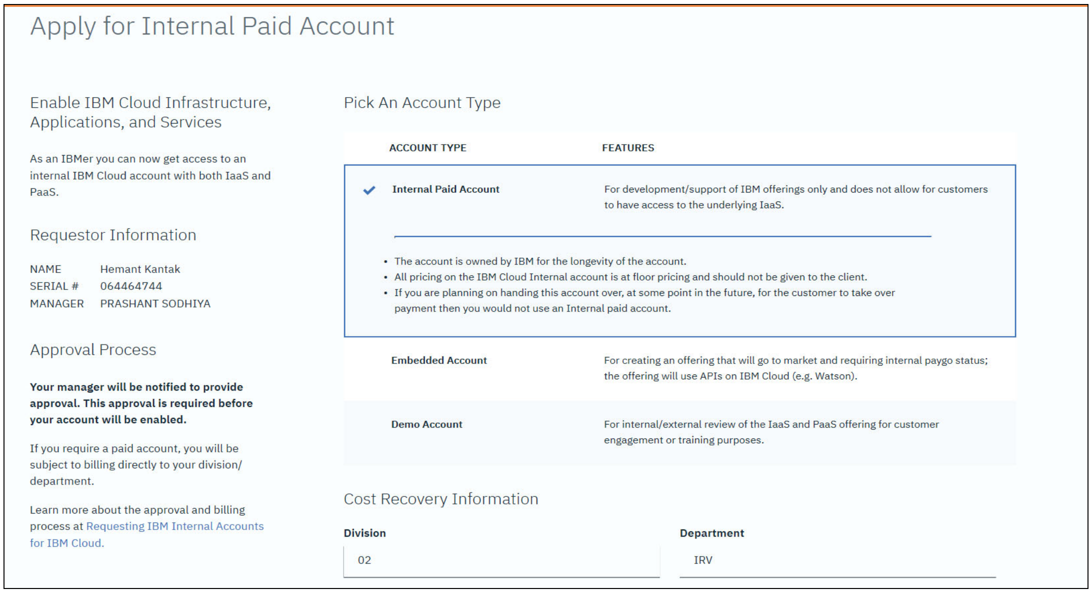
IBM owned account for development, demo or embedded IBM offerings only. Customers will not have access to the IBM Cloud portal.

- If you need to manage your infrastructure security using AppOps.
- Your total solution partner for Development & Testing.

*** You will directed to the AppOps site.**

Figure 56 Select internal paid account

6. Confirm that the Internal Paid Account option is selected (see Figure 57).



Apply for Internal Paid Account

Enable IBM Cloud Infrastructure, Applications, and Services

As an IBMer you can now get access to an internal IBM Cloud account with both IaaS and PaaS.

Requestor Information

NAME	Hemant Kantak
SERIAL #	064464744
MANAGER	PRASHANT SODHIYA

Approval Process

Your manager will be notified to provide approval. This approval is required before your account will be enabled.

If you require a paid account, you will be subject to billing directly to your division/ department.

Learn more about the approval and billing process at Requesting IBM Internal Accounts for IBM Cloud.

Pick An Account Type

ACCOUNT TYPE	FEATURES
✓ Internal Paid Account	For development/support of IBM offerings only and does not allow for customers to have access to the underlying IaaS.
Embedded Account	For creating an offering that will go to market and requiring internal paygo status; the offering will use APIs on IBM Cloud (e.g. Watson).
Demo Account	For internal/external review of the IaaS and PaaS offering for customer engagement or training purposes.

- The account is owned by IBM for the longevity of the account.
- All pricing on the IBM Cloud Internal account is at floor pricing and should not be given to the client.
- If you are planning on handing this account over, at some point in the future, for the customer to take over payment then you would not use an Internal paid account.

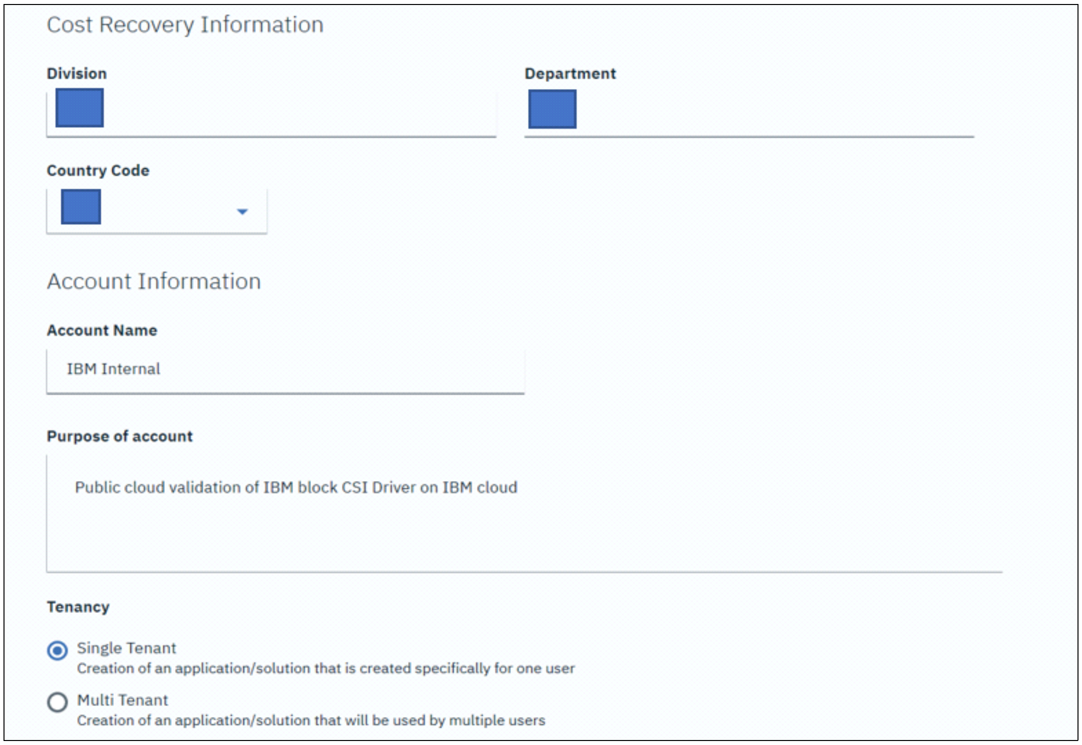
Cost Recovery Information

Division: 02

Department: IRV

Figure 57 Apply for Internal Paid Account window

7. Complete the form in the Cost Recovery Information window and select the **Single Tenant** option at the bottom of the window (see Figure 58).



Cost Recovery Information

Division: [redacted]

Department: [redacted]

Country Code: [redacted]

Account Information

Account Name: IBM Internal

Purpose of account: Public cloud validation of IBM block CSI Driver on IBM cloud

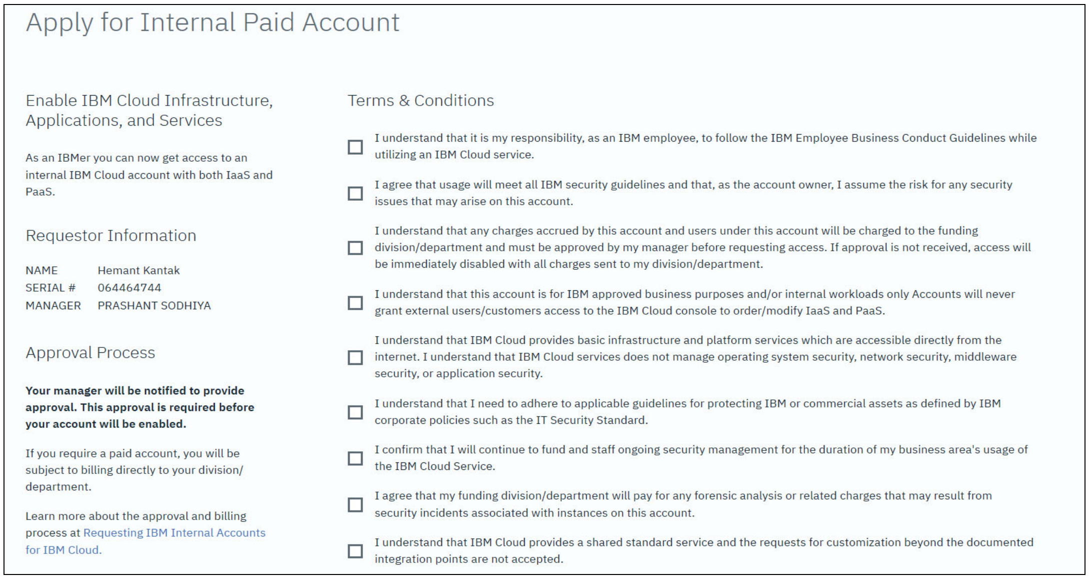
Tenancy

● Single Tenant
Creation of an application/solution that is created specifically for one user

○ Multi Tenant
Creation of an application/solution that will be used by multiple users

Figure 58 Cost Recovery Information window

8. Accept the terms and conditions (see Figure 59).



Apply for Internal Paid Account

Enable IBM Cloud Infrastructure, Applications, and Services

As an IBMer you can now get access to an internal IBM Cloud account with both IaaS and PaaS.

Requestor Information

NAME	Hemant Kantak
SERIAL #	064464744
MANAGER	PRASHANT SODHIYA

Approval Process

Your manager will be notified to provide approval. This approval is required before your account will be enabled.

If you require a paid account, you will be subject to billing directly to your division/ department.

Learn more about the approval and billing process at Requesting IBM Internal Accounts for IBM Cloud.

Terms & Conditions

□ I understand that it is my responsibility, as an IBM employee, to follow the IBM Employee Business Conduct Guidelines while utilizing an IBM Cloud service.

□ I agree that usage will meet all IBM security guidelines and that, as the account owner, I assume the risk for any security issues that may arise on this account.

□ I understand that any charges accrued by this account and users under this account will be charged to the funding division/department and must be approved by my manager before requesting access. If approval is not received, access will be immediately disabled with all charges sent to my division/department.

□ I understand that this account is for IBM approved business purposes and/or internal workloads only Accounts will never grant external users/customers access to the IBM Cloud console to order/modify IaaS and PaaS.

□ I understand that IBM Cloud provides basic infrastructure and platform services which are accessible directly from the internet. I understand that IBM Cloud services does not manage operating system security, network security, middleware security, or application security.

□ I understand that I need to adhere to applicable guidelines for protecting IBM or commercial assets as defined by IBM corporate policies such as the IT Security Standard.

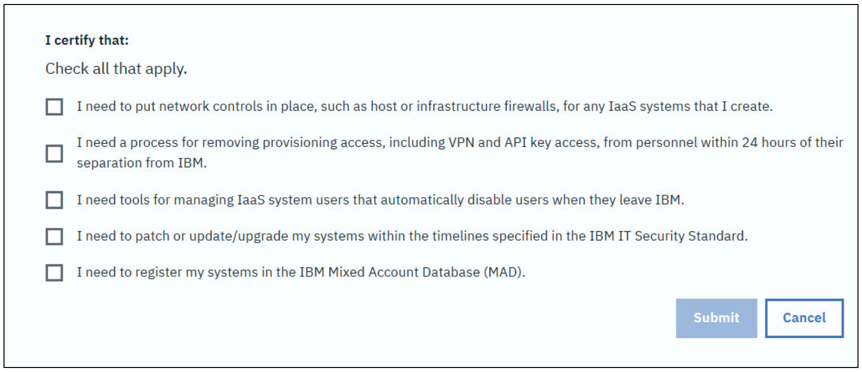
□ I confirm that I will continue to fund and staff ongoing security management for the duration of my business area's usage of the IBM Cloud Service.

□ I agree that my funding division/department will pay for any forensic analysis or related charges that may result from security incidents associated with instances on this account.

□ I understand that IBM Cloud provides a shared standard service and the requests for customization beyond the documented integration points are not accepted.

Figure 59 Terms and Conditions window

9. Select all applicable certifications in the Certify window (see Figure 60).



I certify that:

Check all that apply.

□ I need to put network controls in place, such as host or infrastructure firewalls, for any IaaS systems that I create.

□ I need a process for removing provisioning access, including VPN and API key access, from personnel within 24 hours of their separation from IBM.

□ I need tools for managing IaaS system users that automatically disable users when they leave IBM.

□ I need to patch or update/upgrade my systems within the timelines specified in the IBM IT Security Standard.

□ I need to register my systems in the IBM Mixed Account Database (MAD).

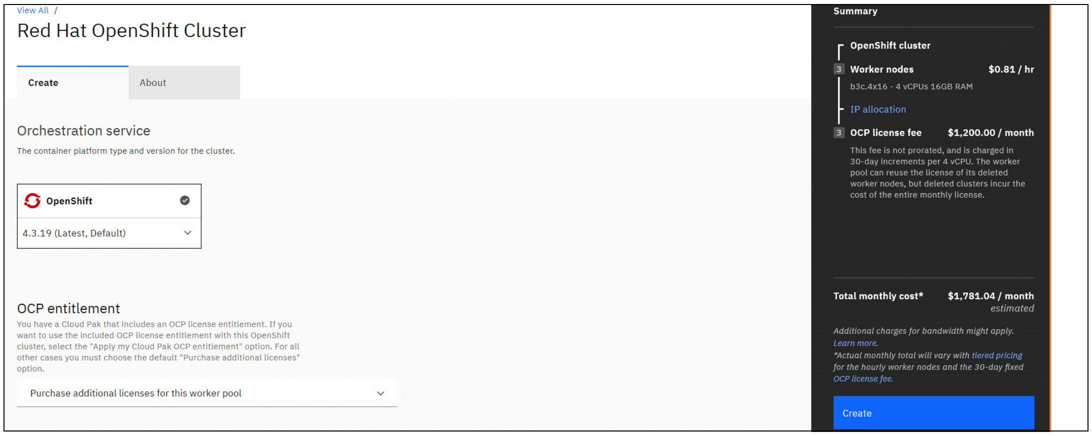
Figure 60 Certify window

10. Click **Submit**.

The request is created, and it is routed to your manager for approval.

After the manager approves the request, your IBM cloud ID is created, and you receive an email from IBM Cloud.

11. Log in with your IBM ID and create an OpenShift Cluster on IBM Cloud. Various options to create the OpenShift cluster on IBM Cloud, as shown in Figure 61, Figure 62, and Figure 63 on page 39. Make the suitable selections.



Red Hat OpenShift Cluster

Orchestration service

The container platform type and version for the cluster.

OpenShift

4.3.19 (Latest, Default)

OCP entitlement

You have a Cloud Pak that includes an OCP license entitlement. If you want to use the included OCP license entitlement with this OpenShift cluster, select the "Apply my Cloud Pak OCP entitlement" option. For all other cases you must choose the default "Purchase additional licenses" option.

Purchase additional licenses for this worker pool

Summary

OpenShift cluster

3 Worker nodes $0.81 / hr

b3c.4x16 - 4 vCPUs 16GB RAM

IP allocation

3 OCP license fee $1,200.00 / month

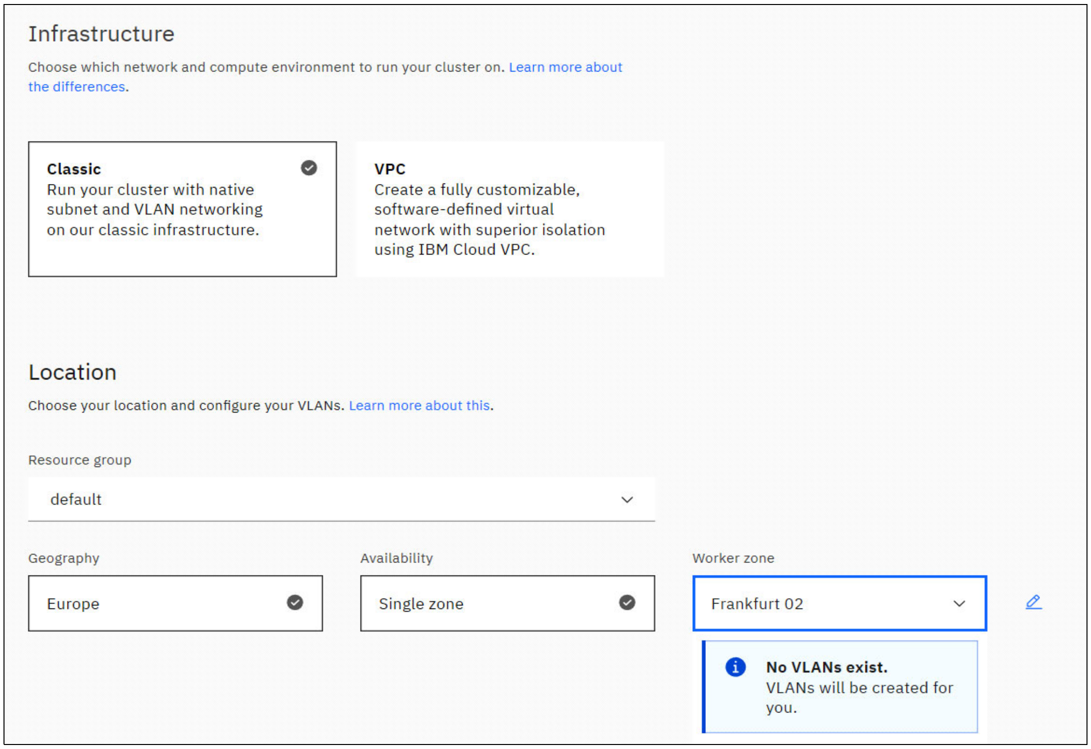
This fee is not prorated, and is charged in 30-day increments per 4 vCPU. The worker pool can reuse the license of its deleted worker nodes, but deleted clusters incur the cost of the entire monthly license.

Total monthly cost* $1,781.04 / month *estimated*

Additional charges for bandwidth might apply. Learn more.

**Actual monthly total will vary with tiered pricing for the hourly worker nodes and the 30-day fixed OCP license fee.*

Figure 61 Create OCP cluster



Infrastructure

Choose which network and compute environment to run your cluster on. Learn more about the differences.

Classic ✓
Run your cluster with native subnet and VLAN networking on our classic infrastructure.

VPC
Create a fully customizable, software-defined virtual network with superior isolation using IBM Cloud VPC.

Location

Choose your location and configure your VLANs. Learn more about this.

Resource group: default

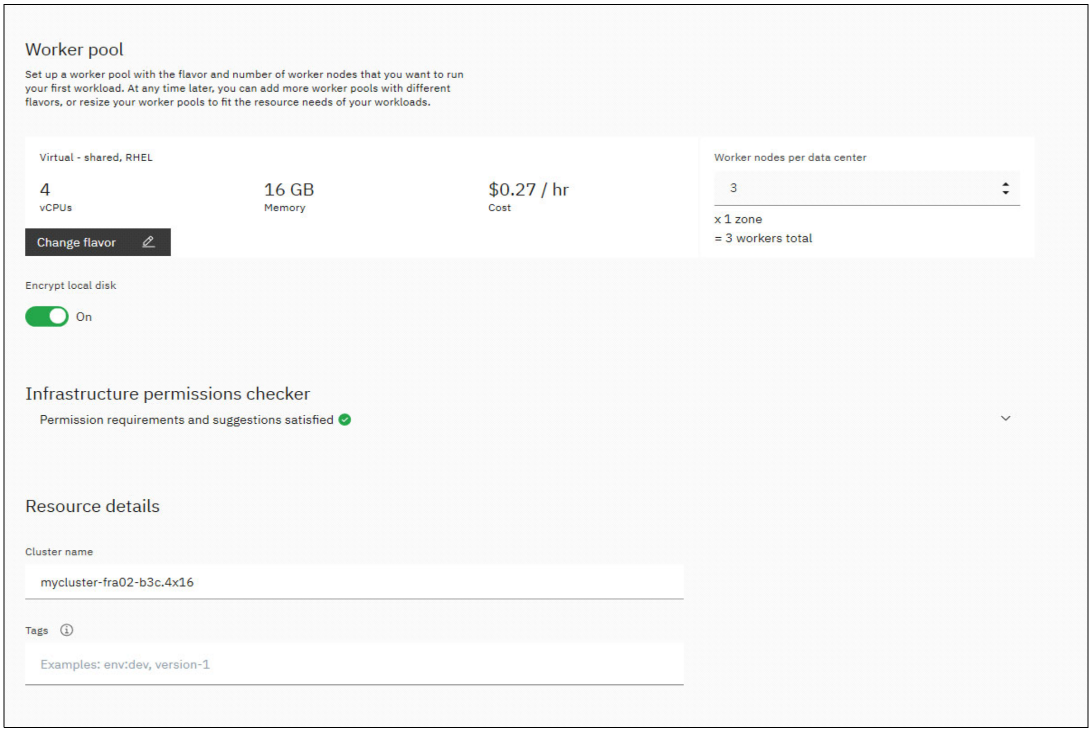
Geography: Europe ✓

Availability: Single zone ✓

Worker zone: Frankfurt 02

No VLANs exist.
VLANs will be created for you.

Figure 62 Infrastructure window



Worker pool

Set up a worker pool with the flavor and number of worker nodes that you want to run your first workload. At any time later, you can add more worker pools with different flavors, or resize your worker pools to fit the resource needs of your workloads.

Virtual - shared, RHEL

4 vCPUs

16 GB Memory

$0.27 / hr Cost

Worker nodes per data center: 3

x 1 zone
= 3 workers total

Encrypt local disk: On

Infrastructure permissions checker

Permission requirements and suggestions satisfied

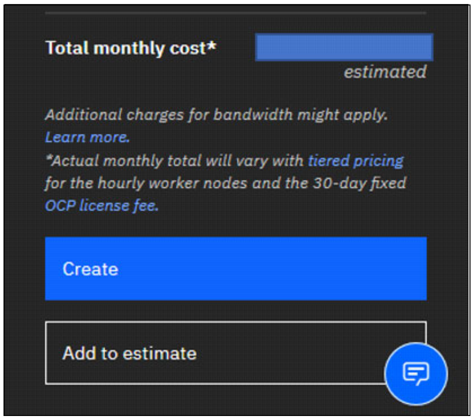
Resource details

Cluster name: mycluster-fra02-b3c.4x16

Tags: Examples: env:dev, version-1

Figure 63 Create OCP cluster

12. Click **Create Cluster** (see Figure 64).



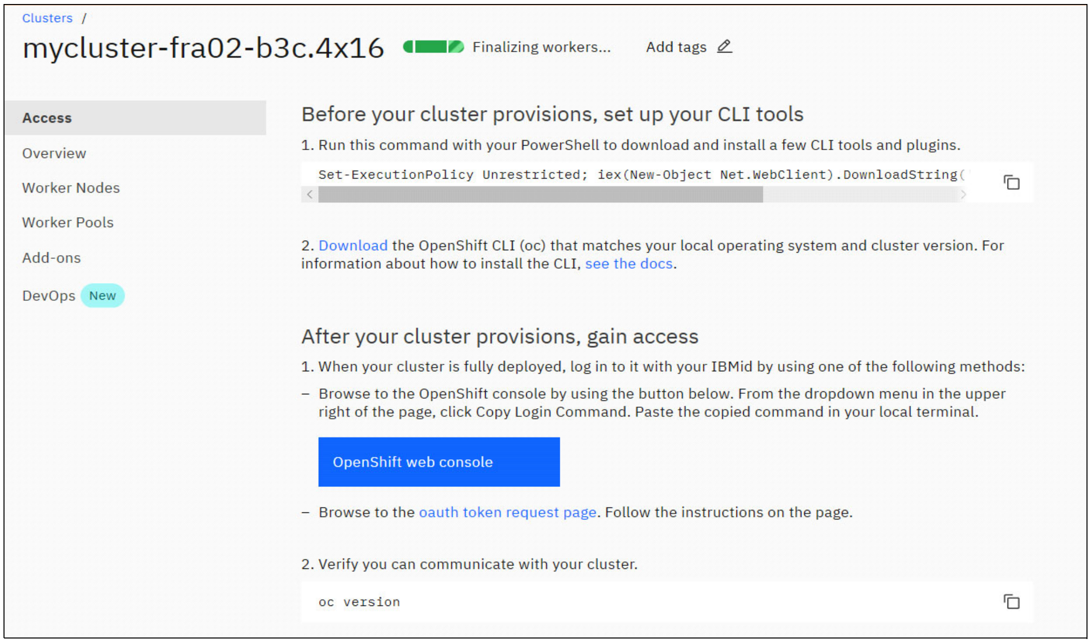
Total monthly cost* [redacted]
estimated

Additional charges for bandwidth might apply. Learn more.

**Actual monthly total will vary with tiered pricing for the hourly worker nodes and the 30-day fixed OCP license fee.*

Figure 64 Selecting Create option

The cluster deployment process starts. You can monitor the status of process, as shown in Figure 65 on page 40, Figure 66 on page 40, Figure 67 on page 40, and Figure 68 on page 41.



Before your cluster provisions, set up your CLI tools

1. Run this command with your PowerShell to download and install a few CLI tools and plugins.

```
Set-ExecutionPolicy Unrestricted; iex(New-Object Net.WebClient).DownloadString(
```

2. Download the OpenShift CLI (oc) that matches your local operating system and cluster version. For information about how to install the CLI, see the docs.

After your cluster provisions, gain access

1. When your cluster is fully deployed, log in to it with your IBMid by using one of the following methods:

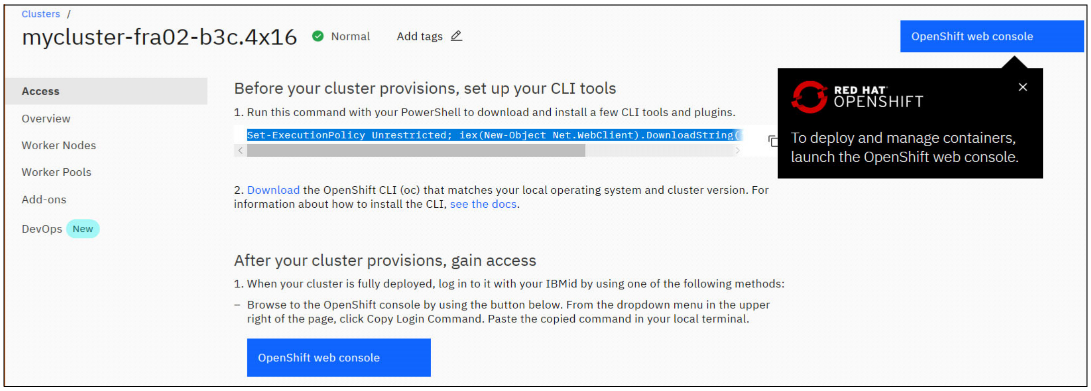
– Browse to the OpenShift console by using the button below. From the dropdown menu in the upper right of the page, click Copy Login Command. Paste the copied command in your local terminal.

– Browse to the oauth token request page. Follow the instructions on the page.

2. Verify you can communicate with your cluster.

```
oc version
```

Figure 65 Setting up CLI tools



To deploy and manage containers, launch the OpenShift web console.

Before your cluster provisions, set up your CLI tools

1. Run this command with your PowerShell to download and install a few CLI tools and plugins.

```
Set-ExecutionPolicy Unrestricted; iex(New-Object Net.WebClient).DownloadString(
```

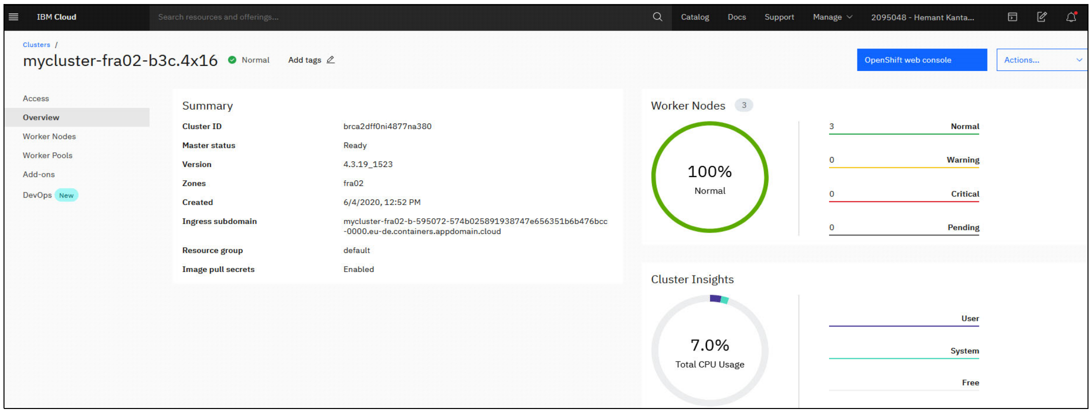
2. Download the OpenShift CLI (oc) that matches your local operating system and cluster version. For information about how to install the CLI, see the docs.

After your cluster provisions, gain access

1. When your cluster is fully deployed, log in to it with your IBMid by using one of the following methods:

– Browse to the OpenShift console by using the button below. From the dropdown menu in the upper right of the page, click Copy Login Command. Paste the copied command in your local terminal.

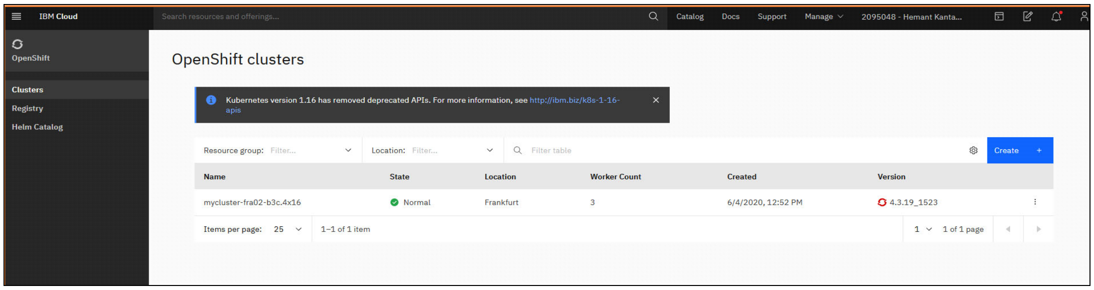
Figure 66 OpenShift web console option



Summary

Cluster ID	brca2dff0ni4877na380
Master status	Ready
Version	4.3.19_1523
Zones	fra02
Created	6/4/2020, 12:52 PM
Ingress subdomain	mycluster-fra02-b-595072-574b025891938747e656351b6b476bcc-0000.eu-de.containers.appdomain.cloud
Resource group	default
Image pull secrets	Enabled

Figure 67 Overview window



OpenShift clusters

Kubernetes version 1.16 has removed deprecated APIs. For more information, see http://ibm.biz/k8s-1-16-apis

Resource group: Filter... Location: Filter... Filter table Create +

Name	State	Location	Worker Count	Created	Version
mycluster-fra02-b3c.4x16	Normal	Frankfurt	3	6/4/2020, 12:52 PM	4.3.19_1523

Items per page: 25 1–1 of 1 item 1 1 of 1 page

Figure 68 OpenShift cluster created

Logging in to OCP console with GUI and CLI

Click the **Actions** icon (see Figure 69) and log in to the OpenShift Web console.

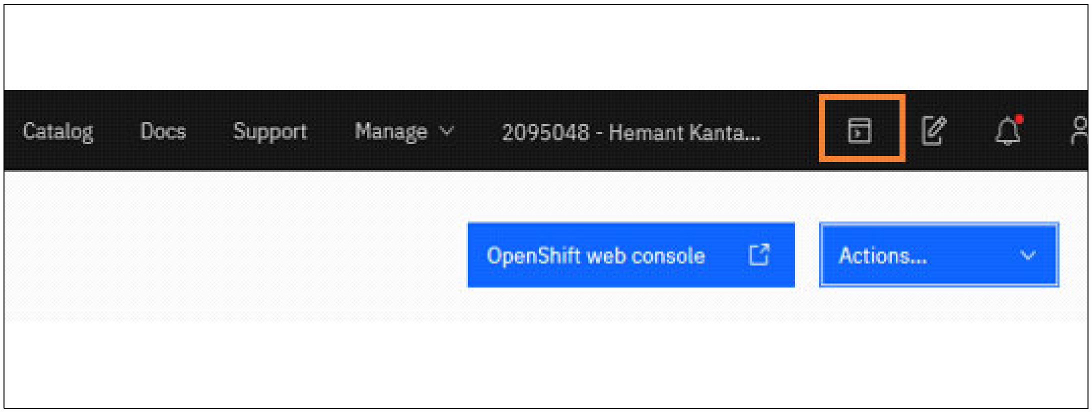
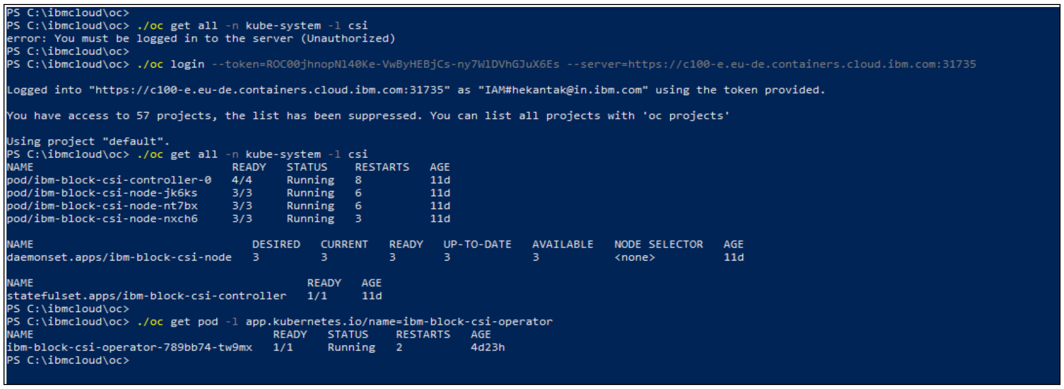


Figure 69 IBM shell icon

You can also log in by using the CLI with the IBM Beta shell, which is available on the IBM console to access and manage the cluster nodes by using **`oc`** and **`kubectl`** commands.

You can also log in by using the CLI from your windows system by way of PowerShell. Complete the following steps:

1. Log in to IBM Cloud console select the OpenShift cluster. Then, click **Action** → **drop down** → **Connect via cli** (follow the prompts that are shown get the auth token request page) → **display token** to log in by using the **`cli`** command.



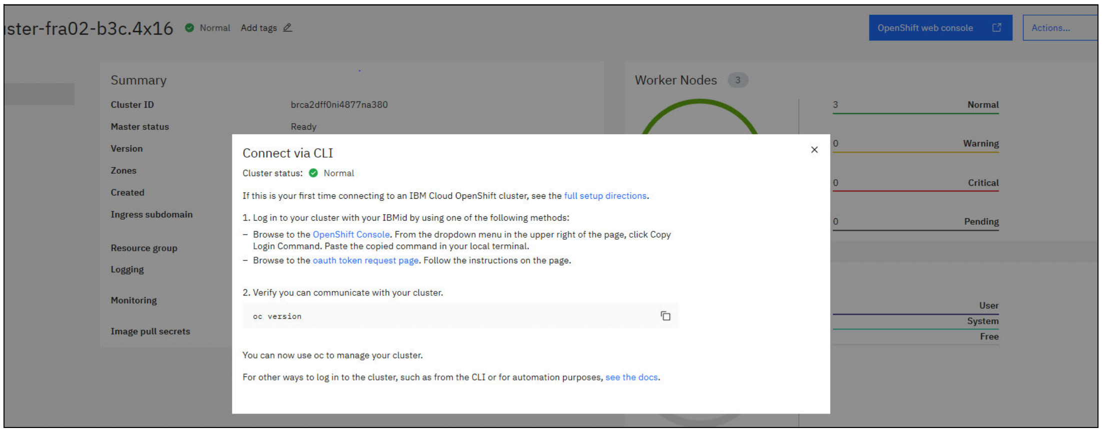
```
PS C:\ibmcloud\oc>
PS C:\ibmcloud\oc> ./oc get all -n kube-system -l csi
error: You must be logged in to the server (Unauthorized)
PS C:\ibmcloud\oc>
PS C:\ibmcloud\oc> ./oc login --token=ROC00jhnopN140Ke-VwByHEBjCs-ny7W1DVhGJuX6Es --server=https://c100-e.eu-de.containers.cloud.ibm.com:31735

Logged into "https://c100-e.eu-de.containers.cloud.ibm.com:31735" as "IAM#hekantak@in.ibm.com" using the token provided.

You have access to 57 projects, the list has been suppressed. You can list all projects with 'oc projects'

Using project "default".
PS C:\ibmcloud\oc> ./oc get all -n kube-system -l csi
NAME                             READY   STATUS    RESTARTS   AGE
pod/ibm-block-csi-controller-0   4/4     Running   8          11d
pod/ibm-block-csi-node-jk6ks     3/3     Running   6          11d
pod/ibm-block-csi-node-nt7bx     3/3     Running   6          11d
pod/ibm-block-csi-node-nxch6     3/3     Running   3          11d

NAME                                DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
daemonset.apps/ibm-block-csi-node   3         3         3       3            3           <none>          11d

NAME                                        READY   AGE
statefulset.apps/ibm-block-csi-controller   1/1     11d
PS C:\ibmcloud\oc>
PS C:\ibmcloud\oc> ./oc get pod -l app.kubernetes.io/name=ibm-block-csi-operator
NAME                                   READY   STATUS    RESTARTS   AGE
ibm-block-csi-operator-789bb74-tw9mx   1/1     Running   2          4d23h
PS C:\ibmcloud\oc>
```

Figure 70 Pod status and OC login

You cannot log in to the OpenShift cluster nodes from the Public IP because login/SSH is restricted. If you must log in to OCP cluster nodes, you must enable root login on the OCP cluster nodes.

Log a case with IBM cloud team, and enable SSH and root log in to cluster nodes. Then, you can log in to the OCP cluster nodes with the Private IP segment.

2. Create a VPN user and enable VPN access for the user and the required data center. Log in to the VPN. After the VPN is enabled, you can log in to the OCP cluster nodes with a private IP.
3. Log in to the OCP cluster nodes by using the username `root` and the password `password` (log in credentials are available in IBM Cloud console/devices.)
4. In the IBM Cloud console, select the OpenShift cluster and then, **Action** → **drop down** → **Connect via cli** (follow the prompts in the window to get the auth token request page) → **display token** to log in by using the **`cli`** command (see Figure 71).



Cluster ID brca2dff0ni4877na380

Master status Ready

Version

Zones

Created

Ingress subdomain

Resource group

Logging

Monitoring

Image pull secrets

Connect via CLI

Cluster status: Normal

If this is your first time connecting to an IBM Cloud OpenShift cluster, see the full setup directions.

1. Log in to your cluster with your IBMid by using one of the following methods:

- Browse to the OpenShift Console. From the dropdown menu in the upper right of the page, click Copy Login Command. Paste the copied command in your local terminal.
- Browse to the oauth token request page. Follow the instructions on the page.

2. Verify you can communicate with your cluster.

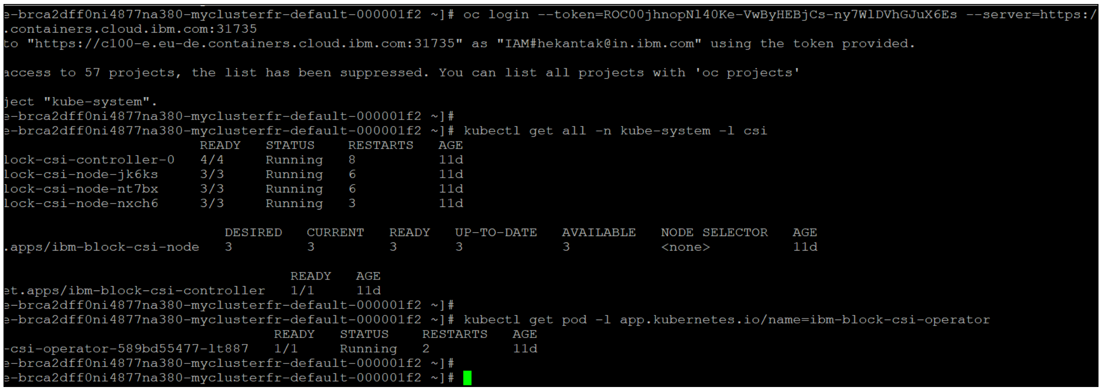
```
oc version
```

You can now use oc to manage your cluster.

For other ways to log in to the cluster, such as from the CLI or for automation purposes, see the docs.

Figure 71 Connecting by using the CLI

5. Check the status of cluster and PODs by using the **oc** commands (see Figure 72).



```
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]# oc login --token=ROC00jhnopNl40Ke-VwByHEBjCs-ny7WlDVhGJuX6Es --server=https:/
.containers.cloud.ibm.com:31735
to "https://c100-e.eu-de.containers.cloud.ibm.com:31735" as "IAM#hekantak@in.ibm.com" using the token provided.

access to 57 projects, the list has been suppressed. You can list all projects with 'oc projects'

ject "kube-system".
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]#
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]# kubectl get all -n kube-system -l csi
                        READY   STATUS    RESTARTS   AGE
lock-csi-controller-0   4/4     Running   8          11d
lock-csi-node-jk6ks     3/3     Running   6          11d
lock-csi-node-nt7bx     3/3     Running   6          11d
lock-csi-node-nxch6     3/3     Running   3          11d

                           DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
.apps/ibm-block-csi-node   3         3         3       3            3           <none>          11d

                                   READY   AGE
et.apps/ibm-block-csi-controller   1/1     11d
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]#
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]# kubectl get pod -l app.kubernetes.io/name=ibm-block-csi-operator
                                 READY   STATUS    RESTARTS   AGE
-csi-operator-589bd55477-lt887   1/1     Running   2          11d
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]#
e-brca2dff0ni4877na380-myclusterfr-default-000001f2 ~]#
```

Figure 72 POD status

For more information about installing IBM block Storage CSI driver, see “Deploying the CSI driver on OCP” on page 27.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Redbooks (logo) ®
IBM®
IBM Cloud®
IBM Spectrum®
IBM Spectrum Storage™
IBM Z®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

July 2020

ISBN 0738459046

REDP-5606-00