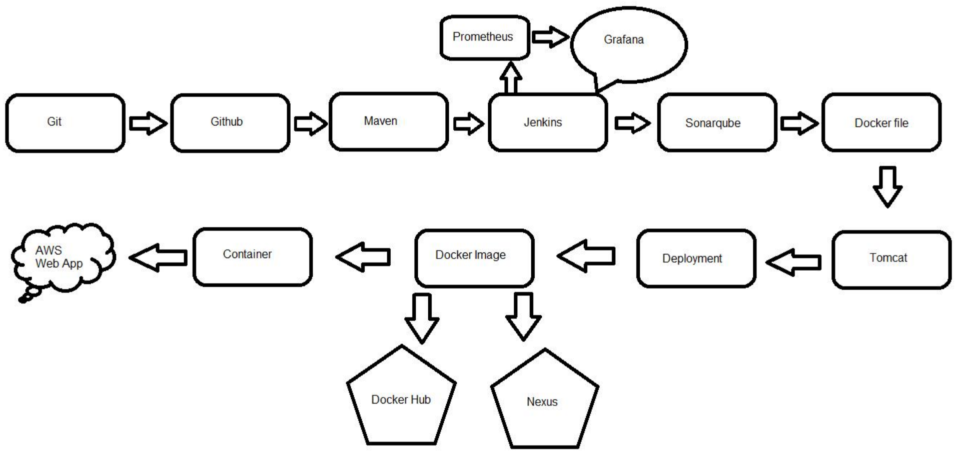
DevOps Project

Continuous Integration and Continuous Deployment/Delivery.

Managed and build a web application image pushed to Docker hub and Nexus Private repo. Deployed in Tomcat Server using Jenkins.

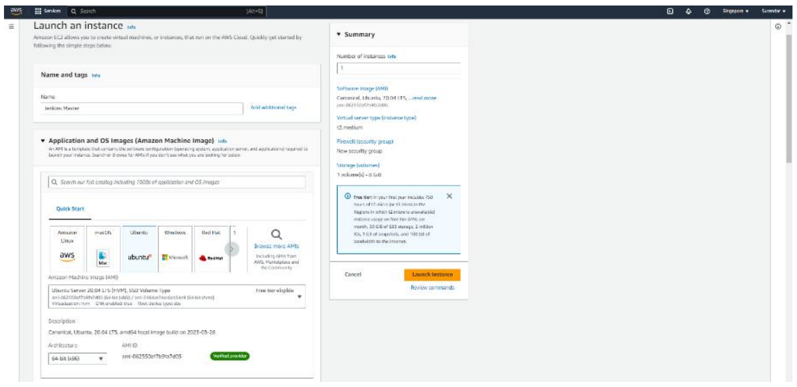
Tools used in DevOps:



Steps to Create CICD Project:

Jenkins EC2 Server

Launch an EC2 instance – Ubuntu 20.04 – RAM t2.medium – Security group (Alltraffic) – Storage 30gib.



Launch an instance

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

Name: Jenkins Master

Application and OS Images (Amazon Machine Image)

Amazon Machine Image (AMI): Ubuntu Server 20.04 LTS (HVM), SSD Volume Type — Free tier eligible

Description: Canonical, Ubuntu, 20.04 LTS, amd64 focal image build on 2023-03-28

Architecture: 64-bit (x86)

AMI ID: ami-062550af7b9fa7d05 — Verified provider

Summary

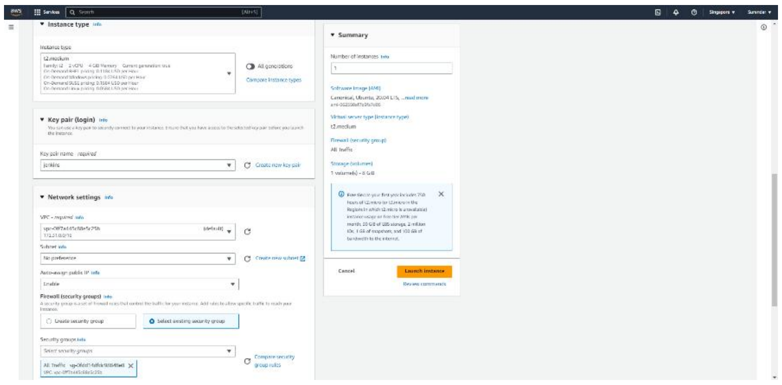
Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 20.04 LTS, ...read more

Virtual server type (instance type): t2.medium

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB



Instance type

Instance type: t2.medium — Family: t2 2 vCPU 4 GiB Memory Current generation: true

On-Demand SUSE pricing: 0.1584 USD per Hour

Key pair (login)

Key pair name - required: jenkins

Network settings

VPC - required: (default)

Subnet: No preference

Auto-assign public IP: Enable

Firewall (security groups): Select existing security group

Security groups: All Traffic

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 20.04 LTS, ...read more

Virtual server type (instance type): t2.medium

Firewall (security group): All Traffic

Storage (volumes): 1 volume(s) - 8 GiB

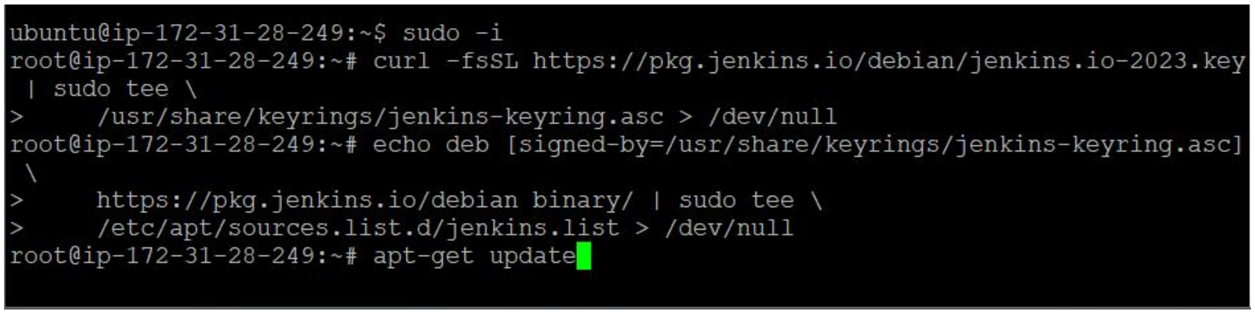
Connect the Jenkins Ec2 server in putty

Steps to Install Java and Jenkins.

Jenkins keys

Add Jenkins key to repo

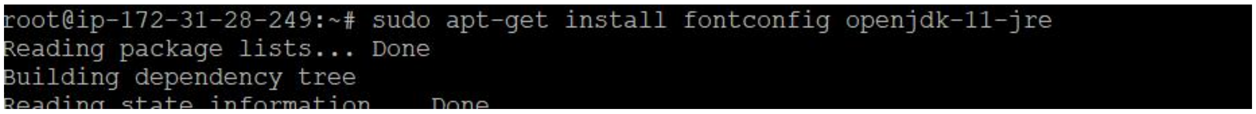
#apt-get update



```
ubuntu@ip-172-31-28-249:~$ sudo -i
root@ip-172-31-28-249:~# curl -fsSL https://pkg.jenkins.io/debian/jenkins.io-2023.key
 | sudo tee \
>     /usr/share/keyrings/jenkins-keyring.asc > /dev/null
root@ip-172-31-28-249:~# echo deb [signed-by=/usr/share/keyrings/jenkins-keyring.asc]
 \
>     https://pkg.jenkins.io/debian binary/ | sudo tee \
>     /etc/apt/sources.list.d/jenkins.list > /dev/null
root@ip-172-31-28-249:~# apt-get update
```

Install Java package.

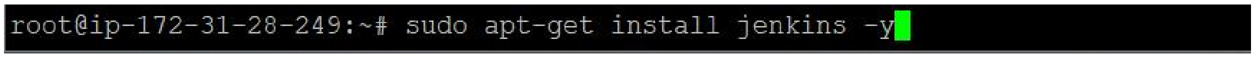
#sudo apt-get install fontconfig openjdk-11-jre -y



```
root@ip-172-31-28-249:~# sudo apt-get install fontconfig openjdk-11-jre
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Now, Install Jenkins package

#sudo apt-get install Jenkins -y

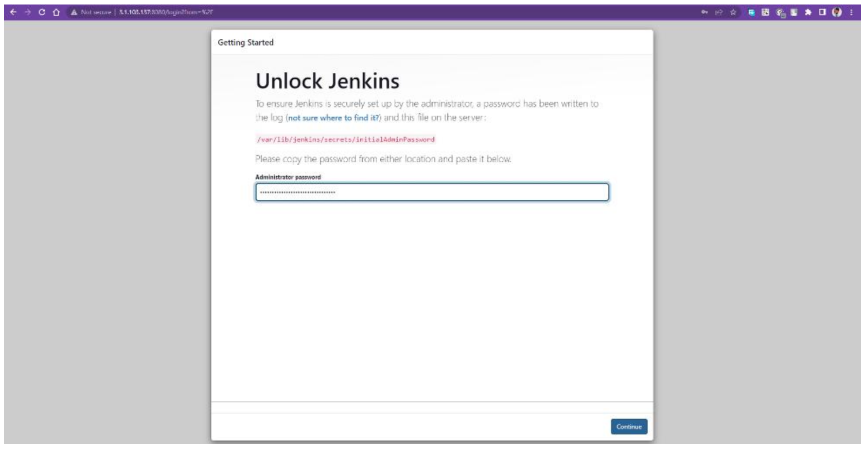


```
root@ip-172-31-28-249:~# sudo apt-get install jenkins -y
```

Copy Jenkins Ec2 Server Ipv4 add

Hit in browser

Copy Admin Password path and paste in Jenkins Ec2 Server



Not secure | 3.1.103.137:8080/login?from=%2F

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.

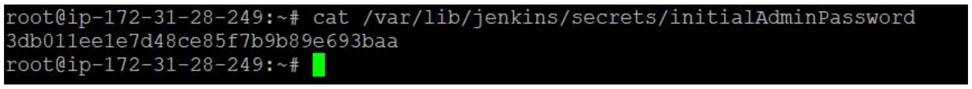
Administrator password

································

Continue

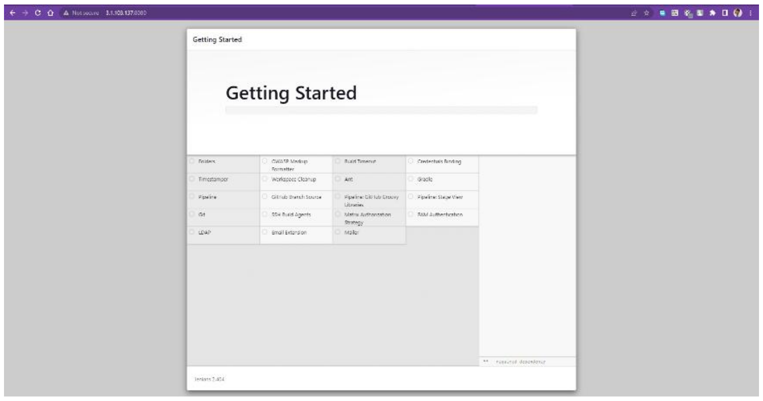
Cat the Administrator Password path in Jenkins Ec2 Server

Copy the admin authentication password Paste in browser to unlock Jenkins.



```
root@ip-172-31-28-249:~# cat /var/lib/jenkins/secrets/initialAdminPassword
3db011ee1e7d48ce85f7b9b89e693baa
root@ip-172-31-28-249:~#
```

Install the Suggest Plugins.



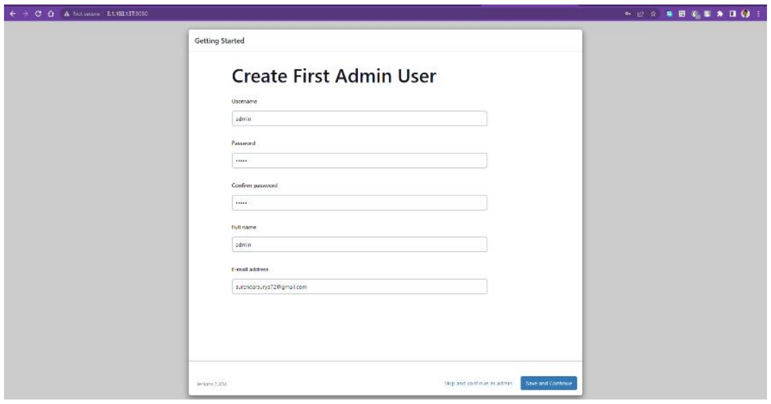
Getting Started

Getting Started

Folders	OWASP Markup Formatter	Build Timeout	Credentials Binding
Timestamper	Workspace Cleanup	Ant	Gradle
Pipeline	GitHub Branch Source	Pipeline: GitHub Groovy Libraries	Pipeline: Stage View
Git	SSH Build Agents	Matrix Authorization Strategy	PAM Authentication
LDAP	Email Extension	Mailer	

Jenkins 2.404

Create a admin user credentials.



Getting Started

Create First Admin User

Username: admin

Password: •••••

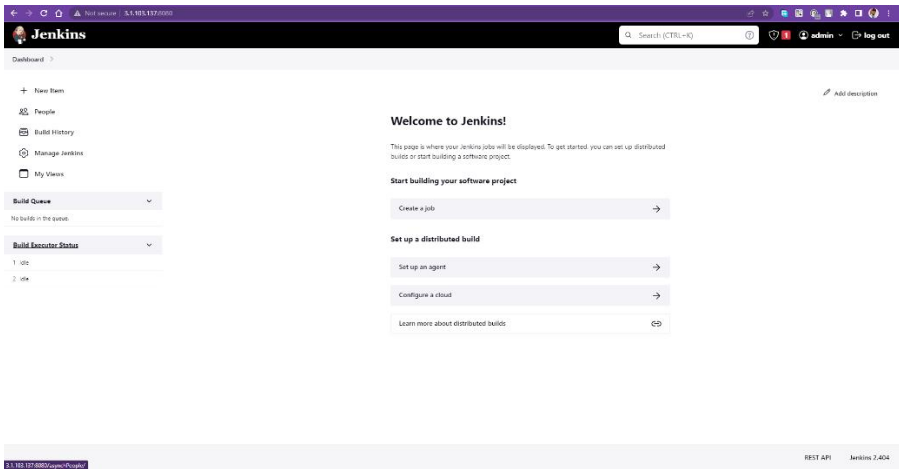
Confirm password: •••••

Full name: admin

E-mail address: surendarsurya72@gmail.com

Jenkins 2.404

Jenkins Dashboard is Successfully Hosted.



Welcome to Jenkins!

This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.

Start building your software project

Set up a distributed build

No builds in the queue.

1 Idle

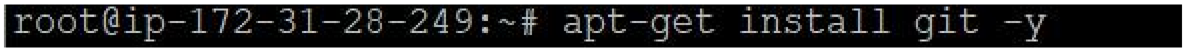
2 Idle

Jenkins 2.404

In Jenkins Ec2 Server.

Install git package.

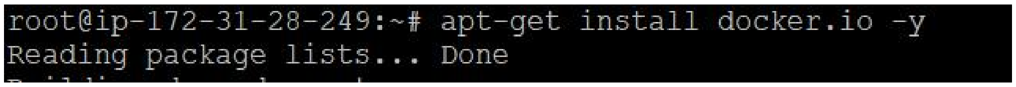
#apt-get install git -y



```
root@ip-172-31-28-249:~# apt-get install git -y
```

Install docker package

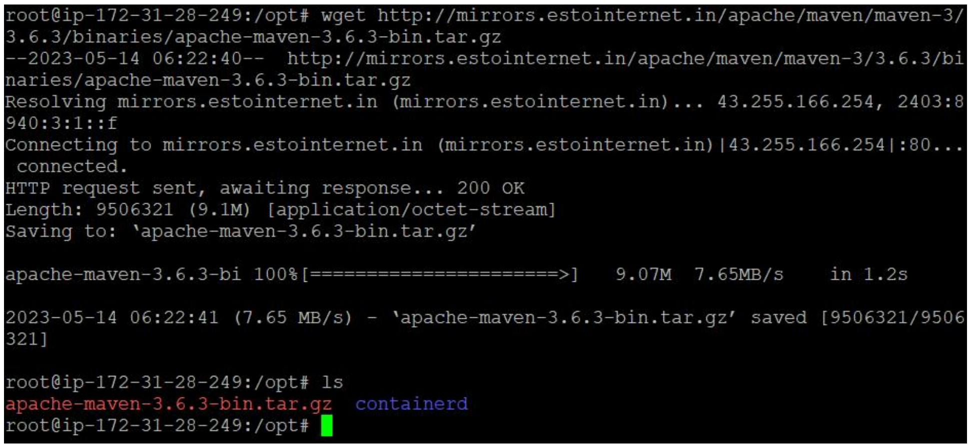
#apt-get install docker.io -y



```
root@ip-172-31-28-249:~# apt-get install docker.io -y
Reading package lists... Done
```

Download Maven tar file using wget cmnd.

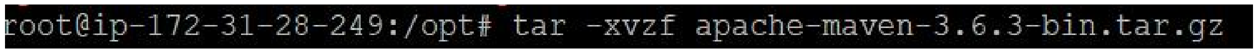
#wget http://mirrors.estointernet.in/apache/maven/maven-3/3.6.3/binaries/apache-maven-3.6.3-bin.tar.gz



```
root@ip-172-31-28-249:/opt# wget http://mirrors.estointernet.in/apache/maven/maven-3/
3.6.3/binaries/apache-maven-3.6.3-bin.tar.gz
--2023-05-14 06:22:40--  http://mirrors.estointernet.in/apache/maven/maven-3/3.6.3/bi
naries/apache-maven-3.6.3-bin.tar.gz
Resolving mirrors.estointernet.in (mirrors.estointernet.in)... 43.255.166.254, 2403:8
940:3:1::f
Connecting to mirrors.estointernet.in (mirrors.estointernet.in)|43.255.166.254|:80...
 connected.
HTTP request sent, awaiting response... 200 OK
Length: 9506321 (9.1M) [application/octet-stream]
Saving to: 'apache-maven-3.6.3-bin.tar.gz'

apache-maven-3.6.3-bi 100%[=====================>]   9.07M  7.65MB/s    in 1.2s

2023-05-14 06:22:41 (7.65 MB/s) - 'apache-maven-3.6.3-bin.tar.gz' saved [9506321/9506
321]

root@ip-172-31-28-249:/opt# ls
apache-maven-3.6.3-bin.tar.gz  containerd
root@ip-172-31-28-249:/opt#
```

Un-tar the maven tar file package using tar cmnd

#tar -xvzf apache-maven-3.6.3-bin.tar.gz

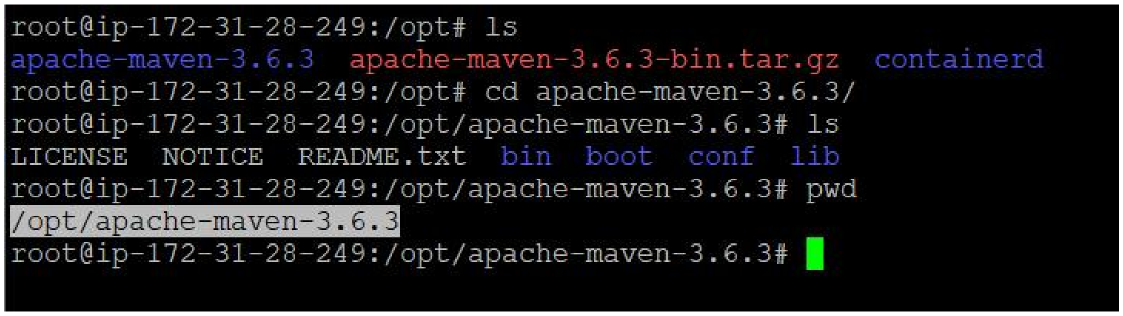


```
root@ip-172-31-28-249:/opt# tar -xvzf apache-maven-3.6.3-bin.tar.gz
```

#cd apache-maven-3.6.3/

#pwd

Copy the maven file path.

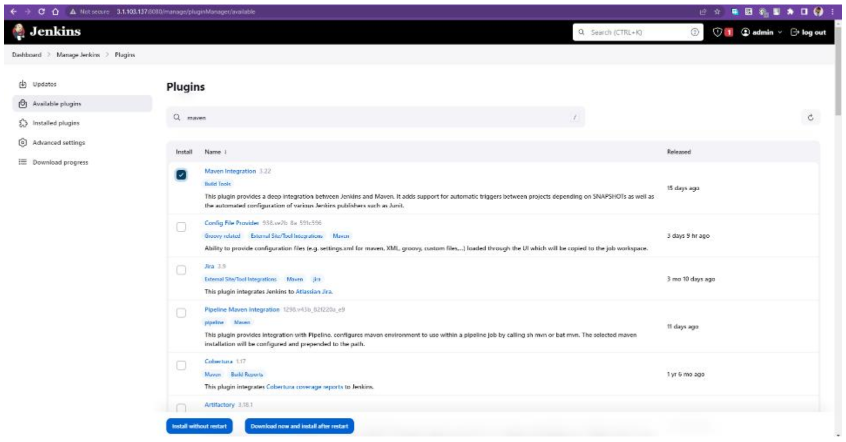


```
root@ip-172-31-28-249:/opt# ls
apache-maven-3.6.3  apache-maven-3.6.3-bin.tar.gz  containerd
root@ip-172-31-28-249:/opt# cd apache-maven-3.6.3/
root@ip-172-31-28-249:/opt/apache-maven-3.6.3# ls
LICENSE  NOTICE  README.txt  bin  boot  conf  lib
root@ip-172-31-28-249:/opt/apache-maven-3.6.3# pwd
/opt/apache-maven-3.6.3
root@ip-172-31-28-249:/opt/apache-maven-3.6.3#
```

In Jenkins Dashboard.

Install the Maven Plugin.

Dashboard – Manage Jenkins – Plugin – search Maven integration in Available plugins – Install without restart.



Not secure 3.1.103.137:8080/manage/pluginManager/available

Jenkins — Search (CTRL+K) — admin — log out

Dashboard > Manage Jenkins > Plugins

Updates
Available plugins
Installed plugins
Advanced settings
Download progress

Plugins

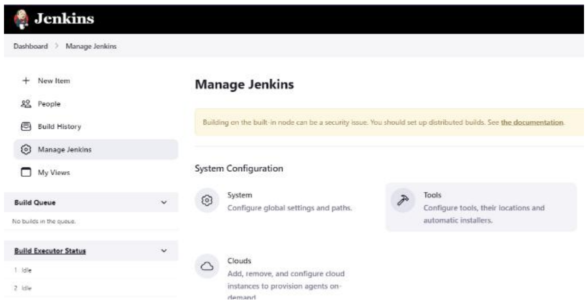
maven

Install	Name ↓	Released
✓	Maven Integration 3.22 Build Tools This plugin provides a deep integration between Jenkins and Maven. It adds support for automatic triggers between projects depending on SNAPSHOTs as well as the automated configuration of various Jenkins publishers such as Junit.	15 days ago
	Config File Provider 938.ve2b8a591c596 Groovy related External Site/Tool Integrations Maven Ability to provide configuration files (e.g. settings.xml for maven, XML, groovy, custom files,...) loaded through the UI which will be copied to the job workspace.	3 days 9 hr ago
	Jira 3.9 External Site/Tool Integrations Maven jira This plugin integrates Jenkins to Atlassian Jira.	3 mo 10 days ago
	Pipeline Maven Integration 1298.v43b_82f220a_e9 pipeline Maven This plugin provides integration with Pipeline, configures maven environment to use within a pipeline job by calling sh mvn or bat mvn. The selected maven installation will be configured and prepended to the path.	11 days ago
	Cobertura 1.17 Maven Build Reports This plugin integrates Cobertura coverage reports to Jenkins.	1 yr 6 mo ago
	Artifactory 3.18.1	

Install without restart   Download now and install after restart

Config the maven plugin path in Jenkins dashboard.

Dashboard – manage Jenkins – Tools.



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

No builds in the queue.

System
Configure global settings and paths.

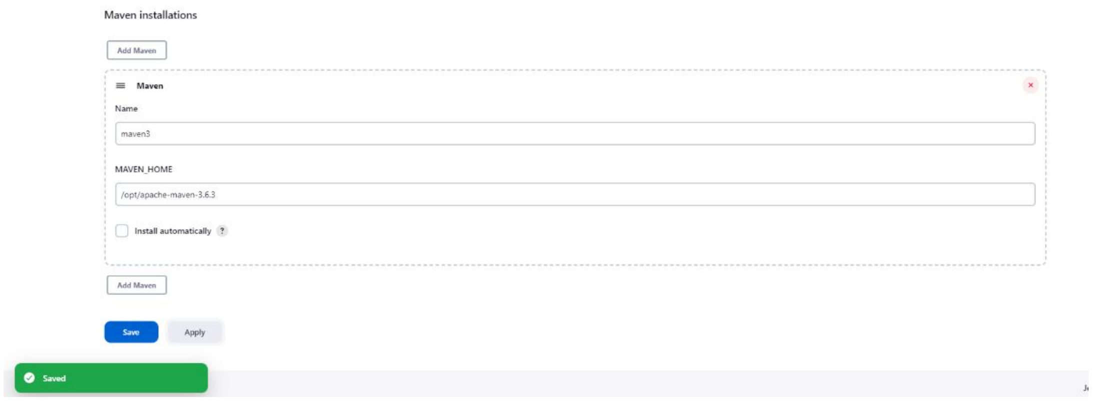
Tools: Configure tools, their locations and automatic installers.

Clouds: Add, remove, and configure cloud instances to provision agents on-demand

Mention the maven name same as given in groovy script

Name: maven3

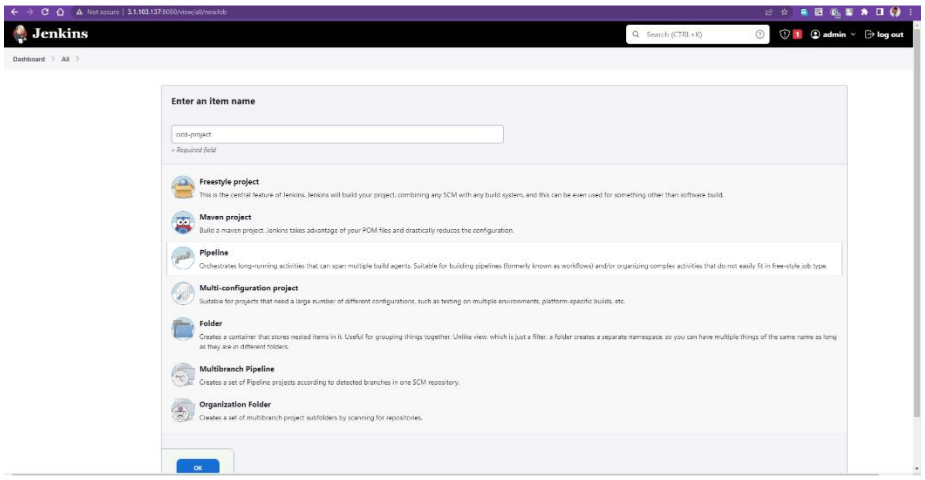
Maven_Home: paste the maven file path (/opt.apache-maven-3.6.3) – apply&save.



Name: maven3

MAVEN_HOME: /opt/apache-maven-3.6.3

Now create a pipeline project.



Not secure | 3.1.103.137:8080/view/all/newJob

Enter an item name

cicd-project

» 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.

Maven project: Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.

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.

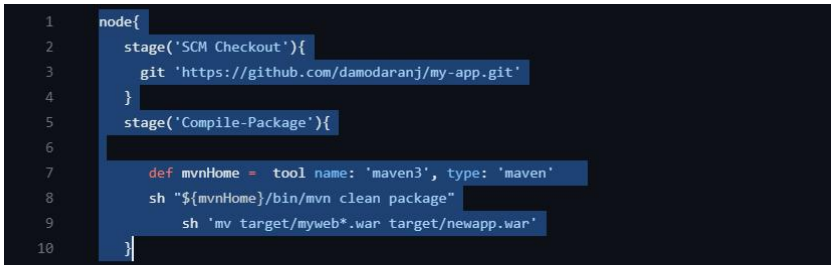
Organization Folder: Creates a set of multibranch project subfolders by scanning for repositories.

I have create a groovy script file and saved in github.

Github link: https://github.com/udhayakumar2507/my-app

Which I've been copy and deploying a respective step by step groovy script stages in Jenkins.

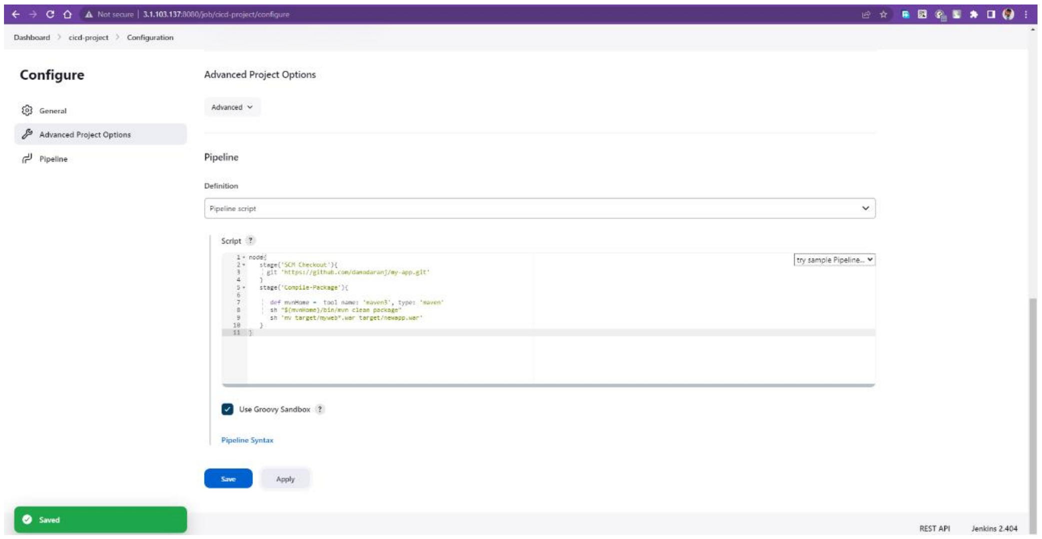
Copying Checkout stage and Maven stage.



```
node{
   stage('SCM Checkout'){
     git 'https://github.com/damodaranj/my-app.git'
   }
   stage('Compile-Package'){

      def mvnHome =  tool name: 'maven3', type: 'maven'
      sh "${mvnHome}/bin/mvn clean package"
          sh 'mv target/myweb*.war target/newapp.war'
   }
```

In pipeline script field.

Paste the checkout and maven stages – Ensure closing (}) is given correctly – apply and save.



Dashboard > cicd-project > Configuration

Configure

Advanced Project Options

Pipeline

Definition: Pipeline script

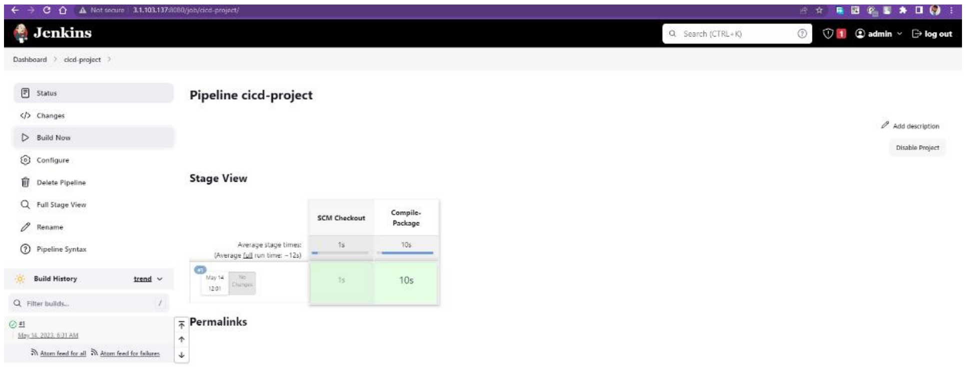
Script

```
node{
    stage('SCM Checkout'){
      git 'https://github.com/damodaranj/my-app.git'
    }
    stage('Compile-Package'){

      def mvnHome =  tool name: 'maven3', type: 'maven'
      sh "${mvnHome}/bin/mvn clean package"
      sh 'mv target/myweb*.war target/newapp.war'
    }
}
```

[✓] Use Groovy Sandbox

Build the pipeline project.

In below image can we see the stages have been deployed successfully.



Dashboard > cicd-project

Pipeline cicd-project

Stage View

	SCM Checkout	Compile-Package
Average stage times: (Average full run time: ~12s)	1s	10s
#1 May 14 12:01 No Changes	1s	10s

Build History

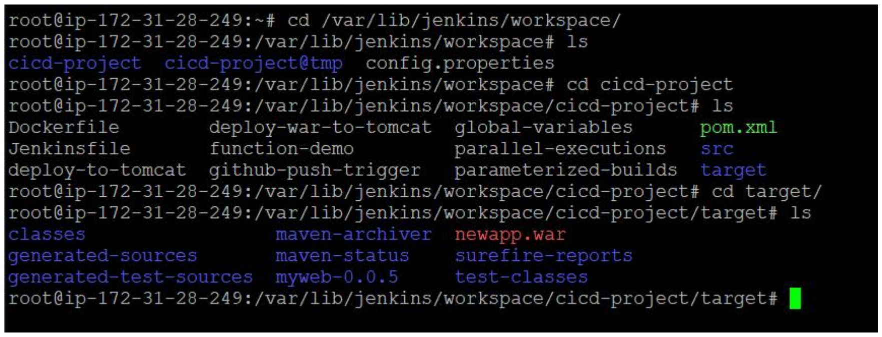
#1 May 14, 2023, 6:31 AM

In Jenkins Ec2 sever

Go the Jenkins workspace default path and ensure all the files have been moved to Jenkins server from github and also successfully created a newapp.war file using maven.

#cd /var/lib/Jenkins/workspace/cicd-project

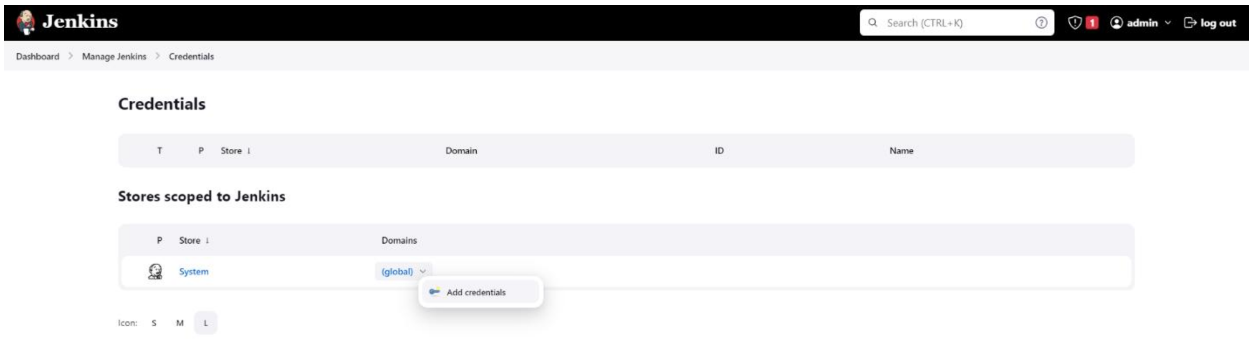
#cd target/



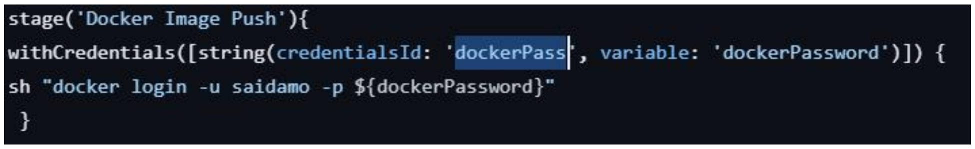
```
root@ip-172-31-28-249:~# cd /var/lib/jenkins/workspace/
root@ip-172-31-28-249:/var/lib/jenkins/workspace# ls
cicd-project  cicd-project@tmp  config.properties
root@ip-172-31-28-249:/var/lib/jenkins/workspace# cd cicd-project
root@ip-172-31-28-249:/var/lib/jenkins/workspace/cicd-project# ls
Dockerfile        deploy-war-to-tomcat  global-variables      pom.xml
Jenkinsfile       function-demo         parallel-executions   src
deploy-to-tomcat  github-push-trigger   parameterized-builds  target
root@ip-172-31-28-249:/var/lib/jenkins/workspace/cicd-project# cd target/
root@ip-172-31-28-249:/var/lib/jenkins/workspace/cicd-project/target# ls
classes                  maven-archiver  newapp.war
generated-sources        maven-status    surefire-reports
generated-test-sources   myweb-0.0.5     test-classes
root@ip-172-31-28-249:/var/lib/jenkins/workspace/cicd-project/target#
```

Now create a password variable for dockerhub login in Jenkins dashboard.

Dashboard – manage Jenkins – credentials – global Add credentials.



Copy the same variable name mention in groovy script.



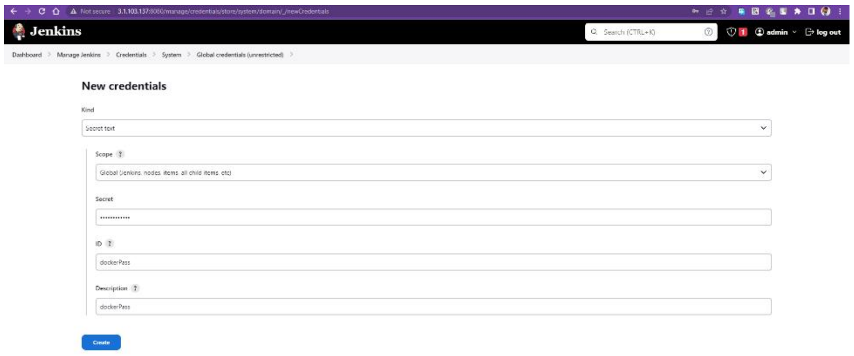
```
stage('Docker Image Push'){
withCredentials([string(credentialsId: 'dockerPass', variable: 'dockerPassword')]) {
sh "docker login -u saidamo -p ${dockerPassword}"
 }
```

Create a new credentials

Choose Script text

In secret: Enter the dockerhub login password.

Id and Description: Paste the variable name. (dockerPass) – Create.



Dashboard > Manage Jenkins > Credentials > System > Global credentials (unrestricted)

New credentials

Kind: Secret text

Scope: Global (Jenkins, nodes, items, all child items, etc)

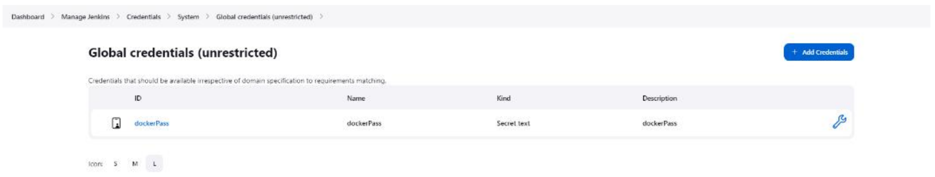
Secret: ••••••••••••

ID: dockerPass

Description: dockerPass

Create

Successfully created an variable name for dockerhub login password.

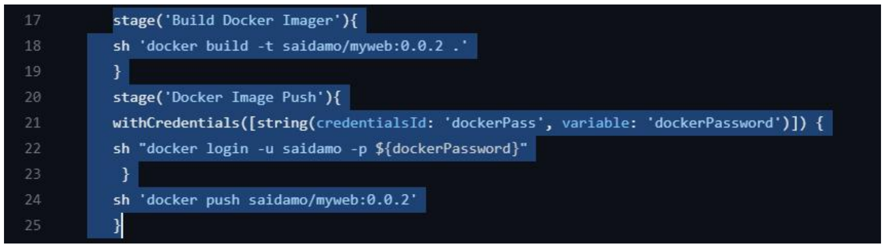

Dashboard > Manage Jenkins > Credentials > System > Global credentials (unrestricted) >

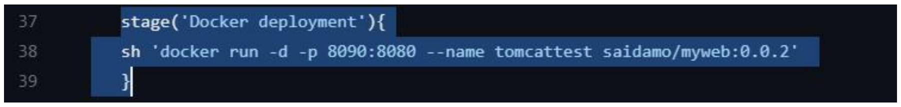
Global credentials (unrestricted)

Credentials that should be available irrespective of domain specification to requirements matching.

ID	Name	Kind	Description
dockerPass	dockerPass	Secret text	dockerPass

Copy the Build docker Image,Docker image push, Docker deployment stage from groovy script.


```
        stage('Build Docker Imager'){
        sh 'docker build -t saidamo/myweb:0.0.2 .'
        }
        stage('Docker Image Push'){
        withCredentials([string(credentialsId: 'dockerPass', variable: 'dockerPassword')]) {
        sh "docker login -u saidamo -p ${dockerPassword}"
         }
        sh 'docker push saidamo/myweb:0.0.2'
        }
```

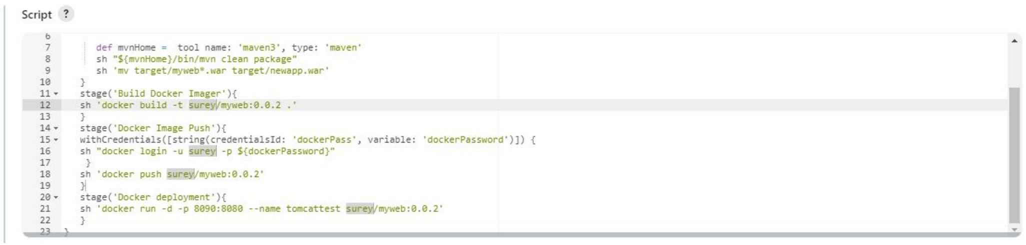

```
        stage('Docker deployment'){
        sh 'docker run -d -p 8090:8080 --name tomcattest saidamo/myweb:0.0.2'
        }
```

Paste the groovy script under the maven stage.

Ensure the (}) is mentioned properly.

Ensure the login usernamename is given correctly

I've changed the docker image name to my own name. (optional) – apply&save.

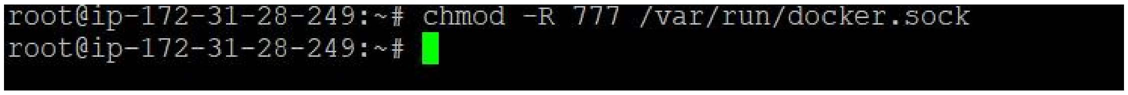

Script ?

```
      def mvnHome =  tool name: 'maven3', type: 'maven'
      sh "${mvnHome}/bin/mvn clean package"
      sh 'mv target/myweb*.war target/newapp.war'
  }
  stage('Build Docker Imager'){
  sh 'docker build -t surey/myweb:0.0.2 .'
  }
  stage('Docker Image Push'){
  withCredentials([string(credentialsId: 'dockerPass', variable: 'dockerPassword')]) {
  sh "docker login -u surey -p ${dockerPassword}"
   }
  sh 'docker push surey/myweb:0.0.2'
  }
  stage('Docker deployment'){
  sh 'docker run -d -p 8090:8080 --name tomcattest surey/myweb:0.0.2'
  }
}
```

In Jenkins ec2 server.

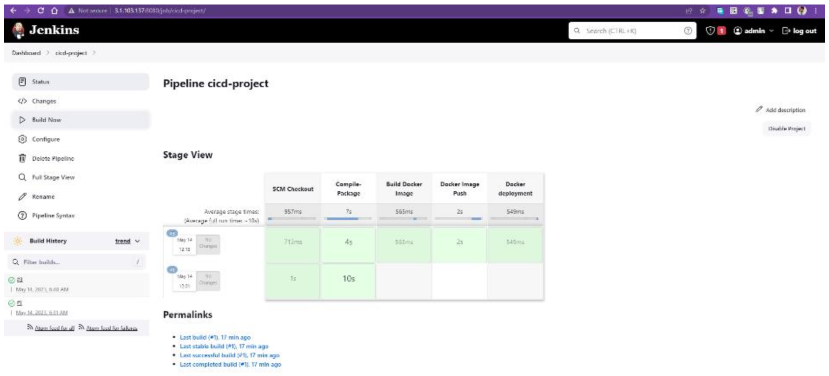
Change the permission to default docker dir path to execute the script.

#chmod -R 777 /var/run/docker.sock


```
root@ip-172-31-28-249:~# chmod -R 777 /var/run/docker.sock
root@ip-172-31-28-249:~# 
```

Now Build the Pipeline project

Below image can we see that the stages have been deployed successfully.



3.1.105.137:8080/job/cicd-project/

Dashboard > cicd-project >

Pipeline cicd-project

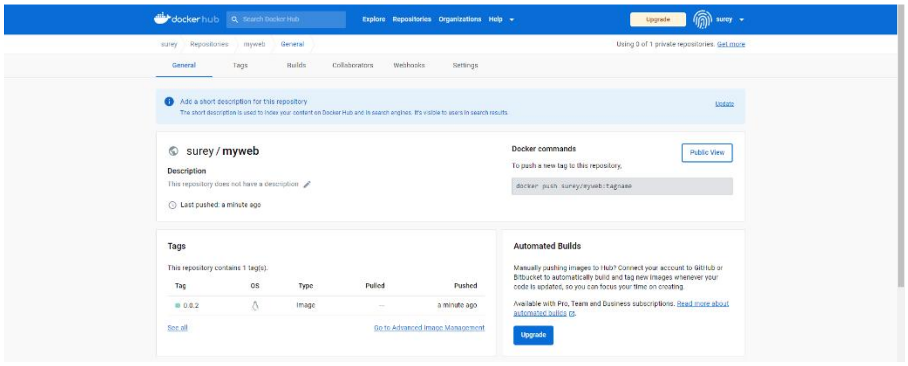
Stage View

	SCM Checkout	Compile-Package	Build Docker Image	Docker Image Push	Docker deployment
Average stage times: (Average full run time: ~10s)	957ms	7s	565ms	2s	549ms
#2 May 14 12:18 No Changes	713ms	4s	565ms	2s	549ms
#1 May 14 12:01 No Changes	1s	10s			

Build History
- #2 May 14, 2023, 6:48 AM
- #1 May 14, 2023, 6:31 AM

Permalinks
- Last build (#1), 17 min ago
- Last stable build (#1), 17 min ago
- Last successful build (#1), 17 min ago
- Last completed build (#1), 17 min ago

Successfully pushed docker image in dockerhub.



surey / myweb

Description

This repository does not have a description

Last pushed: a minute ago

Docker commands

To push a new tag to this repository,

```
docker push surey/myweb:tagname
```

Tags

This repository contains 1 tag(s).

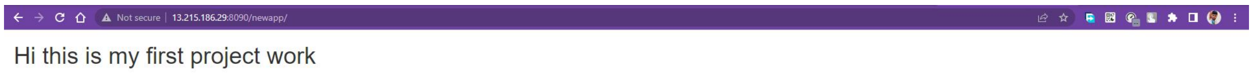
Tag	OS	Type	Pulled	Pushed
0.0.2		Image	—	a minute ago

Automated Builds

Manually pushing images to Hub? Connect your account to GitHub or Bitbucket to automatically build and tag new images whenever your code is updated, so you can focus your time on creating.

Available with Pro, Team and Business subscriptions. Read more about automated builds.

Successfully deployed a war file in tomcat server. (testdemo)



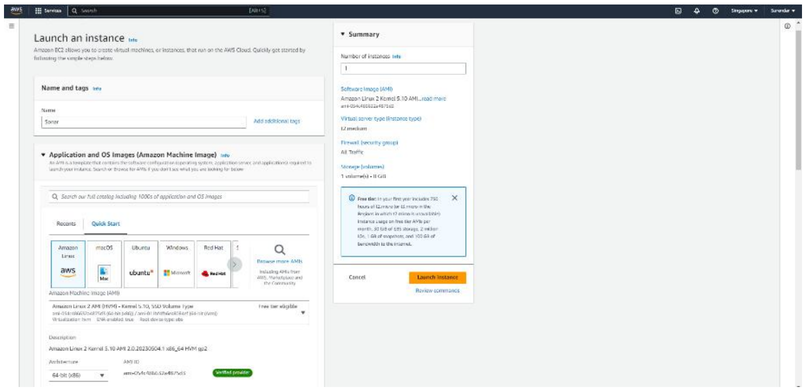
13.215.186.29:8090/newapp/

Hi this is my first project work

Steps to install Sonarqube and deploy in Jenkins pipeline to analyze the SCM for clean code delivery.

Launch an Ec2 Instances for Sonarqube.

Amazon Linux 2 – RAM t2.medium – SG (Alltraffic) – Storage 30gib – Launch an instance.



Launch an instance

Name: Sonar

Application and OS Images (Amazon Machine Image)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible

Description: Amazon Linux 2 Kernel 5.10 AMI 2.0.20230504.1 x86_64 HVM gp2

Architecture: 64-bit (x86)

Summary

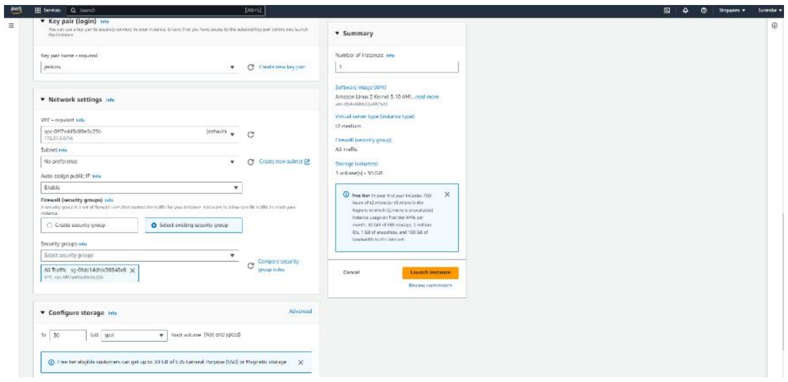
Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...

Virtual server type (instance type): t2.medium

Firewall (security group): All Traffic

Storage (volumes): 1 volume(s) - 8 GiB



Key pair (login)

Key pair name - required: jenkins

Network settings

VPC - required: vpc-0ff7a445c88e5c25b (default) 172.31.0.0/16

Subnet: No preference

Auto-assign public IP: Enable

Firewall (security groups): Select existing security group

Security groups: All Traffic sg-0fdc14dfdc98848e8

Configure storage

1x 30 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more

Virtual server type (instance type): t2.medium

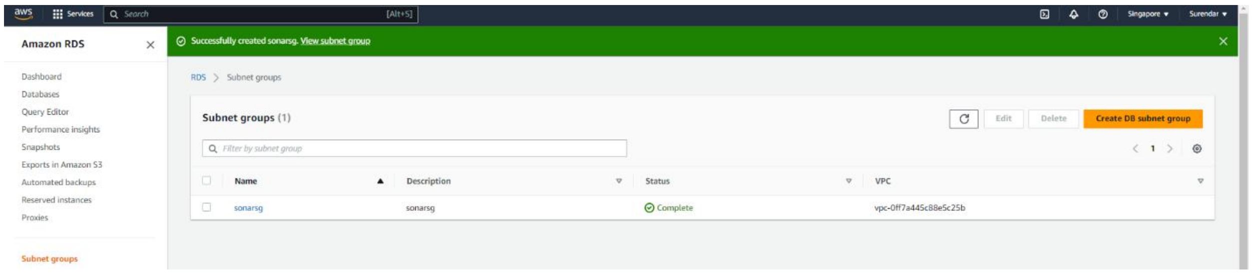
Firewall (security group): All traffic

Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

In RDS create a Mysql database.

Create a subnet group



Successfully created sonarsg. View subnet group

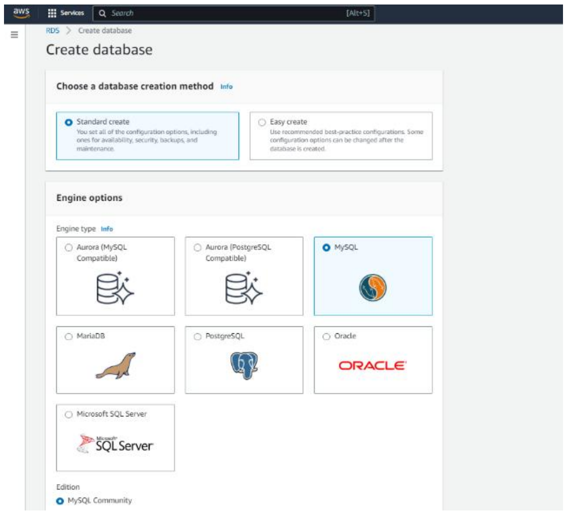
RDS > Subnet groups

Subnet groups (1)

Name	Description	Status	VPC
sonarsg	sonarsg	Complete	vpc-0ff7a445c88e5c25b

Create a database

Standard create – Choose MySQL DB engine.



RDS > Create database

Create database

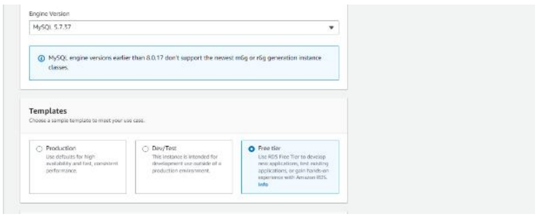
Choose a database creation method: Standard create [✓] / Easy create

Engine options

Engine type: MySQL [✓]

Edition: MySQL Community [✓]

Choose MySQL version (5.7.37) - Free tier Templates.



Engine Version: MySQL 5.7.37

MySQL engine versions earlier than 8.0.17 don't support the newest m6g or r6g generation instance classes.

Templates

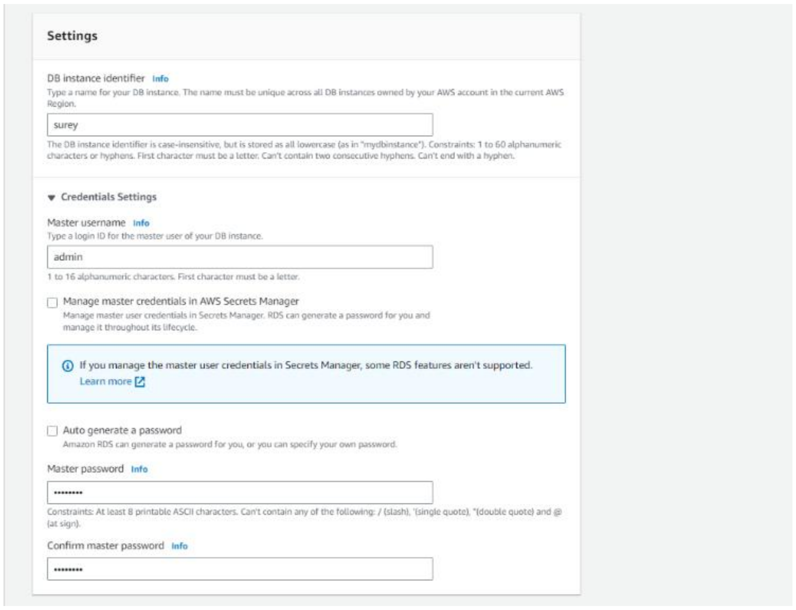
Choose a sample template to meet your use case.

Production / Dev/Test / Free tier [✓]

Free tier: Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.

In setting tab

Create a DB ID Ex: surey – Username (admin) – Master Password – Confirm Master Password.



Settings

DB instance identifier Info
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

surey

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info
Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter.

☐ Manage master credentials in AWS Secrets Manager
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

☐ Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password Info

••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

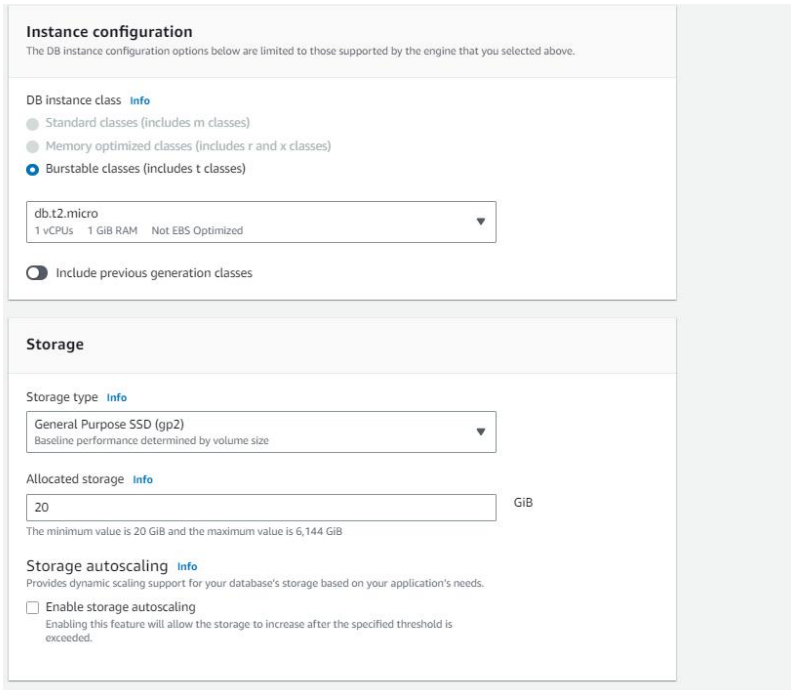
Confirm master password Info

••••••••

In Instance Configuration

Choose db.t2.micro

Storage (Default)



Instance configuration
The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class Info
○ Standard classes (includes m classes)
○ Memory optimized classes (includes r and x classes)
● Burstable classes (includes t classes)

db.t2.micro
1 vCPUs 1 GiB RAM Not EBS Optimized

Include previous generation classes

Storage

Storage type Info
General Purpose SSD (gp2)
Baseline performance determined by volume size

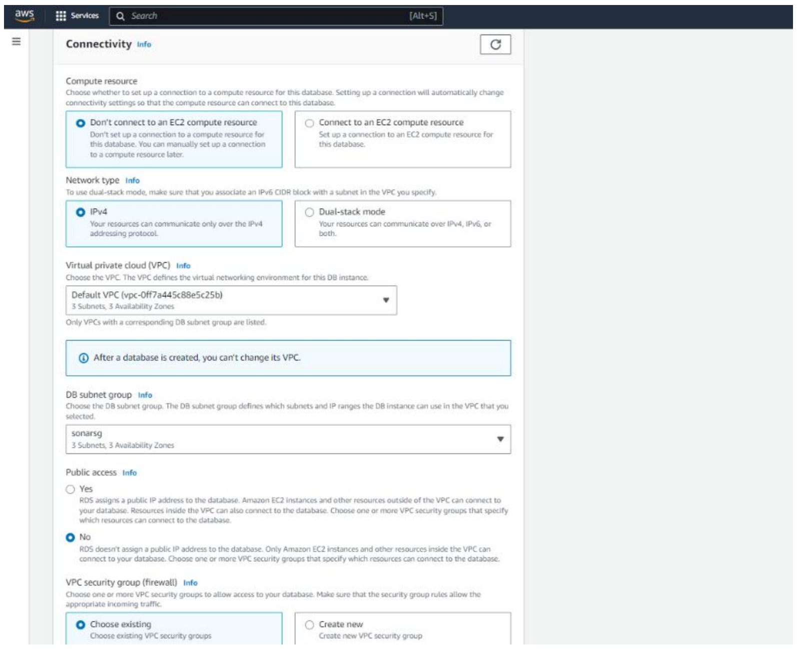
Allocated storage Info
20 GiB
The minimum value is 20 GiB and the maximum value is 6,144 GiB

Storage autoscaling Info
Provides dynamic scaling support for your database's storage based on your application's needs.

☐ Enable storage autoscaling
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

In connectivity

Choose created Subnet Group



Connectivity Info

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

[✓ Don't connect to an EC2 compute resource] Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
Connect to an EC2 compute resource — Set up a connection to an EC2 compute resource for this database.

Network type Info
To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

[✓ IPv4] Your resources can communicate only over the IPv4 addressing protocol.
Dual-stack mode — Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.
Default VPC (vpc-0ff7a445c88e5c25b)
3 Subnets, 3 Availability Zones
Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.
sonarsg
3 Subnets, 3 Availability Zones

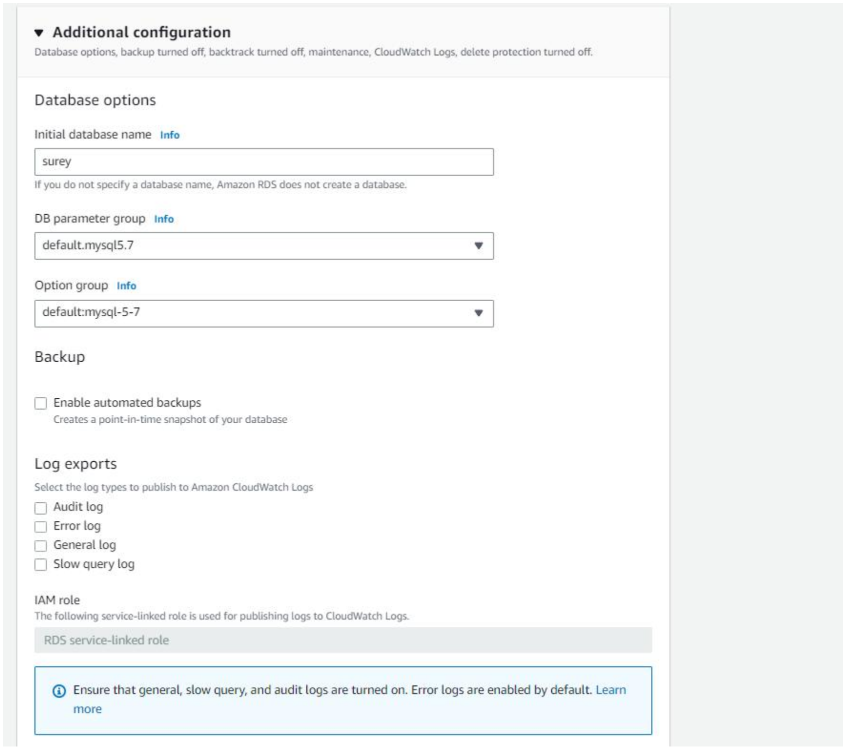
Public access Info
Yes — RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
[✓ No] RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.
[✓ Choose existing] Choose existing VPC security groups
Create new — Create new VPC security group

In Additional configuration

Enter the Initial Database name

Uncheck Backup.



Additional configuration
Database options, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name Info
surey
If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group Info
default.mysql5.7

Option group Info
default:mysql-5-7

Backup

☐ Enable automated backups
Creates a point-in-time snapshot of your database

Log exports
Select the log types to publish to Amazon CloudWatch Logs
☐ Audit log
☐ Error log
☐ General log
☐ Slow query log

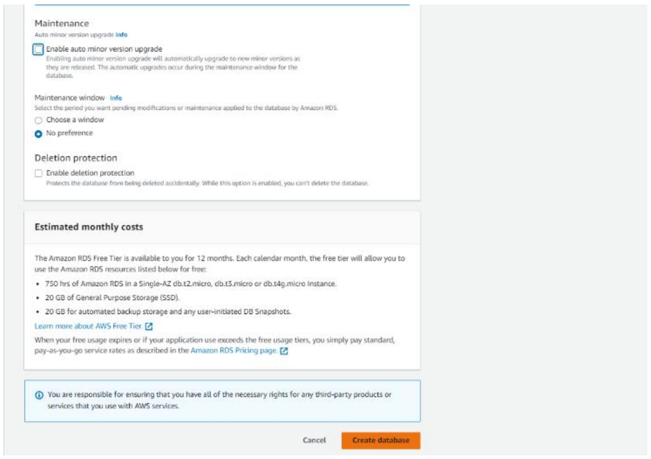
IAM role
The following service-linked role is used for publishing logs to CloudWatch Logs.
RDS service-linked role

Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. Learn more

In Maintenance

Uncheck auto minor version upgrade

Disbale deletion protection – Create database.



Maintenance

Auto minor version upgrade Info

- [ ] Enable auto minor version upgrade
  Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window Info

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

○ Choose a window
● No preference

Deletion protection

- [ ] Enable deletion protection
  Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

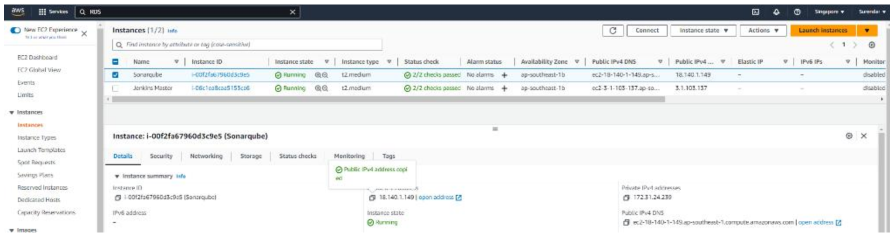
- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro, db.t3.micro or db.t4g.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

Learn more about AWS Free Tier.

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the Amazon RDS Pricing page.

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Connect the Sonarqube Ec2 Server in putty



Instances (1/2) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitor
✓	Sonarqube	i-00f2fa67960d3c9e5	Running	t2.medium	2/2 checks passed	No alarms	ap-southeast-1b	ec2-18-140-1-149.ap-s...	18.140.1.149	–	–	disabled
	Jenkins Master	i-06c1ca8caa5153ca6	Running	t2.medium	2/2 checks passed	No alarms	ap-southeast-1b	ec2-3-1-103-137.ap-so...	3.1.103.137	–	–	disabled

Instance: i-00f2fa67960d3c9e5 (Sonarqube)

Instance summary Info

Instance ID: i-00f2fa67960d3c9e5 (Sonarqube)

Public IPv4 address: 18.140.1.149 | open address

Private IPv4 addresses: 172.31.24.239

IPv6 address: –

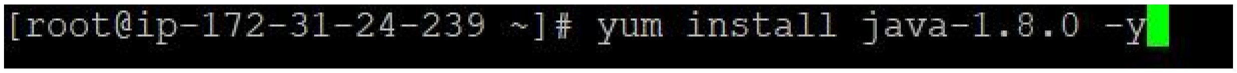
Instance state: Running

Public IPv4 DNS: ec2-18-140-1-149.ap-southeast-1.compute.amazonaws.com | open address

In Sonarqube Ec2 Server

Install Java

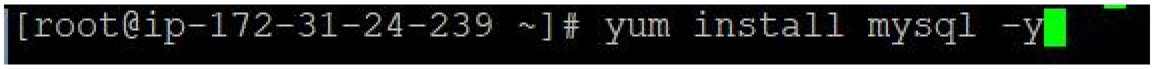
#yum install java-1.8.0 -y



```
[root@ip-172-31-24-239 ~]# yum install java-1.8.0 -y
```

Install MySQL

#yum install mysql -y

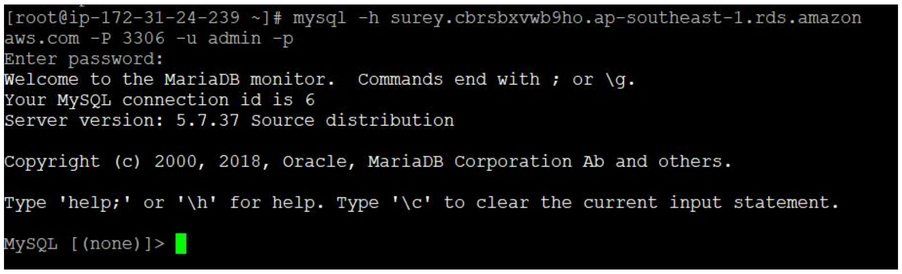


```
[root@ip-172-31-24-239 ~]# yum install mysql -y
```

Connect the Mysql database in putty

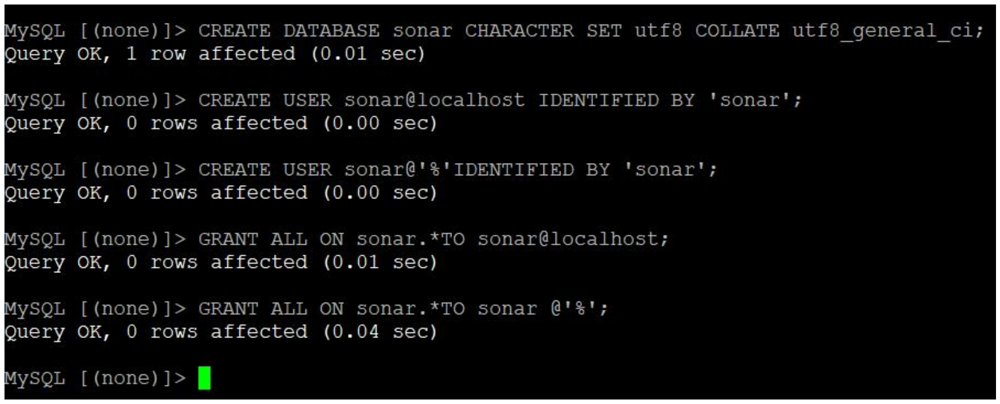
#mysql -h <endpoint> -P 3306 -u admin -p (enter)

Connected to MySQL database.



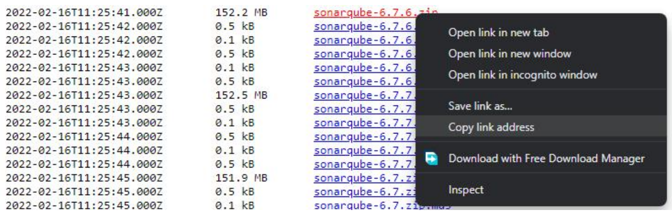
```
[root@ip-172-31-24-239 ~]# mysql -h surey.cbrsbxvwb9ho.ap-southeast-1.rds.amazon
aws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.37 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Now create an Database user for sonar in MySQL and Given all permission



```
MySQL [(none)]> CREATE DATABASE sonar CHARACTER SET utf8 COLLATE utf8_general_ci;
Query OK, 1 row affected (0.01 sec)

MySQL [(none)]> CREATE USER sonar@localhost IDENTIFIED BY 'sonar';
Query OK, 0 rows affected (0.00 sec)

MySQL [(none)]> CREATE USER sonar@'%'IDENTIFIED BY 'sonar';
Query OK, 0 rows affected (0.00 sec)

MySQL [(none)]> GRANT ALL ON sonar.*TO sonar@localhost;
Query OK, 0 rows affected (0.01 sec)

MySQL [(none)]> GRANT ALL ON sonar.*TO sonar @'%';
Query OK, 0 rows affected (0.04 sec)

MySQL [(none)]>
```

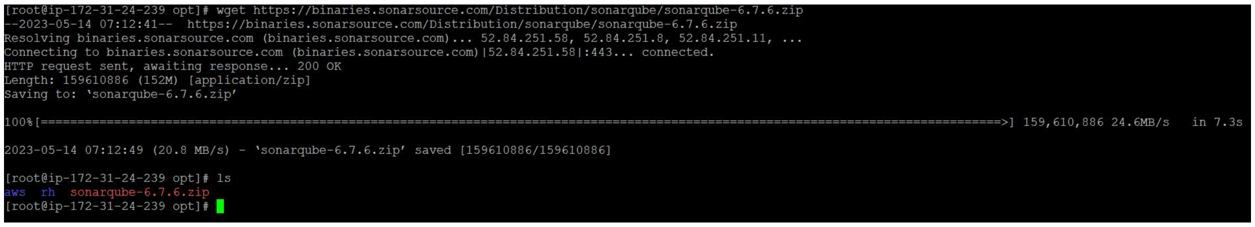
Download Sonarqube zip file (6.7.6 version)



```
2022-02-16T11:25:41.000Z      152.2 MB      sonarqube-6.7.6.zip
2022-02-16T11:25:42.000Z      0.5 kB        sonarqube-6.7.6
2022-02-16T11:25:42.000Z      0.1 kB        sonarqube-6.7.6
2022-02-16T11:25:42.000Z      0.5 kB        sonarqube-6.7.6
2022-02-16T11:25:43.000Z      0.1 kB        sonarqube-6.7.6
2022-02-16T11:25:43.000Z      0.5 kB        sonarqube-6.7.6
2022-02-16T11:25:43.000Z      152.5 MB      sonarqube-6.7.7
2022-02-16T11:25:43.000Z      0.5 kB        sonarqube-6.7.7
2022-02-16T11:25:43.000Z      0.1 kB        sonarqube-6.7.7
2022-02-16T11:25:44.000Z      0.5 kB        sonarqube-6.7.7
2022-02-16T11:25:44.000Z      0.1 kB        sonarqube-6.7.7
2022-02-16T11:25:44.000Z      0.5 kB        sonarqube-6.7.7
2022-02-16T11:25:45.000Z      151.9 MB      sonarqube-6.7.zi
2022-02-16T11:25:45.000Z      0.5 kB        sonarqube-6.7.zi
2022-02-16T11:25:45.000Z      0.1 kB        sonarqube-6.7.zip.md5
```

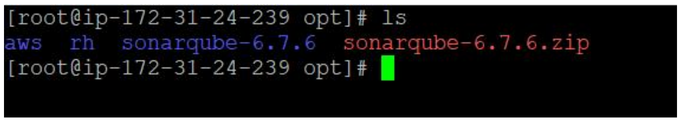
#cd /opt

#wget <sonarqube download link>



```
[root@ip-172-31-24-239 opt]# wget https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-6.7.6.zip
--2023-05-14 07:12:41--  https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-6.7.6.zip
Resolving binaries.sonarsource.com (binaries.sonarsource.com)... 52.84.251.58, 52.84.251.8, 52.84.251.11, ...
Connecting to binaries.sonarsource.com (binaries.sonarsource.com)|52.84.251.58|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 159610886 (152M) [application/zip]
Saving to: 'sonarqube-6.7.6.zip'

100%[==========================================================================================================================>] 159,610,886 24.6MB/s   in 7.3s

2023-05-14 07:12:49 (20.8 MB/s) - 'sonarqube-6.7.6.zip' saved [159610886/159610886]

[root@ip-172-31-24-239 opt]# ls
aws  rh  sonarqube-6.7.6.zip
[root@ip-172-31-24-239 opt]#
```

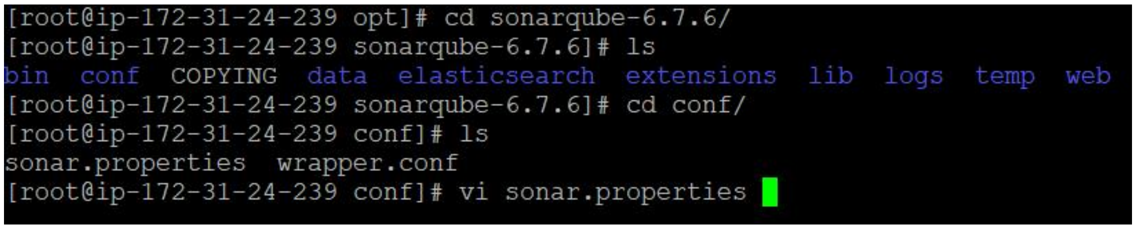
#unzip sonarqube-6.7.6.zip



```
[root@ip-172-31-24-239 opt]# ls
aws  rh  sonarqube-6.7.6  sonarqube-6.7.6.zip
[root@ip-172-31-24-239 opt]#
```

#cd sonarqube-6.7.6/conf

#vi sonar.properties



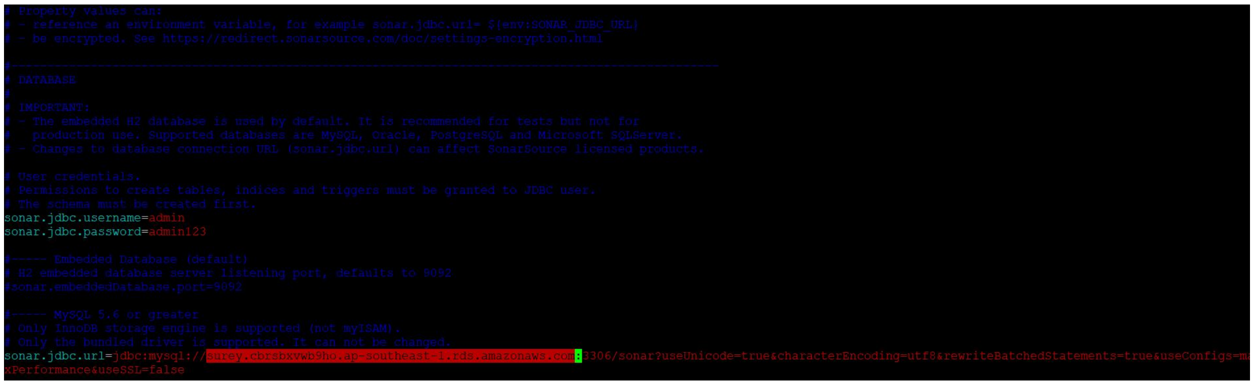
```
[root@ip-172-31-24-239 opt]# cd sonarqube-6.7.6/
[root@ip-172-31-24-239 sonarqube-6.7.6]# ls
bin  conf  COPYING  data  elasticsearch  extensions  lib  logs  temp  web
[root@ip-172-31-24-239 sonarqube-6.7.6]# cd conf/
[root@ip-172-31-24-239 conf]# ls
sonar.properties  wrapper.conf
[root@ip-172-31-24-239 conf]# vi sonar.properties
```

In sonar.properties file

Enter the sonar username=admin

Sonar password=admin123

Sonar url: Paste the database endpoint URL

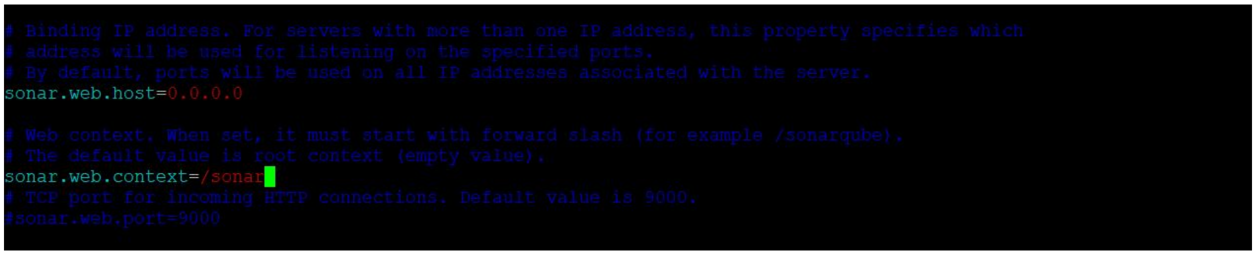


```
# Property values can:
# - reference an environment variable, for example sonar.jdbc.url= ${env:SONAR_JDBC_URL}
# - be encrypted. See https://redirect.sonarsource.com/doc/settings-encryption.html

#--------------------------------------------------------------------------------------------------
# DATABASE
#
# IMPORTANT:
# - The embedded H2 database is used by default. It is recommended for tests but not for
#   production use. Supported databases are MySQL, Oracle, PostgreSQL and Microsoft SQLServer.
# - Changes to database connection URL (sonar.jdbc.url) can affect SonarSource licensed products.

# User credentials.
# Permissions to create tables, indices and triggers must be granted to JDBC user.
# The schema must be created first.
sonar.jdbc.username=admin
sonar.jdbc.password=admin123

#----- Embedded Database (default)
# H2 embedded database server listening port, defaults to 9092
#sonar.embeddedDatabase.port=9092

#----- MySQL 5.6 or greater
# Only InnoDB storage engine is supported (not myISAM).
# Only the bundled driver is supported. It can not be changed.
sonar.jdbc.url=jdbc:mysql://surey.cbrsbxvwb9ho.ap-southeast-1.rds.amazonaws.com:3306/sonar?useUnicode=true&characterEncoding=utf8&rewriteBatchedStatements=true&useConfigs=ma
xPerformance&useSSL=false
```

Remove the (#) sonar.web.host=0.0.0.0

Mention the sonar.web.context-/sonar

:wq!



```
# Binding IP address. For servers with more than one IP address, this property specifies which
# address will be used for listening on the specified ports.
# By default, ports will be used on all IP addresses associated with the server.
sonar.web.host=0.0.0.0

# Web context. When set, it must start with forward slash (for example /sonarqube).
# The default value is root context (empty value).
sonar.web.context=/sonar
# TCP port for incoming HTTP connections. Default value is 9000.
#sonar.web.port=9000
```

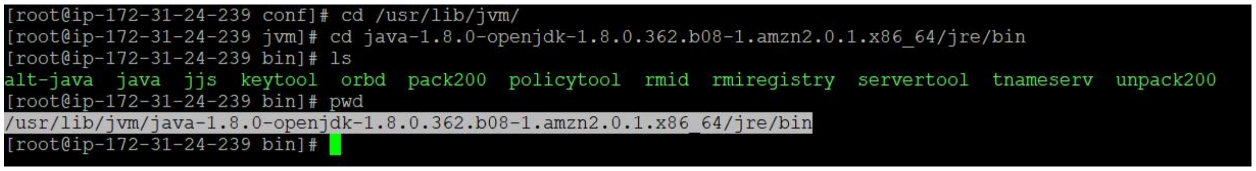
Copy the java script path

#cd /usr/lib/jvm/

#cd java package name/bin

#pwd

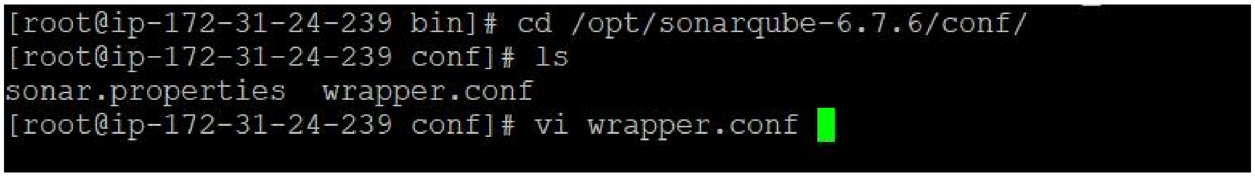
Copy the script path



```
[root@ip-172-31-24-239 conf]# cd /usr/lib/jvm/
[root@ip-172-31-24-239 jvm]# cd java-1.8.0-openjdk-1.8.0.362.b08-1.amzn2.0.1.x86_64/jre/bin
[root@ip-172-31-24-239 bin]# ls
alt-java  java  jjs  keytool  orbd  pack200  policytool  rmid  rmiregistry  servertool  tnameserv  unpack200
[root@ip-172-31-24-239 bin]# pwd
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.362.b08-1.amzn2.0.1.x86_64/jre/bin
[root@ip-172-31-24-239 bin]#
```

#cd /opt/sonarqube-6.7.6/conf/

#vi wrapper.conf

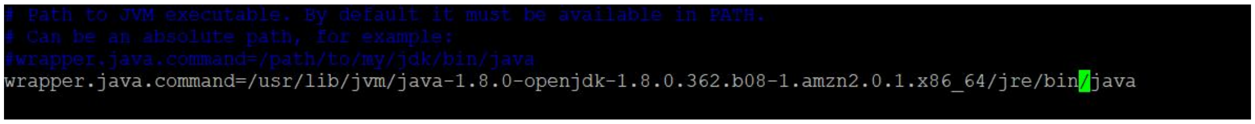


```
[root@ip-172-31-24-239 bin]# cd /opt/sonarqube-6.7.6/conf/
[root@ip-172-31-24-239 conf]# ls
sonar.properties  wrapper.conf
[root@ip-172-31-24-239 conf]# vi wrapper.conf
```

In wrapper.conf file

wrapper.java.command :Paste the java script path/java

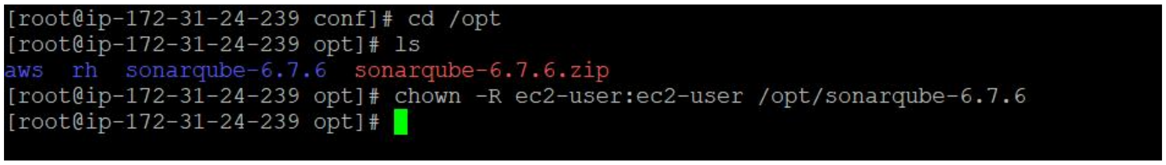
:wq!



```
# Path to JVM executable. By default it must be available in PATH.
# Can be an absolute path, for example:
#wrapper.java.command=/path/to/my/jdk/bin/java
wrapper.java.command=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.362.b08-1.amzn2.0.1.x86_64/jre/bin/java
```

Given the ec2-user access to the sonarqube-6.7.6 package files.

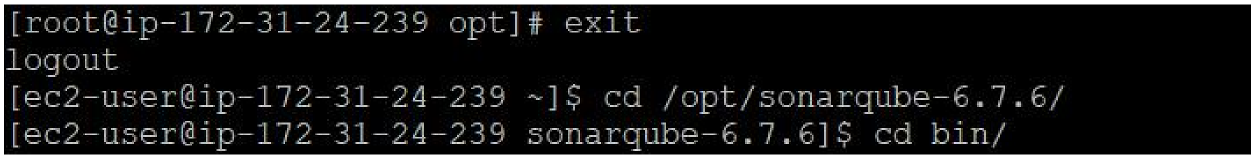
#chown -R ec2-user:ec2-user /opt/sonarqube-6.7.6



```
[root@ip-172-31-24-239 conf]# cd /opt
[root@ip-172-31-24-239 opt]# ls
aws  rh  sonarqube-6.7.6  sonarqube-6.7.6.zip
[root@ip-172-31-24-239 opt]# chown -R ec2-user:ec2-user /opt/sonarqube-6.7.6
[root@ip-172-31-24-239 opt]#
```

#exit

$cd /opt/sonarqube-6.7.6/bin



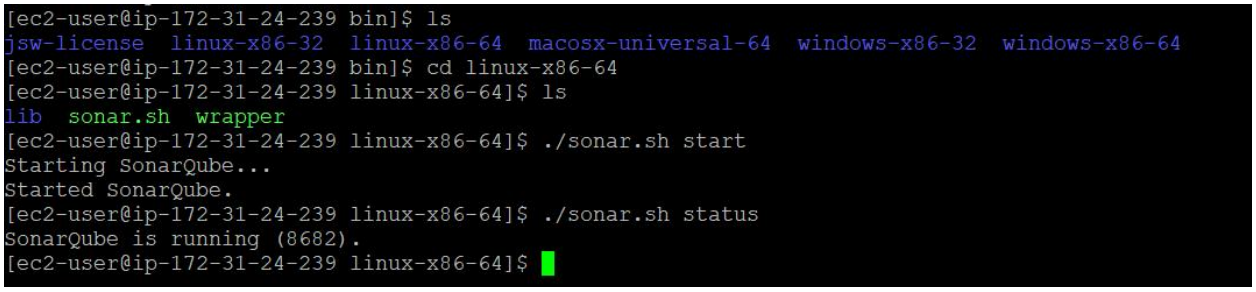
```
[root@ip-172-31-24-239 opt]# exit
logout
[ec2-user@ip-172-31-24-239 ~]$ cd /opt/sonarqube-6.7.6/
[ec2-user@ip-172-31-24-239 sonarqube-6.7.6]$ cd bin/
```

$cd linux-x86-64

$./sonar.sh start

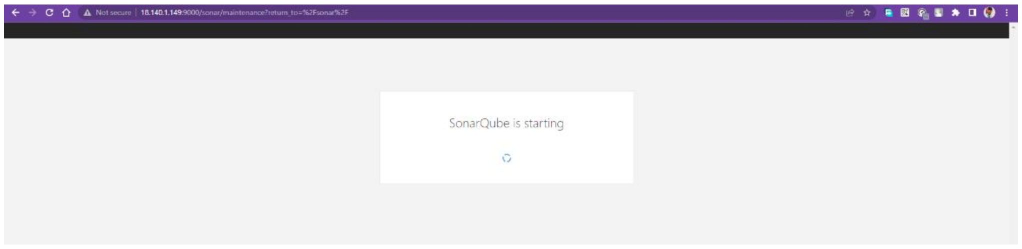
$./sonar.sh status

Sonarqube is running



```
[ec2-user@ip-172-31-24-239 bin]$ ls
jsw-license  linux-x86-32  linux-x86-64  macosx-universal-64  windows-x86-32  windows-x86-64
[ec2-user@ip-172-31-24-239 bin]$ cd linux-x86-64
[ec2-user@ip-172-31-24-239 linux-x86-64]$ ls
lib  sonar.sh  wrapper
[ec2-user@ip-172-31-24-239 linux-x86-64]$ ./sonar.sh start
Starting SonarQube...
Started SonarQube.
[ec2-user@ip-172-31-24-239 linux-x86-64]$ ./sonar.sh status
SonarQube is running (8682).
[ec2-user@ip-172-31-24-239 linux-x86-64]$
```

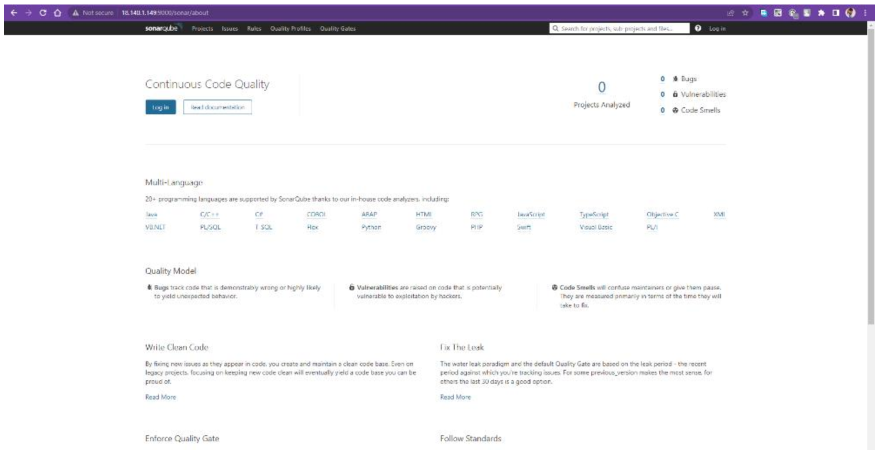
Copy sonarqube Ec2 server Ipv4 add – Hit in browser. By mentioning ipv4add/sonar



Not secure | 18.140.1.149:9000/sonar/maintenance?return_to=%2Fsonar%2F

SonarQube is starting

Sonarqube dashboard is hosted.



Not secure | 18.140.1.149:9000/sonar/about

sonarqube Projects Issues Rules Quality Profiles Quality Gates | Search for projects, sub-projects and files... | Log in

Continuous Code Quality

Log in | Read documentation

0 Projects Analyzed

0 Bugs
0 Vulnerabilities
0 Code Smells

Multi-Language

20+ programming languages are supported by SonarQube thanks to our in-house code analyzers, including:

Java C/C++ C# COBOL ABAP HTML RPG JavaScript TypeScript Objective C XML
VB.NET PL/SQL T-SQL Flex Python Groovy PHP Swift Visual Basic PL/I

Quality Model

Bugs track code that is demonstrably wrong or highly likely to yield unexpected behavior.

Vulnerabilities are raised on code that is potentially vulnerable to exploitation by hackers.

Code Smells will confuse maintainers or give them pause. They are measured primarily in terms of the time they will take to fix.

Write Clean Code

By fixing new issues as they appear in code, you create and maintain a clean code base. Even on legacy projects, focusing on keeping new code clean will eventually yield a code base you can be proud of.

Read More

Fix The Leak

The water leak paradigm and the default Quality Gate are based on the leak period - the recent period against which you're tracking issues. For some previous_version makes the most sense, for others the last 30 days is a good option.

Read More

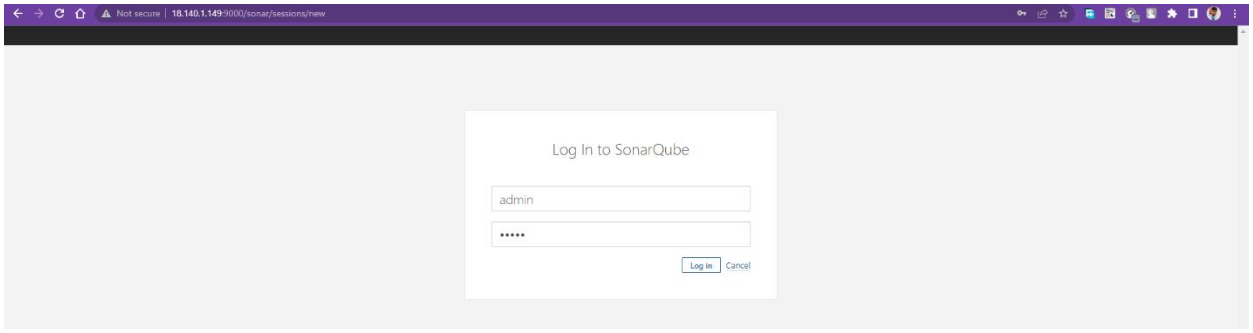
Enforce Quality Gate

Follow Standards

Login the sonarqube acnt (default)

Username: admin

Password: admin



Not secure | 18.140.1.149:9000/sonar/sessions/new

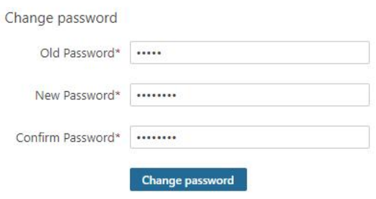
Log In to SonarQube

admin

•••••

Log in Cancel

In security – change the acnt password – generate a token copy the token.



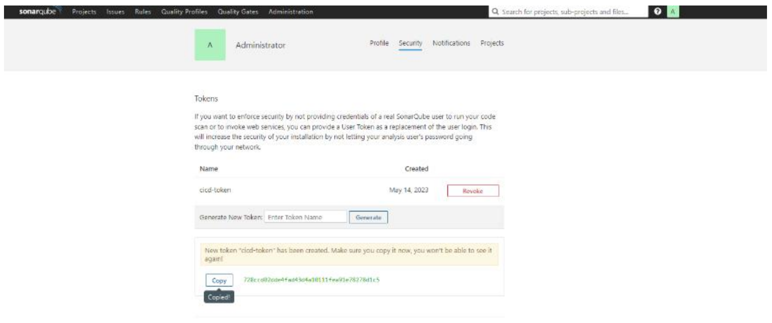
Change password

Old Password* •••••

New Password* ••••••••

Confirm Password* ••••••••

Change password



Tokens

If you want to enforce security by not providing credentials of a real SonarQube user to run your code scan or to invoke web services, you can provide a User Token as a replacement of the user login. This will increase the security of your installation by not letting your analysis user's password going through your network.

Name	Created	
cicd-token	May 14, 2023	Revoke

Generate New Token: Enter Token Name Generate

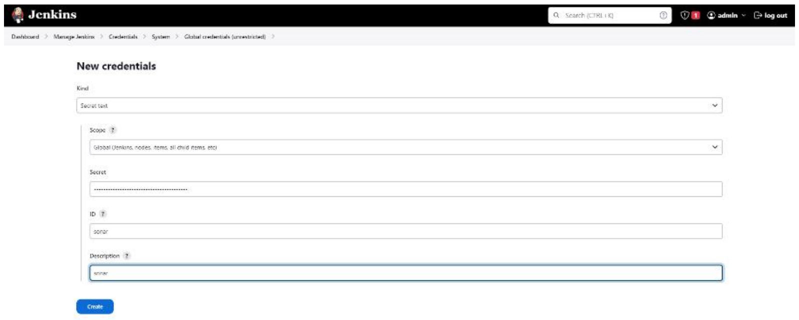
New token "cicd-token" has been created. Make sure you copy it now, you won't be able to see it again!

Copy 728ccd82ede4fad43d4a10111fea91e78278d1c5

Copied!

In Jenkins dashboard – Credential -create a variable for sonarqube login token password.

Choose secret text – Secret (paste the token password) – set ID and Description name as (sonar) – Create.


Jenkins
Search (CTRL+K)
admin
log out
Dashboard > Manage Jenkins > Credentials > System > Global credentials (unrestricted) >

New credentials

Kind: Secret text

Scope: Global (Jenkins, nodes, items, all child items, etc)

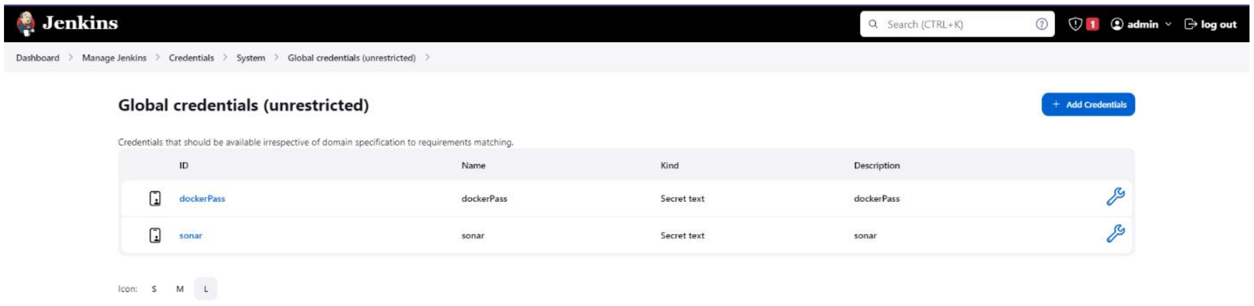
Secret: ··

ID: sonar

Description: sonar

Create

Successfully created a variable for sonarqube login password.


Jenkins
Search (CTRL+K)
admin
log out
Dashboard > Manage Jenkins > Credentials > System > Global credentials (unrestricted) >
Add Credentials

Global credentials (unrestricted)

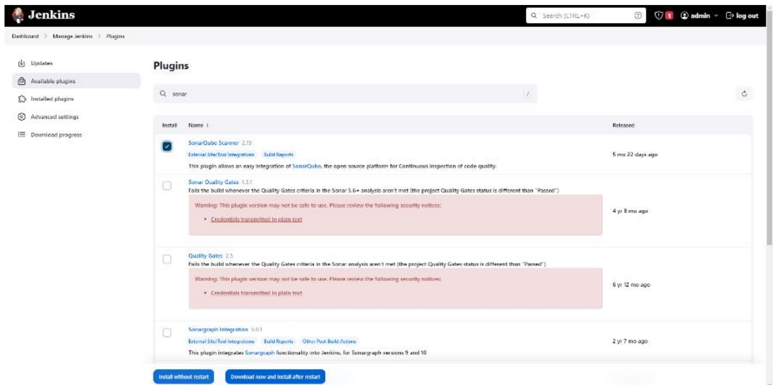
Credentials that should be available irrespective of domain specification to requirements matching.

ID	Name	Kind	Description
dockerPass	dockerPass	Secret text	dockerPass
sonar	sonar	Secret text	sonar

Icon: S M L

Install a plugins for sonarqube

Search (SonarQube Scanner) – Install without restart.



Plugins

sonar

Install	Name ↓	Released
✓	SonarQube Scanner 2.15 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.	5 mo 22 days ago
	Sonar Quality Gates 1.3.1 Fails the build whenever the Quality Gates criteria in the Sonar 5.6+ analysis aren't met (the project Quality Gates status is different than "Passed") Warning: This plugin version may not be safe to use. Please review the following security notices: • Credentials transmitted in plain text	4 yr 8 mo ago
	Quality Gates 2.5 Fails the build whenever the Quality Gates criteria in the Sonar analysis aren't met (the project Quality Gates status is different than "Passed") Warning: This plugin version may not be safe to use. Please review the following security notices: • Credentials transmitted in plain text	6 yr 12 mo ago
	Sonargraph Integration 5.0.1 External Site/Tool Integrations Build Reports Other Post Build Actions This plugin integrates Sonargraph functionality into Jenkins, for Sonargraph versions 9 and 10	2 yr 7 mo ago

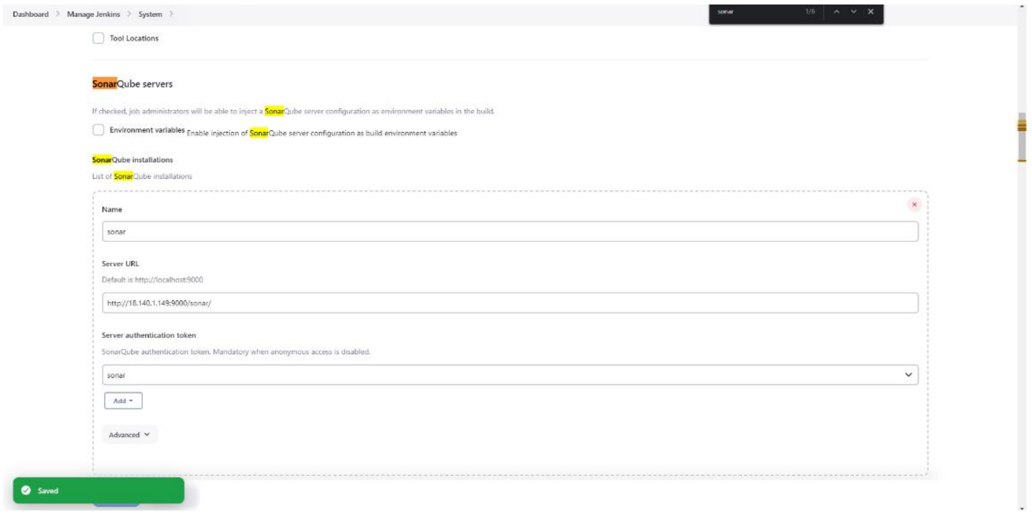
Dashboard – Manage Jenkins – System

SonarQube servers

Name: sonar

Server URl: paste the sonar URL

Save.



SonarQube servers

If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.

Environment variables Enable injection of SonarQube server configuration as build environment variables

SonarQube installations

List of SonarQube installations

Name: sonar

Server URL
Default is http://localhost:9000

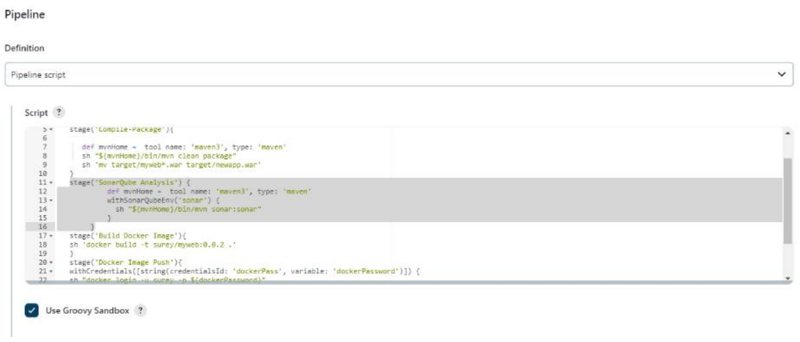
http://18.140.1.149:9000/sonar/

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.

sonar

Go back to already create pipeline project script field

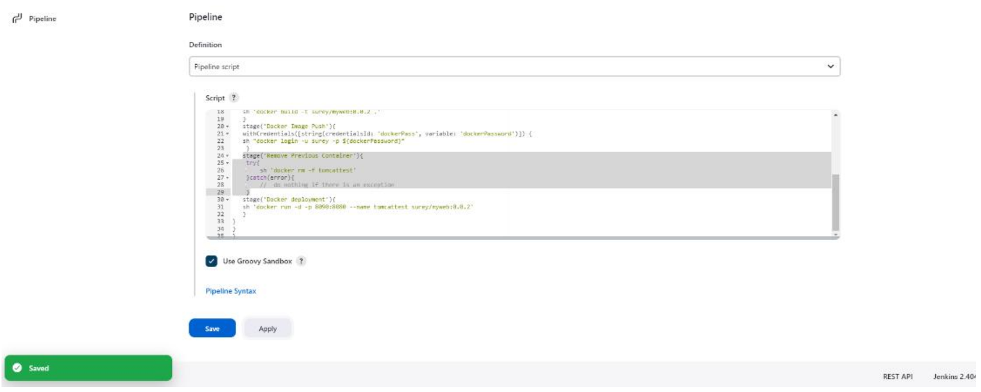
Paste the sonarqube groovy script under the maven stage



Definition: Pipeline script

```
stage('Compile-Package'){

  def mvnHome =  tool name: 'maven3', type: 'maven'
  sh "${mvnHome}/bin/mvn clean package"
  sh 'mv target/myweb*.war target/newapp.war'
}
stage('SonarQube Analysis') {
        def mvnHome =  tool name: 'maven3', type: 'maven'
        withSonarQubeEnv('sonar') {
          sh "${mvnHome}/bin/mvn sonar:sonar"
        }
    }
stage('Build Docker Image'){
sh 'docker build -t surey/myweb:0.0.2 .'
}
stage('Docker Image Push'){
withCredentials([string(credentialsId: 'dockerPass', variable: 'dockerPassword')]) {
sh "docker login -u surey -p ${dockerPassword}"
```

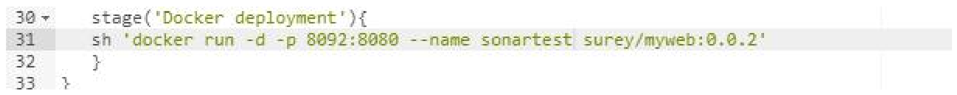
And also add the remove container stage groovy script under the docker image push stage



Definition: Pipeline script

```
sh 'docker build -t surey/myweb:0.0.2 .'
}
stage('Docker Image Push'){
withCredentials([string(credentialsId: 'dockerPass', variable: 'dockerPassword')]) {
sh "docker login -u surey -p ${dockerPassword}"
 }
stage('Remove Previous Container'){
 try{
     sh 'docker rm -f tomcattest'
 }catch(error){
     //  do nothing if there is an exception
 }
stage('Docker deployment'){
sh 'docker run -d -p 8090:8080 --name tomcattest surey/myweb:0.0.2'
}
}
}
}
```

Change the container portnumber and container name (optional) – apply&save.

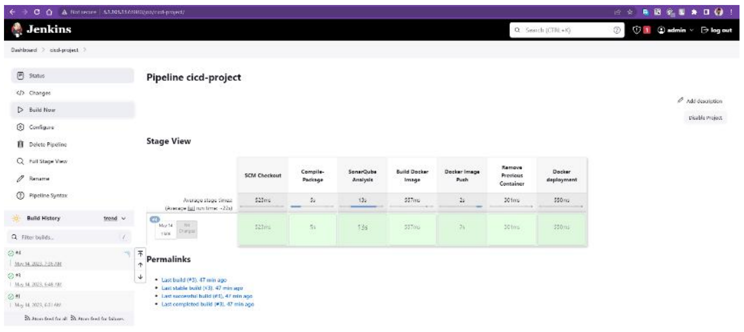


```
    stage('Docker deployment'){
    sh 'docker run -d -p 8092:8080 --name sonartest surey/myweb:0.0.2'
    }
}
```

Build the project.

Below image can see the stages are deployed successfully.

From here the SCM has been compiled in war file – war.file code have been reviewed in sonarqube – warfile have been build into docker image using dockerfile and pushed to docker hub – deployed the newapp war file in tomcat server as a container using Jenkins pipeline.



Jenkins

Dashboard > cicd-project >

Pipeline cicd-project

Stage View

	SCM Checkout	Compile-Package	SonarQube Analysis	Build Docker Image	Docker Image Push	Remove Previous Container	Docker deployment
Average stage times: (Average full run time: ~22s)	523ms	5s	13s	557ms	2s	301ms	550ms
May 14	523ms	5s	13s	557ms	2s	301ms	550ms

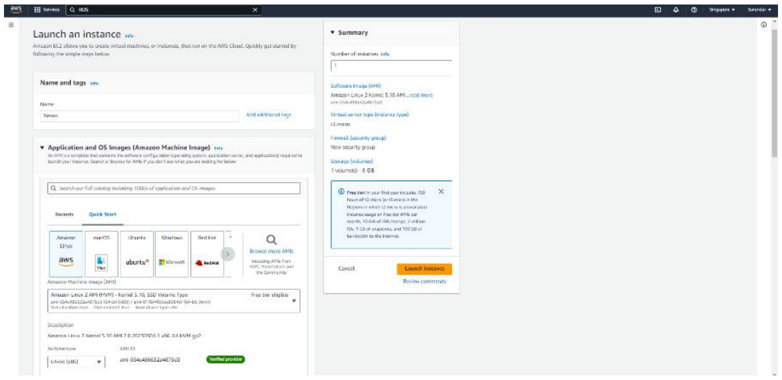
Permalinks

- Last build (#3), 47 min ago
- Last stable build (#3), 47 min ago
- Last successful build (#3), 47 min ago
- Last completed build (#3), 47 min ago

Steps to Create a Nexus repo and push the docker image into it.

Launch an Ec2 instance for nexus server.

AMI amazon linux 2 – t2.medium – SG (All traffic) – Storage 30gib – launch.



Launch an instance

Name and tags

Name: Nexus

Application and OS Images (Amazon Machine Image)

Amazon Machine Image (AMI): Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

Summary

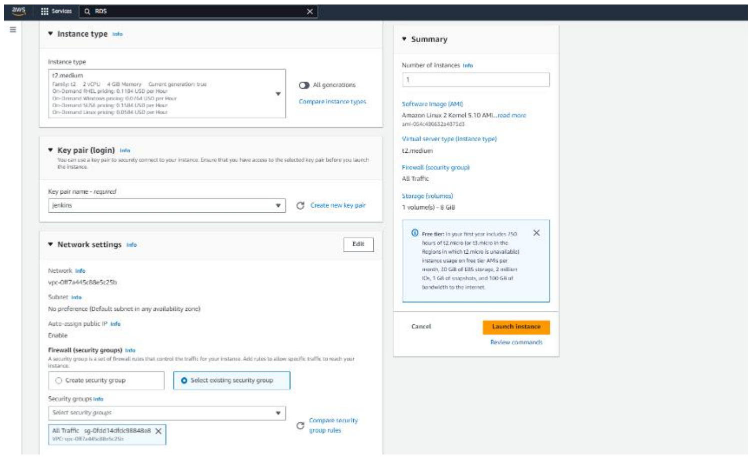
Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB



Instance type: t2.medium

Key pair name - required: jenkins

Network settings

Firewall (security groups): Select existing security group

All Traffic sg-0fdd14dfdc88848e8

Summary

Number of instances: 1

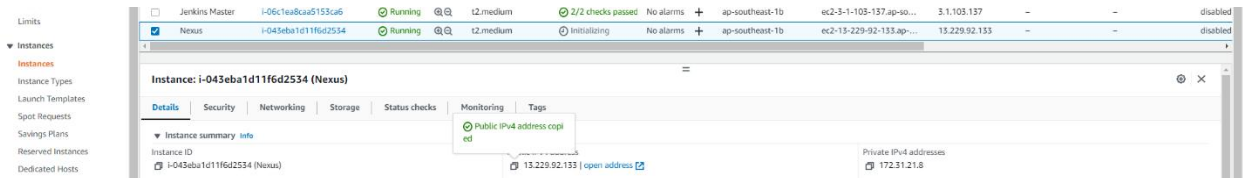
Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more

Virtual server type (instance type): t2.medium

Firewall (security group): All Traffic

Storage (volumes): 1 volume(s) - 8 GiB

Copy the ipv4 - connect putty.



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 address
☐	Jenkins Master	i-06c1ea8caa5153ca6	Running	t2.medium	2/2 checks passed	No alarms	ap-southeast-1b	ec2-3-1-103-137.ap-so...	3.1.103.137
☑	Nexus	i-043eba1d11f6d2534	Running	t2.medium	Initializing	No alarms	ap-southeast-1b	ec2-13-229-92-133.ap-...	13.229.92.133

Instance: i-043eba1d11f6d2534 (Nexus)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Public IPv4 address copied

Instance summary

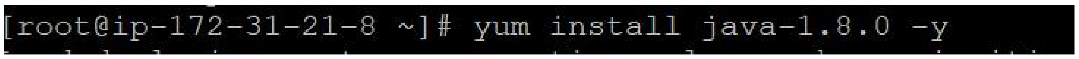
Instance ID: i-043eba1d11f6d2534 (Nexus)

Public IPv4 address: 13.229.92.133 | open address

Private IPv4 addresses: 172.31.21.8

Install java

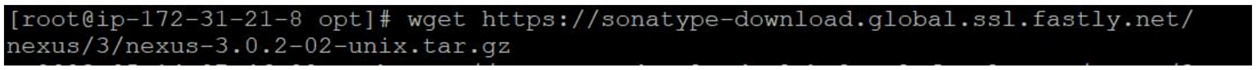
#yum install java-1.8.0 -y



```
[root@ip-172-31-21-8 ~]# yum install java-1.8.0 -y
```

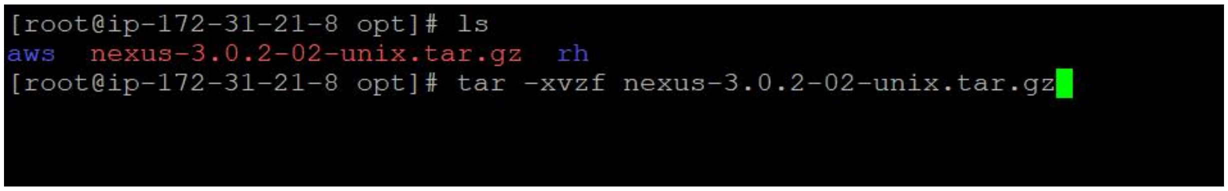
#cd /opt

#wget <nexus download link>



```
[root@ip-172-31-21-8 opt]# wget https://sonatype-download.global.ssl.fastly.net/
nexus/3/nexus-3.0.2-02-unix.tar.gz
```

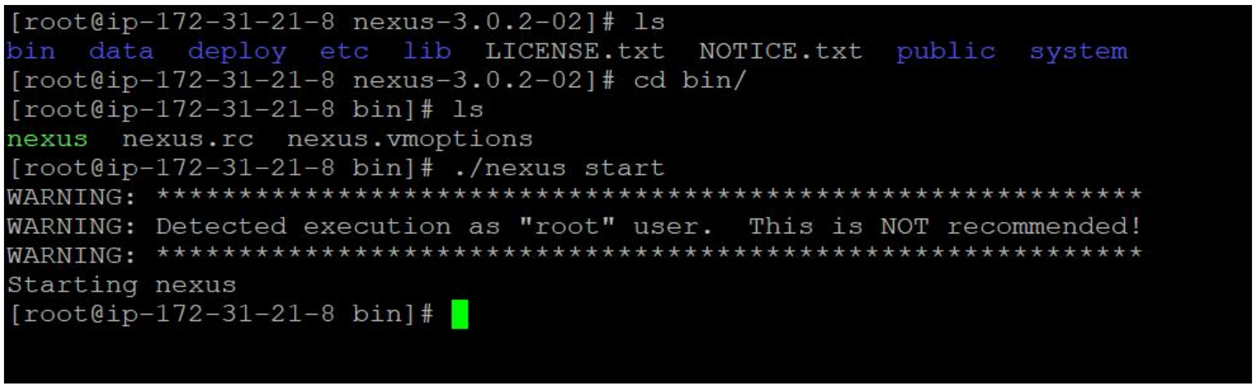
#tar -xvzf nexus-3.0.2-02-unix.tar.gz



```
[root@ip-172-31-21-8 opt]# ls
aws  nexus-3.0.2-02-unix.tar.gz  rh
[root@ip-172-31-21-8 opt]# tar -xvzf nexus-3.0.2-02-unix.tar.gz
```

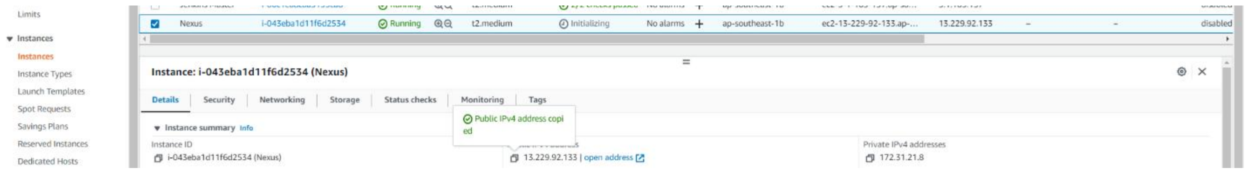
#cd nexus-3.0.2-02/bin

#./nexus start



```
[root@ip-172-31-21-8 nexus-3.0.2-02]# ls
bin  data  deploy  etc  lib  LICENSE.txt  NOTICE.txt  public  system
[root@ip-172-31-21-8 nexus-3.0.2-02]# cd bin/
[root@ip-172-31-21-8 bin]# ls
nexus  nexus.rc  nexus.vmoptions
[root@ip-172-31-21-8 bin]# ./nexus start
WARNING: ************************************************************
WARNING: Detected execution as "root" user.  This is NOT recommended!
WARNING: ************************************************************
Starting nexus
[root@ip-172-31-21-8 bin]#
```

Copy Ipv4 address – Paste Ipv4 add:8081 in browser



☑	Nexus	i-043eba1d11f6d2534	Running	t2.medium	Initializing	No alarms	ap-southeast-1b	ec2-13-229-92-133.ap-...	13.229.92.133	–	–	disabled

Instance: i-043eba1d11f6d2534 (Nexus)

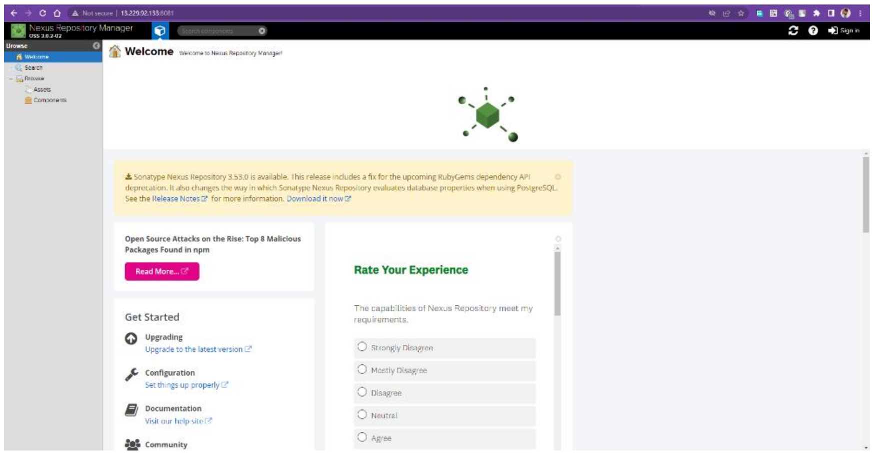
Public IPv4 address copied

Instance ID: i-043eba1d11f6d2534 (Nexus)

13.229.92.133 | open address

Private IPv4 addresses: 172.31.21.8

Nexus Private repo dashboard is hosted



Sonatype Nexus Repository 3.53.0 is available. This release includes a fix for the upcoming RubyGems dependency API deprecation. It also changes the way in which Sonatype Nexus Repository evaluates database properties when using PostgreSQL. See the Release Notes for more information. Download it now

Open Source Attacks on the Rise: Top 8 Malicious Packages Found in npm

Get Started

Upgrading – Upgrade to the latest version

Configuration – Set things up properly

Documentation – Visit our help site

Community

Rate Your Experience

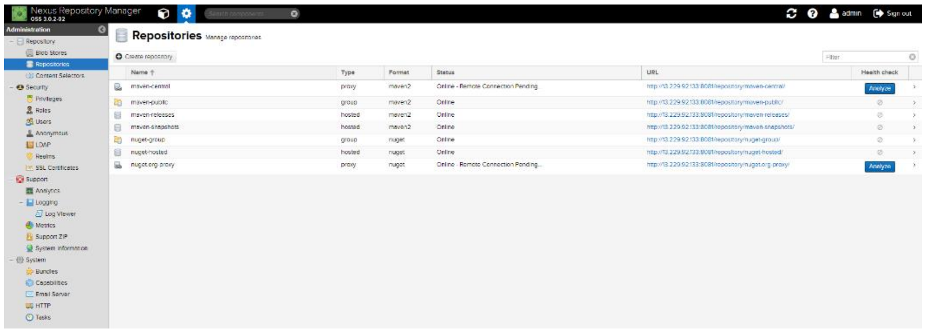
The capabilities of Nexus Repository meet my requirements.

Sigin

user:admin

password:admin123

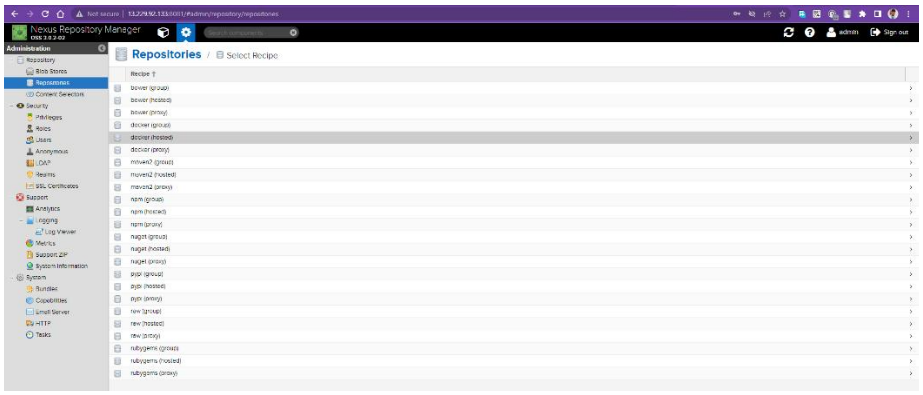
In repositories



Name	Type	Format	Status	URL	Health check
maven-central	proxy	maven2	Online - Remote Connection Pending...	http://13.229.92.133:8081/repository/maven-central/	Analyze
maven-public	group	maven2	Online	http://13.229.92.133:8081/repository/maven-public/	
maven-releases	hosted	maven2	Online	http://13.229.92.133:8081/repository/maven-releases/	
maven-snapshots	hosted	maven2	Online	http://13.229.92.133:8081/repository/maven-snapshots/	
nuget-group	group	nuget	Online	http://13.229.92.133:8081/repository/nuget-group/	
nuget-hosted	hosted	nuget	Online	http://13.229.92.133:8081/repository/nuget-hosted/	
nuget.org-proxy	proxy	nuget	Online - Remote Connection Pending...	http://13.229.92.133:8081/repository/nuget.org-proxy/	Analyze

create a Repositories – docker

select docker (hosted)



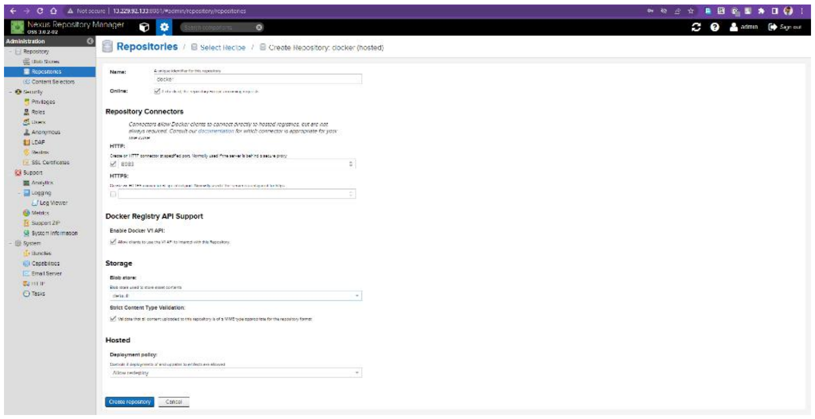
Repositories / Select Recipe

Recipe
bower (group)
bower (hosted)
bower (proxy)
docker (group)
docker (hosted)
docker (proxy)
maven2 (group)
maven2 (hosted)
maven2 (proxy)
npm (group)
npm (hosted)
npm (proxy)
nuget (group)
nuget (hosted)
nuget (proxy)
pypi (group)
pypi (hosted)
pypi (proxy)
raw (group)
raw (hosted)
raw (proxy)
rubygems (group)
rubygems (hosted)
rubygems (proxy)

Set a Name: Docker

Repo HTTP: 8083 < - (repo port)

Enable Docker V1 API – Create Repo.



Repositories / Select Recipe / Create Repository: docker (hosted)

Name: docker

Online: ✓

Repository Connectors

Connectors allow Docker clients to connect directly to hosted registries, but are not always required. Consult our documentation for which connector is appropriate for your use case.

HTTP: ✓ 8083

HTTPS:

Docker Registry API Support

Enable Docker V1 API: ✓ Allow clients to use the V1 API to interact with this Repository.

Storage

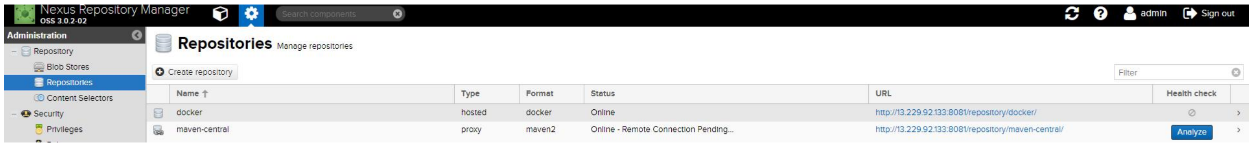
Blob store: default

Strict Content Type Validation: ✓ Validate that all content uploaded to this repository is of a MIME type appropriate for the repository format.

Hosted

Deployment policy: Allow redeploy

Docker repo has been created in nexus.

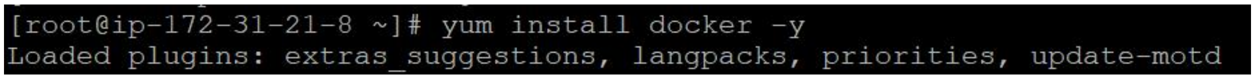


Repositories Manage repositories

Name	Type	Format	Status	URL	Health check
docker	hosted	docker	Online	http://13.229.92.133:8081/repository/docker/	
maven-central	proxy	maven2	Online - Remote Connection Pending...	http://13.229.92.133:8081/repository/maven-central/	Analyze

Install docker in nexus Ec2 Server.

#yum install docker -y



```
[root@ip-172-31-21-8 ~]# yum install docker -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
```

#cd /etc/docker

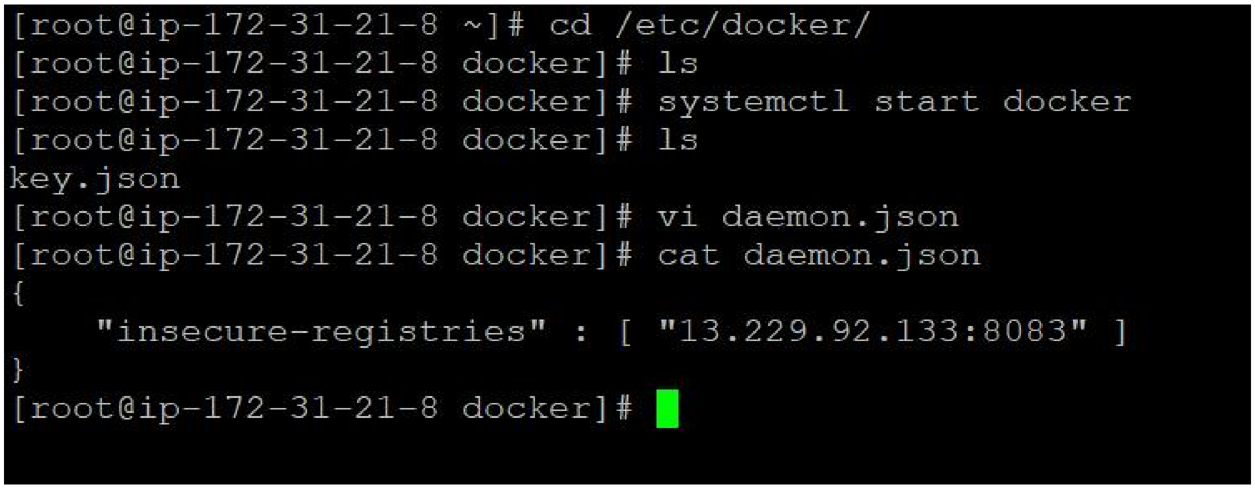
Start the docker service

#systemctl start docker

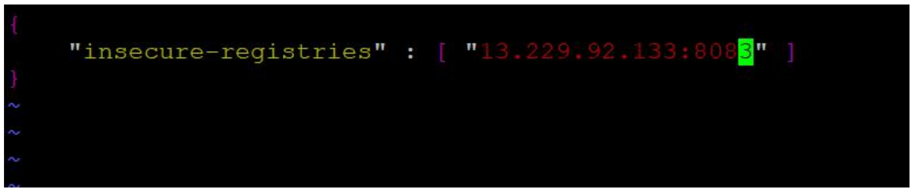
#vi daemon.json

```
{
        “insecure-registries” : [ “nexus Server IPv4:Repo Portno” ]
}
```

:wq!

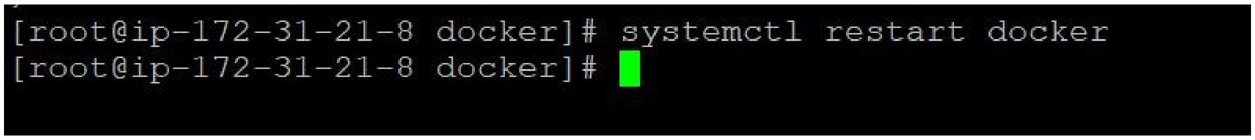


```
[root@ip-172-31-21-8 ~]# cd /etc/docker/
[root@ip-172-31-21-8 docker]# ls
[root@ip-172-31-21-8 docker]# systemctl start docker
[root@ip-172-31-21-8 docker]# ls
key.json
[root@ip-172-31-21-8 docker]# vi daemon.json
[root@ip-172-31-21-8 docker]# cat daemon.json
{
    "insecure-registries" : [ "13.229.92.133:8083" ]
}
[root@ip-172-31-21-8 docker]#
```



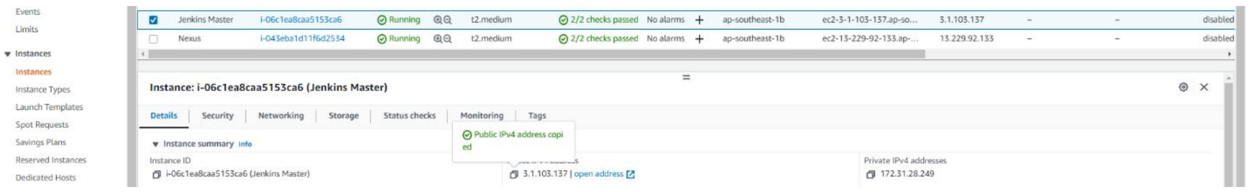
```
{
    "insecure-registries" : [ "13.229.92.133:8083" ]
}
~
~
~
```

#systemctl restart docker



```
[root@ip-172-31-21-8 docker]# systemctl restart docker
[root@ip-172-31-21-8 docker]#
```

Connect the Jenkins Ec2 server



```
Events
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
```

✓	Jenkins Master	i-06c1ea8caa5153ca6	Running	t2.medium	2/2 checks passed	No alarms	ap-southeast-1b	ec2-3-1-103-137.ap-so...	3.1.103.137	–	–	disabled
	Nexus	i-043eba1d11f6d2534	Running	t2.medium	2/2 checks passed	No alarms	ap-southeast-1b	ec2-13-229-92-133.ap-...	13.229.92.133	–	–	disabled

Instance: i-06c1ea8caa5153ca6 (Jenkins Master)

Instance summary Info

Public IPv4 address copied

Instance ID: i-06c1ea8caa5153ca6 (Jenkins Master)

3.1.103.137 | open address

Private IPv4 addresses: 172.31.28.249

#cd /etc/docker

#vi daemon.json

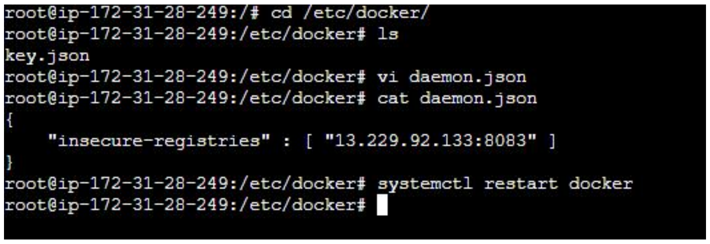
{

“insecure-registries” : [“nexus Server IPv4:Repo Portno”]

}

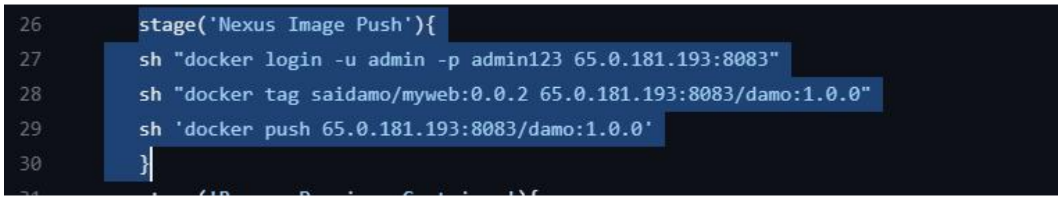
:wq!

#systemctl restart docker



```
root@ip-172-31-28-249:/# cd /etc/docker/
root@ip-172-31-28-249:/etc/docker# ls
key.json
root@ip-172-31-28-249:/etc/docker# vi daemon.json
root@ip-172-31-28-249:/etc/docker# cat daemon.json
{
    "insecure-registries" : [ "13.229.92.133:8083" ]
}
root@ip-172-31-28-249:/etc/docker# systemctl restart docker
root@ip-172-31-28-249:/etc/docker# 
```

Copy the nexus groovy script stage

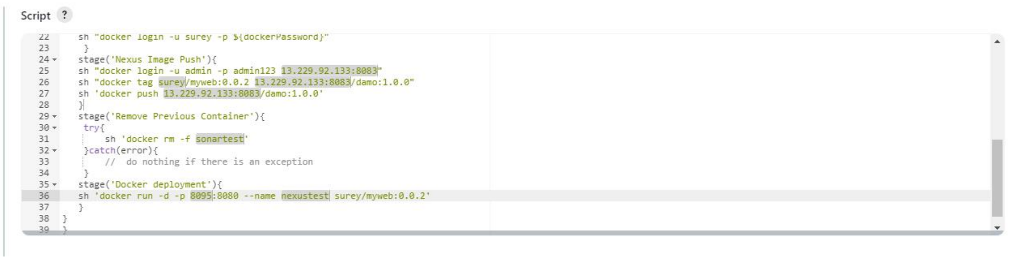


```
        stage('Nexus Image Push'){
        sh "docker login -u admin -p admin123 65.0.181.193:8083"
        sh "docker tag saidamo/myweb:0.0.2 65.0.181.193:8083/damo:1.0.0"
        sh 'docker push 65.0.181.193:8083/damo:1.0.0'
        }
```

In Jenkins dashboard

In pipeline script

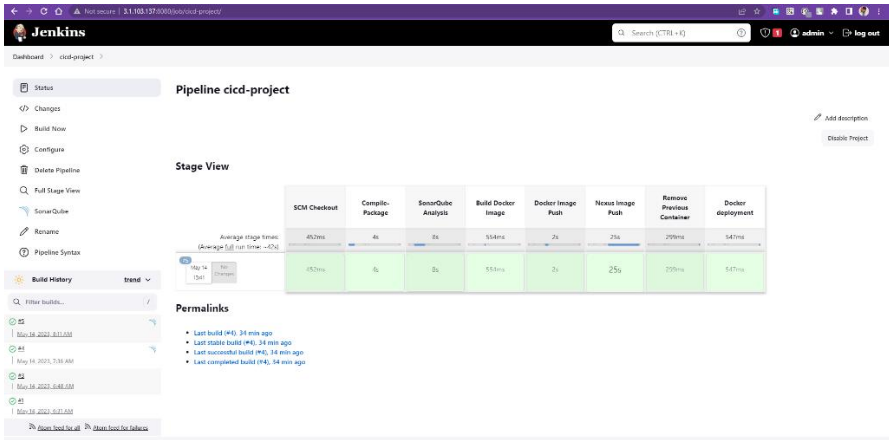
Paste the nexus stage under docker image push stage – apply and save.



Script

```
   sh "docker login -u surey -p ${dockerPassword}"
    }
   stage('Nexus Image Push'){
   sh "docker login -u admin -p admin123 13.229.92.133:8083"
   sh "docker tag surey/myweb:0.0.2 13.229.92.133:8083/damo:1.0.0"
   sh 'docker push 13.229.92.133:8083/damo:1.0.0'
   }
   stage('Remove Previous Container'){
    try{
        sh 'docker rm -f sonartest'
    }catch(error){
        //  do nothing if there is an exception
    }
   stage('Docker deployment'){
   sh 'docker run -d -p 8095:8080 --name nexustest surey/myweb:0.0.2'
   }
}
}
```

Build the Jenkins pipeline project



Pipeline cicd-project

Stage View

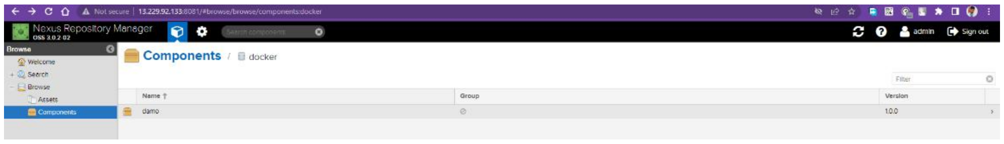
	SCM Checkout	Compile-Package	SonarQube Analysis	Build Docker Image	Docker Image Push	Nexus Image Push	Remove Previous Container	Docker deployment
Average stage times: (Average full run time: ~42s)	452ms	4s	8s	554ms	2s	25s	299ms	547ms
May 14 15:41 No Changes	452ms	4s	8s	554ms	2s	25s	299ms	547ms

Permalinks

- Last build (#4), 34 min ago
- Last stable build (#4), 34 min ago
- Last successful build (#4), 34 min ago
- Last completed build (#4), 34 min ago

Now go to the nexus hub and check the image have been pushed successfully in nexus repo.

From here the SCM has been compiled in war file – war.file code have been reviewed in sonarqube – warfile have been build into docker image using dockerfile and pushed to docker hub and nexus repo – deploy the newapp war file in tomcat server as a container using Jenkins pipeline.



Components / docker

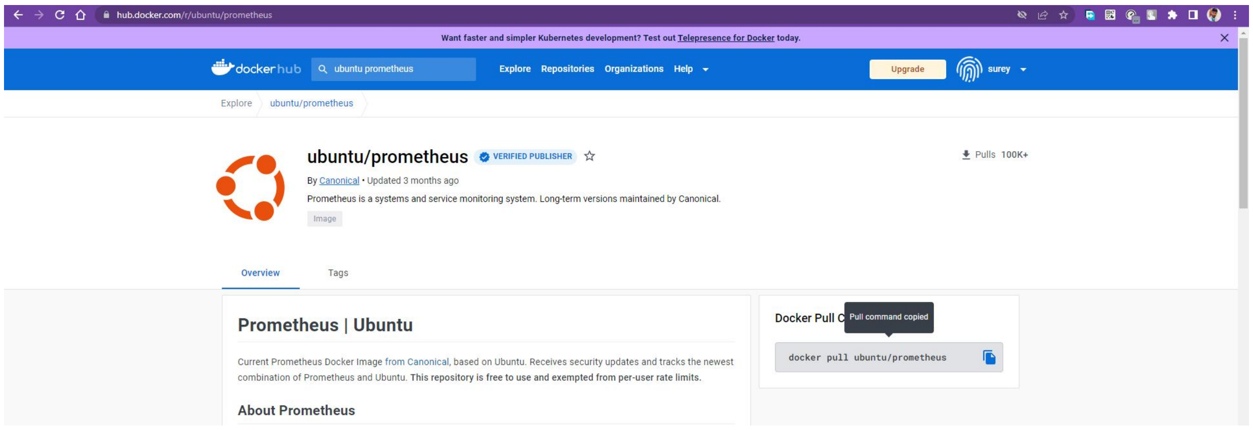
Name	Group	Version
damo		1.0.0

Steps to add monitoring tools with Jenkins to view the metrics of Jenkins pipeline project

In docker hub

Search ubuntu8 prometheus

Copy the pull command.



hub.docker.com/r/ubuntu/prometheus

Want faster and simpler Kubernetes development? Test out Telepresence for Docker today.

Explore / ubuntu/prometheus

ubuntu/prometheus VERIFIED PUBLISHER

By Canonical • Updated 3 months ago

Prometheus is a systems and service monitoring system. Long-term versions maintained by Canonical.

Pulls 100K+

Prometheus | Ubuntu

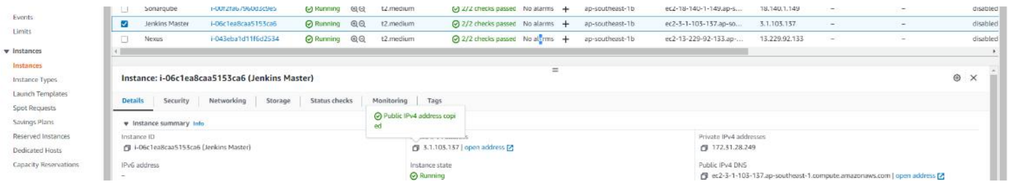
Current Prometheus Docker Image from Canonical, based on Ubuntu. Receives security updates and tracks the newest combination of Prometheus and Ubuntu. This repository is free to use and exempted from per-user rate limits.

About Prometheus

Docker Pull C Pull command copied

```
docker pull ubuntu/prometheus
```

Connect the Jenkins ec2 server.



	Name	Instance ID	State		Type	Status check	Alarm		Zone	Public DNS	Public IP			Monitoring
☐	Sonarqube	i-00f2fa67960d3c9e5	Running		t2.medium	2/2 checks passed	No alarms	+	ap-southeast-1b	ec2-18-140-1-149.ap-s...	18.140.1.149	–	–	disabled
✓	Jenkins Master	i-06c1ea8caa5153ca6	Running		t2.medium	2/2 checks passed	No alarms	+	ap-southeast-1b	ec2-3-1-103-137.ap-so...	3.1.103.137	–	–	disabled
☐	Nexus	i-043eba1d11f6d2534	Running		t2.medium	2/2 checks passed	No alarms	+	ap-southeast-1b	ec2-13-229-92-133.ap-...	13.229.92.133	–	–	disabled

Instance: i-06c1ea8caa5153ca6 (Jenkins Master)

Instance summary Info

Instance ID: i-06c1ea8caa5153ca6 (Jenkins Master)

Public IPv4 address copied

3.1.103.137 | open address

Private IPv4 addresses: 172.31.28.249

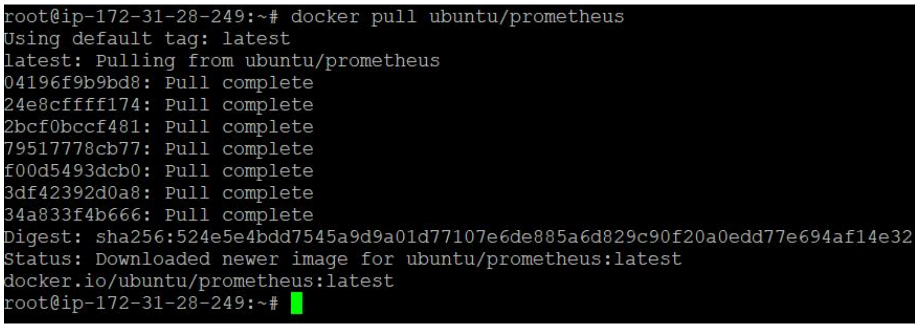
IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-3-1-103-137.ap-southeast-1.compute.amazonaws.com | open address

Pull the Prometheus Docker Image

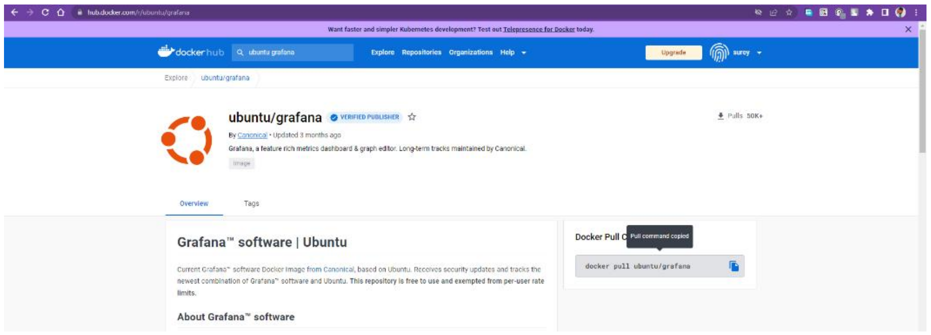
#docker pull ubuntu/prometheus



```
root@ip-172-31-28-249:~# docker pull ubuntu/prometheus
Using default tag: latest
latest: Pulling from ubuntu/prometheus
04196f9b9bd8: Pull complete
24e8cffff174: Pull complete
2bcf0bccf481: Pull complete
79517778cb77: Pull complete
f00d5493dcb0: Pull complete
3df42392d0a8: Pull complete
34a833f4b666: Pull complete
Digest: sha256:524e5e4bdd7545a9d9a01d77107e6de885a6d829c90f20a0edd77e694af14e32
Status: Downloaded newer image for ubuntu/prometheus:latest
docker.io/ubuntu/prometheus:latest
root@ip-172-31-28-249:~#
```

In Docker hub

Search ubuntu Grafana – copy the pull cmnd



hub.docker.com/r/ubuntu/grafana

Want faster and simpler Kubernetes development? Test out Telepresence for Docker today.

Explore / ubuntu/grafana

ubuntu/grafana VERIFIED PUBLISHER

By Canonical • Updated 3 months ago

Grafana, a feature rich metrics dashboard & graph editor. Long-term tracks maintained by Canonical.

Pulls 50K+

Grafana™ software | Ubuntu

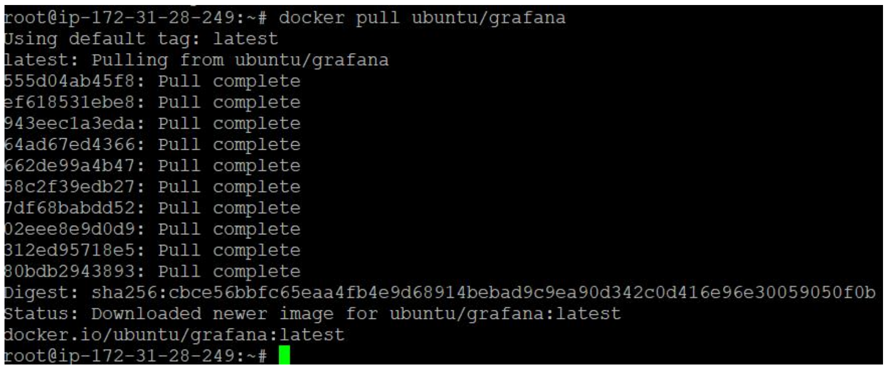
Current Grafana™ software Docker Image from Canonical, based on Ubuntu. Receives security updates and tracks the newest combination of Grafana™ software and Ubuntu. This repository is free to use and exempted from per-user rate limits.

About Grafana™ software

Docker Pull C Pull command copied

```
docker pull ubuntu/grafana
```

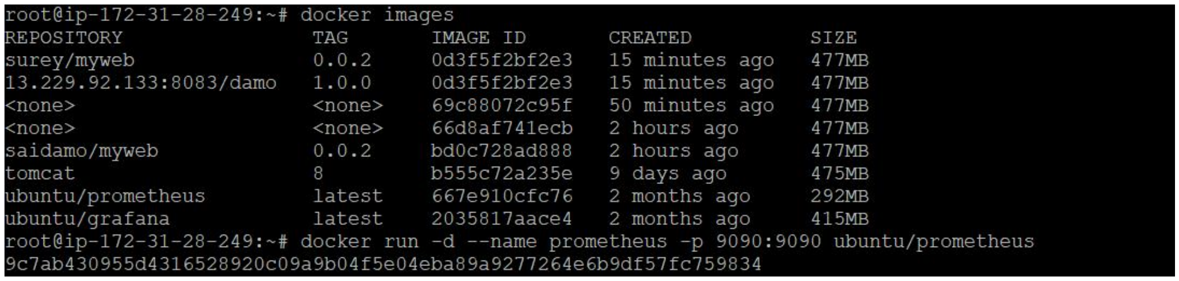
#docker pull ubuntu/grafana



```
root@ip-172-31-28-249:~# docker pull ubuntu/grafana
Using default tag: latest
latest: Pulling from ubuntu/grafana
555d04ab45f8: Pull complete
ef618531ebe8: Pull complete
943eec1a3eda: Pull complete
64ad67ed4366: Pull complete
662de99a4b47: Pull complete
58c2f39edb27: Pull complete
7df68babdd52: Pull complete
02eee8e9d0d9: Pull complete
312ed95718e5: Pull complete
80bdb2943893: Pull complete
Digest: sha256:cbce56bbfc65eaa4fb4e9d68914bebad9c9ea90d342c0d416e96e30059050f0b
Status: Downloaded newer image for ubuntu/grafana:latest
docker.io/ubuntu/grafana:latest
root@ip-172-31-28-249:~# 
```

#docker images

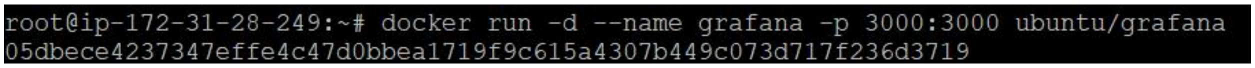
#docker run -d –name prometheus -p 9090:9090 ubuntu/prometheus



```
root@ip-172-31-28-249:~# docker images
REPOSITORY                 TAG       IMAGE ID       CREATED          SIZE
surey/myweb                0.0.2     0d3f5f2bf2e3   15 minutes ago   477MB
13.229.92.133:8083/damo    1.0.0     0d3f5f2bf2e3   15 minutes ago   477MB
<none>                     <none>    69c88072c95f   50 minutes ago   477MB
<none>                     <none>    66d8af741ecb   2 hours ago      477MB
saidamo/myweb              0.0.2     bd0c728ad888   2 hours ago      477MB
tomcat                     8         b555c72a235e   9 days ago       475MB
ubuntu/prometheus          latest    667e910cfc76   2 months ago     292MB
ubuntu/grafana             latest    2035817aace4   2 months ago     415MB
root@ip-172-31-28-249:~# docker run -d --name prometheus -p 9090:9090 ubuntu/prometheus
9c7ab430955d4316528920c09a9b04f5e04eba89a9277264e6b9df57fc759834
```

Create a Grafana container using docker image

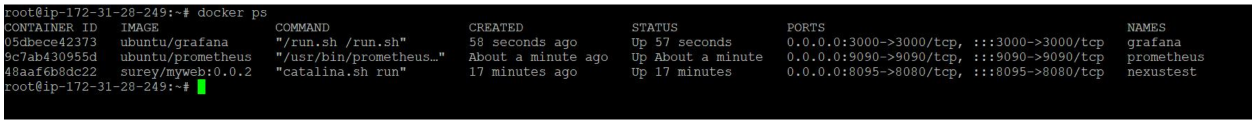
#docker run -d –name Grafana -p 3000:3000 ubuntu/grafana



```
root@ip-172-31-28-249:~# docker run -d --name grafana -p 3000:3000 ubuntu/grafana
05dbece4237347effe4c47d0bbea1719f9c615a4307b449c073d717f236d3719
```

#docker ps

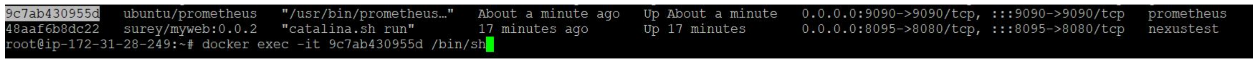
There can see the grafana and Prometheus container has been running.



```
root@ip-172-31-28-249:~# docker ps
CONTAINER ID   IMAGE               COMMAND                  CREATED              STATUS              PORTS                                       NAMES
05dbece42373   ubuntu/grafana      "/run.sh /run.sh"        58 seconds ago       Up 57 seconds       0.0.0.0:3000->3000/tcp, :::3000->3000/tcp   grafana
9c7ab430955d   ubuntu/prometheus   "/usr/bin/prometheus…"   About a minute ago   Up About a minute   0.0.0.0:9090->9090/tcp, :::9090->9090/tcp   prometheus
48aaf6b8dc22   surey/myweb:0.0.2   "catalina.sh run"        17 minutes ago       Up 17 minutes       0.0.0.0:8095->8080/tcp, :::8095->8080/tcp   nexustest
root@ip-172-31-28-249:~# 
```

To go access the container

#docker exec -it <containerID> /bin/sh

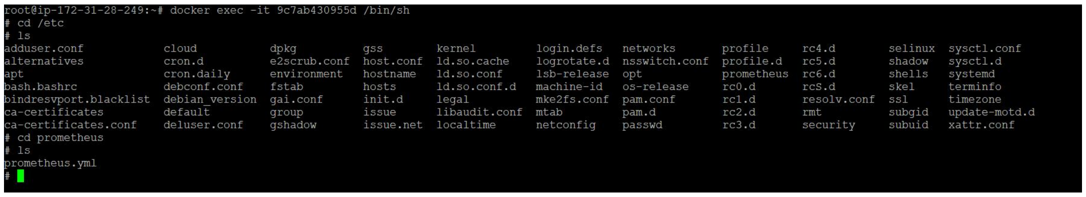


```
9c7ab430955d   ubuntu/prometheus   "/usr/bin/prometheus…"   About a minute ago   Up About a minute   0.0.0.0:9090->9090/tcp, :::9090->9090/tcp   prometheus
48aaf6b8dc22   surey/myweb:0.0.2   "catalina.sh run"        17 minutes ago       Up 17 minutes       0.0.0.0:8095->8080/tcp, :::8095->8080/tcp   nexustest
root@ip-172-31-28-249:~# docker exec -it 9c7ab430955d /bin/sh
```

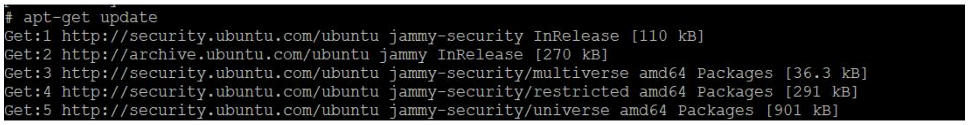
#cd /etc/prometheus/

#apt-get update

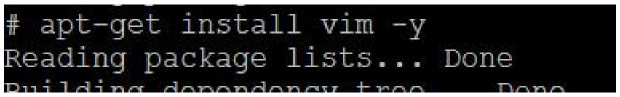
#apt-get install vim -y



```
root@ip-172-31-28-249:~# docker exec -it 9c7ab430955d /bin/sh
# cd /etc
# ls
adduser.conf            cloud           dpkg          gss        kernel          login.defs    networks       profile     rc4.d        selinux   sysctl.conf
alternatives            cron.d          e2scrub.conf  host.conf  ld.so.cache     logrotate.d   nsswitch.conf  profile.d   rc5.d        shadow    sysctl.d
apt                     cron.daily      environment   hostname   ld.so.conf      lsb-release   opt            prometheus  rc6.d        shells    systemd
bash.bashrc             debconf.conf    fstab         hosts      ld.so.conf.d    machine-id    os-release     rc0.d       rcS.d        skel      terminfo
bindresvport.blacklist  debian_version  gai.conf      init.d     legal           mke2fs.conf   pam.conf       rc1.d       resolv.conf  ssl       timezone
ca-certificates         default         group         issue      libaudit.conf   mtab          pam.d          rc2.d       rmt          subgid    update-motd.d
ca-certificates.conf    deluser.conf    gshadow       issue.net  localtime       netconfig     passwd         rc3.d       security     subuid    xattr.conf
# cd prometheus
# ls
prometheus.yml
#
```



```
# apt-get update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [36.3 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [291 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [901 kB]
```



```
# apt-get install vim -y
Reading package lists... Done
Building dependency tree... Done
```

#vi prometheus.yml

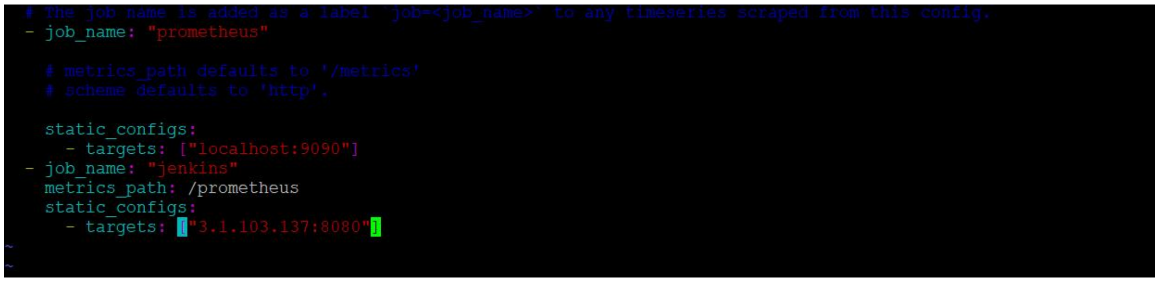
- job_name: “Jenkins”

  metrics_path: /prometheus

  static_configs:

  - targets: [“Jenkins server IPv4:8080”]

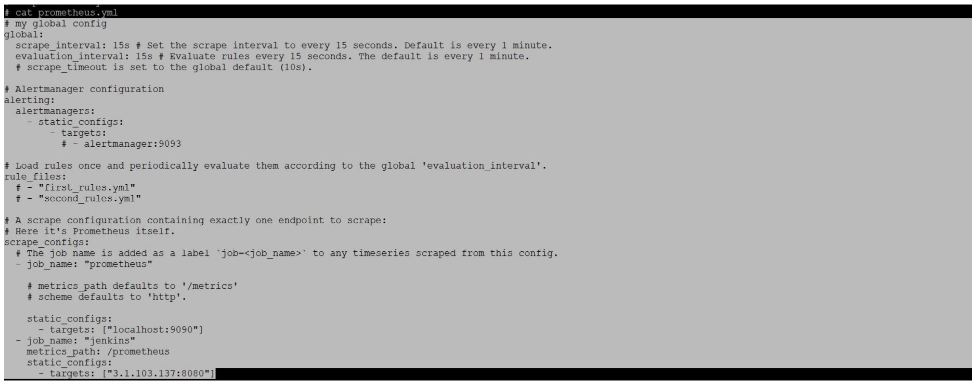
:wq!



```
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["localhost:9090"]
  - job_name: "jenkins"
    metrics_path: /prometheus
    static_configs:
      - targets: ["3.1.103.137:8080"]
~
~
```

#cat prometheus.yml

Copy yml script

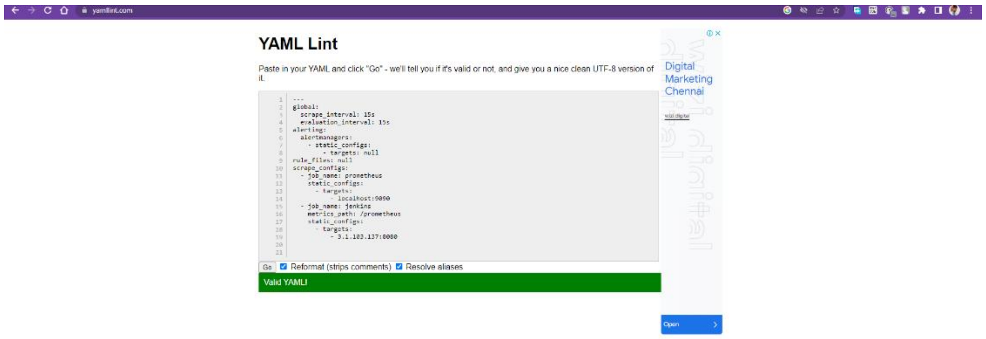


```
# cat prometheus.yml
# my global config
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
        - targets:
          # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["localhost:9090"]
  - job_name: "jenkins"
    metrics_path: /prometheus
    static_configs:
      - targets: ["3.1.103.137:8080"]
```

In browser search YAML Lint

Paste the content

Check the YAML script in valid.



YAML Lint

Paste in your YAML and click "Go" - we'll tell you if it's valid or not, and give you a nice clean UTF-8 version of it.

```
---
global:
  scrape_interval: 15s
  evaluation_interval: 15s
alerting:
  alertmanagers:
    - static_configs:
        - targets: null
rule_files: null
scrape_configs:
  - job_name: prometheus
    static_configs:
      - targets:
          - localhost:9090
  - job_name: jenkins
    metrics_path: /prometheus
    static_configs:
      - targets:
          - 3.1.103.137:8080
```

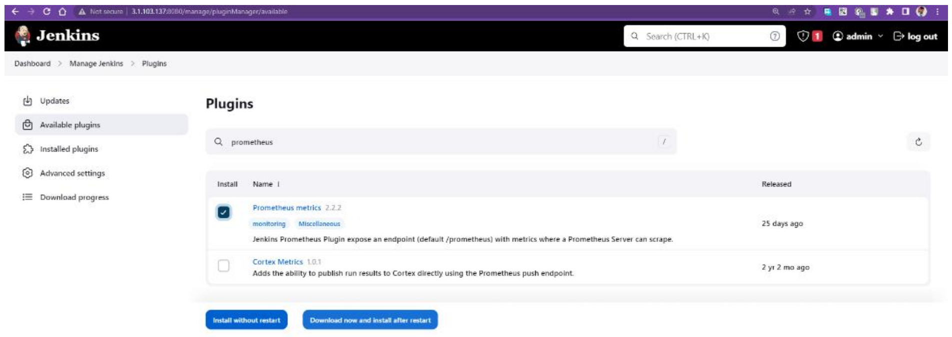
Go ☑ Reformat (strips comments) ☑ Resolve aliases

Valid YAML!

In Jenkins dashboard

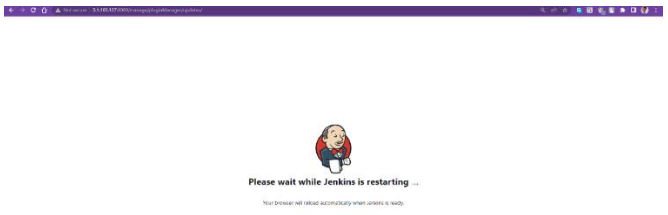
Dashboard – Manage Jenkins – plugins – Available plugins

Search Prometheus metrics – Install without restart



Plugins

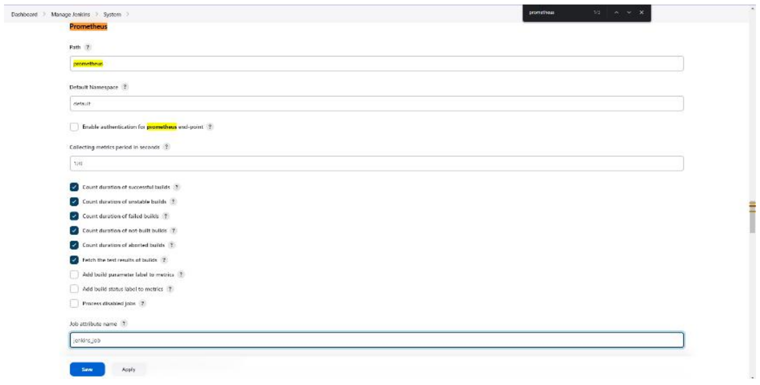
Install	Name	Released
✓	Prometheus metrics 2.2.2 monitoring Miscellaneous Jenkins Prometheus Plugin expose an endpoint (default /prometheus) with metrics where a Prometheus Server can scrape.	25 days ago
	Cortex Metrics 1.0.1 Adds the ability to publish run results to Cortex directly using the Prometheus push endpoint.	2 yr 2 mo ago



Please wait while Jenkins is restarting ...

Your browser will reload automatically when Jenkins is ready.

Dashboard – Manage Jenkins – System – Prometheus – apply & Save.



Prometheus

Path: prometheus

Default Namespace: default

☐ Enable authentication for prometheus end-point

Collecting metrics period in seconds: 120

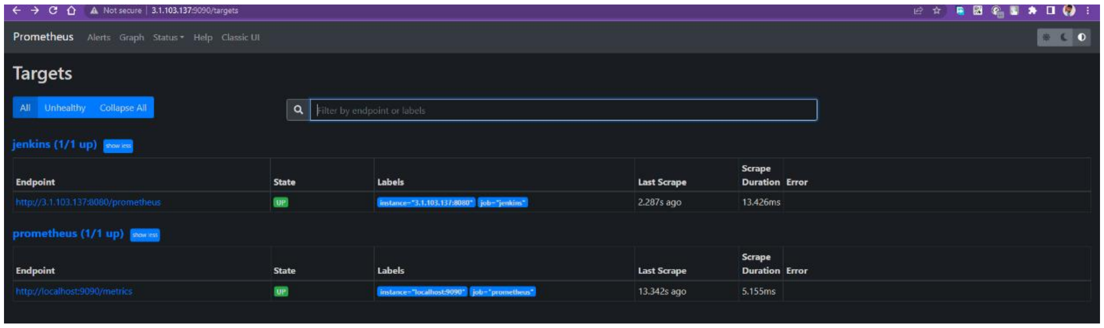
☑ Count duration of successful builds
☑ Count duration of unstable builds
☑ Count duration of failed builds
☑ Count duration of not-built builds
☑ Count duration of aborted builds
☑ Fetch the test results of builds
☐ Add build parameter label to metrics
☐ Add build status label to metrics
☐ Process disabled jobs

Job attribute name: jenkins_job

Hit in browser

Jenkins serverIPV4:9090

There can see Jenkins server metrics state is in UP



Not secure | 3.1.103.137:9090/targets

Targets

jenkins (1/1 up)

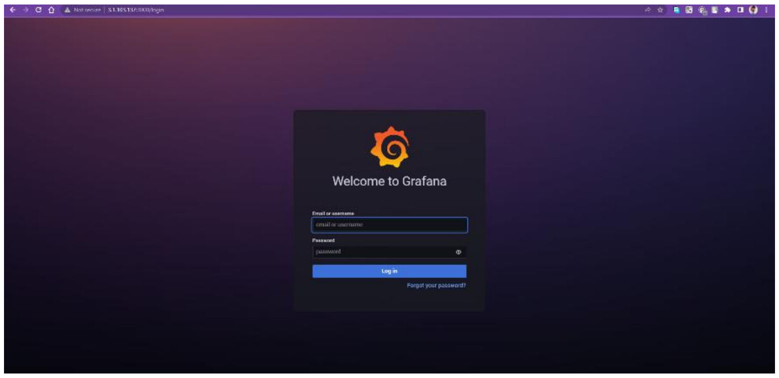
Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://3.1.103.137:8080/prometheus	UP	instance="3.1.103.137:8080" job="jenkins"	2.287s ago	13.426ms	

prometheus (1/1 up)

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9090/metrics	UP	instance="localhost:9090" job="prometheus"	13.342s ago	5.155ms	

Then Connect the grafana dashboard

Paste Jenkins ServerIPv4:3000

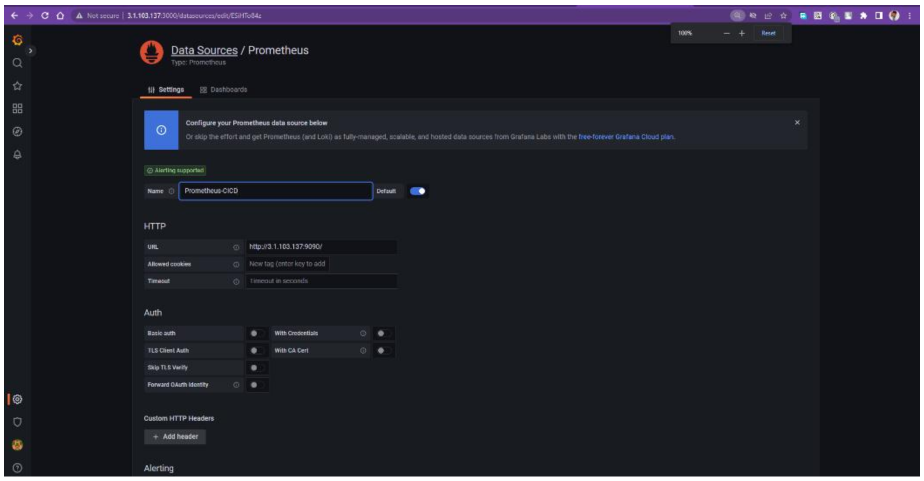


Settings – Create datasource – Choose Prometheus

Set a name: PrometheusCICD

URL : <Prometheus URL>

Save&test



Not secure | 3.1.103.137:3000/datasources/edit/ESiHTo84z

Data Sources / Prometheus

Type: Prometheus

Configure your Prometheus data source below

Or skip the effort and get Prometheus (and Loki) as fully-managed, scalable, and hosted data sources from Grafana Labs with the free-forever Grafana Cloud plan.

Alerting supported

Name: Prometheus-CICD Default: on

HTTP

URL: http://3.1.103.137:9090/

Allowed cookies: New tag (enter key to add

Timeout: Timeout in seconds

Auth

Basic auth: off With Credentials: off

TLS Client Auth: off With CA Cert: off

Skip TLS Verify: off

Forward OAuth Identity: off

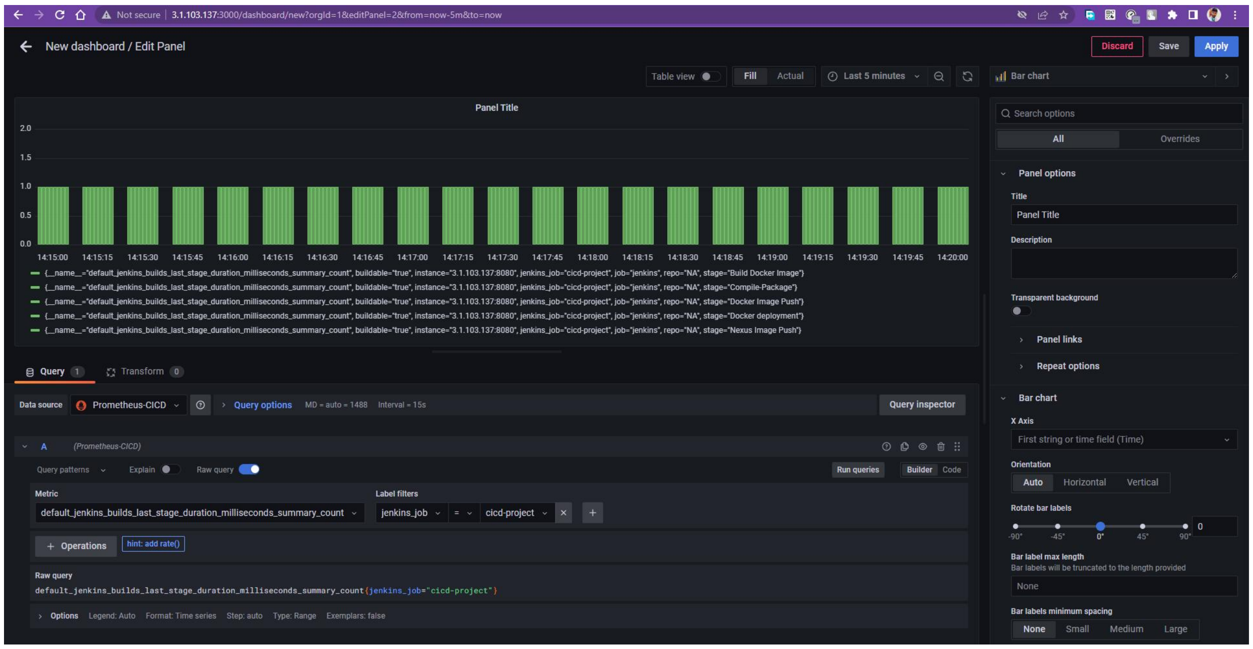
Custom HTTP Headers

+ Add header

Alerting

Create a new dashboard attach the datasource with new panel

There we can monitor the Jenkins dashboard and pipeline project utilization metrics – Apply.



URL: 3.1.103.137:3000/dashboard/new?orgId=1&editPanel=2&from=now-5m&to=now

New dashboard / Edit Panel

Panel Title

```
{__name__="default_jenkins_builds_last_stage_duration_milliseconds_summary_count", buildable="true", instance="3.1.103.137:8080", jenkins_job="cicd-project", job="jenkins", repo="NA", stage="Build Docker Image"}
{__name__="default_jenkins_builds_last_stage_duration_milliseconds_summary_count", buildable="true", instance="3.1.103.137:8080", jenkins_job="cicd-project", job="jenkins", repo="NA", stage="Compile-Package"}
{__name__="default_jenkins_builds_last_stage_duration_milliseconds_summary_count", buildable="true", instance="3.1.103.137:8080", jenkins_job="cicd-project", job="jenkins", repo="NA", stage="Docker Image Push"}
{__name__="default_jenkins_builds_last_stage_duration_milliseconds_summary_count", buildable="true", instance="3.1.103.137:8080", jenkins_job="cicd-project", job="jenkins", repo="NA", stage="Docker deployment"}
{__name__="default_jenkins_builds_last_stage_duration_milliseconds_summary_count", buildable="true", instance="3.1.103.137:8080", jenkins_job="cicd-project", job="jenkins", repo="NA", stage="Nexus Image Push"}
```

Data source: Prometheus-CICD — Query options: MD = auto = 1488, Interval = 15s

Metric: default_jenkins_builds_last_stage_duration_milliseconds_summary_count

Label filters: jenkins_job = cicd-project

Raw query

```
default_jenkins_builds_last_stage_duration_milliseconds_summary_count{jenkins_job="cicd-project"}
```

Options: Legend: Auto, Format: Time series, Step: auto, Type: Range, Exemplars: false

Visualization: Bar chart — Panel options: Title: Panel Title; X Axis: First string or time field (Time); Orientation: Auto; Rotate bar labels: 0; Bar label max length: None; Bar labels minimum spacing: None