INSTALLATION GUIDE OF CLOUD SCHEDULER

Version 1.0

August 30, 2022

CRITICALRIVER TECHNOLOGIES PVT LTD

Table of Contents

[1. Introduction 4](#_Toc112748097)

[1.1. Purpose: 4](#_Toc112748098)

[1.2. Scope: 4](#_Toc112748099)

[1.3. Audience: 5](#_Toc112748100)

[2. Environment Setup 6](#_Toc112748101)

[2.1. Google Cloud SDK: 6](#_Toc112748102)

[2.1.1. Prerequisites to install Google Cloud SDK: 6](#_Toc112748103)

[2.1.2. Installation of Google Cloud SDK using Apt Repository 6](#_Toc112748104)

[2.1.3. Initialize Cloud SDK 7](#_Toc112748105)

[2.2. AWS-CLI: 9](#_Toc112748106)

[Step 1: Curl Command 9](#_Toc112748107)

[Step 2: Unzip the Installer 9](#_Toc112748108)

[Step 3: Install Program 9](#_Toc112748109)

[Step 4: Move the file 9](#_Toc112748110)

[Step 5: Check the version 10](#_Toc112748111)

[Step 6: Authenticate AWS Account through AWS-CLI 10](#_Toc112748112)

[2.3. Terraform: 10](#_Toc112748113)

[2.3.1. Installation of Terraform on Ubuntu 10](#_Toc112748114)

[2.3.2. Service Account for terraform: 13](#_Toc112748115)

[2.4. Velero 15](#_Toc112748116)

[2.4.1. Create Google Service Account (GSA): 15](#_Toc112748117)

[2.4.2. Create Custom Role with Permissions for the Velero GSA: 16](#_Toc112748118)

[2.4.3. Grant access to Velero 16](#_Toc112748119)

[2.4.4. Velero on AWS 17](#_Toc112748120)

[2.5. Jenkins Pipeline Setup: 18](#_Toc112748121)

[2.5.1. Creating Pipeline Jobs in Jenkins: 18](#_Toc112748122)

[3. Cloud Scheduler 21](#_Toc112748123)

[3.1. Job 1: Auto Shutdown and Start-up 21](#_Toc112748124)

[3.2. Job 2: VM Start and Shutdown 21](#_Toc112748125)

[3.3. Job 3: Terraform restore and destroy 22](#_Toc112748126)

[3.4. Job 4: Velero Backup and Restore 22](#_Toc112748127)

[4. Troubleshooting Guide 24](#_Toc112748128)

[4.1. Issues with AWS-CLI setup 24](#_Toc112748129)

[4.2. Issues with AWS- Authentication 24](#_Toc112748130)

[4.3. Issues with Google Cloud-CLI Authentication 24](#_Toc112748131)

[4.4. Issues with Terraform Setup 24](#_Toc112748132)

[4.5. Issues with setting up IAM Users, Roles, and Policies through CLI 24](#_Toc112748133)

[4.6. Issues with Velero Setup 25](#_Toc112748134)

[4.7. Issues with setting up pipeline jobs in Jenkins 25](#_Toc112748135)

[Appendix A: Installation of Jenkins in Ubuntu 27](#_Toc112748136)

[A.1. Prerequisites for Jenkins installation: 27](#_Toc112748137)

[A.2. Installation of Java: 27](#_Toc112748138)

[A.3. Jenkins Installation: 27](#_Toc112748139)

[A.4. Starting Jenkins: 28](#_Toc112748140)

[A.5. Setting Up Jenkins 28](#_Toc112748141)

[Glossary 33](#_Toc112748142)

[Revision History 34](#_Toc112748143)

**List of Figures**

[Figure 1: Terraform - Add-HashiCorp-signed-gpg-keys 11](#_Toc112748173)

[Figure 2: Terraform - Add-the-HashiCorp-repository 11](#_Toc112748174)

[Figure 3: Terraform - sudo-apt-update 12](#_Toc112748175)

[Figure 4: Terraform - Install-terraform-on-ubuntu-20.04 12](#_Toc112748176)

[Figure 5: Terraform - check-terraform-version 13](#_Toc112748177)

[Figure 6: Credentials for Velero 18](#_Toc112748178)

[Figure 7:Jenkins - New Job 19](#_Toc112748179)

[Figure 8:Jenkins - Job Description 19](#_Toc112748180)

[Figure 9: Jenkins - pipeline 20](#_Toc112748181)

[Figure 10: Jenkins - Git repo 20](#_Toc112748182)

[Figure 11: Jenkins File - Auto shutdown and start-up 21](#_Toc112748183)

[Figure 12: Jenkins File - VM Start-up 22](#_Toc112748184)

[Figure 13: Jenkins File - VM Shutdown 22](#_Toc112748185)

[Figure 14: Jenkins File - Terraform 22](#_Toc112748186)

[Figure 15: Jenkins File - Velero Backup 23](#_Toc112748187)

[Figure 16: Jenkins File - Velero Restore 23](#_Toc112748188)

[Figure 17: Jenkins - Unlock Jenkins 28](#_Toc112748189)

[Figure 18: Jenkins - Select Plugin to Install 29](#_Toc112748190)

[Figure 19: Jenkins - Plugin Installation 29](#_Toc112748191)

[Figure 20: Jenkins - Create Admin User 30](#_Toc112748192)

[Figure 21: Jenkins - Admin User Details 30](#_Toc112748193)

[Figure 22: Jenkins - Jenkins URL 31](#_Toc112748194)

[Figure 23: Jenkins - Installation Finish 32](#_Toc112748195)

[Figure 24: Jenkins - Welcome Page 32](#_Toc112748196)

# Introduction

The adaptation of cloud-based solutions has grown rapidly in recent times. Recent studies says that nearly 70% of the organizations are migrating more workloads to the cloud and 50% of the organizations are developing their solutions with cloud-first strategy. With this rapid growth trend in cloud migration, the organizations bare more OpEx costs and around 65% of the organizations which are working with cloud are looking for solutions or strategies to cut down their costs without impacting the productivity.

Cloud Scheduler is a customizable solution to auto schedule the active period of cloud compute services and clusters. The main problems that this cloud scheduler addresses to reduce the cloud costs upto70% are:

1. Schedule auto shutdown and start-up of VMs through automation.
2. Auto provision and decommission of cloud managed container solutions.
3. Auto scheduling of backup and restore operations for container-based solutions.

This solution can be used with non-production environments in the cloud which doesn’t require active period of 24 hours. It is easily scalable for as many VMs as you want and for as many clusters as you want.

## Purpose:

The main purpose of this document is to walk you through various steps to setup and utilize the **Cloud Scheduler** in efficient manner to auto schedule start-up and shutdown of the VMs through pipelines and schedule the backup and restore process of cloud managed clusters during non-active period.

## Scope:

The scope of this guide is:

* To cover the installation and setup of Google Cloud SDK and AWS CLI to actively manage scripts and pipelines.
* To cover the installation and setup of Terraform to provision and destroy the cloud resources scheduled and on-demand.
* To cover the installation and setup of Velero with AWS and GCP Kubernetes clusters to manage the scheduled and on-demand backup and restoration.
* To cover the basic troubleshooting steps while setting up and running these pipelines through Jenkins.

The out of the scope elements are:

* Installation and setup of any other Infrastructure as Code (IaC) tool. However, you can extend this knowledge to other tools.
* Installation and setup of pipelines through any other automation tool except Jenkins. However, same knowledge can be extended to other tools.
* Every other error while setting up and operating all these tools, scripts, templates, and pipelines. Basic troubleshooting steps are provided. Should you get any error please refer to the relevant documents available online.

## Audience:

This guide is intended for end-users, cloud administrators, operations teams, and technical personnel who is willing to reduce and optimize the GCP and AWS compute costs without effecting the operations during the active period and spending extended time to manage them.

# Environment Setup

This section describes the software required for the environment setup and the procedure to install them.

## Google Cloud SDK:

**Google Cloud SDK** (Software Development Kit) provides a set of tools that are used to manage resources hosted on Google Cloud Platform (GCP). The SDK provides gcloud, gsutil, and bq commands with the ability to access the Google Cloud via the terminal.

If you are using instances in Google Cloud Platform Google Cloud SDK will be Preinstall in the instance.

Otherwise here are the steps to install Google Cloud SDK:

### Prerequisites to install Google Cloud SDK:

Login to your Ubuntu system with a sudo privileged account.

Open a terminal and execute the following commands to install required packages on your system.

**$ sudo apt update**

**$ sudo apt install apt-transport-https ca-certificates gnupg**

### Installation of Google Cloud SDK using Apt Repository

Follow below steps:

#### Step 1: Import GPG key

First, import the apt GPG key to your system with below command.

**$ curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key add**

#### Step 2: Create a PPA file

Then create a PPA file in your system with referring to the cloud-sdk in Google packages repository

**$ echo "deb https://packages.cloud.google.com/apt cloud-sdk main" | sudo tee -a /etc/apt/sources.list.d/google-cloud-sdk.list**

#### Step 3: Install google-cloud-sdk

Finally, update the apt cache and install Google Cloud Packages on your Ubuntu system

**$ sudo apt update**

**$ sudo apt install google-cloud-sdk**

Press ‘y’ and hit enter for any confirmation asked by the installer.

### Initialize Cloud SDK

After you install Cloud SDK successfully on your system. The next step is to perform initialize the environment with **gcloud init** command. This authorizes Cloud SDK tools to use your Google account credentials to access Google Cloud and manage it.

To initialize the **gcloud CLI**:

#### Step 1: Run gcloud init:

**$ sudo gcloud init**

#### Step 2: Create or select a configuration if prompted

If you are initializing a new **gcloud CLI** installation**, gcloud init** creates a configuration named **default** for you and sets it as the active configuration. If you have existing configurations, **gcloud init** prompts you to choose between three options — re-initialize the active one, switch to another one and re-initialize it, or create a new one.

#### Step 3: Complete the authorization step when prompted

Depending on whether you have previously authorized access to Google Cloud, you might be prompted to log in and grant access in a web browser or to select an existing account.

**$ sudo gcloud init –console-only**

If you used the **--console-only** flag and login is required, you must then copy and paste the provided authorization URL into another browser window and follow the prompts provided.

When this step is completed**, gcloud init** sets the **account**property in the configuration to the specified account.

#### Step 4: Choose a current Google Cloud project if prompted

If you only have access to one project, including the default project for your user account**, gcloud init** selects it for you.

Otherwise, you can select a project from a list of projects for which you have **Owner**, **Editor** or **Viewer** permissions. **gcloud init** sets the **project**property in the configuration to the property you choose. If you have access to more than 200 projects, you will be prompted to enter a project id, create a new project, or list projects.

**This account has a lot of projects! Listing them all can take a while.**

**[1] Enter a project ID**

**[2] Create a new project**

**[3] List projects**

**Please enter your numeric choice:**

#### Step 5: Choose a default Compute Engine zone if prompted

If you don't have the Compute Engine API enabled or have a default zone in your project-level metadata, you will not see this step**. gcloud init** sets the region and zone properties in the configuration using the zone you choose.

When **gcloud init** finishes, it prints the properties in the active configuration to the terminal:

**[compute]**

**region = us-east1**

**zone = us-east1-b**

**[core]**

**account = user@google.com**

**disable\_usage\_reporting = False**

**project = example-project**

You can view these properties at any other time using the [**gcloud config list**](https://cloud.google.com/sdk/gcloud/reference/config/list)command.

## AWS-CLI:

The AWS Command Line Interface (AWS CLI) is an open-source tool that enables you to interact with AWS services using commands in your command-line shell. With minimal configuration, the AWS CLI enables you to start running commands that implement functionality equivalent to that provided by the browser-based AWS Management Console from the command prompt in your terminal program.

The installation of AWS-CLI can be done by executing the following commands:

### Step 1: Curl Command

Use the **curl** command – The **-o** option specifies the file name that the downloaded package is written to. The options on the following example command write the downloaded file to the current directory with the local name awscliv2.zip.

**$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip" -o "awscliv2.zip"**

### Step 2: Unzip the Installer

Unzip the installer. If your Linux distribution doesn't have a built-in unzip command, use an equivalent to unzip it. The following example command unzips the package and creates a directory named **aws**under the current directory.

**$ unzip awscliv2.zip**

### Step 3: Install Program

Run the install program. The installation command uses a file named install in the newly unzipped **aws** directory. By default, the files are all installed to **/usr/local/aws-cli,** and a symbolic link is created in **/usr/local/bin**. The command includes **sudo** to grant write permissions to those directories.

**$ sudo ./aws/install**

### Step 4: Move the file

Move the downloaded file to the path, The default value is **/usr/local/bin**.

**$ ./aws/install -i /usr/local/aws-cli -b /usr/local/bin**

### Step 5: Check the version

Now, Check the version of the aws-cli by running the following command. And the output is given below.

**$ aws –version**

**aws-cli/2.4.5 Python/3.8.8 Linux/4.14.133-113.105.amzn2.x86\_64 botocore/2.4.5**

### Step 6: Authenticate AWS Account through AWS-CLI

To create and manage any AWS resource through AWS-CLI, you must authenticate first and this AWS account must be having related permissions for the services.

Run below command and provide the necessary details to authenticate.

**$ aws configure**

**AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE**

**AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY**

**Default region name [None]: us-west-2**

**Default output format [None]: json**

For more information on authenticating via AWS-CLI, please follow official documentation from AWS (link is below):

<https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-quickstart.html>

## Terraform:

There are many tools to implement infrastructure as code like **Ansible**, **CloudFormation**, **Azure Resource Manager**, **Chef**, **Google Cloud deployment manager** and more. Terraform is one of the powerful tools (by **HashiCorp**) that belong to this list. It helps to build, change, and manage your infrastructure easily with versioning manifest. Every cloud vendor has its own **IaC** tool but **Terraform** is cloud-agnostic. So, you can use a single tool to manage your multi-cloud environment. Infrastructure as Code (IaC) is a term used when you codify your whole infrastructure for automation with DevOps.

### Installation of Terraform on Ubuntu

#### **Step1- Register HashiCorp GPG keys**

To check the authenticity of packages, you must add **HashiCorp** **signed gpg keys** to your system. You will see the "**OK**" message if it is added successfully. Copy this command except for the**$** sign and paste it to your Ubuntu system.

**$ curl -fsSL https://apt.releases.hashicorp.com/gpg | sudo apt-key add -**

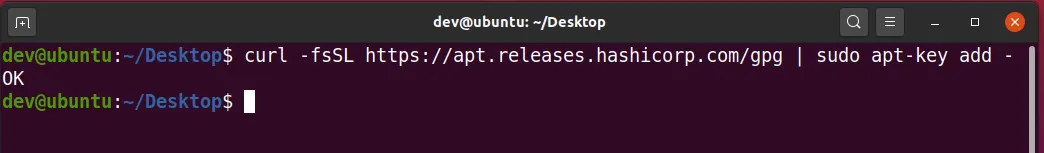


Figure 1: Terraform - Add-HashiCorp-signed-gpg-keys

\*\*\* If you are getting "**curl: command not found error**". Please install it first using below mentioned command.

**$ sudo apt install curl**

#### **Step2- Add HashiCorp package repository**

After adding the gpg key successfully. You need to add the *HashiCorp repository* to download and install terraform packages using **apt**.

**$ sudo apt-add-repository "deb [arch=$(dpkg --print-architecture)] https://apt.releases.hashicorp.com $(lsb\_release -cs) main"**

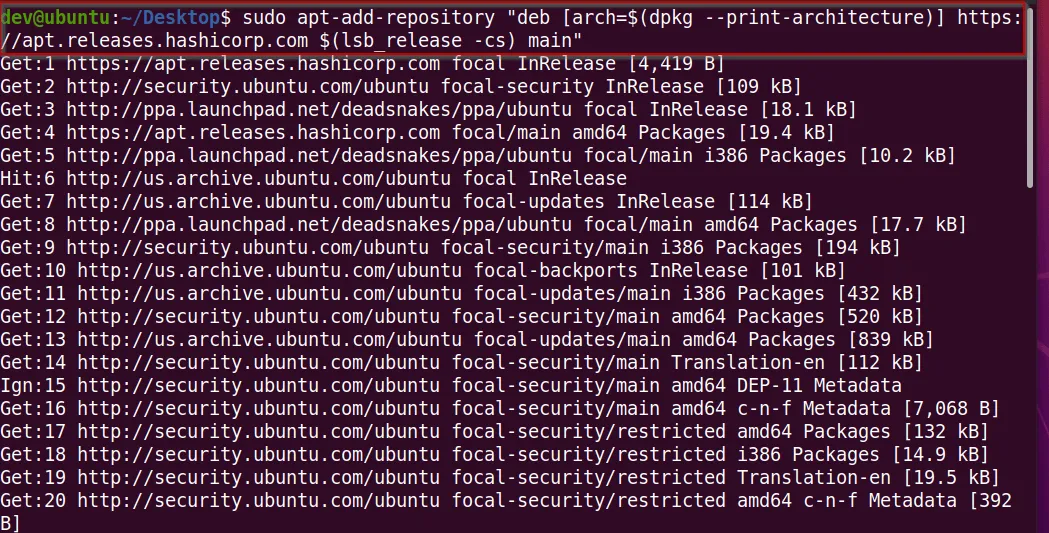


Figure 2: Terraform - Add-the-HashiCorp-repository

#### **Step3- Update "Ubuntu" packages list**

Always update packages list once you install and add any repository in Ubuntu.

**$ sudo apt update**

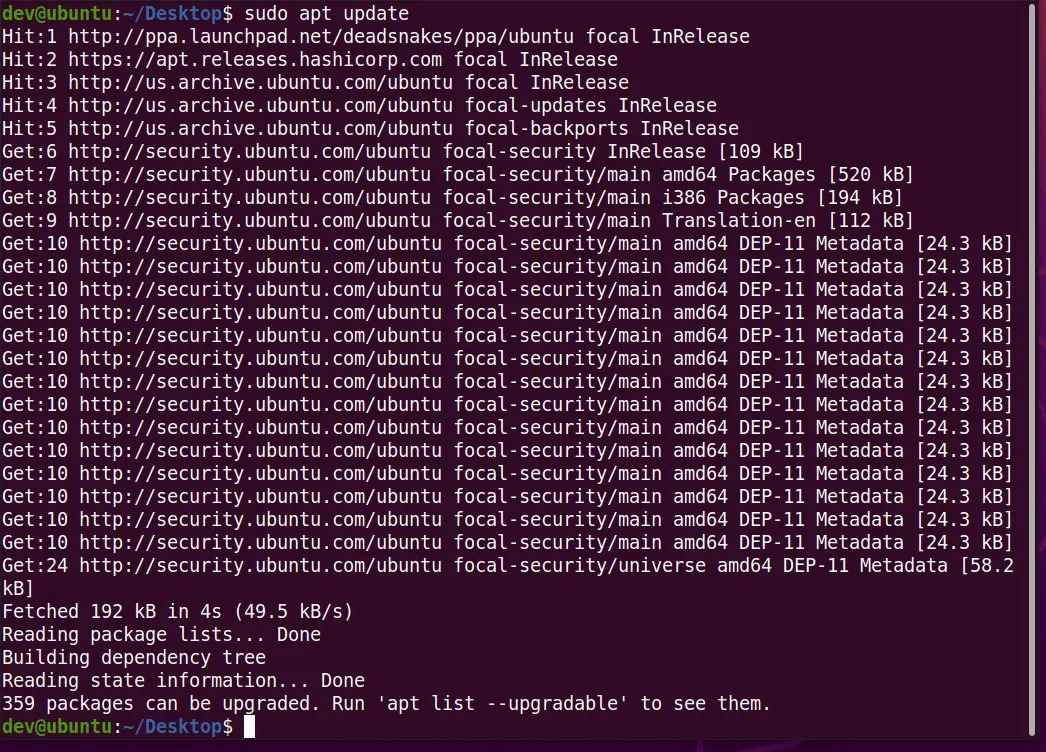


Figure 3: Terraform - sudo-apt-update

#### **Step4- Install Terraform on Ubuntu**

Please run following command to install Terraform.

**$ sudo apt install terraform**

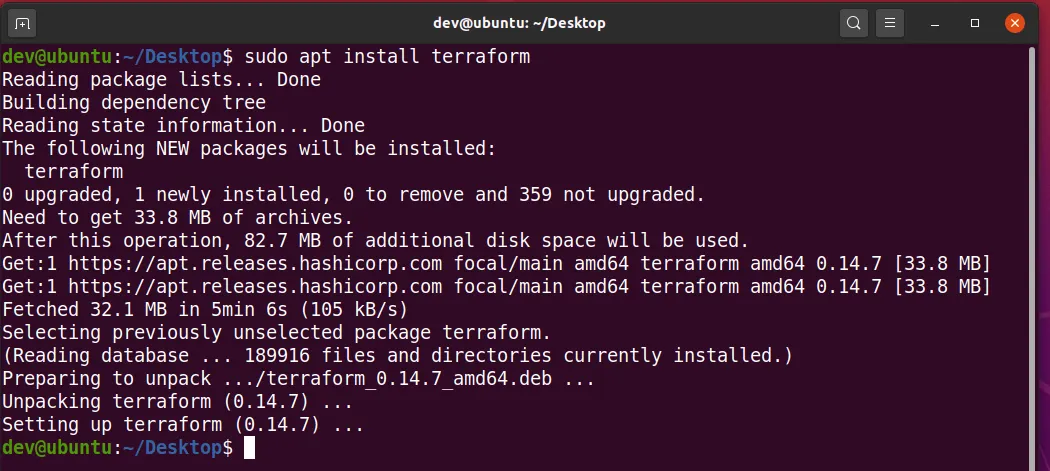


Figure 4: Terraform - Install-terraform-on-ubuntu-20.04

#### **Step5 - Check Terraform version**

Run**"terraform -v"**command to get the version.

Also, you can run "**which"**command to check the "**PATH**" of terraform command. It is**"/usr/bin/terraform**" as shown in image.

**# Check version of Terraform**

**$ terraform-v**

**# Check PATH of Terraform**

**$ which**

Text

Description automatically generated

Figure 5: Terraform - check-terraform-version

### Service Account for terraform:

#### Google Cloud Platform:

In Google Cloud Platform you need to create a service account with the following permissions for terraform to create resources

You need to create a service account for terraform with the following permissions:

* 1. compute.admin
  2. iam.serviceAccountUser
  3. resourcemanager.projectIamAdmin
  4. container.clusterAdmin
  5. compute.vieyour
  6. compute.securityAdmin
  7. container.developer
  8. iam.serviceAccountAdmin
  9. resourcemanager.projectIamAdmin
  10. storage.admin

To create service account, follow the below steps:

##### Step1: Create service account

To create the service account, run the **gcloud iam service-accounts create**command:

**gcloud iam service-accounts create SERVICE\_ACCOUNT\_ID \  
    --description="DESCRIPTION" \  
    --display-name="DISPLAY\_NAME"**

Replace the following values:

* + *SERVICE\_ACCOUNT\_ID*: the ID for the service account
  + *DESCRIPTION*: an optional description of the service account
  + *DISPLAY\_NAME*: a service account name to display in the console

##### Step2: Grant Policy to service account

To grant your service account an **IAM role** on your project, run the **gcloud projects add-iam-policy-binding** command:

**gcloud projects add-iam-policy-binding *PROJECT\_ID* \  
    --member="serviceAccount:*SERVICE\_ACCOUNT\_ID*@*PROJECT\_ID*.iam.gserviceaccount.com" \  
    --role="*ROLE\_NAME*"**

Replace the following values:

* + *PROJECT\_ID*: the project ID
  + *SERVICE\_ACCOUNT\_ID*: the service account ID
  + *ROLE\_NAME*: a role name, such as roles/compute.admin

#### AWS:

You need to create an IAM User for Terraform with the following permissions:

* IAM User with Administrative Access
* Amazon EC2 Full Access
* Amazon S3 Full Access
* Amazon EKS Full Access
* Amazon DynamoDB Full Access
* Amazon VPC Full Access

The above-mentioned permissions need to be attached to the IAM User created for Provisioning AWS Resources through Terraform and AWS-CLI.

To create service account, run below commands in AWS-CLI:

##### Step 1: Create User

**$ aws iam create-user**

##### Step 2: Create Role

**$ aws iam create-role --role-name EXAMPLE\_ROLE**

##### Step 3: Attach Policy to Role

**$ aws iam attach-role-policy --policy-arn arn:aws:iam::ACCOUNT\_ID:policy/EXAMPLE\_POLICY --role-name AmazonEKS\_EBS\_CSI\_DriverRole**

## Velero

### Create Google Service Account (GSA):

To integrate Velero with GCP, create a Velero-specific Service Account. Please run following commands in GCloud-CLI:

#### Step 1: View the current config

View your current config settings:

**gcloud config list**

#### Step 2: Variable

Store the project value from the results in the environment variable $PROJECT\_ID.

**PROJECT\_ID=$(gcloud config get-value project)**

#### Step 3: Create a service account:

**GSA\_NAME=velero**

**gcloud iam service-accounts create $GSA\_NAME \**

**--display-name "Velero service account"**

Then list all accounts and find the velero account you just created:

**gcloud iam service-accounts list**

Set the $SERVICE\_ACCOUNT\_EMAIL variable to match its email value.

**SERVICE\_ACCOUNT\_EMAIL=$(gcloud iam service-accounts list \**

**--filter="displayName:Velero service account" \**

**--format 'value(email)')**

### Create Custom Role with Permissions for the Velero GSA:

These permissions are required by Velero to manage snapshot resources in the GCP Project. Paste below lines in CLI and run:

**```bash**

**ROLE\_PERMISSIONS=(**

**compute.disks.get**

**compute.disks.create**

**compute.disks.createSnapshot**

**compute.snapshots.get**

**compute.snapshots.create**

**compute.snapshots.useReadOnly**

**compute.snapshots.delete**

**compute.zones.get**

**storage.objects.create**

**storage.objects.delete**

**storage.objects.get**

**storage.objects.list**

**)**

**gcloud iam roles create velero.server \**

**--project $PROJECT\_ID \**

**--title "Velero Server" \**

**--permissions "$(IFS=","; echo "${ROLE\_PERMISSIONS[\*]}")"**

**gcloud projects add-iam-policy-binding $PROJECT\_ID \**

**--member serviceAccount:$SERVICE\_ACCOUNT\_EMAIL \**

**--role projects/$PROJECT\_ID/roles/velero.server**

**```**

### Grant access to Velero

This involves creating a Google Service Account Key and using it as --secret-file during installation.

Create a service account key, specifying an output file (credentials-velero) in your local directory:

**gcloud iam service-accounts keys create credentials-velero \**

**--iam-account $SERVICE\_ACCOUNT\_EMAIL**

### Velero on AWS

#### Creating AWS IAM Account:

To integrate Velero with AWS, create a Velero-specific IAM User. Please run following commands**:**

**aws iam create-user –user-name velero**

#### Create Custom Role policies for Velero IAM User:

Add the following permissions to the Velero IAM User

**{  
 "Version":"2012-10-17",  
 "Statement":[  
 {  
 "Effect":"Allow",  
 "Action":[  
 "ec2:DescribeVolumes",  
 "ec2:DescribeSnapshots",  
 "ec2:CreateTags",  
 "ec2:CreateVolume",  
 "ec2:CreateSnapshot",  
 "ec2:DeleteSnapshot"  
 ],  
 "Resource":"\*"  
 },  
 {  
 "Effect":"Allow",  
 "Action":[  
 "s3:GetObject",  
 "s3:DeleteObject",  
 "s3:PutObject",  
 "s3:AbortMultipartUpload",  
 "s3:ListMultipartUploadParts"  
 ],  
 "Resource":[  
 "arn:aws:s3:::${VELERO\_BUCKET}/\*"  
 ]  
 },  
 {  
 "Effect":"Allow",  
 "Action":[  
 "s3:ListBucket"  
 ],  
 "Resource":[  
 "arn:aws:s3:::${VELERO\_BUCKET}"  
 ]  
 }  
 ]  
 }**

#### Configuring AWS Credentials:

To configure Velero with AWS, please run following command:

**aws configure**

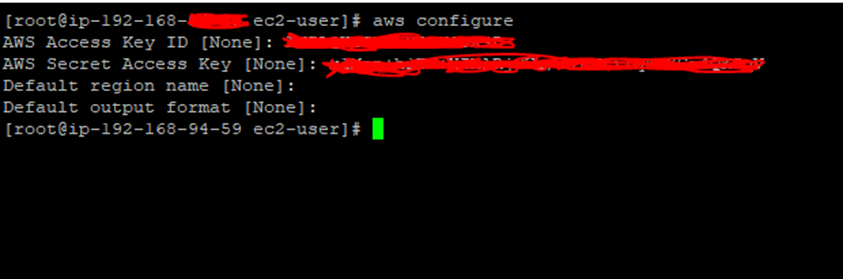


Figure 6: Credentials for Velero

Replace the Access key, secret key, default region and default output format with specific values.

## Jenkins Pipeline Setup:

Please refer “Appendix A: Installation of Jenkins in Ubuntu” for the steps to install and configure the Jenkins in Ubuntu. For other distributions or OS, please refer official documentation.

### Creating Pipeline Jobs in Jenkins:

**Step 1:** In Jenkins, click on**‘New Item’** to create a new project.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 7:Jenkins - New Job

**Step 2: Give your project a name, then choose ‘Pipeline’ and finally, click on ‘OK’.**

Graphical user interface, text

Description automatically generated with medium confidence

Figure 8:Jenkins - Job Description

**Step3:** In the Definition choose Pipeline script from SCM from the Drop Down and Git in the SCM from the drop down.

**Step4:** Input the GitHub private SSH repo URL in Repository URL. In the credentials field choose the GitHub credentials from the drop down.

Graphical user interface, text, application, email

Description automatically generated

Figure 9: Jenkins - pipeline

**Step 5**: Specify the branch name of GitHub and the pipeline script path.

Graphical user interface, text, application, email, Teams

Description automatically generated

Figure 10: Jenkins - Git repo

# Cloud Scheduler

For the cloud scheduler you must store the code in the GitHub repository. And create four pipeline jobs in Jenkins.

## Job 1: Auto Shutdown and Start-up

The Auto Shutdown and Start-up job will schedule the resources with the help of cron jobs. You need to give the start-up and shut down time in the auto start-up and shutdown Jenkins file (autostsh.jenkins). In the Jenkins file under **pipelineTriggers** you need to make the changes. You need to provide the time as cron job and the time zone of the resources. Along with the time in cron job you must provide the variable and the value of the variable.

Below is as example:

Text

Description automatically generated with low confidence

Figure 11: Jenkins File - Auto shutdown and start-up

In this example time zone is set as Asia/Calcutta i.e., **TZ=Asia/Calcutta**

For the start-up job of SBX environment in GCP you are setting time as 09:15 AM every day from Monday to Friday and passing the variable and it parameter as **Environs=SBX;Mode=STARTUP;Provier=GCP.**

For the start-up job of SBX environment in GCP you are setting time as 06:45 PM every day from Monday to Friday passing the variable and it parameter as **Environs=SBX;Mode=STARTUP;Provier=GCP.**

For cron job you can refer this website to convert time to cron [Crontab.guru - The cron schedule expression editor](https://crontab.guru/)

## Job 2: VM Start and Shutdown

The VM Start ad shutdown job will start and shutdown the VM’s as per the schedule. In the Jenkins file (vmstsh.jenkins) you have to provide the desired VM details. In the Jenkins file under the **stage,** you must provide the instance details such as: instance name, instance zone and the instance project id.

Below is as example:

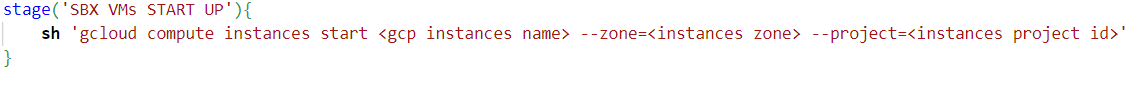


Figure 12: Jenkins File - VM Start-up

In the example you must provide the instance name, instances zone and instances project id for the instance you like to include in SBX environment.

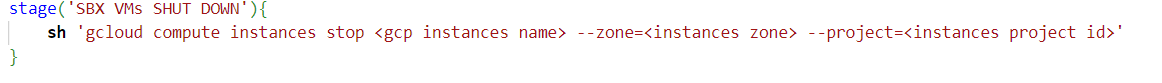


Figure 13: Jenkins File - VM Shutdown

Same way for shutdown also you must provide the instance name, instances zone and instances project id for the instance you like to include in SBX environment.

## Job 3: Terraform restore and destroy

The Terraform restore and destroy pipeline job will create the cluster upon receiving restore parameter and will destroy the cluster upon receiving destroy parameter. In the Jenkins file tfcrdt.jenkins you have to provide the cluster name and the zone of the cluster under stage.

Text

Description automatically generated

Figure 14: Jenkins File - Terraform

For this example of SBX Environment you must provide the GCP cluster name and the zone of the cluster.

You have to provide the details of the cluster in the variables\_auto.tfvars file.

## Job 4: Velero Backup and Restore

In the Velero backup and restore job will perform the backup of cluster and restoring of the cluster. In the Jenkins file vlrcbc.jenkins you have to provide the cluster name and the bucket name.

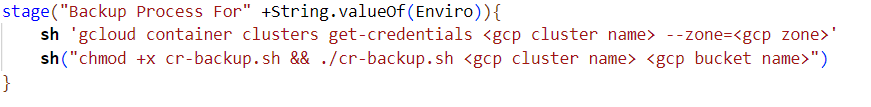


Figure 15: Jenkins File - Velero Backup

In the example you must provide the GCP cluster name and GCP zone and GCP bucket name.

Same way for restore also you must provide the details.

Text

Description automatically generated with medium confidence

Figure 16: Jenkins File - Velero Restore

In the example you must provide the GCP cluster name, GCP zone and GCP bucket name.

**Note:**

1. The same pipeline jobs can be configured for AWS with the help of provided pipeline Jenkins templates in the artifacts. Similar configurations can be maintained for EC2 instances, S3 buckets for backups and restoration of EKS clusters through Velero.
2. You can verify the backups by checking the S3 buckets in AWS or Cloud Storage in GCP.

# Troubleshooting Guide

## Issues with AWS-CLI setup

While setting up AWS-CLI make sure you are installing the latest version. And you may also phase some common errors like not moving the downloaded binary file to the correct location. And check the version after moving the file to a particular location.

Correct location: **$ ./aws/install -i /usr/local/aws-cli -b /usr/local/bin**

## Issues with AWS- Authentication

While running the **$ aws configure** command need to double-check whether we are pasting the right credentials like access key, secret access key, and region code.

## Issues with Google Cloud-CLI Authentication

Once Google Cloud SDK in installed make sure you initialize the Gcloud CLI by using the **init** command. If your system does not support browser, then use **init** **--console-only**.

Make sure you login with the correct username to view the list of projects you have access.

When prompted for the project id and default zone make sure you have selected the correct project id and default zone same as the Jenkins worker node project and zone.

## Issues with Terraform Setup

While installing Terraform make sure you are installing the latest version of Terraform. And while moving the downloaded binary file make sure that you are moving the file to the correct location.

Correct location: **sudo mv terraform /usr/local/bin**

Check Version: **terraform -version**

**Terraform v1.2.6**

**on linux\_amd64**

## Issues with setting up IAM Users, Roles, and Policies through CLI

While setting up IAM users, roles, policies through AWS-CLI / Google Cloud CLI, ensure to have the authenticated user has valid permissions to perform those operations. If not, assign the necessary permissions to the authenticated user first and try setting up policies to other resources.

Make sure you create two separate service account for terraform to create the resources and velero to take backup of the Kubernetes clusters. Then generate the json key for the both the account and upload it to the Jenkin’s worker node for terraform and velero to have access to the service account json files. Keep a copy of the json files in other location with limited accessibility as a backup, if your Jenkin’s worker node json files gets corrupted you can replace with the backup one.

## Issues with Velero Setup

Velero setup might face issues if any of the mentioned permissions are not assigned to the IAM user created for Velero setup. Refer the official documents for assigning roles and permissions to a user through AWS-CLI / Google Cloud CLI.

## Issues with setting up pipeline jobs in Jenkins

It is recommended to maintain separate worker nodes for GCP and AWS environments to avoid conflicts while working with Kubernetes clusters.

Refer the below article for creating worker nodes under Jenkins master node.

<https://chathura-siriwardhana.medium.com/step-by-step-guide-to-add-jenkins-slave-nodes-f2e756c8849e>

1. While setting up auto shutdown and start-up Jenkin’s job 1, you must follow valid format for cron job timer else pipelines might fail to auto shutdown or start-up when needed.
2. In Pipeline Job 1, make sure you pass on correct value for the variable along with the cron job.
3. While setting up VM start and shutdown Jenkin’s job 2, you must specify the correct machine name and zone and project id of the machine for GCP and for AWS you must specify the correct VM id.
4. While setting up terraform restore and destroy Jenkin’s job 3, make sure you are passing the correct variable file and specifying the correct value for “environment” variable.
5. If you get error “403 permission denied” while running terraform Jenkin’s job 3, you must give required permission to the terraform service account.
6. While giving permission to the service account user must login with user account which have access to IAM.
7. While setting up the velero backup and restore Jenkin’s job 4, you must give correct Kubernetes cluster and cloud bucket name for velero to take backup of the cluster.
8. In Jenkin’s job 4, make sure you are using the same backet name for both backup and restore process of the Kubernetes cluster.
9. For these jobs to work, you must setup AWS-CLI / Google Cloud SDK and authentication in the worker node. Also, ensure to assign valid permissions.
10. Ensure to provide valid values for variables in Terraform templates and Terraform setup must follow above mentioned instructions to create or destroy resources.
11. Ensure Velero setup is properly done to perform backup and restore operations in Kubernetes clusters.

# Appendix A: Installation of Jenkins in Ubuntu

## A.1. Prerequisites for Jenkins installation:

Minimum hardware requirements:

* 256 MB of RAM
* 1 GB of drive space

Recommended hardware configuration for a small team:

* 4 GB+ of RAM
* 50 GB+ of drive space

## A.2. Installation of Java:

Java is required to run Jenkins.

To install Java, run following in terminal:

**$ sudo apt update**

**$ sudo apt install openjdk-11-jre**

## A.3. Jenkins Installation:

The version of Jenkins included with the default Ubuntu packages is often behind the latest available version from the project itself. To ensure you have the latest fixes and features, use the project-maintained packages to install Jenkins.

First, add the repository key to the system:

**$ wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add –**

After the key is added the system will return with OK.

Next, let’s append the Debian package repository address to the server’s ‘**sources.list’**:

**$ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'**

After both commands have been entered, you’ll run update so that apt will use the new repository.

**$ sudo apt update**

Finally, you’ll install Jenkins and its dependencies.

**$ sudo apt install jenkins**

Now that Jenkins and its dependencies are in place, you’ll start the Jenkins server.

## A.4. Starting Jenkins:

Let’s start Jenkins by using [systemctl](https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units):

**$ sudo systemctl start Jenkins**

Since **systemctl** doesn’t display status output, you’ll use the status command to verify that Jenkins started successfully:

**$ sudo systemctl status Jenkins**

Now that Jenkins is up and running, let’s adjust your firewall rules so that you can reach it from a web browser to complete the initial setup.

## A.5. Setting Up Jenkins

To set up your installation, visit Jenkins on its default port, 8080, using your server domain name or IP address: http://your\_server\_ip\_or\_domain:8080

You should receive the Unlock Jenkins screen, which displays the location of the initial password:

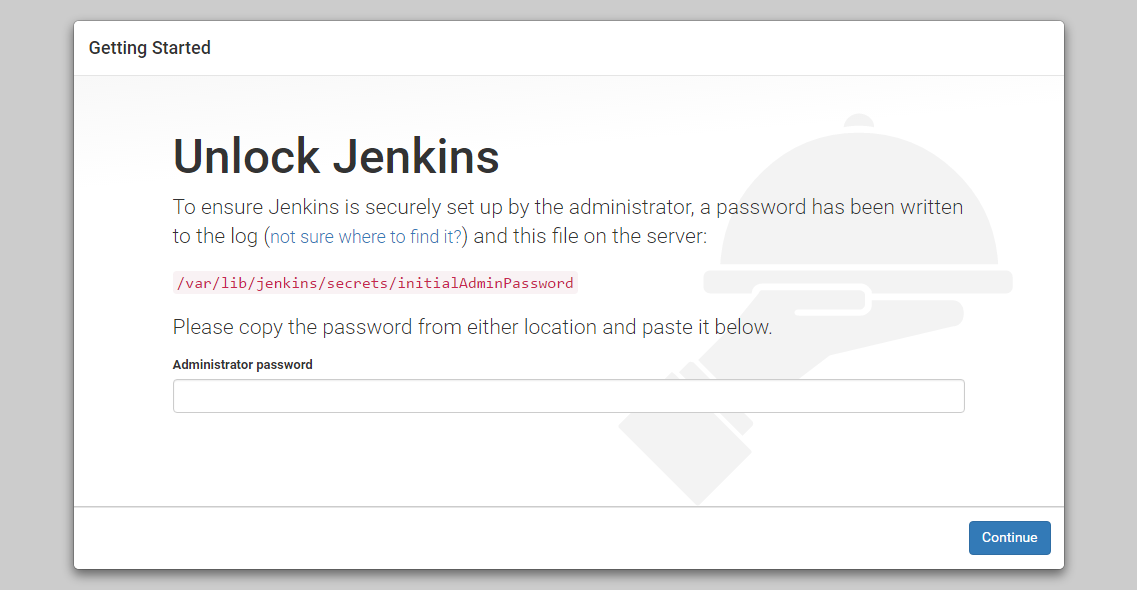


Figure 17: Jenkins - Unlock Jenkins

In the terminal window, use the **cat** command to display the password:

**$ sudo cat /var/lib/Jenkins/secrets/initialAdminPassword**

Copy the 32-character alphanumeric password from the terminal and paste it into the Administrator password field, then click Continue.

The next screen presents the option of installing suggested plugins or selecting specific plugins:

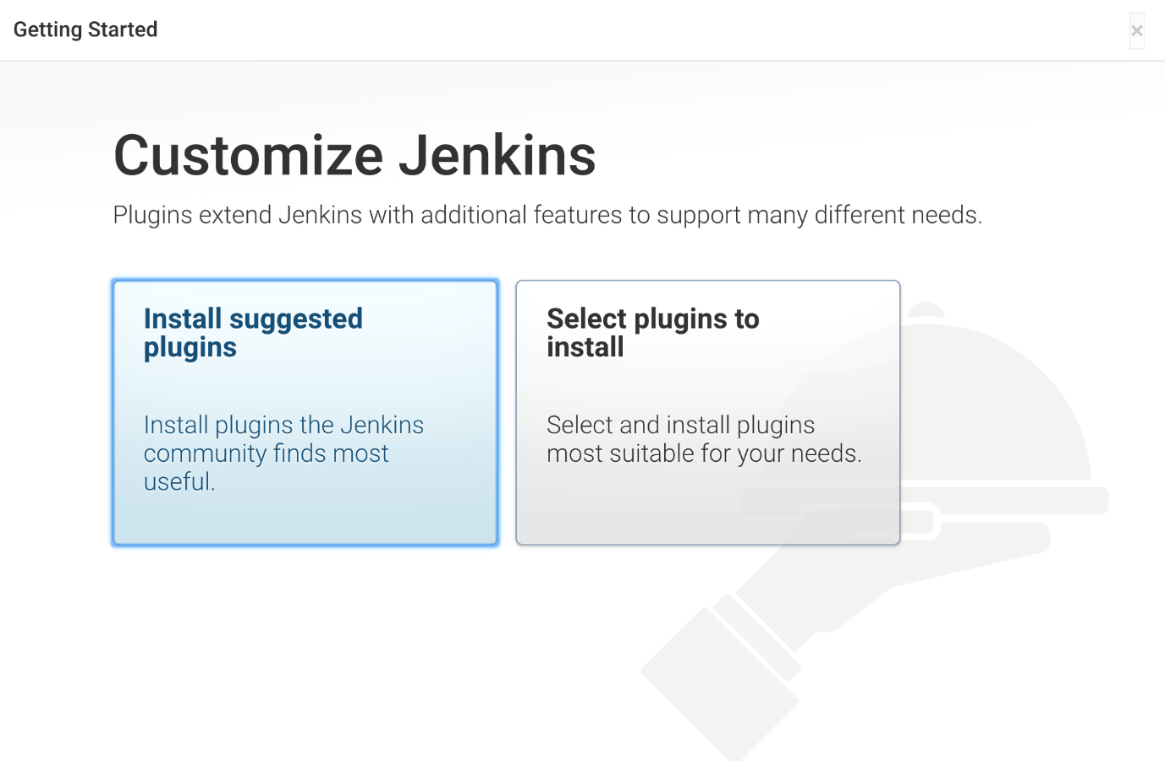


Figure 18: Jenkins - Select Plugin to Install

Click the Install suggested plugins option, to begin the installation process.

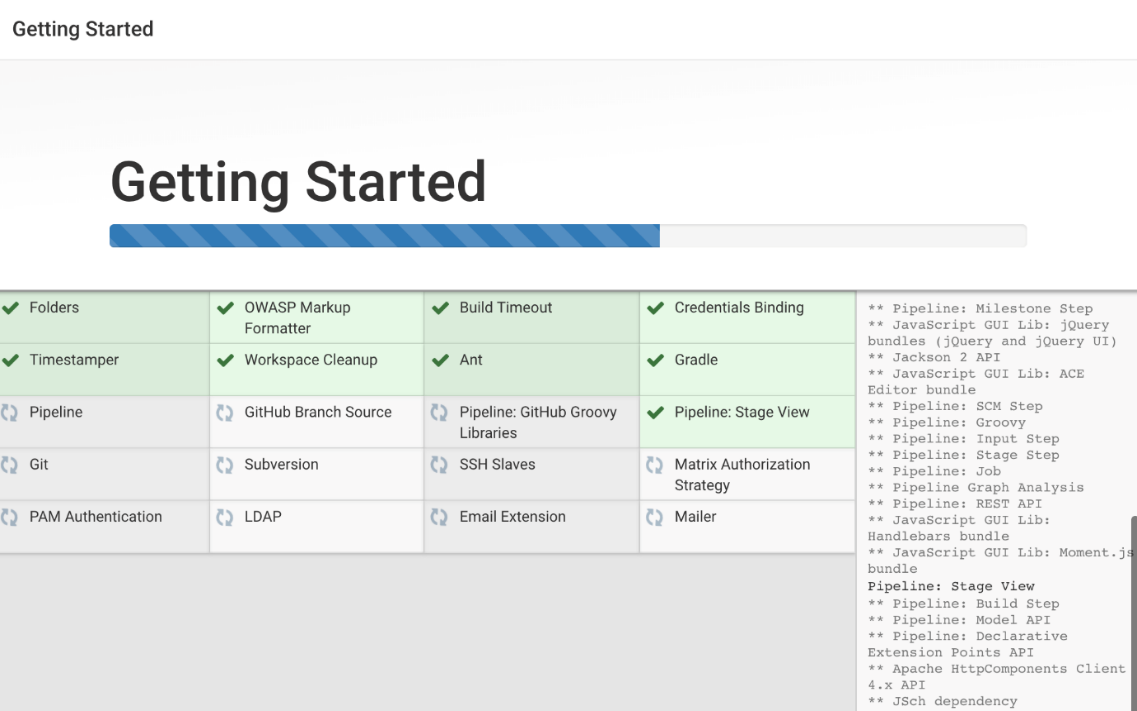


Figure 19: Jenkins - Plugin Installation

When the installation is complete, you’ll be prompted to set up the first administrative user. It’s possible to skip this step and continue as admin using the initial password you used above, but you’ll take a moment to create the user.

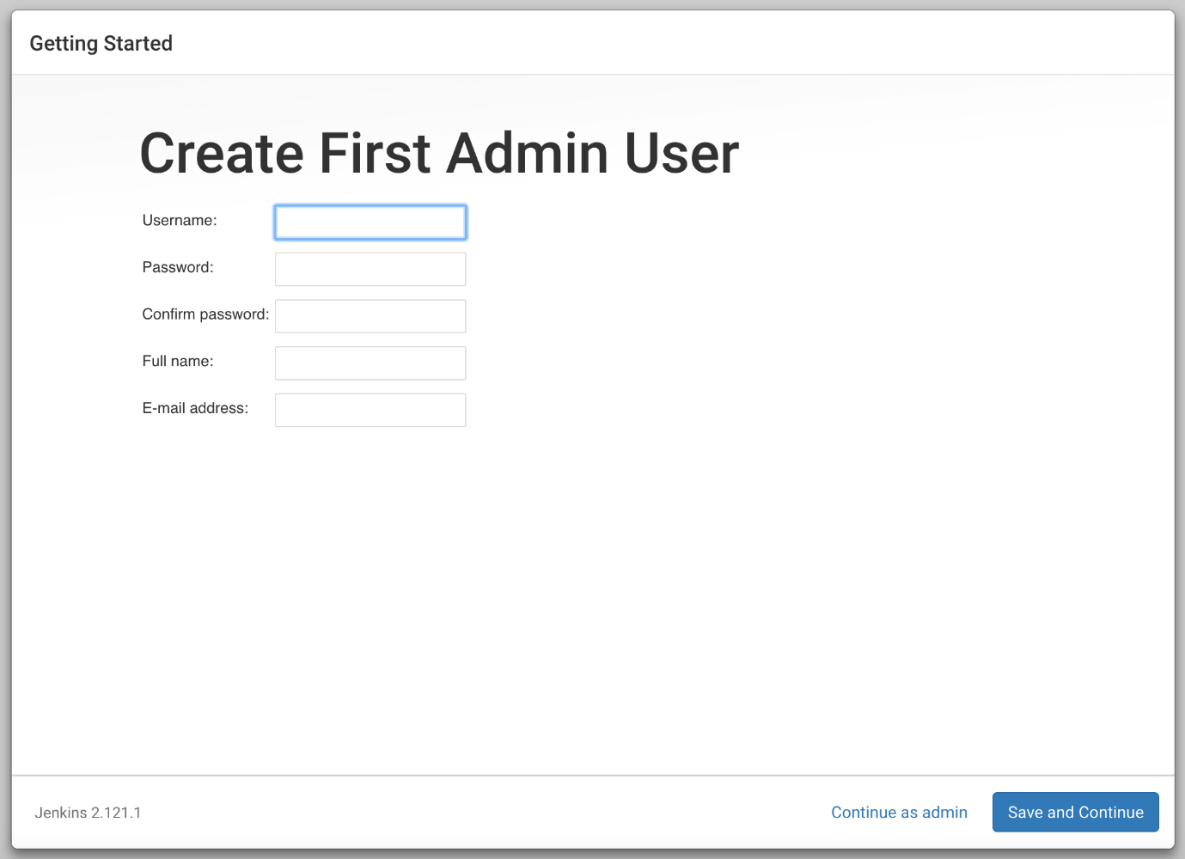


Figure 20: Jenkins - Create Admin User

Enter the name and password for your user:

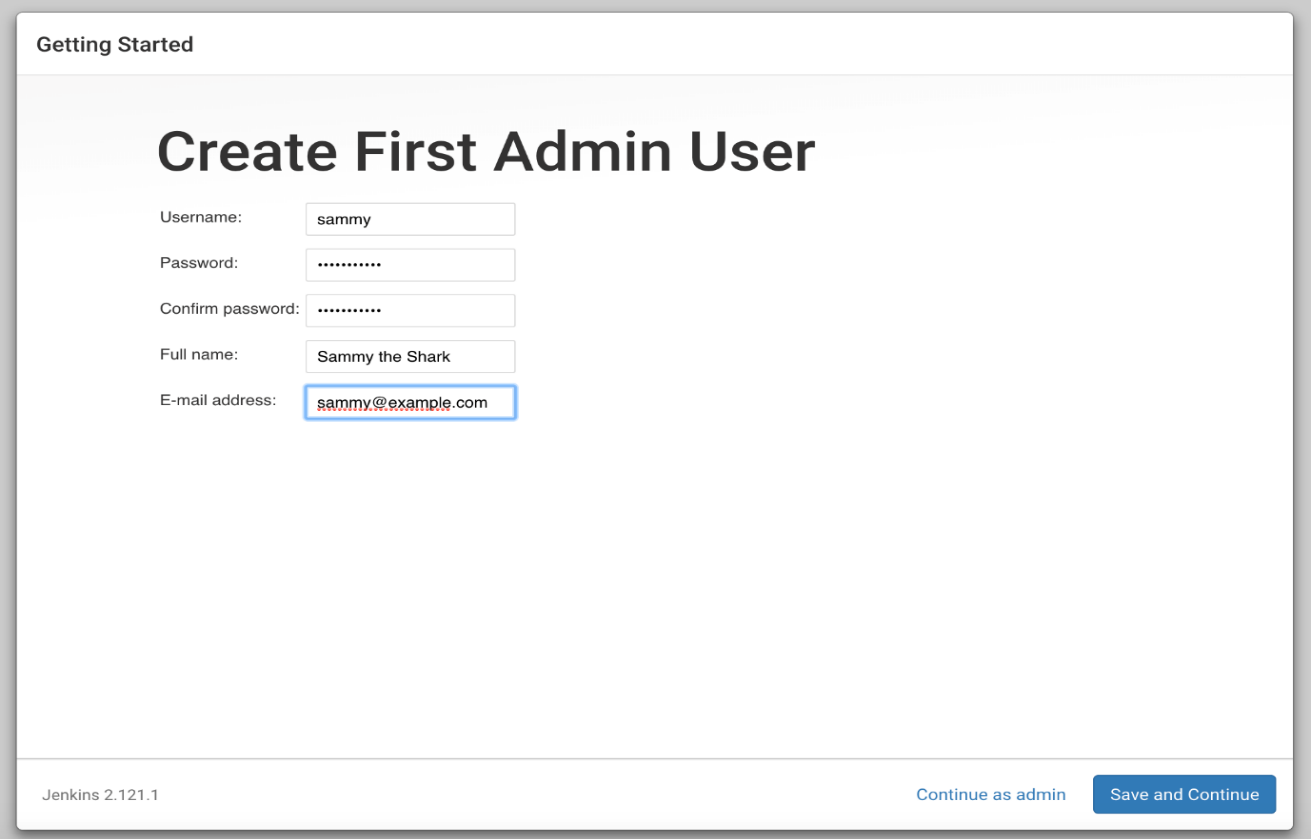


Figure 21: Jenkins - Admin User Details

You’ll receive an **Instance Configuration** page that will ask you to confirm the preferred URL for your Jenkins instance. Confirm either the domain name for your server or your server’s IP address:

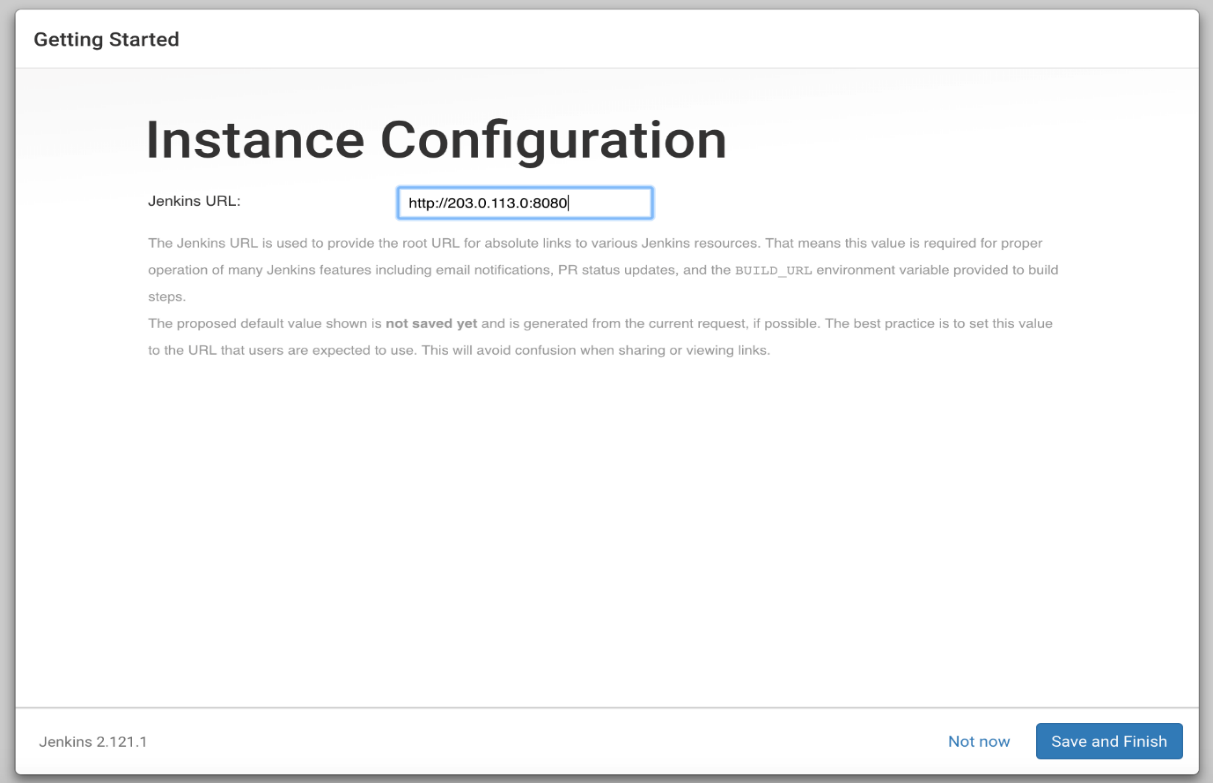


Figure 22: Jenkins - Jenkins URL

After confirming the appropriate information, click **Save and Finish**. You’ll receive a confirmation page confirming that **“Jenkins is Ready!”:**

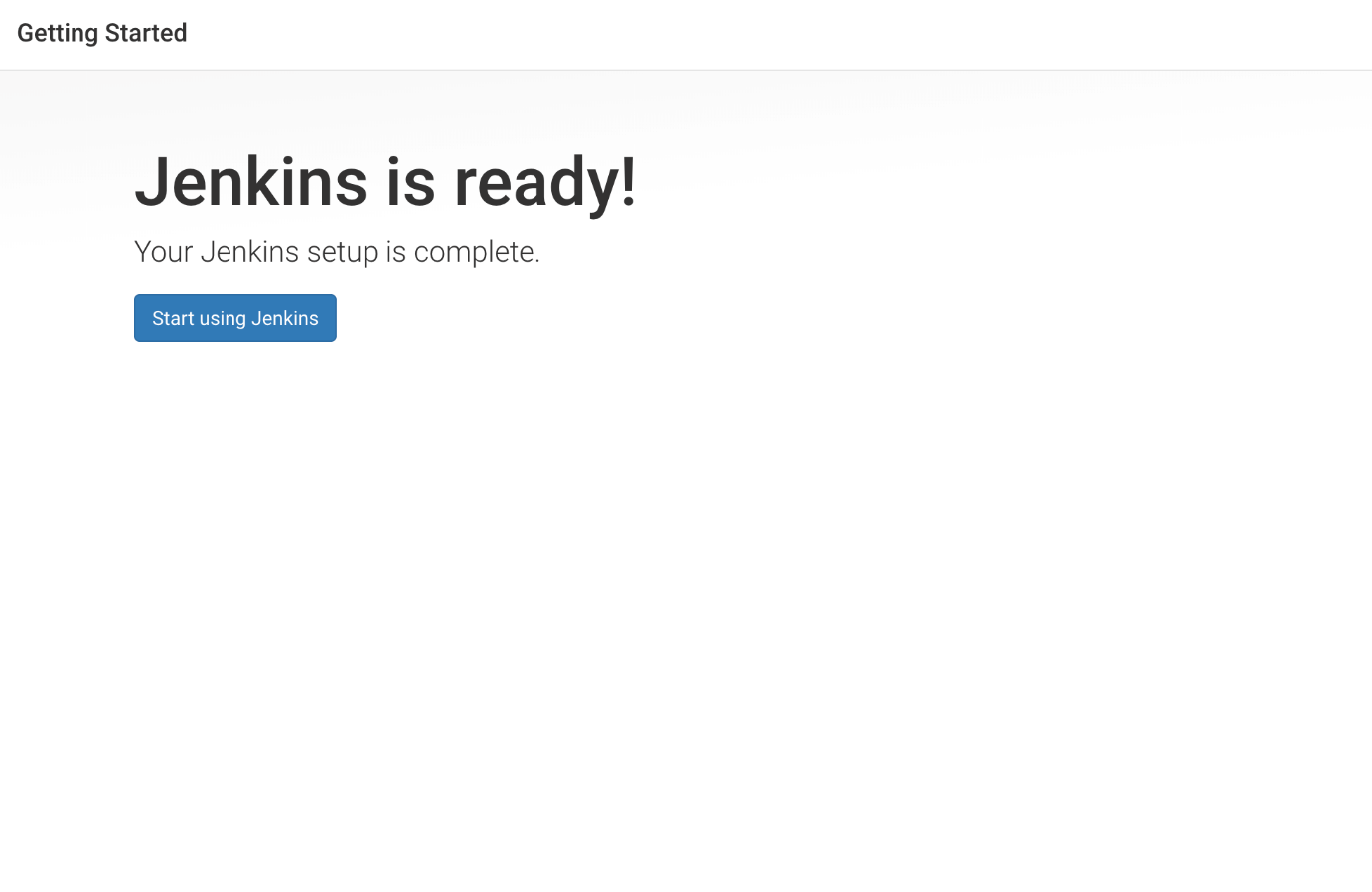


Figure 23: Jenkins - Installation Finish

Click **Start** using **Jenkins** to visit the main Jenkins dashboard:

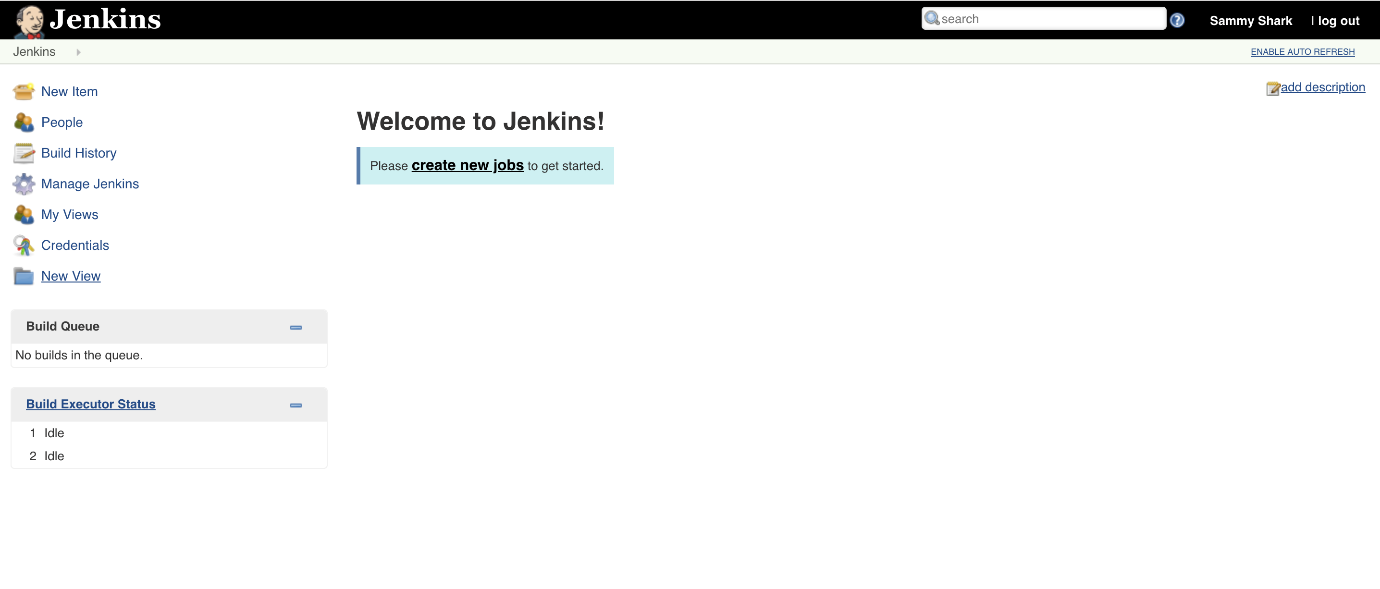


Figure 24: Jenkins - Welcome Page

At this point, you have completed a successful installation of Jenkins.

|  |  |
| --- | --- |
| **TERM** | **DEFINITION** |
| GCP | Google Cloud Platform |
| AWS | Amazon Web Services |
| AWS-CLI | AWS-Command Line Interface |
| SBX | Sand Box Environment |
| VM | Virtual Machine |
| SDK | Software Development Kit |

# Glossary

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Section Changed** | **Description** | **Author** |
| 23 Aug. 2022 | 1.0 | All | Initial Draft | Ashok Das, Tinku Manivikesh Chukkapalli |
|  |  |  |  |  |