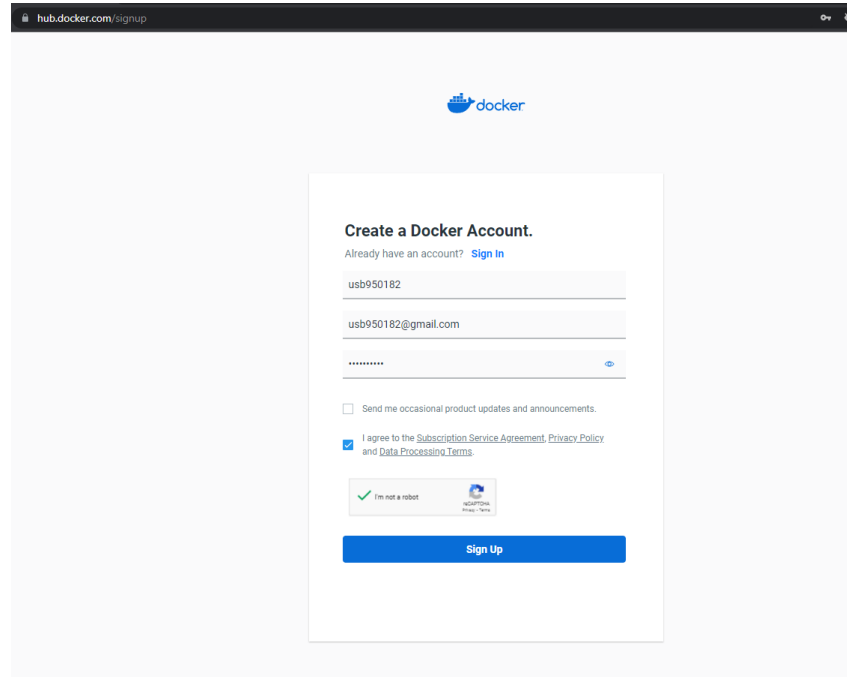


Setup/Installation Instructions

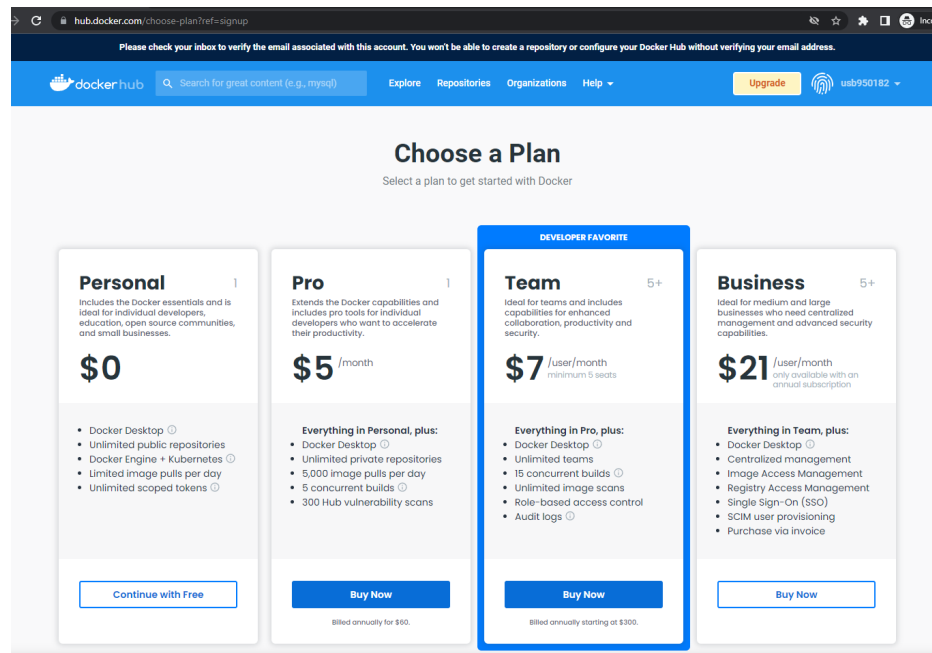
I. Dockerhub Setup

A. Signup for a docker account at: <https://hub.docker.com/>



The screenshot shows the Docker Hub signup page. At the top, there's a navigation bar with the Docker logo and the text "hub.docker.com/signup". Below this, the main heading is "Create a Docker Account." with a link "Already have an account? Sign In". The form contains fields for a username (usb950182), email (usb950182@gmail.com), and a password (masked with asterisks). There are checkboxes for "Send me occasional product updates and announcements." and "I agree to the Subscription Service Agreement, Privacy Policy and Data Processing Terms." (checked). A "Sign Up" button is at the bottom.

B. Continue with the free tier

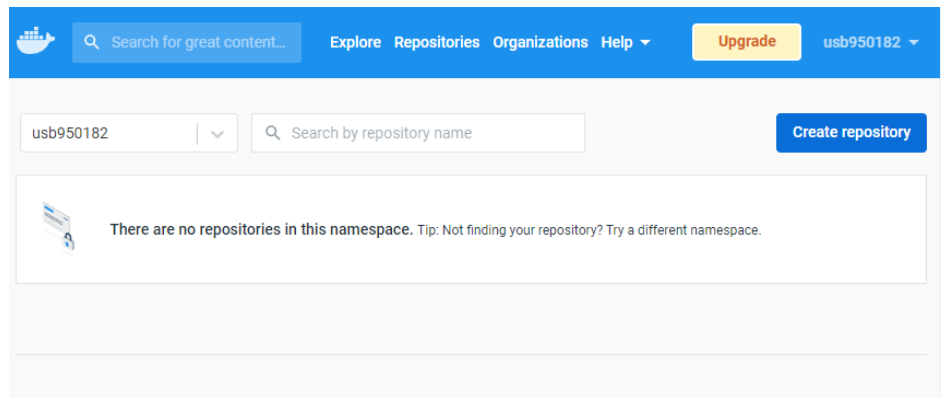


The screenshot shows the "Choose a Plan" page on Docker Hub. The header includes a navigation bar with the Docker Hub logo, a search bar, and links for Explore, Repositories, Organizations, and Help. A banner at the top says "Please check your inbox to verify the email associated with this account. You won't be able to create a repository or configure your Docker Hub without verifying your email address." Below this, the "Choose a Plan" section is displayed with four options: Personal (\$0), Pro (\$5/month), Team (\$7/user/month), and Business (\$21/user/month). The Team plan is highlighted as the "DEVELOPER FAVORITE". Each plan lists its features and includes a "Buy Now" button. The Personal plan has a "Continue with Free" button.

Plan	Price	Features	Button
Personal	\$0	Docker Desktop, Unlimited public repositories, Docker Engine + Kubernetes, Limited image pulls per day, Unlimited scoped tokens	Continue with Free
Pro	\$5/month	Everything in Personal, plus: Docker Desktop, Unlimited private repositories, 5,000 image pulls per day, 5 concurrent builds, 300 Hub vulnerability scans	Buy Now
Team	\$7/user/month	Everything in Pro, plus: Docker Desktop, Unlimited teams, 15 concurrent builds, Unlimited image scans, Role-based access control, Audit logs	Buy Now
Business	\$21/user/month	Everything in Team, plus: Docker Desktop, Centralized management, Image Access Management, Registry Access Management, Single Sign-On (SSO), SCIM user provisioning, Purchase via invoice	Buy Now

C. Verify your email address

D. Create a Dockerhub repository

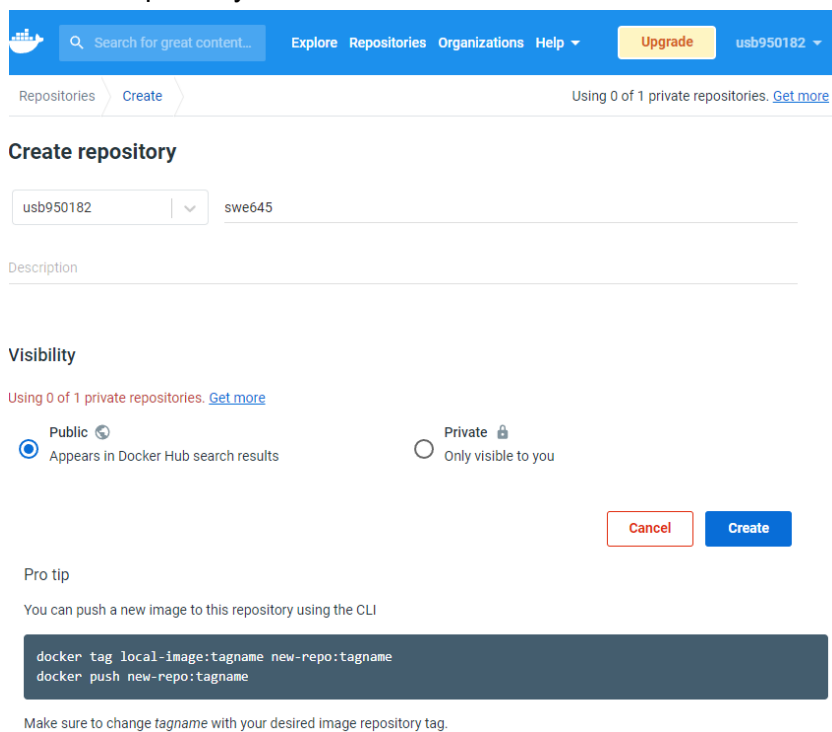


usb950182 | Search for great content... Explore Repositories Organizations Help Upgrade usb950182

usb950182 | Search by repository name Create repository

There are no repositories in this namespace. Tip: Not finding your repository? Try a different namespace.

E. Enter a Repository name



usb950182 | Search for great content... Explore Repositories Organizations Help Upgrade usb950182

Repositories Create Using 0 of 1 private repositories. [Get more](#)


Create repository


usb950182 | swe645

Description

Visibility

Using 0 of 1 private repositories. [Get more](#)

☒ Public  Appears in Docker Hub search results

☐ Private  Only visible to you

Cancel Create

Pro tip

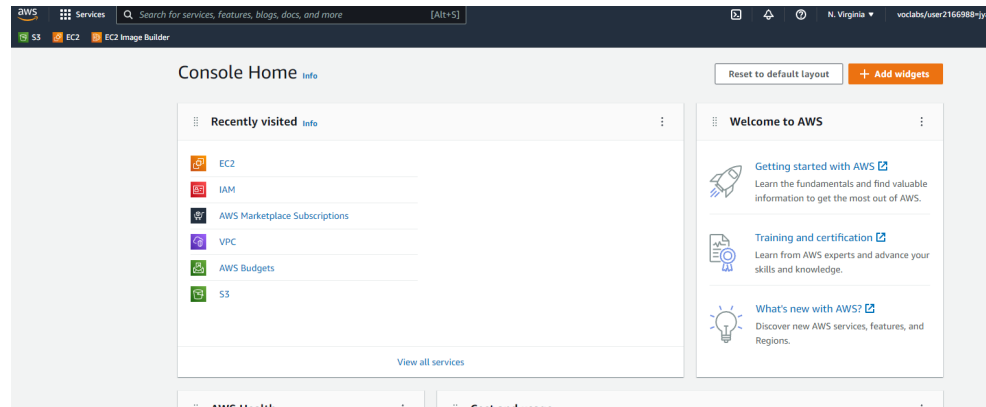
You can push a new image to this repository using the CLI

```
docker tag local-image:tagname new-repo:tagname
docker push new-repo:tagname
```

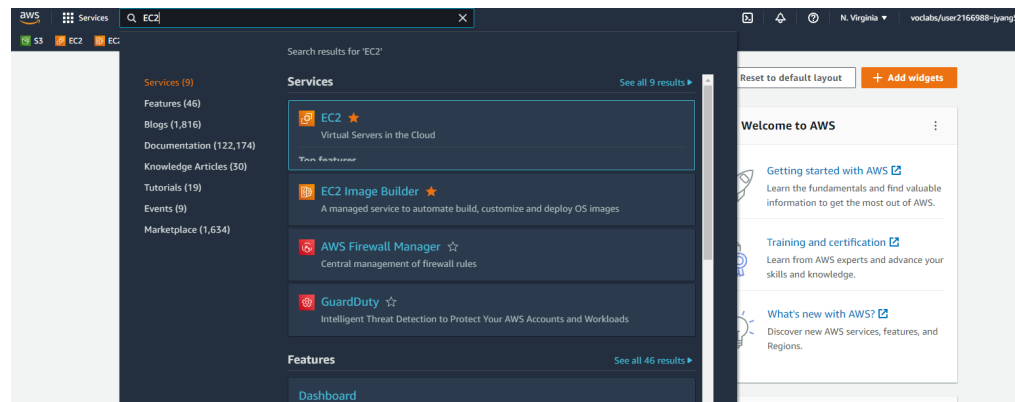
Make sure to change *tagname* with your desired image repository tag.

II. EC2 Instance Setup

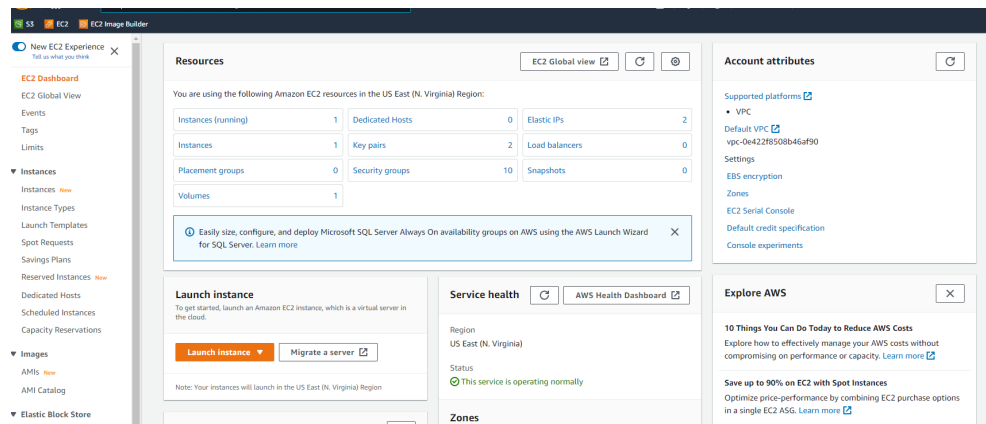
A. Log in to the AWS console



B. Search for and select "EC2" in the search bar



C. Select the Launch Instance button



D. Create the Instance

1. Enter a name

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

Jenkins

Add additional tags

2. Select Ubuntu Server 20.04 LTS (HVM)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

S

>

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-0149b2da6ceec4bb0 (64-bit (x86)) / ami-00266f51b6b22db58 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 20.04 LTS, amd64 focal image build on 2022-09-14

Architecture

AMI ID

64-bit (x86)

ami-0149b2da6ceec4bb0

Verified provider

3. Select the "t2.medium" instance type

▼ Instance type [Info](#)

Instance type

t2.medium

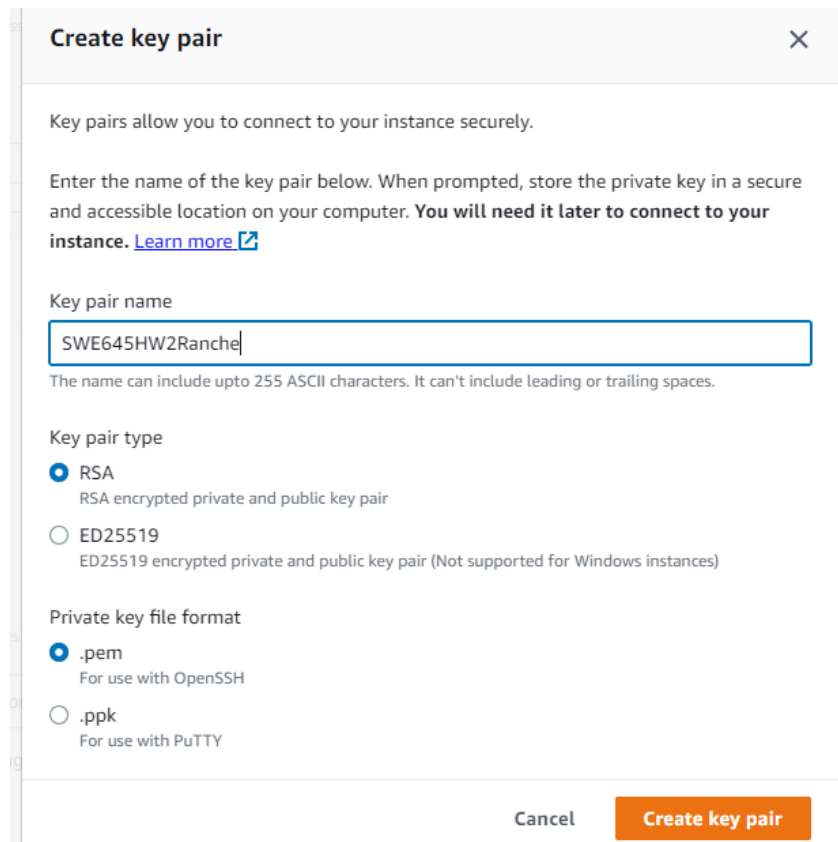
Family: t2 2 vCPU 4 GiB Memory

On-Demand Linux pricing: 0.0464 USD per Hour

On-Demand Windows pricing: 0.0644 USD per Hour

Compare instance types

4. Create a Key pair (login). Use a key type of “RSA” and a private key file format of “.pem” Make sure to save it onto your local machine.



The screenshot shows the 'Create key pair' dialog box. At the top, it says 'Create key pair' with a close button. Below that, a message states: 'Key pairs allow you to connect to your instance securely.' This is followed by instructions: 'Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)'. The 'Key pair name' field contains 'SWE645HW2Ranche'. A note below the field says: 'The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.' Under 'Key pair type', 'RSA' is selected with a radio button, and its description is 'RSA encrypted private and public key pair'. 'ED25519' is also an option, with the note 'ED25519 encrypted private and public key pair (Not supported for Windows instances)'. Under 'Private key file format', '.pem' is selected with a radio button, and its description is 'For use with OpenSSH'. '.ppk' is also an option, with the description 'For use with PuTTY'. At the bottom right, there are 'Cancel' and 'Create key pair' buttons.

Create key pair [X]

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

SWE645HW2Ranche

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel Create key pair

5. Under Network Settings, ensure that “ssh”, “HTTPS”, and “HTTP” are all checked, and the source type is from “Anywhere - 0.0.0.0/0”, with ports

22, 443, and 80 exposed

▼ Network settings Info

VPC - required Info

vpc-0e422f8508b46af90 (default) ↕

172.31.0.0/16

Subnet Info

No preference ▼

↕ Create new subnet

Auto-assign public IP Info

Enable ▼

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

launch-wizard-10

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .-:/()#,@[]+=&;!\$*

Description - required Info

launch-wizard-10 created 2022-10-18T22:59:03.198Z

Inbound security groups rules

▶ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

▶ Security group rule 2 (TCP, 443, 0.0.0.0/0) Remove

▶ Security group rule 3 (TCP, 80, 0.0.0.0/0) Remove

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Add security group rule

6. Launch your new instance

E. Click “View all Instances”

F. Select the blue link under “Instance ID” to make note of the Instance Info

BWS Services Search for services, features, blogs, docs, and more [Alt+S]

US S3 EC2 EC2 Image Builder

New EC2 Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits

▼ Instances Instances new Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances new Dedicated Hosts Scheduled Instances Capacity Reservations

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
Rancher 2	i-09fad108sec185421	Running	t2.medium	2/2 checks passed	No alarms	us-east-1d	ec2-52-206-103-201.co...	52.206.103.201
Jenkins	i-088861cb40b4f8ae2	Running	t2.medium	-	No alarms	us-east-1d	ec2-54-164-166-246.co...	54.164.166.246

G. You'll see the instance summary for your instance, take note of the Public IPv4

Instance summary for i-088861cb40b4f8ae2 (Jenkins) Info		
Updated less than a minute ago		
Instance ID i-088861cb40b4f8ae2 (Jenkins)	Public IPv4 address 54.164.166.246 open address	Private IPv4 addresses 172.31.82.105
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-164-166-246.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-82-105.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-82-105.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.medium	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 54.164.166.246 [Public IP]	VPC ID vpc-0e422f8508b46af90	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0da91a1979ef24a98	

DNS

H. On the same page, in the left side bar menu, you'll see an entry called "Elastic IPs" under Network & Security. Select it.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

S3

EC2

EC2 Image Builder

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances New

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs New

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups New

EC2 > Instances > i-088861cb40b4f8ae2

Instance summary for i-088861cb40b4f8ae2 (Jenkins) Info

Updated less than a minute ago

Instance ID
i-088861cb40b4f8ae2 (Jenkins)

IPv6 address
-

Hostname type
IP name: ip-172-31-82-105.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
54.164.166.246 [Public IP]

IAM Role
-

Details

Security

Networking

Storage

Status checks

Instance details Info

Platform
Ubuntu (Inferred)

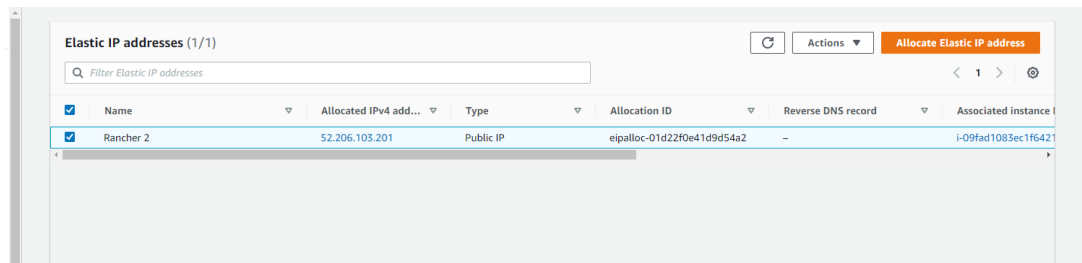
Platform details
Linux/UNIX

Stop protection
Disabled

Instance auto-recovery
Default

AMI Launch index
0

I. Select “Allocate Elastic IP Address”



J. Ensure that the Network Border Group matches the instance's, and click Allocate

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) [Learn more](#)
- ☐ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

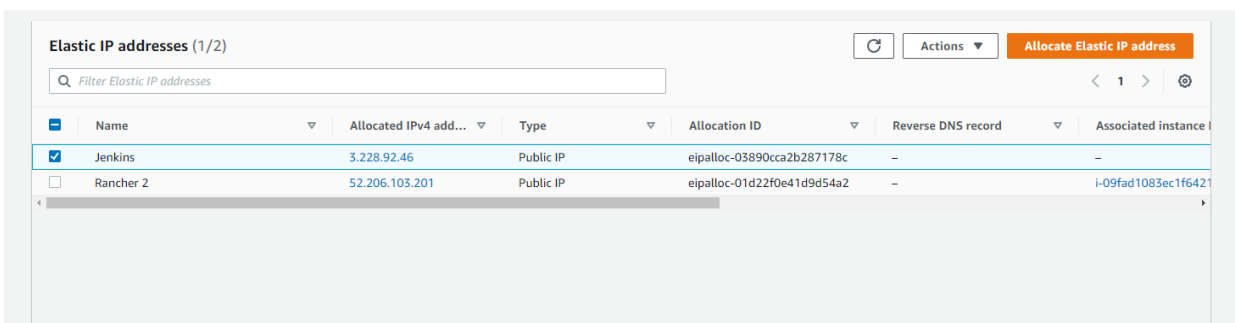
No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tag

[Cancel](#) [Allocate](#)

K. Edit the name of your new Elastic IP address and click the blue link under Allocated IPv4 Address



L. Click Associate Elastic IP Address

EC2 > Elastic IP addresses > 3.228.92.46

3.228.92.46

Actions ▾ Associate Elastic IP address

Summary			
Allocated IPv4 address 3.228.92.46	Type Public IP	Allocation ID eipalloc-03890cca2b287178c	Reverse DNS record -
Association ID -	Scope VPC	Associated instance ID -	Private IP address -
Network interface ID -	Network interface owner account ID -	Public DNS -	NAT Gateway ID -
Address pool Amazon	Network Border Group us-east-1		

M. Select the new Instance name and click Associate

EC2 > Elastic IP addresses > 3.228.92.46 > Associate Elastic IP address

Associate Elastic IP address


Choose the instance or network interface to associate to this Elastic IP address (3.228.92.46)

Elastic IP address: 3.228.92.46

Resource type
Choose the type of resource with which to associate the Elastic IP address.

☒ Instance

☐ Network interface

 If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. [Learn more](#)

Instance

i-09fad1083ec1f6421 (Rancher 2) - running

i-088861cb40b4f8ae2 (Jenkins) - running

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

☐ Allow this Elastic IP address to be reassociated

Cancel Associate

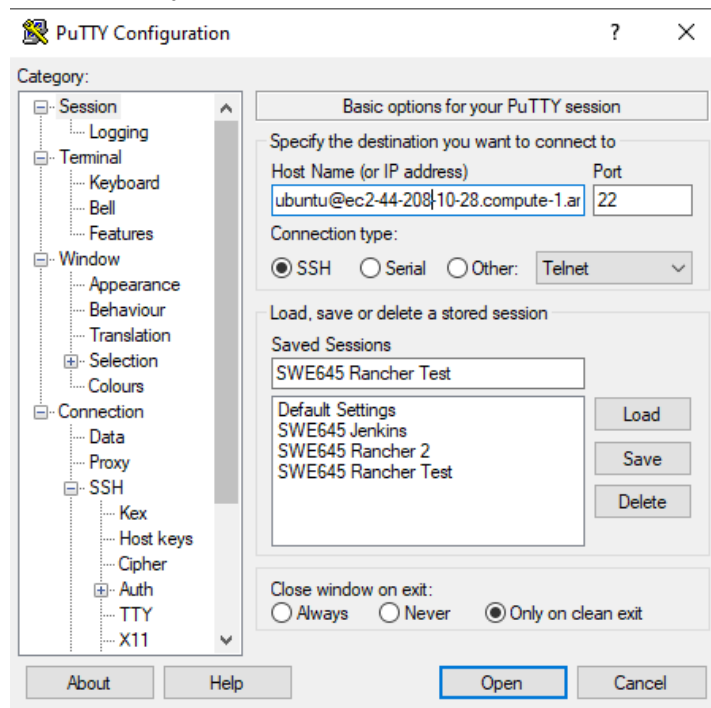
N. Enjoy the new EC2 instance! Associating an Elastic IP address hardened the public IPv4 DNS address by providing a permanent reference instead of creating a new one every time the instance stops and restarts

III. GKE Cluster Setup

- A. Creating Kubernetes Cluster on GCP
- B. Login to cloud.google.com using your credentials and then navigate to the Console
- C. Create a project – In GCP, any work is done inside a project
- D. Enable Kubernetes Engine API
- E. Under the Navigation menu, select Kubernetes Engine and then select Project1, Click on Create to create a Kubernetes Cluster
- F. Configure using the standard option and create the name of the cluster, zone(US-east-1)

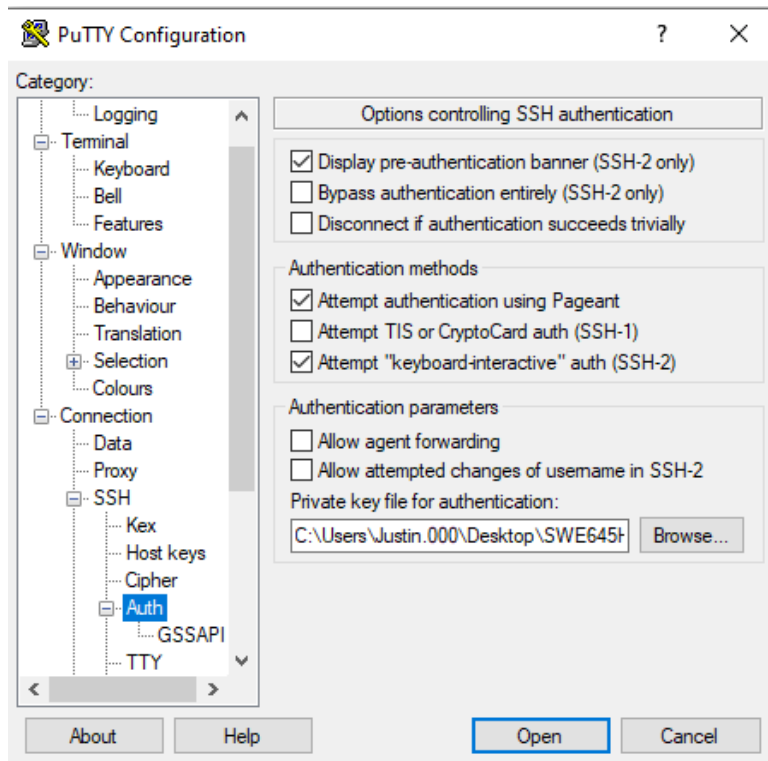
IV. Rancher Setup

- A. Create and EC2 instance with the above steps
- B. Connect to your new EC2 Instance
 - 1. If on Windows, download and install PuTTY.
 - a) For the Host Name, enter 'ubuntu@<EC2 PUBLIC IPv4 DNS>'
 - b) Use Port: 22
 - c) Connection type: SSH



- d)
- e) On the left side menu, Click “Connection”, then “SSH”, then “Auth”

- f) In the “Private key file for Authentication” field, Browse for the .pem file from the key login section of the EC2 instance setup



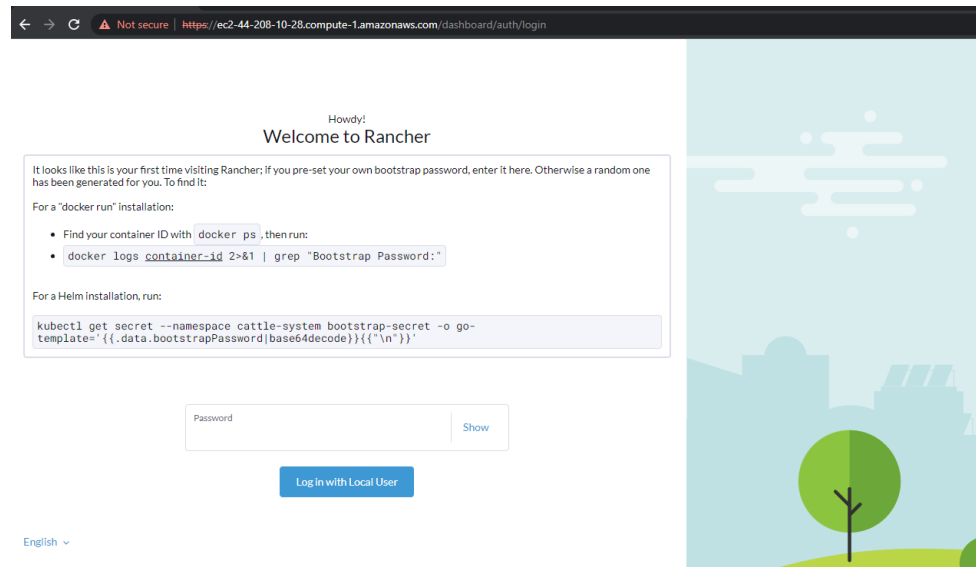
2. If on Mac or Linux, open a terminal window and enter the following command with the appropriate field:

a) `ssh -i <YOUR .PEM FILE LOCATION> ubuntu@<EC2 INSTANCE PUBLIC IPv4 DNS>`

- C. Once ssh'd into the instance, update it by running 'sudo apt-get update'
- D. Install docker with 'sudo apt install docker.io'
- E. Verify docker is installed by running 'docker -v'
- F. Install Rancher by running 'sudo docker run --privileged=true -d --restart=unless-stopped -p 80:80 -p 443:443 rancher/rancher'
- G. Enter the command 'sudo docker ps' and note the Container ID. This will be important later

```
ubuntu@ip-172-31-89-90:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CR
759a5fca4a8e   rancher/rancher  "entrypoint.sh"         6
ubuntu@ip-172-31-89-90:~$
```

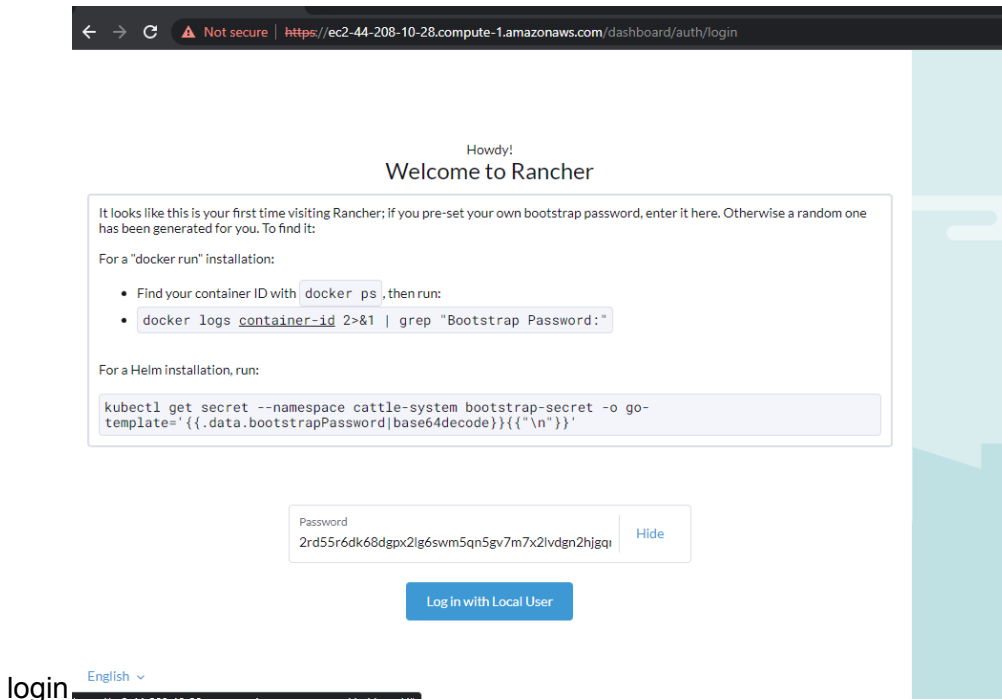
- H. Open your browser and copy/paste your EC2 public IPv4 address. Accept the browser privacy warning and you should land on this page



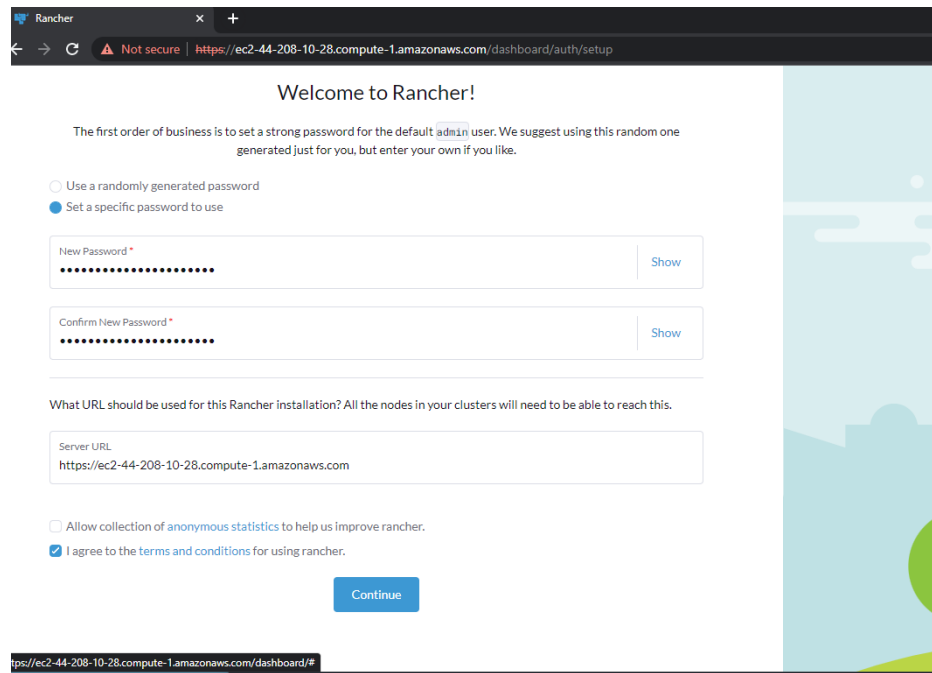
- I. Enter 'sudo docker logs <CONTAINER ID> 2>&1 | grep "Bootstrap Password:"', where <CONTAINER ID> is the value from step 7. You'll see the Bootstrap Password.

```
ubuntu@ip-172-31-89-90:~$ sudo docker logs 759a5fca4a8e 2>&1 | grep "Bootstrap Password:"
2022/10/19 00:24:11 [INFO] Bootstrap Password: 2rd55r6dk68dgp2lg6swm5qn5gv7m7x2lvdgn2hjgqngw8tlf6nhc
ubuntu@ip-172-31-89-90:~$
```

- J. Copy and paste the Bootstrap Password into the Rancher UI Password field and

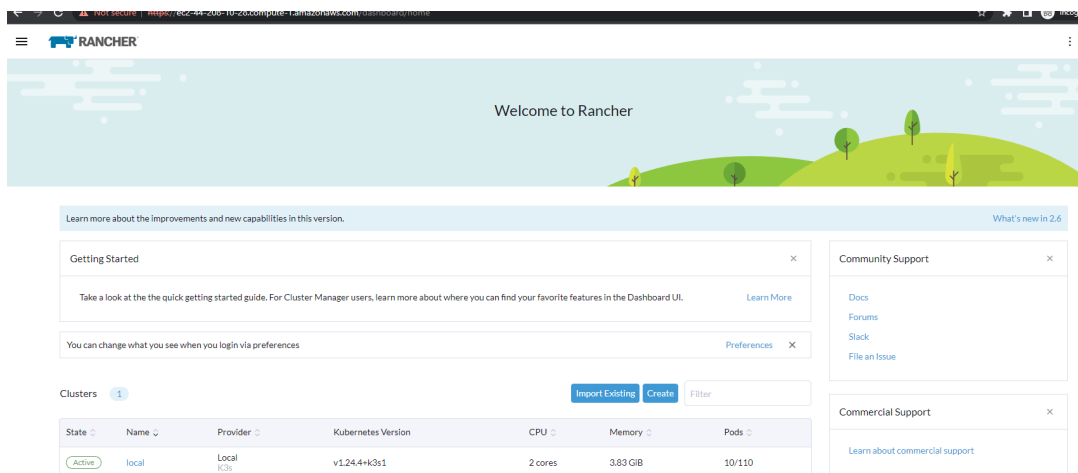


K. Create a new password and agree to the terms, then hit 'Continue'



The screenshot shows the Rancher setup page in a web browser. The browser's address bar shows the URL: `https://ec2-44-208-10-28.compute-1.amazonaws.com/dashboard/auth/setup`. The page has a title "Welcome to Rancher!". Below the title, a message states: "The first order of business is to set a strong password for the default admin user. We suggest using this random one generated just for you, but enter your own if you like." There are two radio buttons: "Use a randomly generated password" (unselected) and "Set a specific password to use" (selected). Below these are two password input fields, each with a "Show" button. The first field is labeled "New Password *" and the second is "Confirm New Password *". Below the password fields, a message asks: "What URL should be used for this Rancher installation? All the nodes in your clusters will need to be able to reach this." There is a text input field labeled "Server URL" containing the value `https://ec2-44-208-10-28.compute-1.amazonaws.com`. Below this, there are two checkboxes: "Allow collection of anonymous statistics to help us improve rancher." (unselected) and "I agree to the terms and conditions for using rancher." (selected). At the bottom right is a blue "Continue" button. The browser's address bar at the bottom shows the URL: `https://ec2-44-208-10-28.compute-1.amazonaws.com/dashboard/#`.

L. You'll be taken to the home screen!



The screenshot shows the Rancher home screen. The browser's address bar shows the URL: `https://ec2-44-208-10-28.compute-1.amazonaws.com/dashboard/#`. The page has a header with the Rancher logo and a hamburger menu. Below the header is a large banner with the text "Welcome to Rancher" and a landscape illustration. Below the banner, there is a section titled "Learn more about the improvements and new capabilities in this version." with a "What's new in 2.6" link. There are two panels: "Getting Started" and "Community Support". The "Getting Started" panel contains a link to "Learn More" and a link to "Preferences". The "Community Support" panel contains links to "Docs", "Forums", "Slack", and "File an Issue". Below these panels is a "Clusters" section with a "1" badge, "Import Existing", "Create", and "Filter" buttons. Below the buttons is a table with the following data:

State	Name	Provider	Kubernetes Version	CPU	Memory	Pods
Active	local	Local K3s	v1.24.4-k3s1	2 cores	3.83 GiB	10/110

Below the table are two more panels: "Commercial Support" with a "Learn about commercial support" link, and "What's new in 2.6" with a "What's new in 2.6" link.

M. Next to the Clusters section of the Home Page, click 'Import Existing'

The screenshot shows the 'Cluster: Import' page. On the left is a sidebar with a 'Cluster Management' menu containing 'Clusters', 'Cloud Credentials', 'Drivers', 'Pod Security Policies', 'RKE1 Configuration', and 'Advanced'. The main content area is titled 'Cluster: Import' and has a subtitle 'Register an existing cluster in a hosted Kubernetes provider'. It features three large buttons for 'Amazon EKS', 'Azure AKS', and 'Google GKE'. Below these is a section titled 'Import any Kubernetes cluster' with a 'Generic' button.

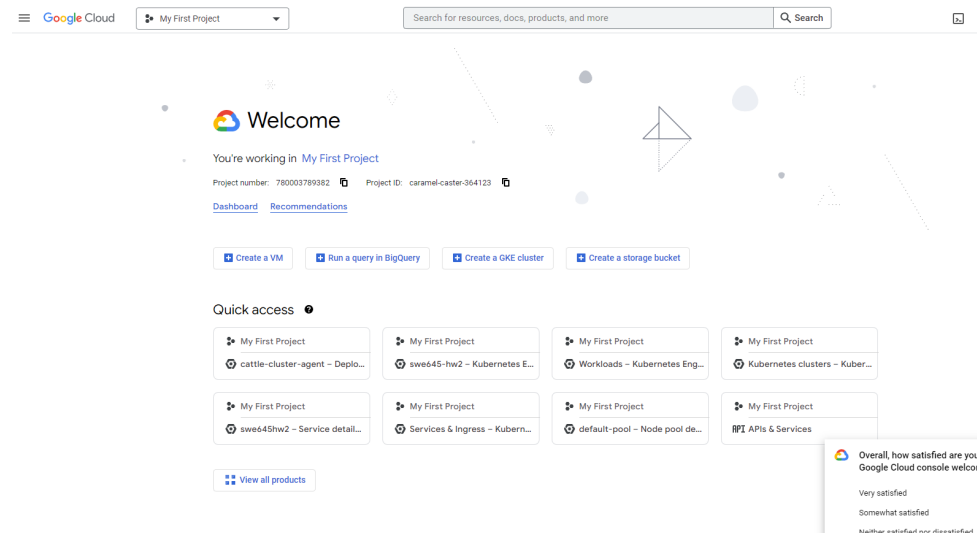
N. Select your Cluster to import. I'll be continuing with GKE

The screenshot shows the 'Import GKE' form. It includes a 'Cluster Name' field with a placeholder 'e.g. sandbox' and an 'Add a Description' link. Below are expandable sections for 'Member Roles' and 'Labels & Annotations'. The 'Google Account Access' section is expanded, showing fields for 'Google Project ID', 'Cloud Credentials' (with a dropdown and 'Add New' button), 'Name' (with a placeholder 'e.g. production-credentials' and 'Add a Description' link), 'Cloud Credential Type' (set to 'Google'), and 'Service Account' (with a 'Read from a file' button). A text area for the 'Service account private key JSON file' is also present. At the bottom, there is a 'Create' button and a 'Cancel' button. A note at the bottom provides instructions on creating a service account and lists required IAM roles: Project Viewer, Kubernetes Engine Admin, Service Account User, and Compute Viewer.

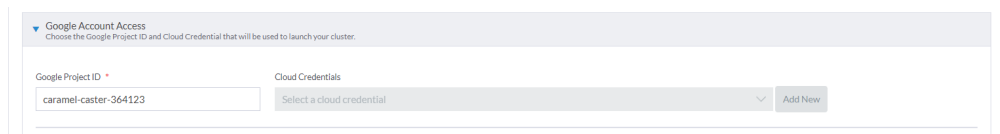
O. Insert a name for your cluster

This screenshot is a close-up of the 'Import GKE' form, specifically the 'Cluster Name' field. The field now contains the text 'Test Cluster'.

P. From the Google Cloud Project Page, find the Project ID and copy it

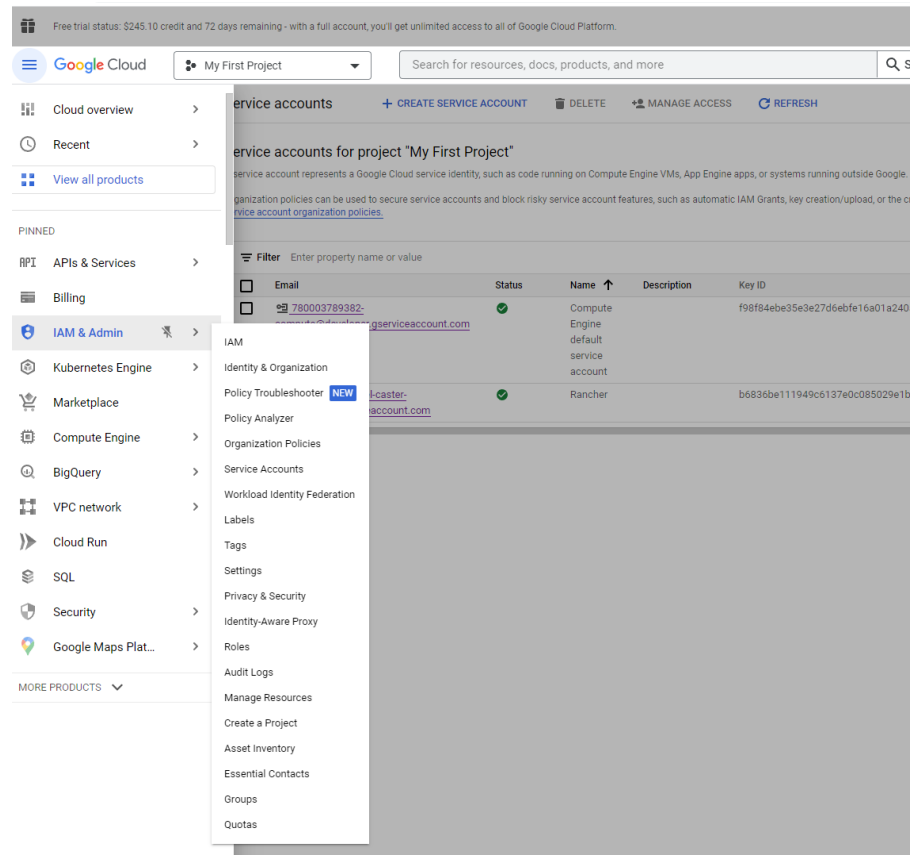


Q. Within the Google Account Access section, copy that Project ID into the Google Project ID field





R. Create a Service Account within GKE

1. Within the Google Cloud Console, open the left sidebar. Select the IAM & Admin option



2. Within the left sidebar, select Service Accounts

 IAM & Admin

 IAM

Identity & Organization

Policy Troubleshooter NEW

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Federation

Labels

Tags

Settings

Privacy & Security

Identity-Aware Proxy

Roles

Audit Logs


Asset Inventory


Essential Contacts

Groups

Quotas

IAM

 GRANT ACCESS

 REMOVE ACCESS

PERMISSIONS

RECOMMENDATIONS HISTORY

Permissions for project "My First Project"





These permissions affect this project and all of its descendant projects.

VIEW BY PRINCIPALS

VIEW BY ROLES

Filter

Enter property name or value

<input type="checkbox"/>	Type	Principal ↑
<input type="checkbox"/>		780003789382-compute@developer.gserviceaccount.com
<input type="checkbox"/>		780003789382@cloudservices.gserviceaccount.com
<input type="checkbox"/>		rancher@caramel-caster-364123.iam.gserviceaccount.com
<input type="checkbox"/>		yang9501@gmail.com

3. Select 'Create Service Account' near the top of the window

Service accounts [+ CREATE SERVICE ACCOUNT](#) [DELETE](#) [MANAGE ACCESS](#) [REFRESH](#)

Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service account keys. [Learn more about organization policies](#)

Filter Enter property name or value

<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key
<input type="checkbox"/>	780003789382-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		f98f84e3e35e3e27d6ebfe16a01a240ad24ccd3a	Oct
<input type="checkbox"/>	rancher@caramel-caster-364123.iam.gserviceaccount.com	✓	Rancher		b6836be111949c6137e0c085029e1b9569e064fa	Oct

4. Enter the Service Account Details

IAM & Admin [← Create service account](#)

Service account details

Service account name:

Display name for this service account:

Service account ID: [X](#) [C](#)

Email address: test-821@caramel-caster-364123.iam.gserviceaccount.com [C](#)

Service account description:

Describe what this service account will do

[CREATE AND CONTINUE](#)

Grant this service account access to project (optional)

Grant users access to this service account (optional)

[DONE](#) [CANCEL](#)

Navigation:

- IAM
- Identity & Organization
- Policy Troubleshooter **NEW**
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federation
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Roles
- Audit Logs
- Asset Inventory
- Essential Contacts
- Groups
- Quotas

5. Add the Compute Viewer, (Project) Viewer, Kubernetes Engine Admin, and Service Account User roles to the Service Account. Or alternatively, if you can't find all the necessary roles, just make the Service Account an

Owner.

←

Create service account

NEW

station

✓

Service account details

2

Grant this service account access to project (optional)

Grant this service account access to My First Project so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role

Compute Viewer

Read-only access to get and list information about all Compute Engine resources, including instances, disks, and firewalls. Allows getting and listing information about disks, images, and snapshots, but does not allow reading the data stored on them.

IAM condition (optional) ?

+ ADD IAM CONDITION

Role

Kubernetes Engine Admin

Full management of Kubernetes Clusters and their Kubernetes API objects.

IAM condition (optional) ?

+ ADD IAM CONDITION

Role

Service Account User

Run operations as the service account.

IAM condition (optional) ?

+ ADD IAM CONDITION

+ ADD ANOTHER ROLE

CONTINUE

3

Grant users access to this service account (optional)

DONE

CANCEL

6. Within the Service Account management page, click the Actions button(the three vertical dots) associated with your new Service Account

and select “Manage Keys”

zation

ooter **NEW**

icies

s

y Federation

y

roxy

ts

Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value

Email	Status	Name	Description	Key ID	Key creation date	Actions
<input type="checkbox"/> 780003789282-compute@developer.gserviceaccount.com	✔	Compute Engine default service account		f98f84eb35e3e27d5ebfe16a01a240a2d4ccd3a	Oct 15, 2022	⋮
<input type="checkbox"/> rancher@caramel-caster-364123.iam.gserviceaccount.com	✔	Rancher		b6836be111949c6137e0c85029e1b9f56fe064fa	Oct 15, 2022	⋮
<input checked="" type="checkbox"/> test-343@caramel-caster-364123.iam.gserviceaccount.com	✔	Test	No keys			⋮

Manage details

Manage permissions

Manage keys

View metrics

View logs

Disable

Delete

7. Add a new key by selecting the Create New Key option from the Add Key dropdown menu

Keys

⚠

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the [Workload Identity](#) accounts on Google Cloud [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).
[Learn more about setting organization policies for service accounts](#)

ADD KEY

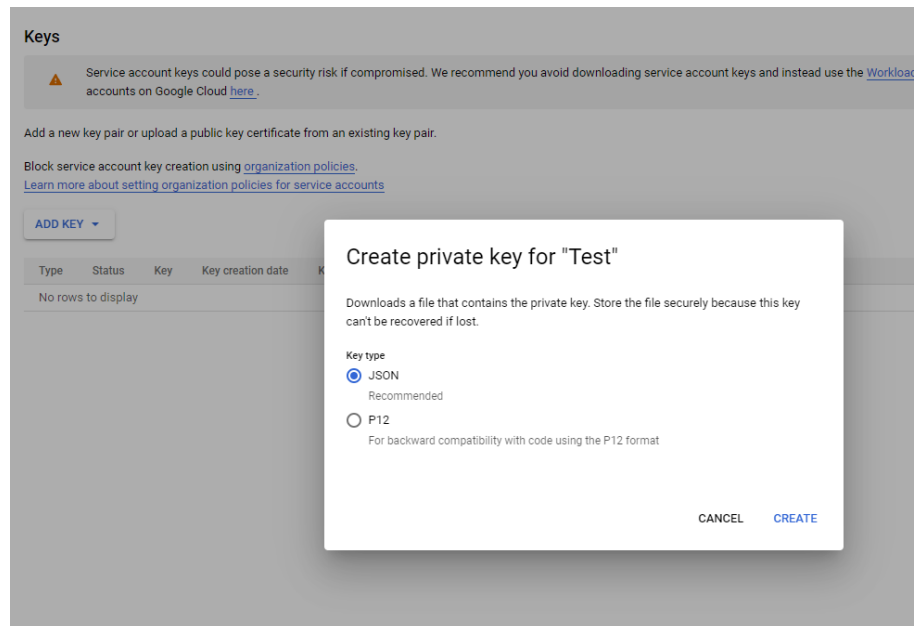
Create new key

Upload existing key

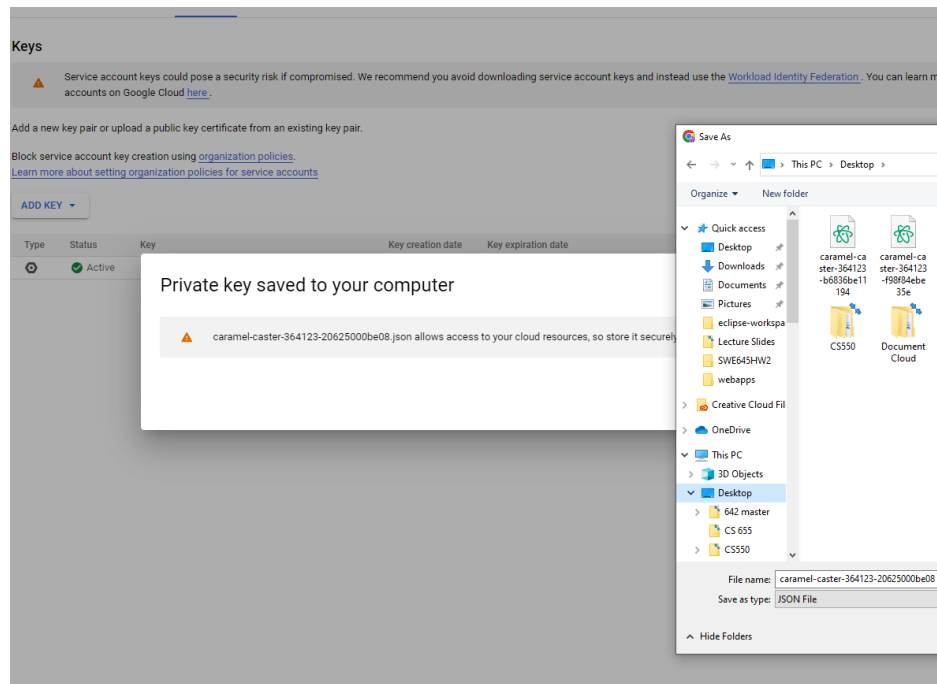
Key creation date

Key expiration date

8. Select JSON and Create



9. Save the key file on your local machine



10. Back within Rancher, upload the key file into the Service account field using the “Read from a file” button

e.g. production-credentials

Cloud Credential Type

Google

Service Account *

Read from a file

```
{
  "type": "service_account",
  "project_id": "caramel-caster-364123",
  "private_key_id": "b6836be111949c6137e0c085029e1b9569e064fa",
  "private_key": "-----BEGIN PRIVATE KEY-----
  \nMIEVQIBADANBgkqhkiG9w0BAQEFAASCBCkwggSjAgEAAoIBAQC808t0iQ26S6WnrfEeqkQY8jKSEglMkmtLwRT+9avukAz+VWZg1K6hU8ih50YxEJCSjP1K4A0/n8V64dyqEDR2Bxcl5K2Yw6PQgE8Pbo
  eQIN7VbFHY7H7GjyY4bNs+HTEYzqTJC2R6rvgj0oJub+440xHHTA+QGNB9e96jLICgMIIMAZP1pp1K0Yc3w+faRQZQwzNaRuiDqyA7ZIRvpllo/IZAJ1KML5uSP0sYLSu87+amSZ68Su7WNQKUKZCg+4jilPwIn
  GVLnprFN5sqKPR3INEgJ9nRamJGyuNINFINM/RhnrObkYEQuU6z54NSGdzYv+mfJv7Ad/D3dzAgMBAAECggEARz25y6/QVms6xDd4s5G9BWDecBHR0qP5ataZ2XyToDj7n3wl78fJgnY0xg7bV8gZHLmWbZGJt
  -----END PRIVATE KEY-----"
}
```

Create a Service Account with a JSON private key and provide the JSON here. See [Google Cloud docs](#) for more info about creating a service account. These IAM roles are required: Compute Viewer, (Project) Viewer, Kubernetes Engine Admin, Service Account User. More info on roles can be found [here](#).

11. Select the appropriate Zone for your Cluster Location

Cluster Location

Choose a region or zone to import an GKE cluster from.

Location Type

☒ Zonal

☐ Regional

Zone

us-east1-b

Cancel Load Clusters

12. Click Load Clusters

13. Choose the appropriate cluster to load from your cloud provider in the Choose Cluster Section

Choose Cluster

Choose an GKE cluster to register

Cluster To register *

swe645-hw2

14. Register the cluster!

15. It will take a while to get ready

Clusters

Import Existing Create

Download kubeconfig Download YAML Delete Filter

State	Name	Version	Provider	Machines	Age	
Active	local	v1.24.4+k3s1	Local	1	36 mins	Explore
Pending	testcluster	-	Imported Google GKE	0	11 secs	Explore

V. Jenkins Setup

- A. Create another EC2 instance using the steps above

1. Make sure to add an additional Inbound Rule under the Security Groups section with Custom TCP type, Port Range of 8080, and Source of Anywhere IPv4.

sgr-03538694f8a51a418

Custom TCP

TCP

8080

Anywhere-IPv4

0.0.0.0/0

sgr-01fe436d2b31564eb

SSH

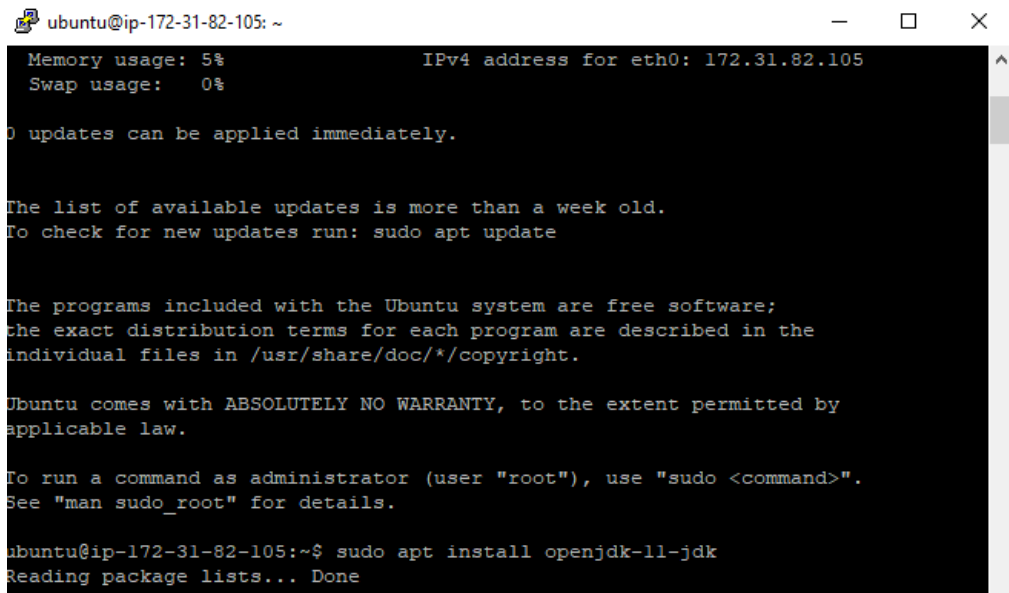
TCP

22

Anywhere-IPv4

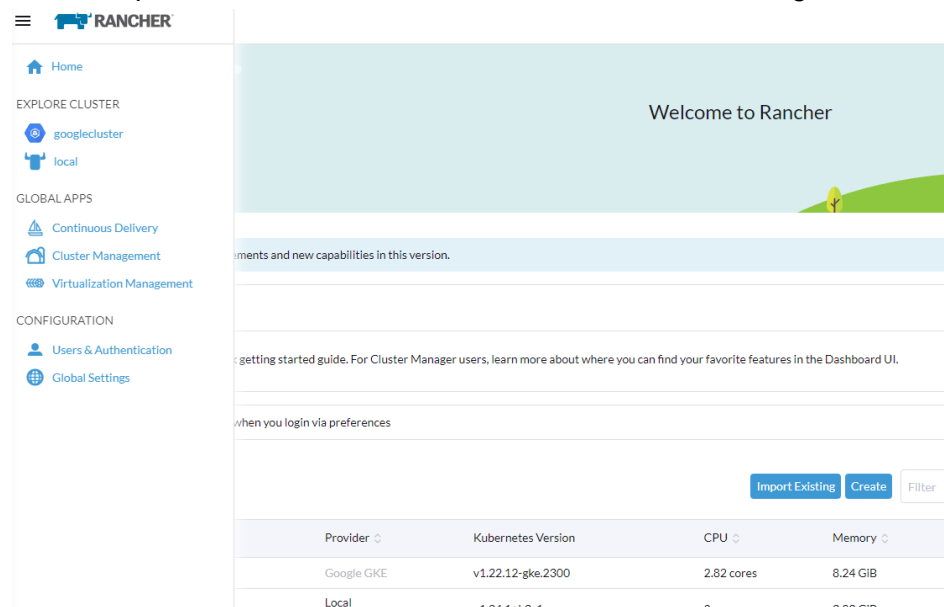
0.0.0.0/0

- B. Connect to the EC2 instance using the terminal on Mac or Linux, or Putty on Windows
- C. Install JDK 11: 'sudo apt install openjdk-11-jdk'

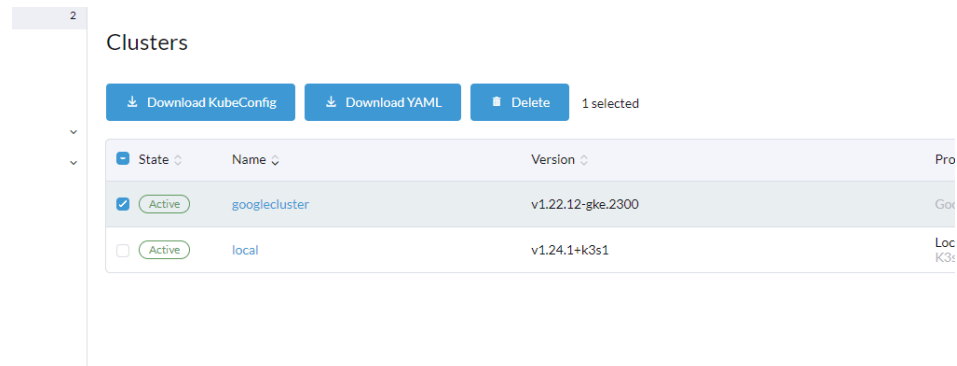
A terminal window titled 'ubuntu@ip-172-31-82-105: ~' with standard window controls. The terminal output shows system status: 'Memory usage: 5%', 'Swap usage: 0%', and 'IPv4 address for eth0: 172.31.82.105'. It then displays a message about updates: '0 updates can be applied immediately.' followed by 'The list of available updates is more than a week old. To check for new updates run: sudo apt update'. A disclaimer about Ubuntu's warranty is shown. The user then runs 'sudo apt install openjdk-11-jdk', and the terminal shows 'Reading package lists... Done'.

- D. Import the GPG keys of the Jenkins Repository
 - 1. `wget -q -O - https://pkg.jenkins.io/debian/jenkins.io.key | sudo apt-key add`
 -
- E. Add the Jenkins repository to the system
 - 1. `sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'`
- F. Once ssh'd into the instance, update it by running 'sudo apt-get update'
- G. Install docker with 'sudo apt install docker.io'
- H. Verify docker is installed by running 'docker -v'
- I. Install Jenkins with the following commands:
 - 1. `sudo apt update`
 - 2. `sudo apt install jenkins`
- J. The Jenkins service will automatically start after installation. Check status with
 - 1. `Systemctl status jenkins`
- K. Install Kubectl
 - 1. `sudo apt install snapd`
 - 2. `sudo snap install kubectl --classic`
- L. Add the jenkins user to the docker user group
 - 1. `sudo usermod -a -G docker jenkins`
- M. Reboot the Jenkins Host in the EC2 console for the user group changes to take effect
- N. We also need to add the kubeconfig file into the Jenkins host for reference when using kubectl commands in the Pipeline job
 - 1. Visit your Rancher dashboard

2. On the expandable menu on the left side, click Cluster Management



3. Check the cluster corresponding to your deployment and click the Download KubeConfig button



4. You'll download a yaml file onto your local machine. Make note of the directory location
5. Enter the following command to switch to the jenkins user in the command line of the Jenkins host
 - a) `sudo su jenkins`

```
ubuntu@ip-172-31-95-21:~$ sudo usermod -a -G docker jenkins
ubuntu@ip-172-31-95-21:~$ sudo su jenkins
jenkins@ip-172-31-95-21:/home/ubuntu$
```

6. Navigate to the working directory of the Jenkins user, in this case `/var/lib/jenkins`. If you're not sure which directory it is, skip this step and perform it after Step 19. The Home directory is found in the Jenkins UI

under Dashboard -> Manage Jenkins -> Configure System.

```
jenkins@ip-172-31-95-21:/home/ubuntu$ cd ..
jenkins@ip-172-31-95-21:/home$ cd ..
jenkins@ip-172-31-95-21:/$ cd var/lib/jenkins/
jenkins@ip-172-31-95-21:~$
```

7. Create a new directory called .kube
 - a) mkdir .kube
8. Enter the new .kube directory and create a file called 'config'. Copy paste the contents of the downloaded yaml file into this new config file.

```
jenkins@ip-172-31-95-21:~/.kube$ touch config
jenkins@ip-172-31-95-21:~/.kube$ vi config
jenkins@ip-172-31-95-21:~/.kube$
```

O. Get the password on the terminal with this command

1. sudo cat /var/lib/jenkins/secrets/initialAdminPassword

```
ubuntu@ip-172-31-95-21:~$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
1b41a7254afc4f92b136ca2da469ff8d
ubuntu@ip-172-31-95-21:~$
```

P. In your browser, navigate to http://your_ip_or_domain:8080 and past the password into the appropriate field

1. Make sure to use the http prefix, NOT https

Getting Started

Unlock Jenkins

To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:

```
/var/lib/jenkins/secrets/initialAdminPassword
```

Please copy the password from either location and paste it below.

Administrator password

Q. Install the suggested plugins

Getting Started

Customize Jenkins

Plugins extend Jenkins with additional features to support many different needs.

Install suggested plugins

Install plugins the Jenkins community finds most useful.

Select plugins to install

Select and install plugins most suitable for your needs.

R. Create an admin user

Getting Started

Create First Admin User

Username:

admin

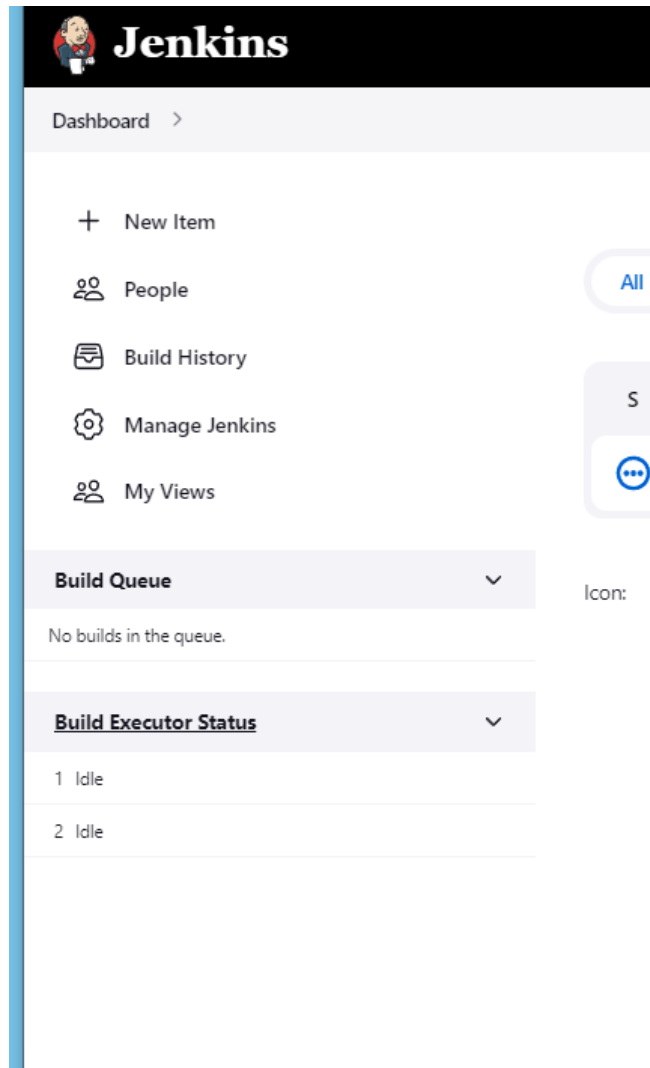
Password:

Confirm password:

Full name:

E-mail address:


- S. You should see a dashboard at some point once you've completed initial setup. Click the "New Item" option in the left sidebar to create your first pipeline





T. Enter a name and select the Pipeline option


Enter an item name


> Required field


**Freestyle project**
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

**Pipeline**
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.


**Multi-configuration project**
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

**Folder**
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

**Multibranch Pipeline**
Creates a set of Pipeline projects according to detected branches in one SCM repository.

**Organization Folder**
Creates a set of multibranch project subfolders by scanning for repositories.

If you want to create a new item from other existing, you can use this option:

**Copy from**

OK

U. Select the Github hook trigger for GITScm polling option in the Build Triggers

Build Triggers

☐ Build after other projects are built ?

☐ Build periodically ?

☒ GitHub hook trigger for GITScm polling ?

☐ Poll SCM ?

☐ Quiet period ?

☐ Trigger builds remotely (e.g., from scripts) ?

section

V. Within the Pipeline section, choose the following

1. Definition: Pipeline script from SCM
2. SCM: Git
3. RepositoryURL: Your git repository URL

4. Branch Specifier: Your git branch you want to build
5. Script Path: Jenkinsfile
6. Lightweight checkout: UNCHECKED

Definition

Pipeline script from SCM

SCM

Git

Repositories

Repository URL

Credentials

Branches to build

Branch Specifier (blank for 'any')

Repository browser

Additional Behaviours

Script Path

☐ Lightweight checkout

[Pipeline Syntax](#)

W. Exit back to the Dashboard. Select Manage Jenkins from the left sidebar, then Configure System.

Jenkins Search (C)

Dashboard > Manage Jenkins

+ New Item

People

Build History

Manage Jenkins

My Views

Build Queue

No builds in the queue.

Build Executor Status

1 Idle

2 Idle

Manage Jenkins

Building on the built-in node can be a security issue. You should set up distributed builds. See [the documentation](#).

System Configuration

Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Manage Nodes and Clouds
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Security

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Manage Credentials
Configure credentials

Manage Users
Create/delete/modify users that can log in to this Jenkins.

X. Under Global Properties, check Environment Variables box and click Add

Global properties

☐ Disable deferred wipeout on this node ?

☒ Environment variables

List of variables ?

Add

☐ Tool Locations

Y. Add the following environment variable for use in the Jenkinsfile

1. Name: DOCKERHUB_PASS
2. Value: swe645hw2docker

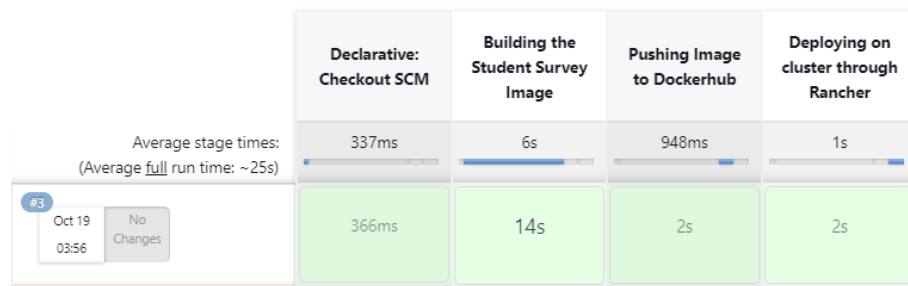
Z. Open the project repository in Github

1. Enter the settings tab for that repository
2. Click the “Webhooks” option in the left sidebar menu
3. Add a webhook with the Payload URL pointed towards: <AWS URL>:8080/github_webhook/ and leave the other settings as default.

AA. We're ready to test the pipeline. Committing and pushing a trivial change in the codebase with git will trigger the webhook to be sent to the Jenkins /github_webhook/ API, which will trigger our new pipeline to run.

Pipeline SWE645HW2

Stage View



VI. Project Configuration Setup(Dockerfile/Jenkinsfile)

A. Dockerfile

Dockerfile	studentSurvey.html
1 FROM tomcat:9.0-jdk11	
2 COPY SWE645HW2.war /usr/local/tomcat/webapps/	
3	

B. Jenkinsfile

Jenkinsfile	Dockerfile	studentSurvey.html	googlecluster.yaml
<pre> 1 pipeline { 2 agent any 3 stages { 4 stage("Building the Student Survey Image"){ 5 steps{ 6 script { 7 git 'https://github.com/yang9501/SWE645HW2.git' 8 sh 'pwd' 9 sh 'ls' 10 sh 'rm -rf *.war' 11 //The .war file creation process breaks if there are any foreign files in the folder structure. Have to isolate the filepath w 12 sh 'jar -cvf SWE645HW2.war -C src/main/webapp/ .' 13 sh 'ls' 14 sh 'echo \${BUILD_TIMESTAMP}' 15 sh 'docker login -u yang9501 -p \${DOCKERHUB_PASS}' 16 sh 'docker build -t yang9501/swe645hw2:latest .' 17 } 18 } 19 } 20 stage("Pushing Image to Dockerhub"){ 21 steps{ 22 script { 23 sh 'docker push yang9501/swe645hw2:latest' 24 } 25 } 26 } 27 stage("Deploying on cluster through Rancher"){ 28 steps{ 29 script { 30 //Jenkins uses the 'jenkins' user on the host to perform actions on the host. .kube/config is a folder that grants access to p 31 sh 'kubectl --kubeconfig /var/lib/jenkins/.kube/config version' 32 sh 'kubectl --kubeconfig /var/lib/jenkins/.kube/config set image deployment/swe645hw2 container-0=yang9501/swe645hw2:latest' 33 //After the cluster receives the image, you have to redeploy the pods in order for the new image to take effect 34 sh 'kubectl --kubeconfig /var/lib/jenkins/.kube/config rollout restart deployment/swe645hw2' 35 } 36 } 37 } 38 } 39 } 40 </pre>			