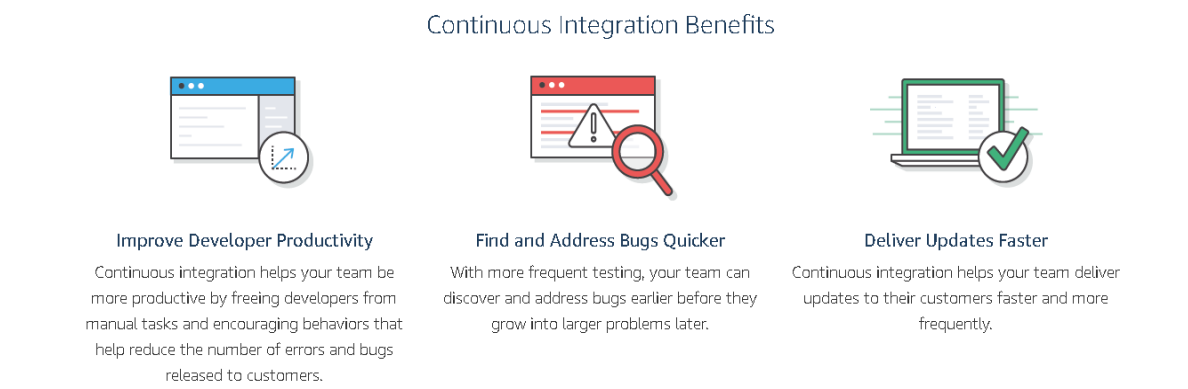
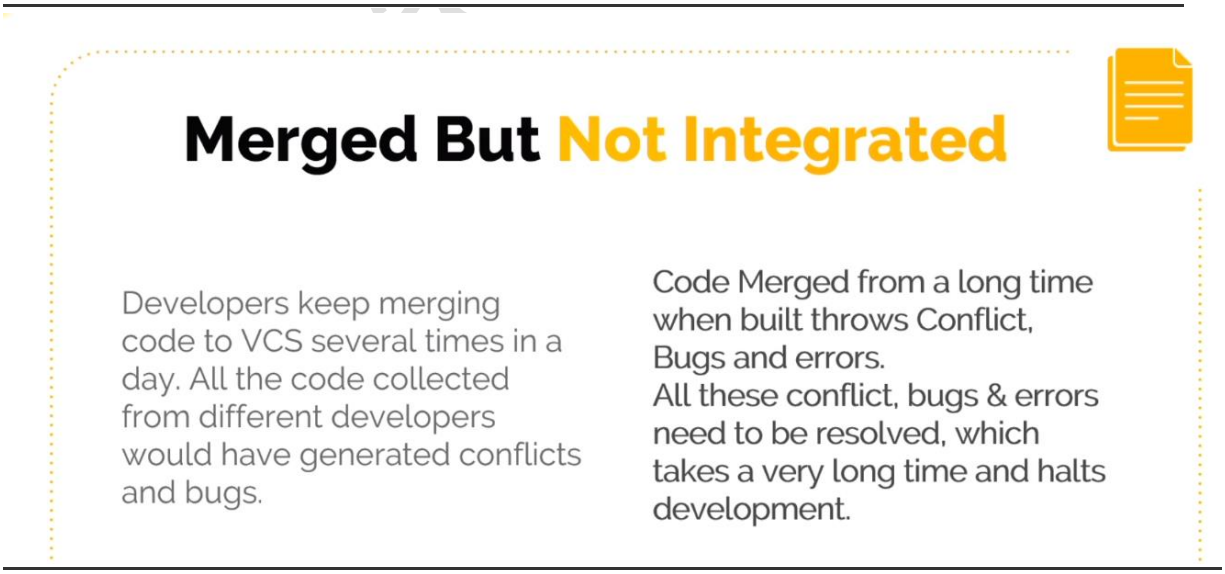
# A Project Demonstration on Continuous Integration using Jenkins, SonarQube and Nexus

## What is Continuous Integration (C.I)?

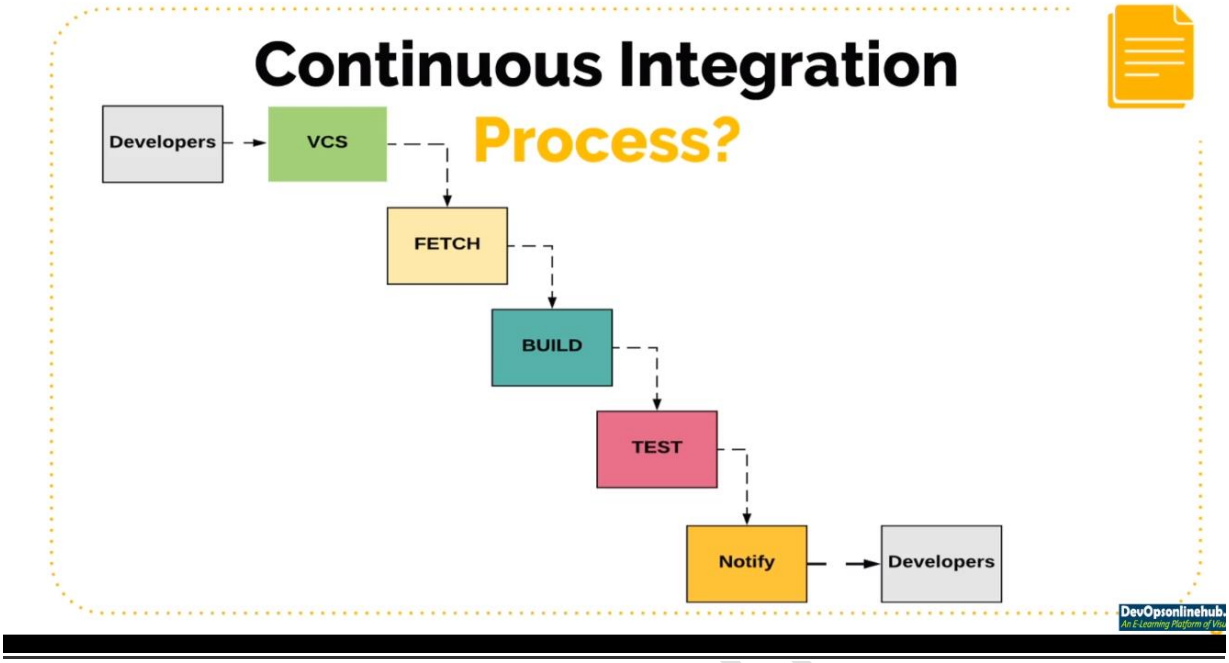
Continuous integration is a DevOps software development practice where developers regularly merge their code changes into a central repository, after which automated builds and tests are run.
The key goals of continuous integration are to find and address bugs quicker, improve software quality, and reduce the time it takes to validate and release new software updates.

## Benefits:

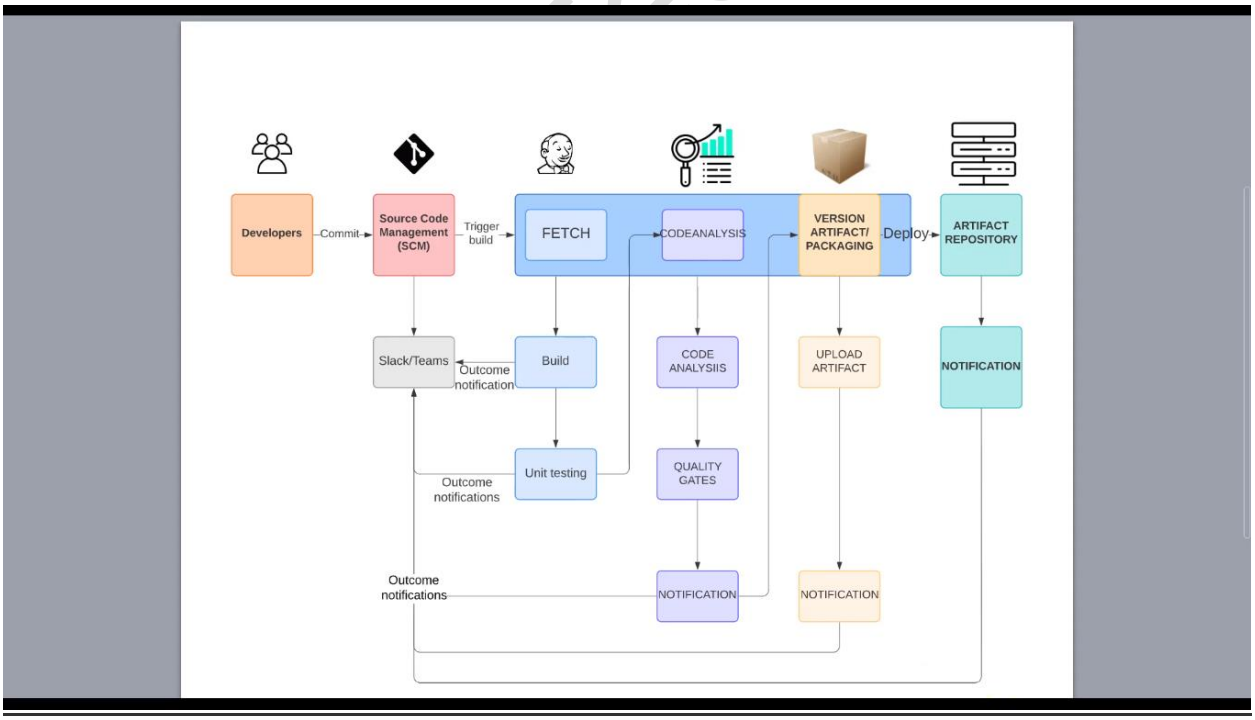


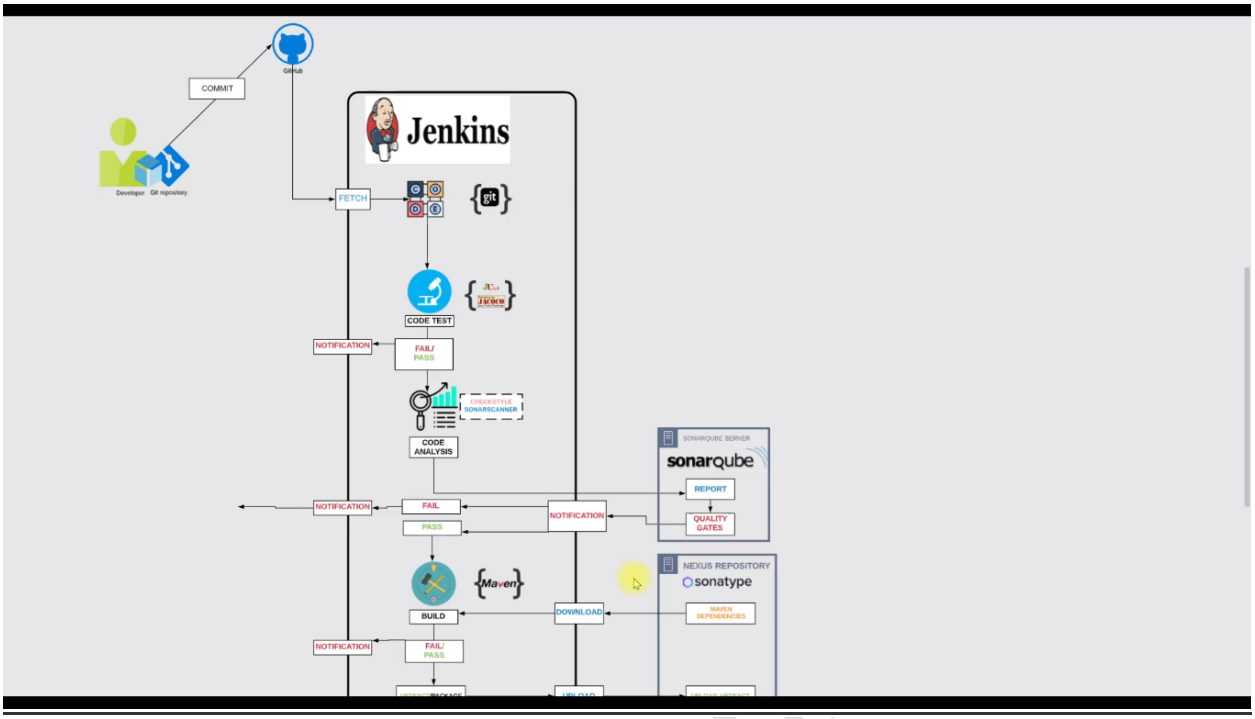



## Process of CI:-




## Continuous Integration WorkFlow:-






## Pre-requisites:

1. Basic understanding of Jenkins
2. Basic knowledge of EC2 instances and linux
3. Awareness of Tools such as Nexus and SonarQube

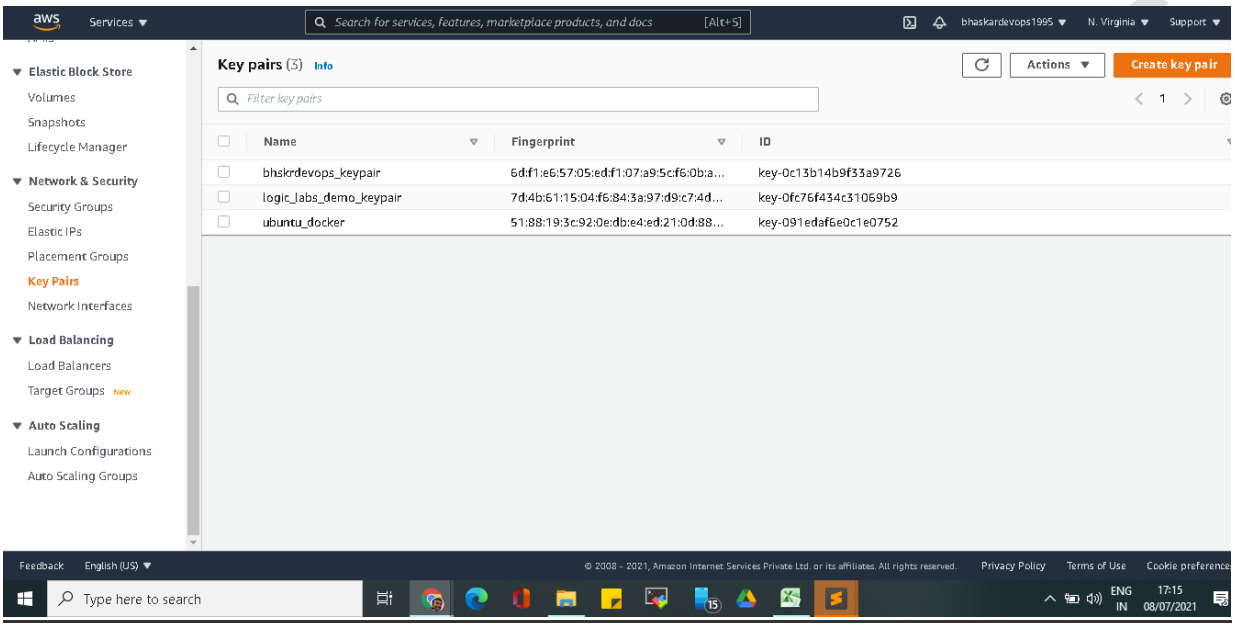
## Tools used:

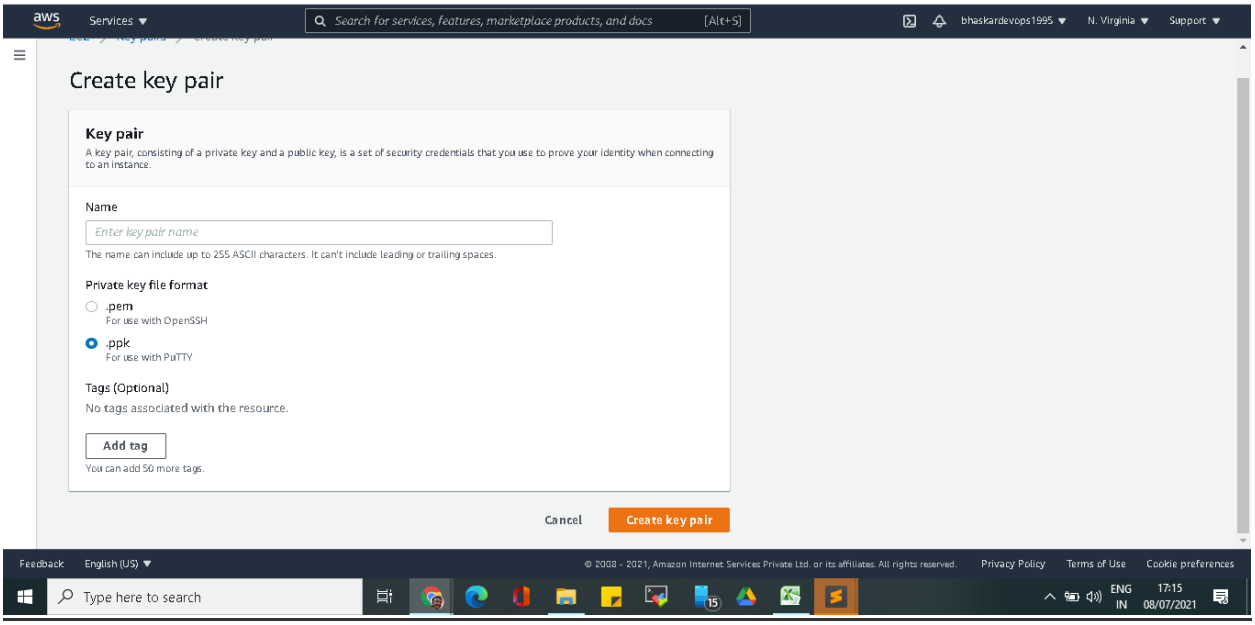
| | | | | |
|---|---|---|---|---|
| Jenkins | Git | Maven | SonarQube | |
| Checkstyle | AWS EC2 | Nexus3 | | |

# Stage -1

## Key pair setup

Login to the AWS management console → EC2 service→ Keypair and Create a new keypair for the purpose of creating EC2 instances

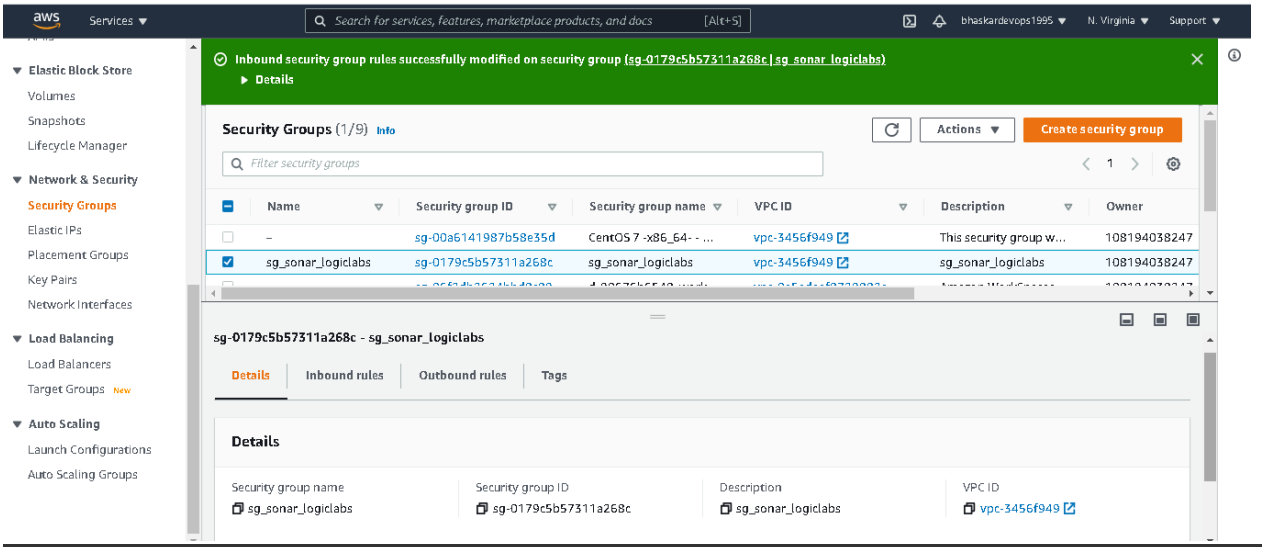


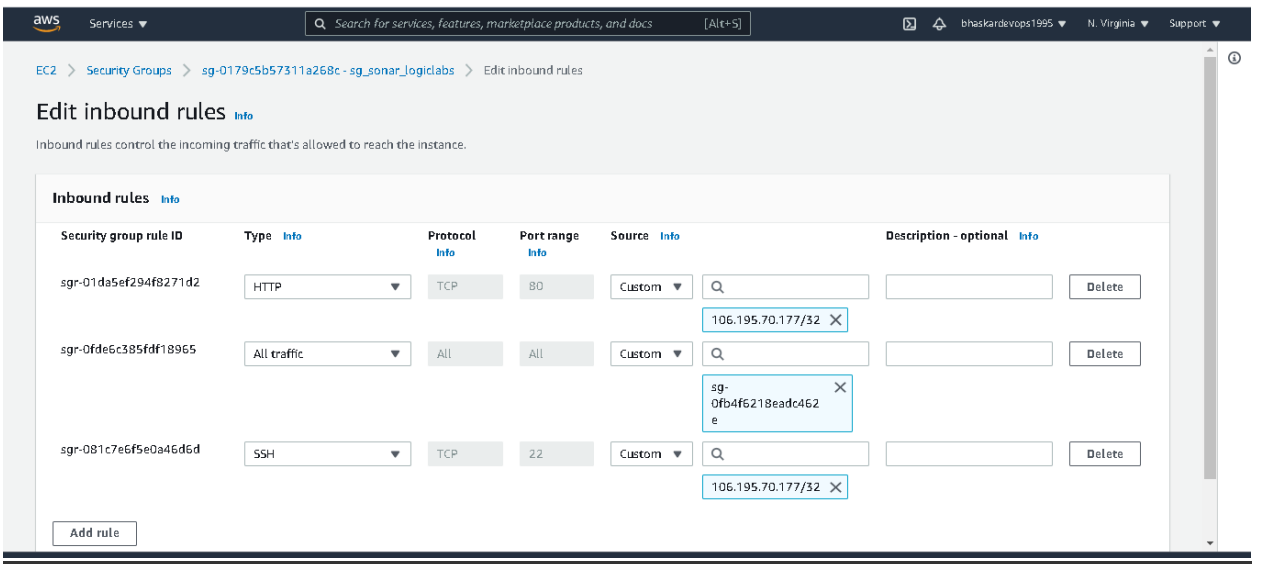



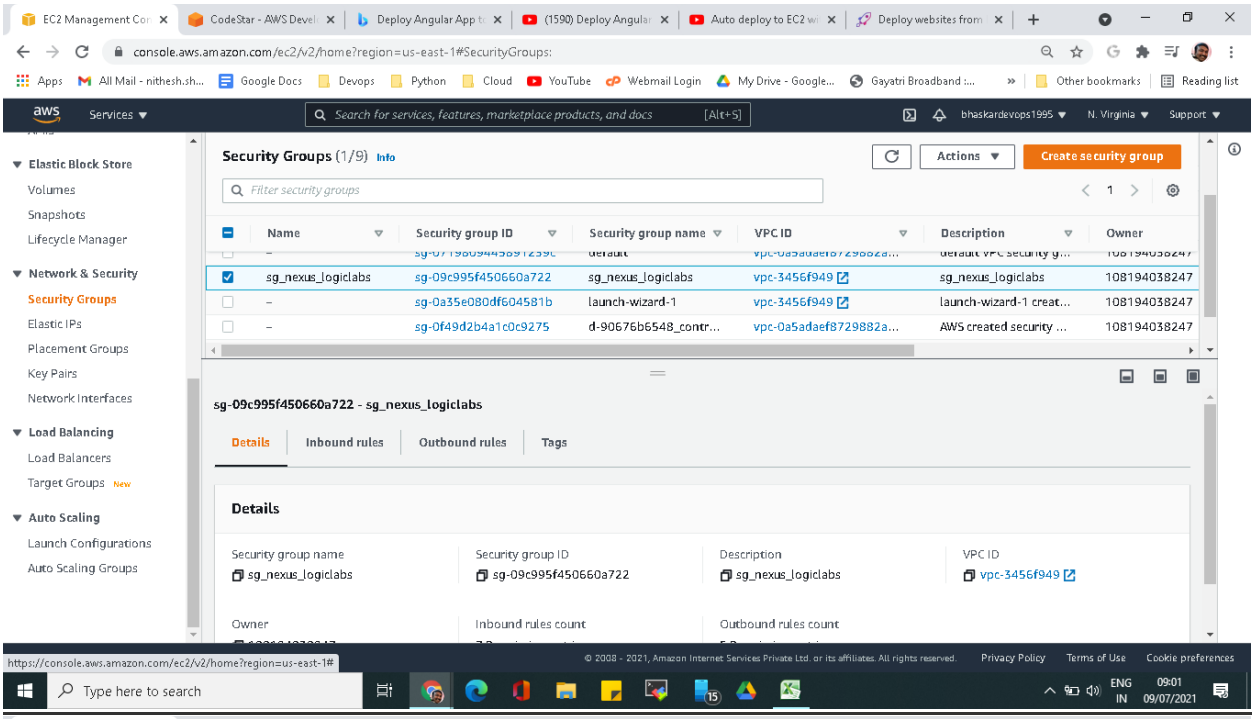
## Security Groups setup

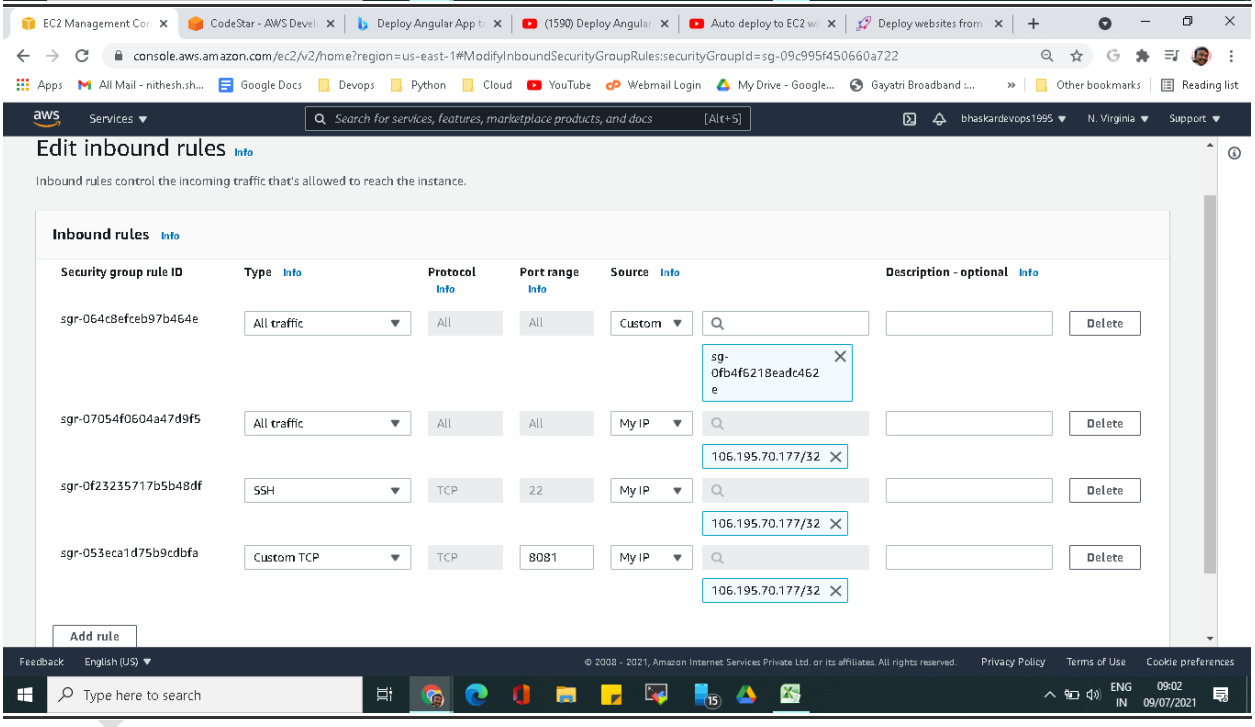
1. Login to AWS  console-> Ec2-> Security Groups
2. Create three Security Groups (S.Gs) one for each- Jenkins, Sonar and Nexus
3. Edit inbound rules for each security group as per the screenshot below and leave outbound as it is.
4. If unclear  about inbound rules, set “Allow all” for the practice purpose.

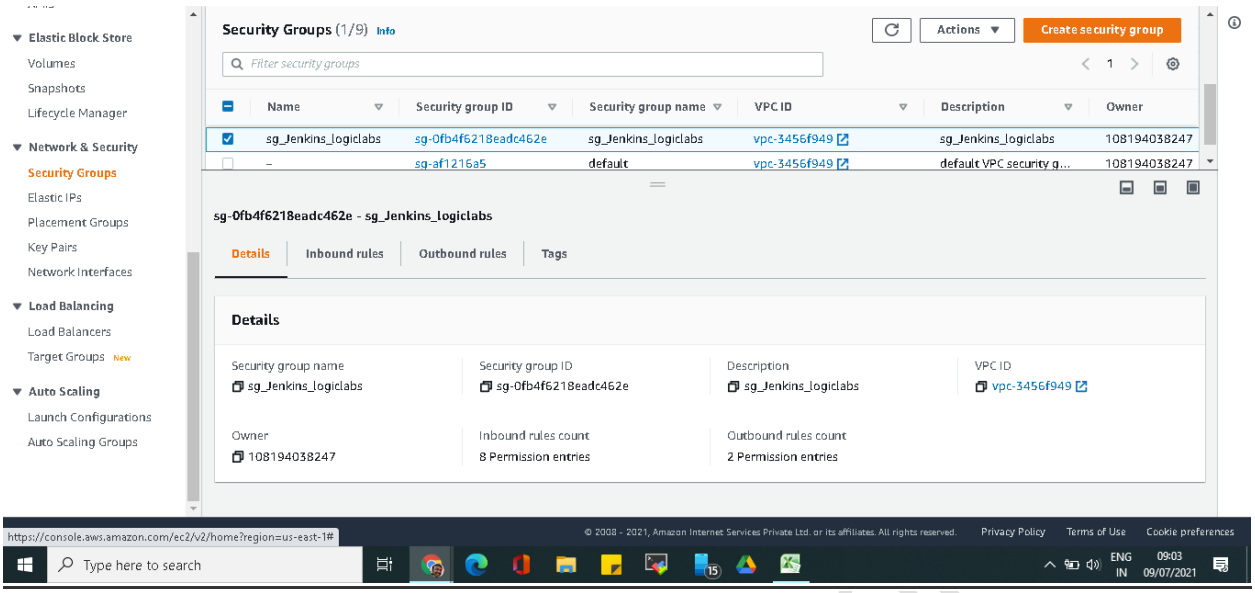
### Creating  security groups

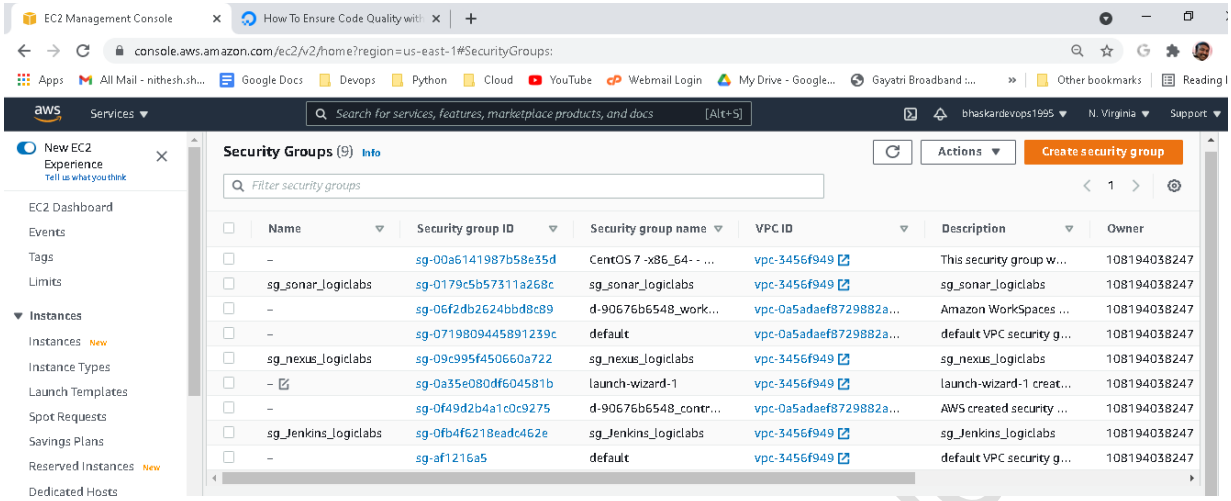


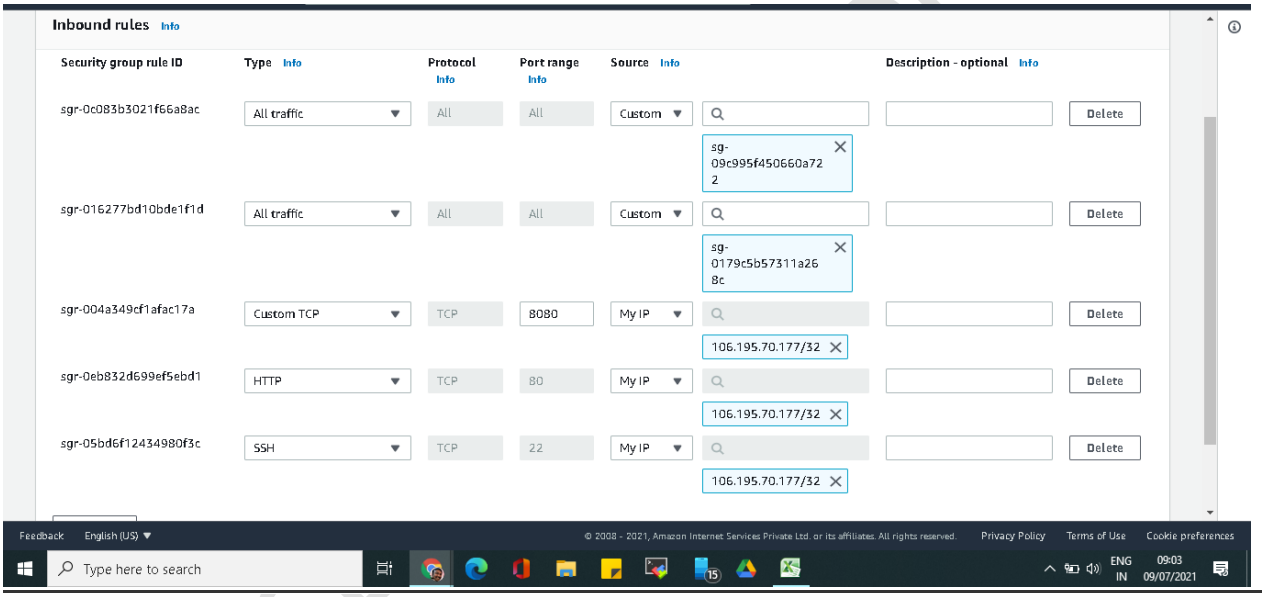




Security Groups (1/9) Info
Actions
Create security group
Filter security groups
Name
Security group ID
Security group name
VPC ID
Description
Owner
sg_nexus_logiclabs
sg-09c995f450660a722
launch-wizard-1
sg-0a35e080df604581b
sg-0f49d2b4a1c0c9275
sg-09c995f450660a722 - sg_nexus_logiclabs
Details
Inbound rules
Outbound rules
Tags
Security group name
Security group ID
Description
VPC ID
Owner
Inbound rules count
Outbound rules count


Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-064c8efceb97b464e
All traffic
Custom
sg-0fb4f6218eadc462e
sgr-07054f0604a47d9f5
My IP
106.195.70.177/32
sgr-0f23235717b5b48df
SSH
TCP
22
sgr-053eca1d75b9cdbfa
Custom TCP
8081
Delete
Add rule






## Server setup

We need to create 3 servers for Jenkins, Sonar and Nexus3.

Step1: clone source code and user data from repository

https://github.com/gnsharma530/Logiclabs-cidemo.git

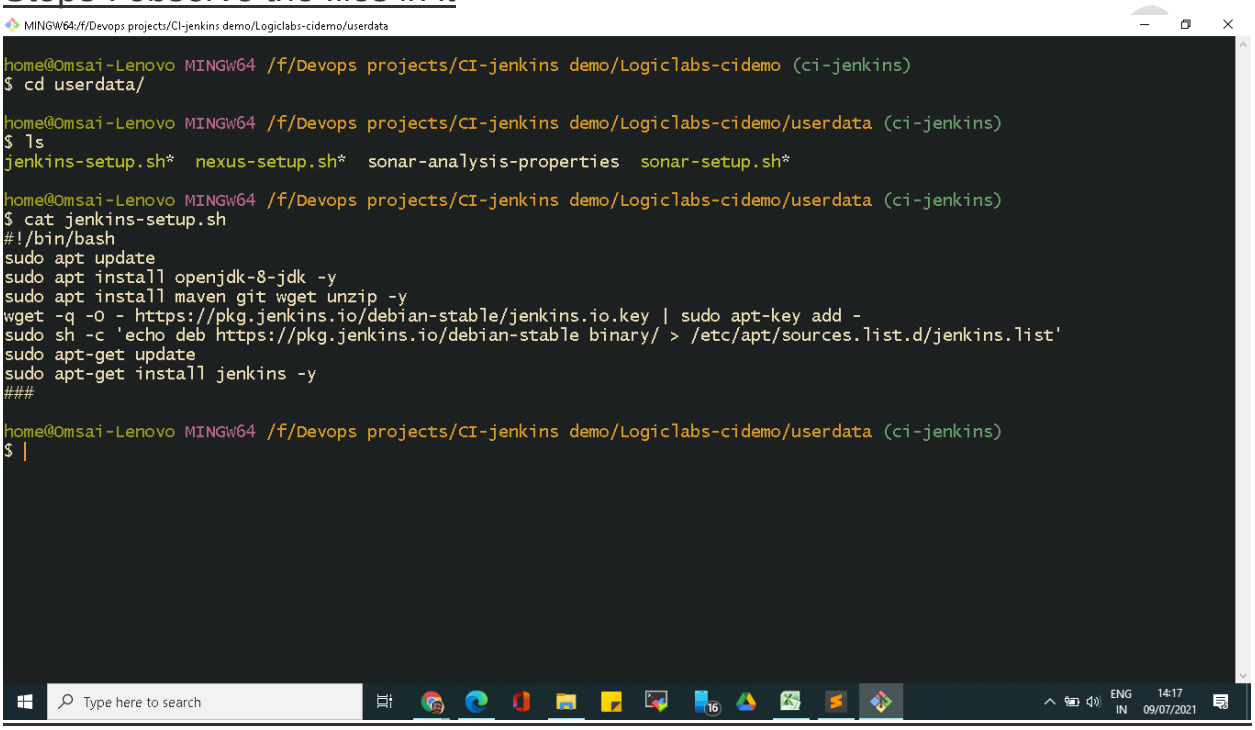
Step2: checkout to ci-jenkins branch and open userdata folder:

Commands to checkout branch:

*git checkout ci-jenkins*

*cd  userdata*

Step3 : observe the files in it



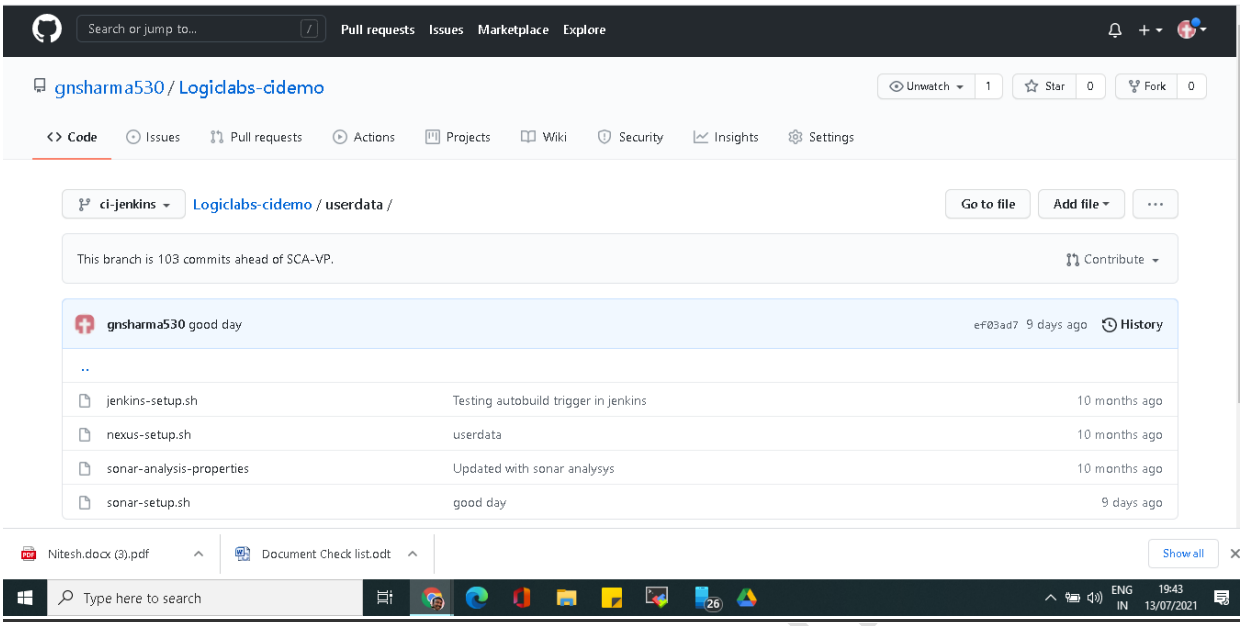

step4 : open the AWS console to create the server ec2 instances

AWS console→ ec2→ create instance

**Choice of Instance:**
**Jenkins:t2.small**
**SonarQube:t2.small**
**Nexus: t2.medium**

**-Select the relevant security groups**
**-paste the proper user data from the user data folder of the repository.**

Clone the repository to the user data:
https://github.com/gnsharma530/Logiclabs-cidemo.git

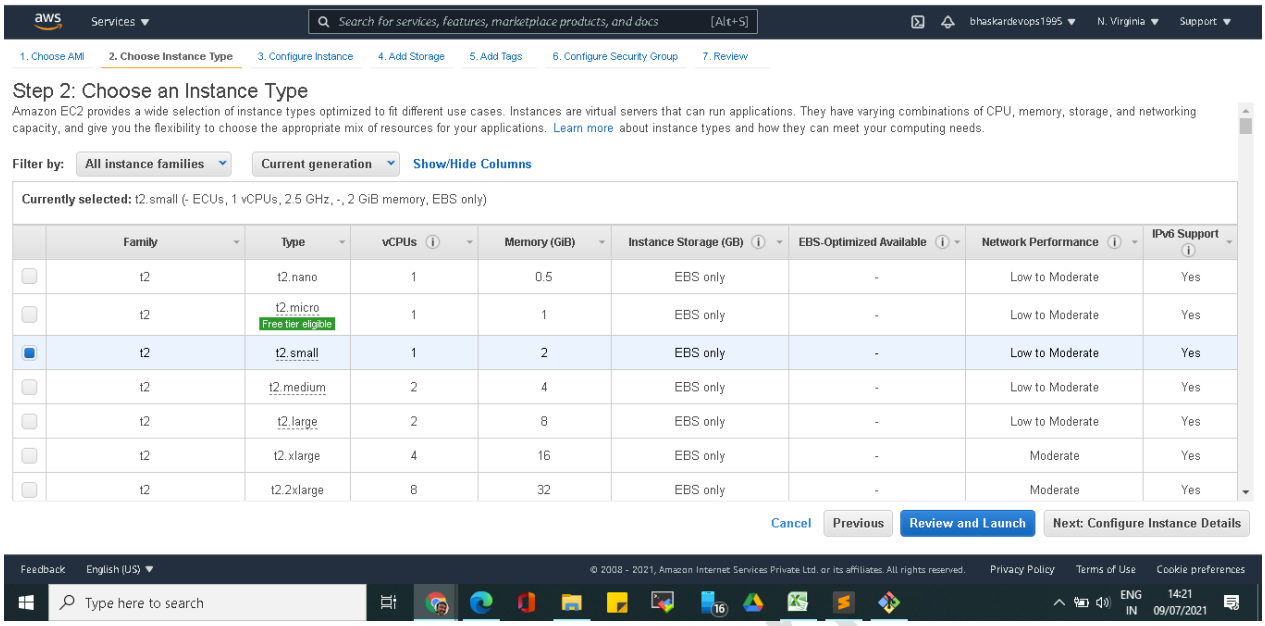



Step 4.1:

**Jenkins server creation** : OS→ UBUNTU

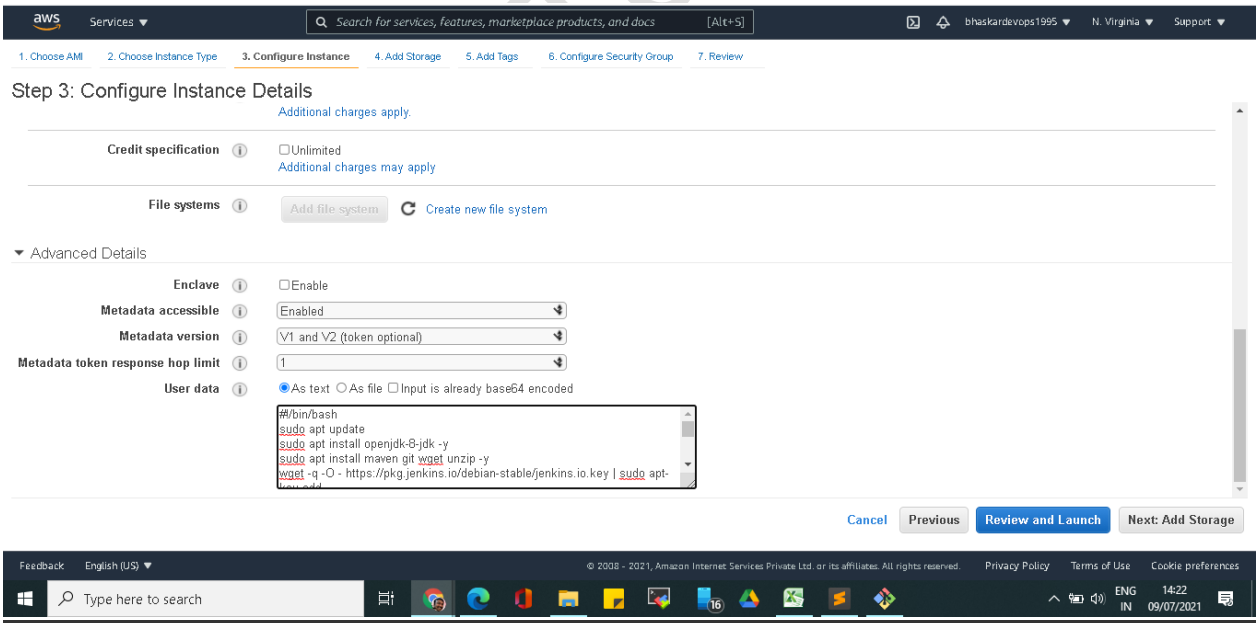
Instance type → t2 small/medium

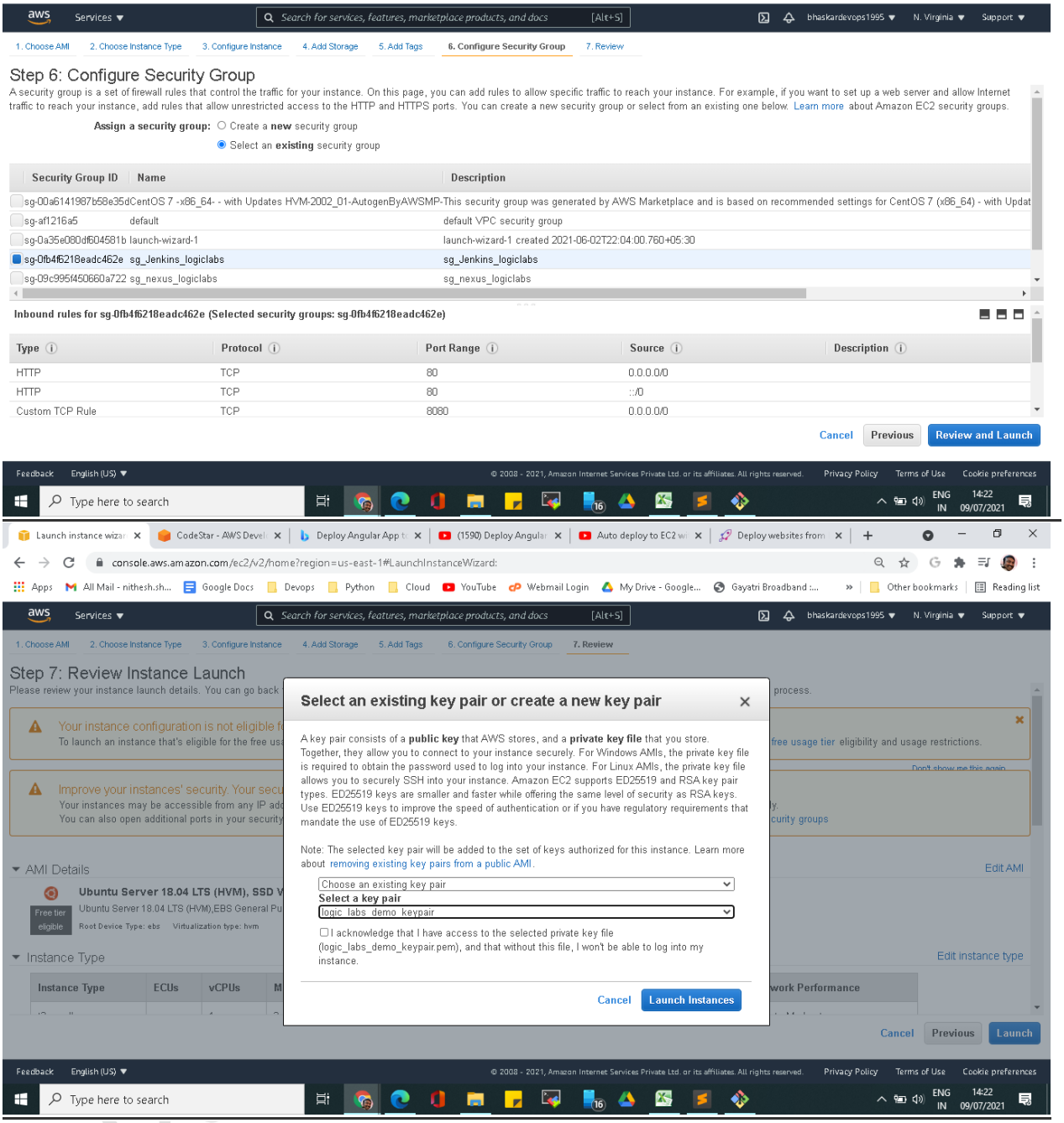
** Avoid t2 micro as it might not handle the load smoothly




Copy user data from the cloned repo and paste in the user data field. Select the relevant security group

https://github.com/gnsharma530/Logiclabs-cidemo/tree/ci-jenkins/userdata




Services
Search for services, features, marketplace products, and docs [Alt+S]
bhaskardevops1995
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group: Create a new security group
Select an existing security group
Security Group ID
Name
Description
sg-00a6141987b58e35d CentOS 7 -x86_64- - with Updates HVM-2002_01-AutogenByAWSMP- This security group was generated by AWS Marketplace and is based on recommended settings for CentOS 7 (x86_64) - with Updat
sg-af1216a5 default default VPC security group
sg-0a35e080df604581b launch-wizard-1 launch-wizard-1 created 2021-06-02T22:04:00.760+05:30
sg-0fb4f6218eadc462e sg_Jenkins_logiclabs sg_Jenkins_logiclabs
sg-09c995f450660a722 sg_nexus_logiclabs sg_nexus_logiclabs
Inbound rules for sg-0fb4f6218eadc462e (Selected security groups: sg-0fb4f6218eadc462e)
Type
Protocol
Port Range
Source
Description
HTTP TCP 80 0.0.0.0/0
HTTP TCP 80 ::/0
Custom TCP Rule TCP 8080 0.0.0.0/0
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
ENG
IN
14:22
09/07/2021

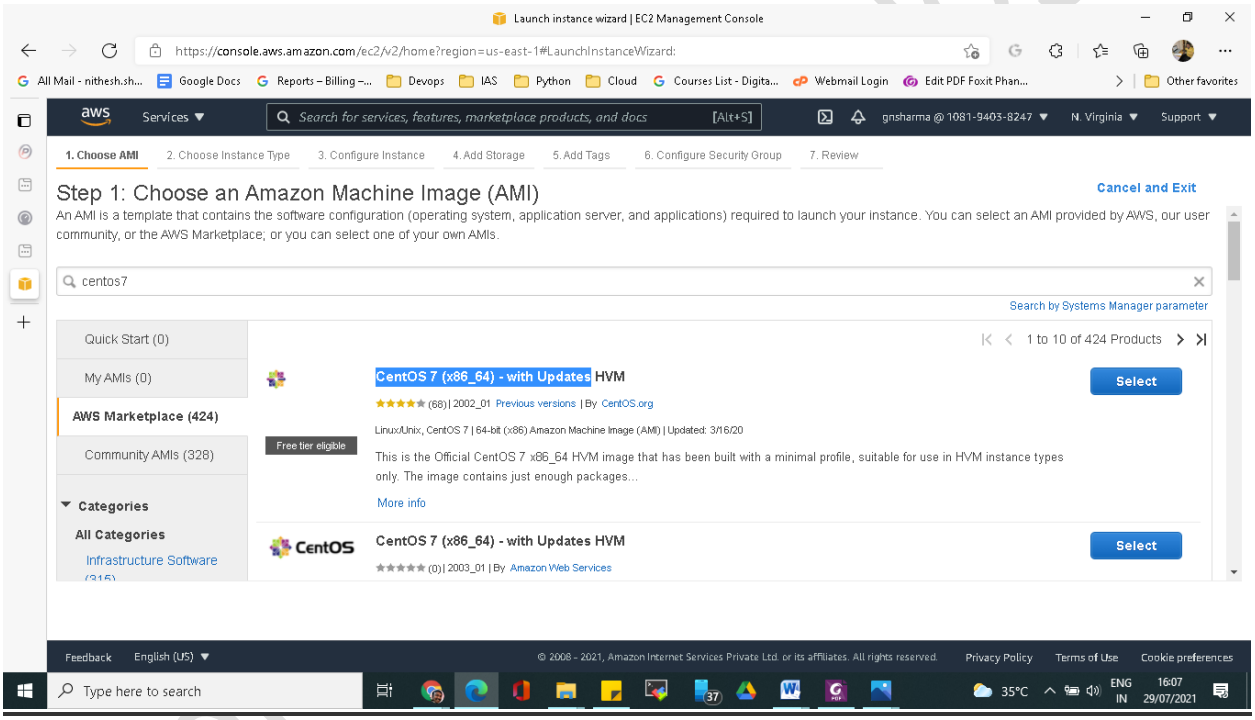

console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Step 7: Review Instance Launch
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types. ED25519 keys are smaller and faster while offering the same level of security as RSA keys. Use ED25519 keys to improve the speed of authentication or if you have regulatory requirements that mandate the use of ED25519 keys.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
logic_labs_demo_keypair
I acknowledge that I have access to the selected private key file (logic_labs_demo_keypair.pem), and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances
AMI Details
Edit AMI
Instance Type
Edit instance type
Cancel
Previous
Launch

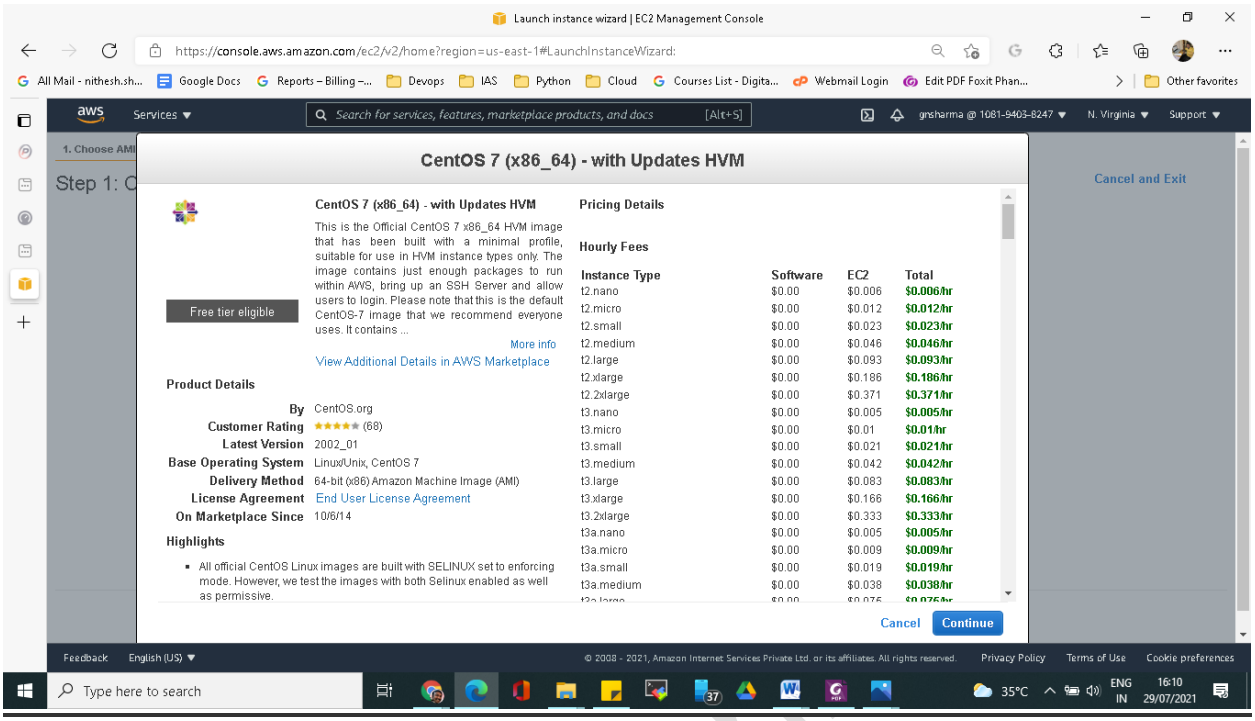
## Step 5: Repeat the same steps for the below servers

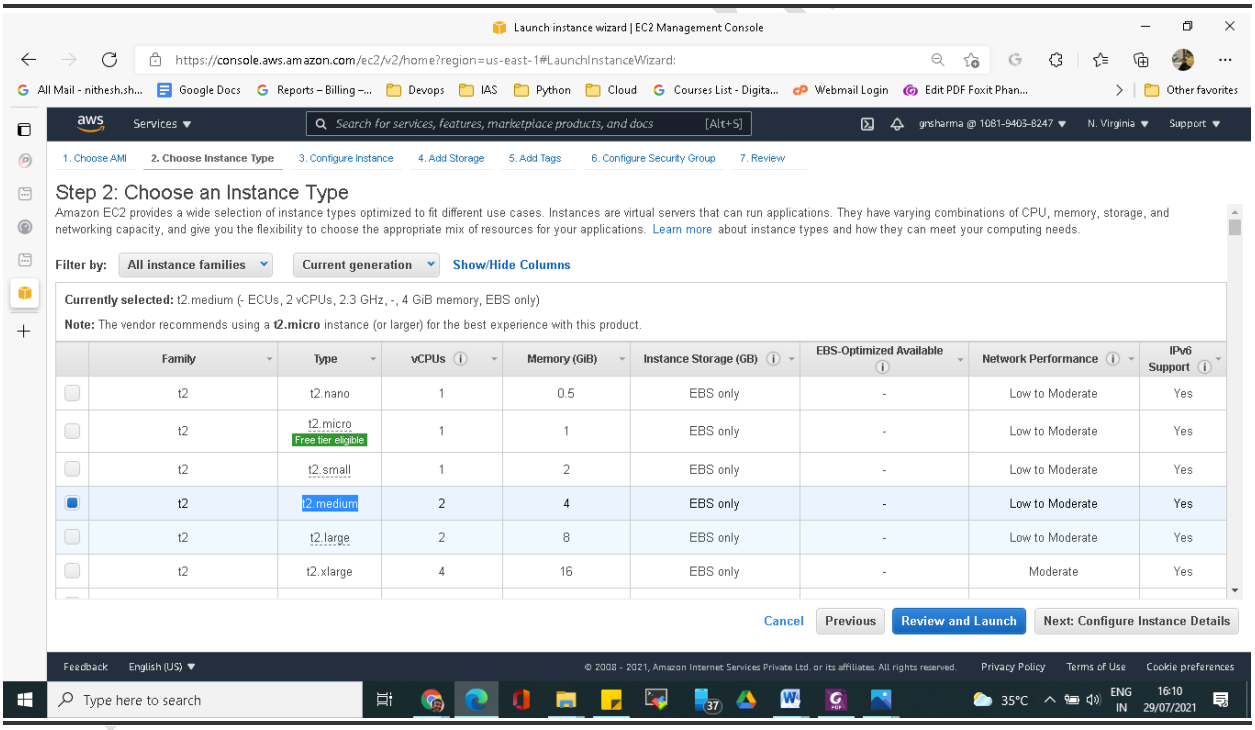
## Sonatype Nexus3 server:

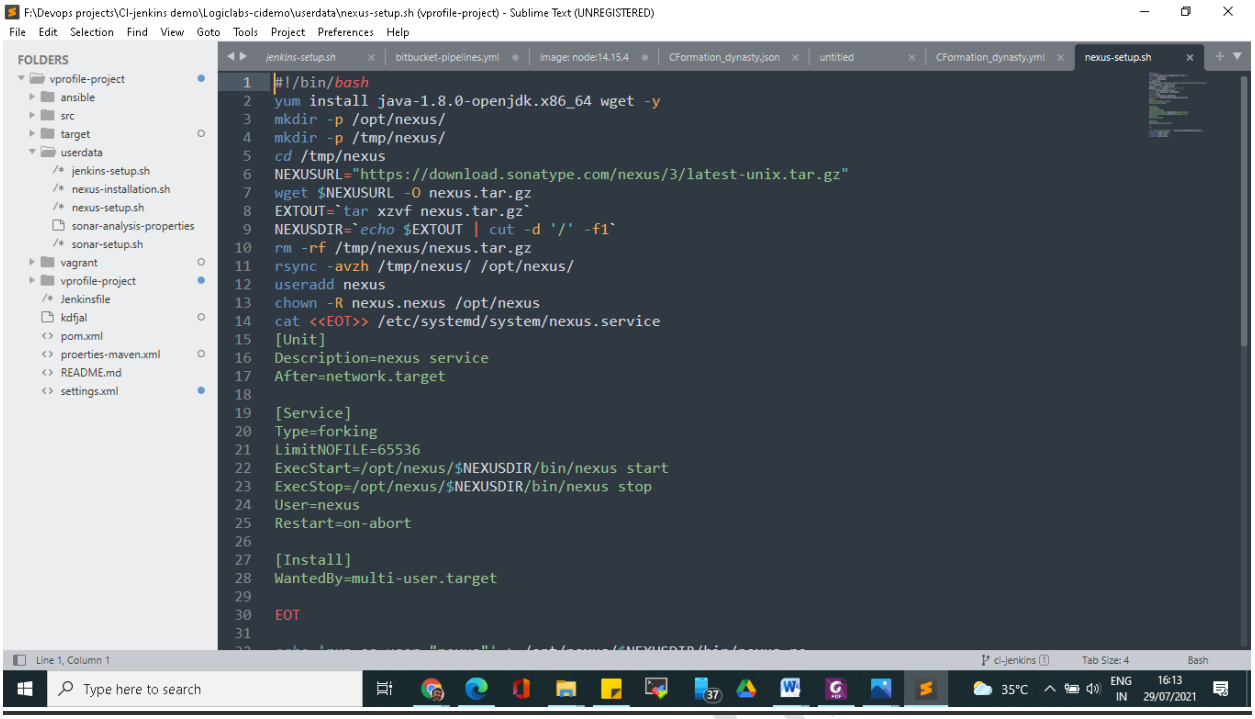
OS: Centos7 & Instance type: t2 medium

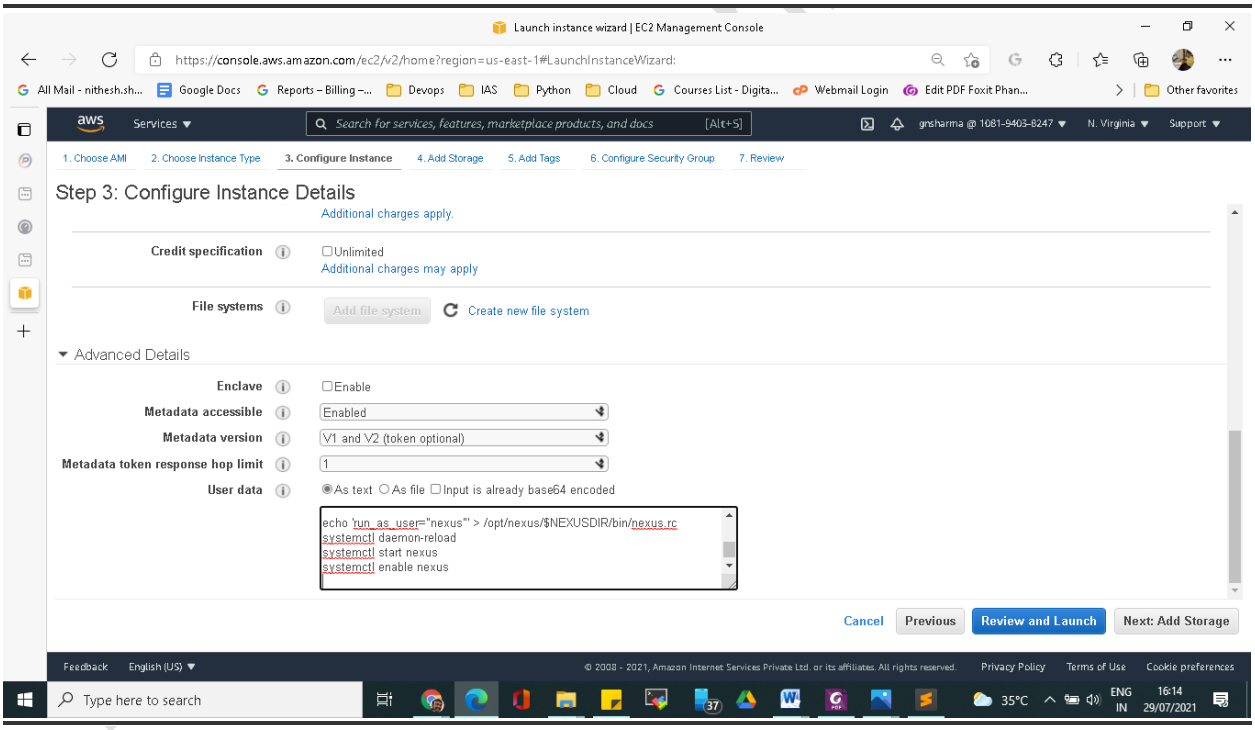
## NEXUS SERVER SETUP

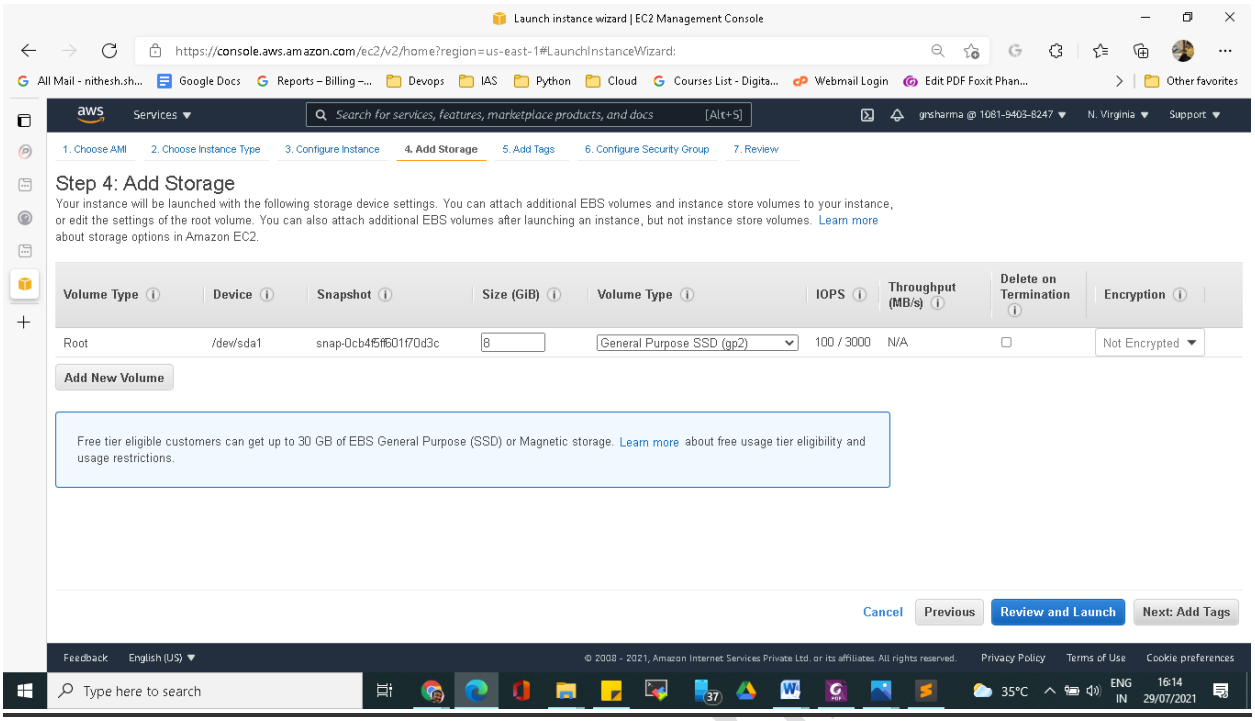


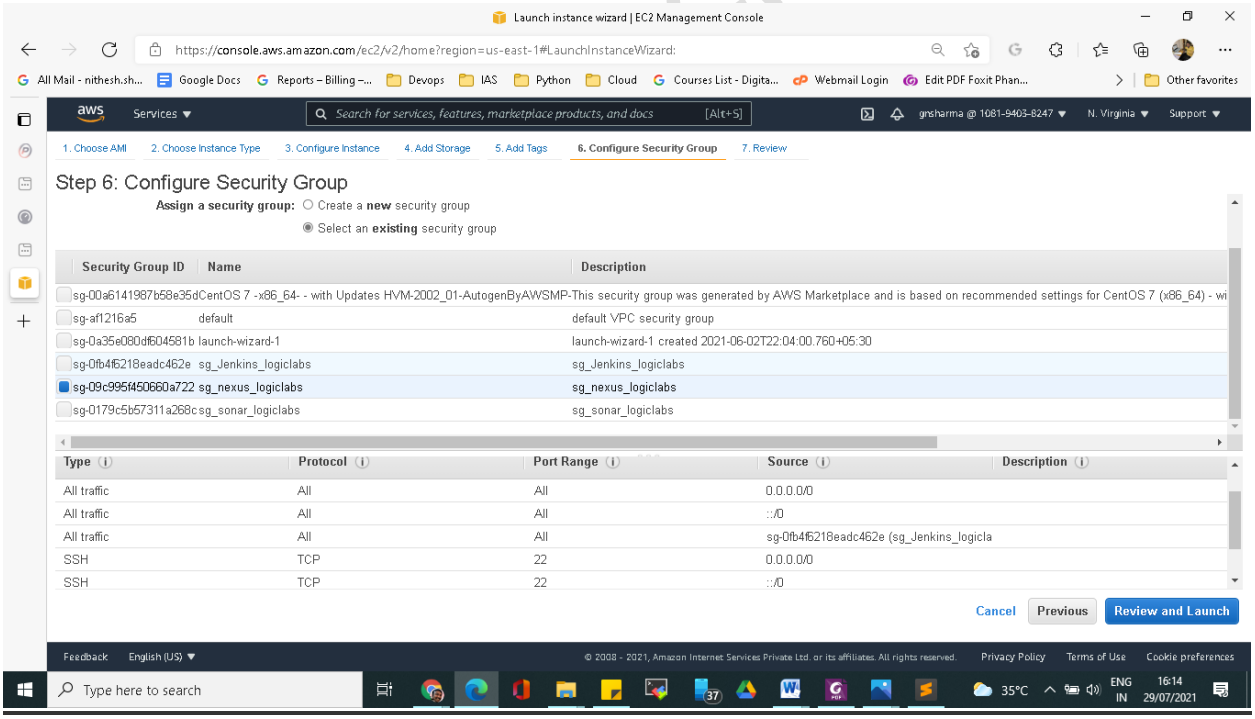

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
Step 1: C
Cancel and Exit
CentOS 7 (x86_64) - with Updates HVM
CentOS 7 (x86_64) - with Updates HVM
This is the Official CentOS 7 x86_64 HVM image that has been built with a minimal profile, suitable for use in HVM instance types only. The image contains just enough packages to run within AWS, bring up an SSH Server and allow users to login. Please note that this is the default CentOS-7 image that we recommend everyone uses. It contains ...
More info
View Additional Details in AWS Marketplace
Free tier eligible
Product Details
By CentOS.org
Customer Rating (68)
Latest Version 2002_01
Base Operating System Linux/Unix, CentOS 7
Delivery Method 64-bit (x86) Amazon Machine Image (AMI)
License Agreement End User License Agreement
On Marketplace Since 10/6/14
Highlights
All official CentOS Linux images are built with SELINUX set to enforcing mode. However, we test the images with both Selinux enabled as well as permissive.
Pricing Details
Hourly Fees
Instance Type Software EC2 Total
t2.nano $0.00 $0.006 $0.006/hr
t2.micro $0.00 $0.012 $0.012/hr
t2.small $0.00 $0.023 $0.023/hr
t2.medium $0.00 $0.046 $0.046/hr
t2.large $0.00 $0.093 $0.093/hr
t2.xlarge $0.00 $0.186 $0.186/hr
t2.2xlarge $0.00 $0.371 $0.371/hr
t3.nano $0.00 $0.005 $0.005/hr
t3.micro $0.00 $0.01 $0.01/hr
t3.small $0.00 $0.021 $0.021/hr
t3.medium $0.00 $0.042 $0.042/hr
t3.large $0.00 $0.083 $0.083/hr
t3.xlarge $0.00 $0.166 $0.166/hr
t3.2xlarge $0.00 $0.333 $0.333/hr
t3a.nano $0.00 $0.005 $0.005/hr
t3a.micro $0.00 $0.009 $0.009/hr
t3a.small $0.00 $0.019 $0.019/hr
t3a.medium $0.00 $0.038 $0.038/hr
Cancel
Continue
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG IN
16:10 29/07/2021

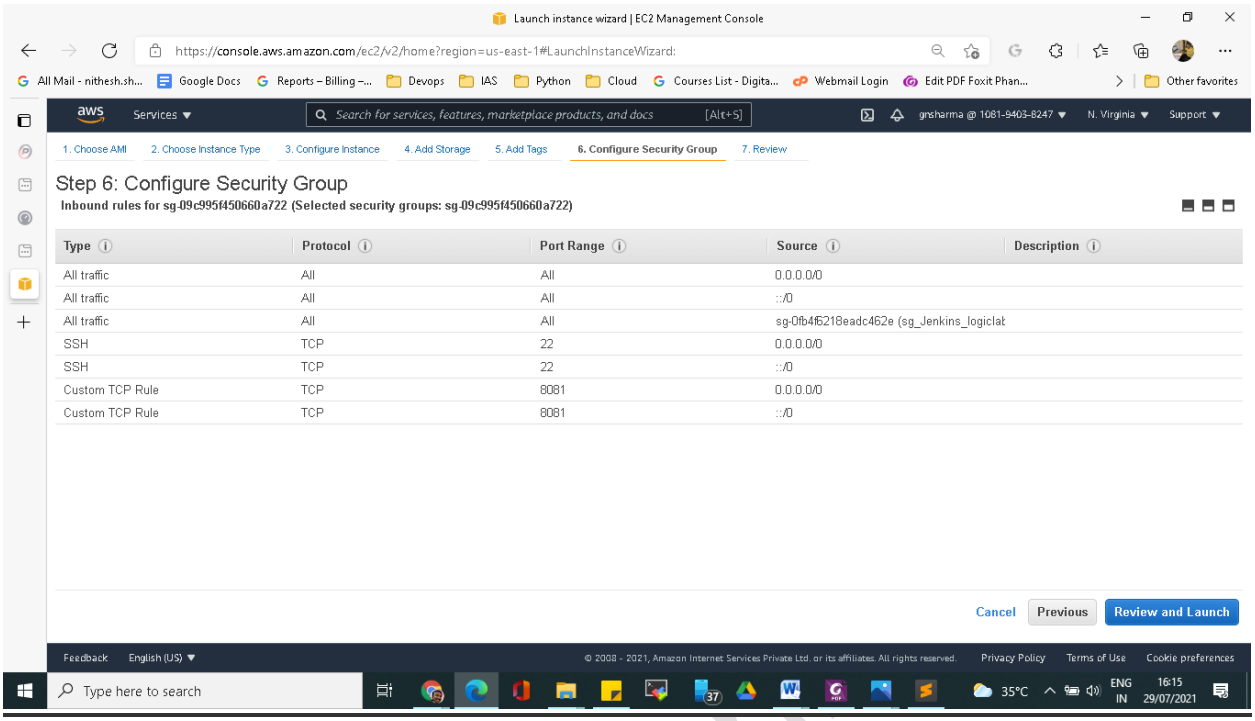

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by: All instance families Current generation Show/Hide Columns
Currently selected: t2.medium (- ECUs, 2 vCPUs, 2.3 GHz, -, 4 GiB memory, EBS only)
Note: The vendor recommends using a t2.micro instance (or larger) for the best experience with this product.
Family Type vCPUs Memory (GiB) Instance Storage (GB) EBS-Optimized Available Network Performance IPv6 Support
t2 t2.nano 1 0.5 EBS only - Low to Moderate Yes
t2 t2.micro Free tier eligible 1 1 EBS only - Low to Moderate Yes
t2 t2.small 1 2 EBS only - Low to Moderate Yes
t2 t2.medium 2 4 EBS only - Low to Moderate Yes
t2 t2.large 2 8 EBS only - Low to Moderate Yes
t2 t2.xlarge 4 16 EBS only - Moderate Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG IN
16:10 29/07/2021

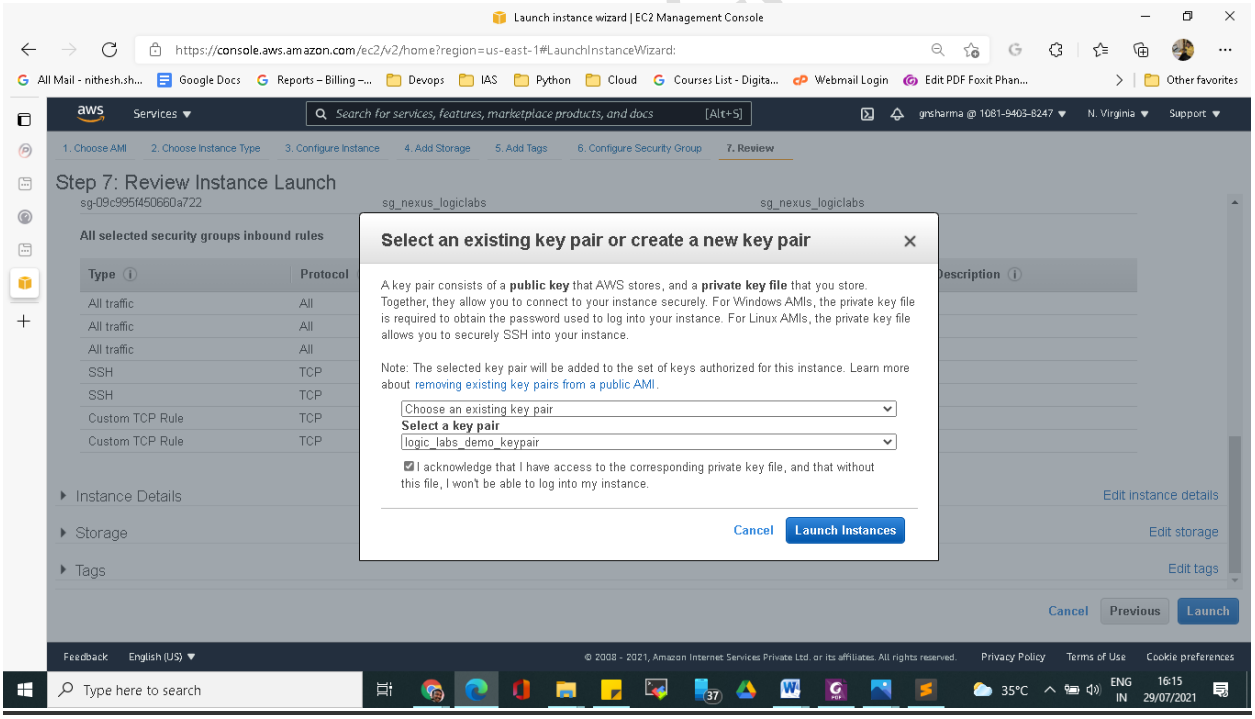

F:\Devops projects\CI-jenkins demo\Logiclabs-cidemo\userdata\nexus-setup.sh (vprofile-project) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
vprofile-project
ansible
src
target
userdata
jenkins-setup.sh
nexus-installation.sh
nexus-setup.sh
sonar-analysis-properties
sonar-setup.sh
vagrant
vprofile-project
Jenkinsfile
kdfjal
pom.xml
proerties-maven.xml
README.md
settings.xml
jenkins-setup.sh
bitbucket-pipelines.yml
image: node:14.15.4
CFormation_dynasty.json
untitled
CFormation_dynasty.yml
nexus-setup.sh
#!/bin/bash
yum install java-1.8.0-openjdk.x86_64 wget -y
mkdir -p /opt/nexus/
mkdir -p /tmp/nexus/
cd /tmp/nexus
NEXUSURL="https://download.sonatype.com/nexus/3/latest-unix.tar.gz"
wget $NEXUSURL -O nexus.tar.gz
EXTOUT=`tar xzvf nexus.tar.gz`
NEXUSDIR=`echo $EXTOUT | cut -d '/' -f1`
rm -rf /tmp/nexus/nexus.tar.gz
rsync -avzh /tmp/nexus/ /opt/nexus/
useradd nexus
chown -R nexus.nexus /opt/nexus
cat <<EOT>> /etc/systemd/system/nexus.service
[Unit]
Description=nexus service
After=network.target
[Service]
Type=forking
LimitNOFILE=65536
ExecStart=/opt/nexus/$NEXUSDIR/bin/nexus start
ExecStop=/opt/nexus/$NEXUSDIR/bin/nexus stop
User=nexus
Restart=on-abort
[Install]
WantedBy=multi-user.target
EOT
Line 1, Column 1
Tab Size: 4
Bash
Type here to search
35°C
ENG IN
16:13
29/07/2021


Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Additional charges apply.
Credit specification
Unlimited
Additional charges may apply
File systems
Add file system
Create new file system
Advanced Details
Enclave
Enable
Metadata accessible
Enabled
Metadata version
V1 and V2 (token optional)
Metadata token response hop limit
1
User data
As text
As file
Input is already base64 encoded
echo 'run_as_user="nexus"' > /opt/nexus/$NEXUSDIR/bin/nexus.rc
systemctl daemon-reload
systemctl start nexus
systemctl enable nexus
Cancel
Previous
Review and Launch
Next: Add Storage
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG IN
16:14
29/07/2021


Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/sda1
snap-0cb4f5ff601f70d3c
8
General Purpose SSD (gp2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG
IN
16:14
29/07/2021

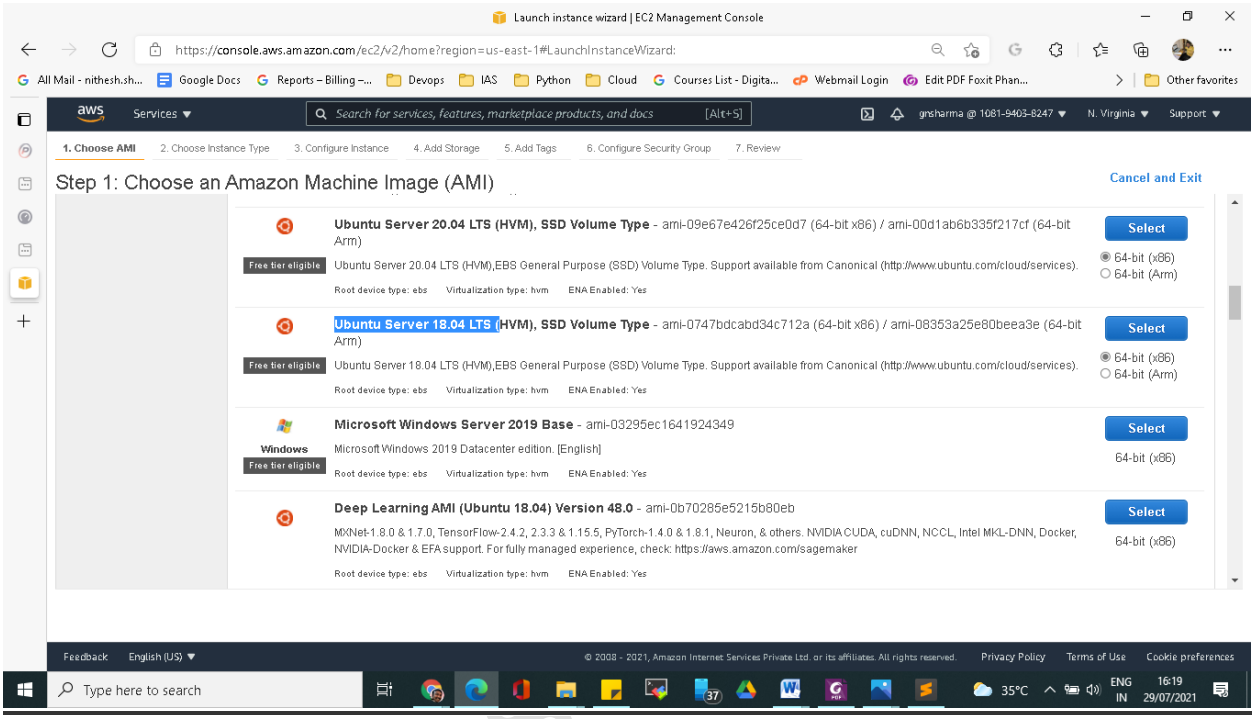

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
Assign a security group: Create a new security group
Select an existing security group
Security Group ID
Name
Description
sg-00a6141987b58e35d CentOS 7 -x86_64- - with Updates HVM-2002_01-AutogenByAWSMP- This security group was generated by AWS Marketplace and is based on recommended settings for CentOS 7 (x86_64) - wi
sg-af1216a5 default default VPC security group
sg-0a35e080df604581b launch-wizard-1 launch-wizard-1 created 2021-06-02T22:04:00.760+05:30
sg-0fb4f6218eadc462e sg_Jenkins_logiclabs sg_Jenkins_logiclabs
sg-09c995f450660a722 sg_nexus_logiclabs sg_nexus_logiclabs
sg-0179c5b57311a268c sg_sonar_logiclabs sg_sonar_logiclabs
Type
Protocol
Port Range
Source
Description
All traffic All All 0.0.0.0/0
All traffic All All ::/0
All traffic All All sg-0fb4f6218eadc462e (sg_Jenkins_logicla
SSH TCP 22 0.0.0.0/0
SSH TCP 22 ::/0
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG
IN
16:14
29/07/2021

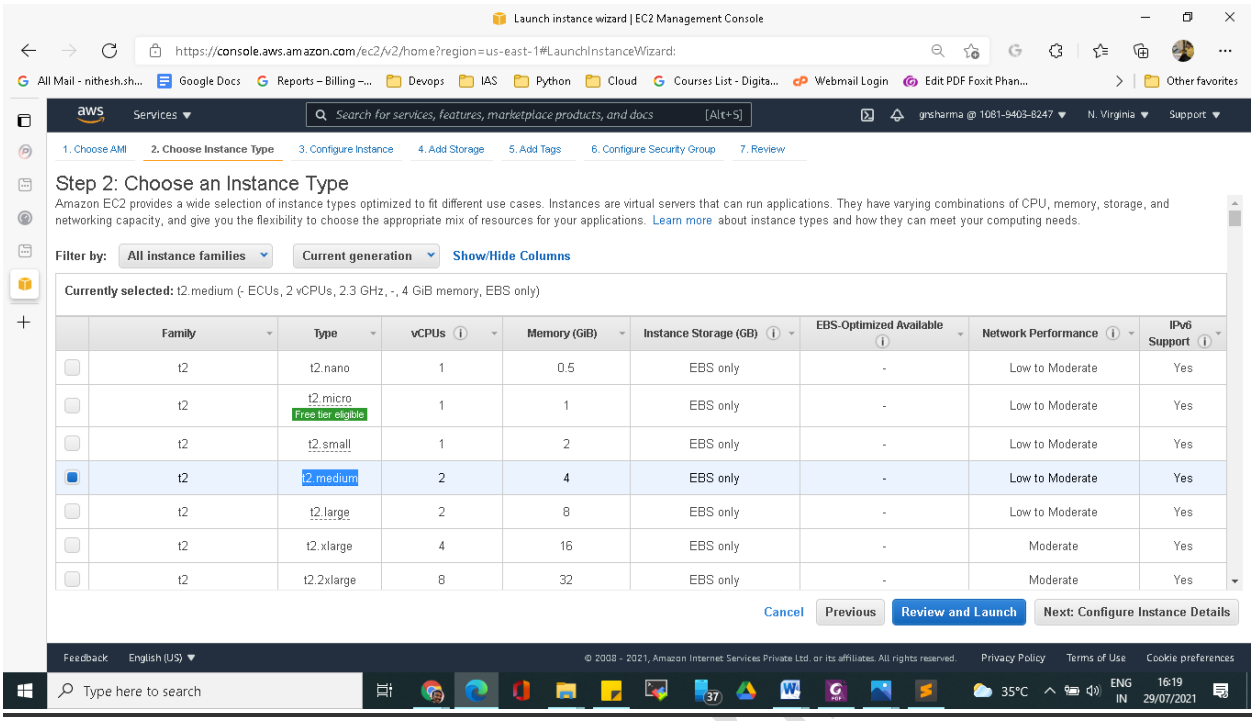

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Step 6: Configure Security Group
Inbound rules for sg-09c995f450660a722 (Selected security groups: sg-09c995f450660a722)
Type | Protocol | Port Range | Source | Description
All traffic | All | All | 0.0.0.0/0
All traffic | All | All | ::/0
All traffic | All | All | sg-0fb4f6218eadc462e (sg_Jenkins_logiclat
SSH | TCP | 22 | 0.0.0.0/0
SSH | TCP | 22 | ::/0
Custom TCP Rule | TCP | 8081 | 0.0.0.0/0
Custom TCP Rule | TCP | 8081 | ::/0
Cancel
Previous
Review and Launch

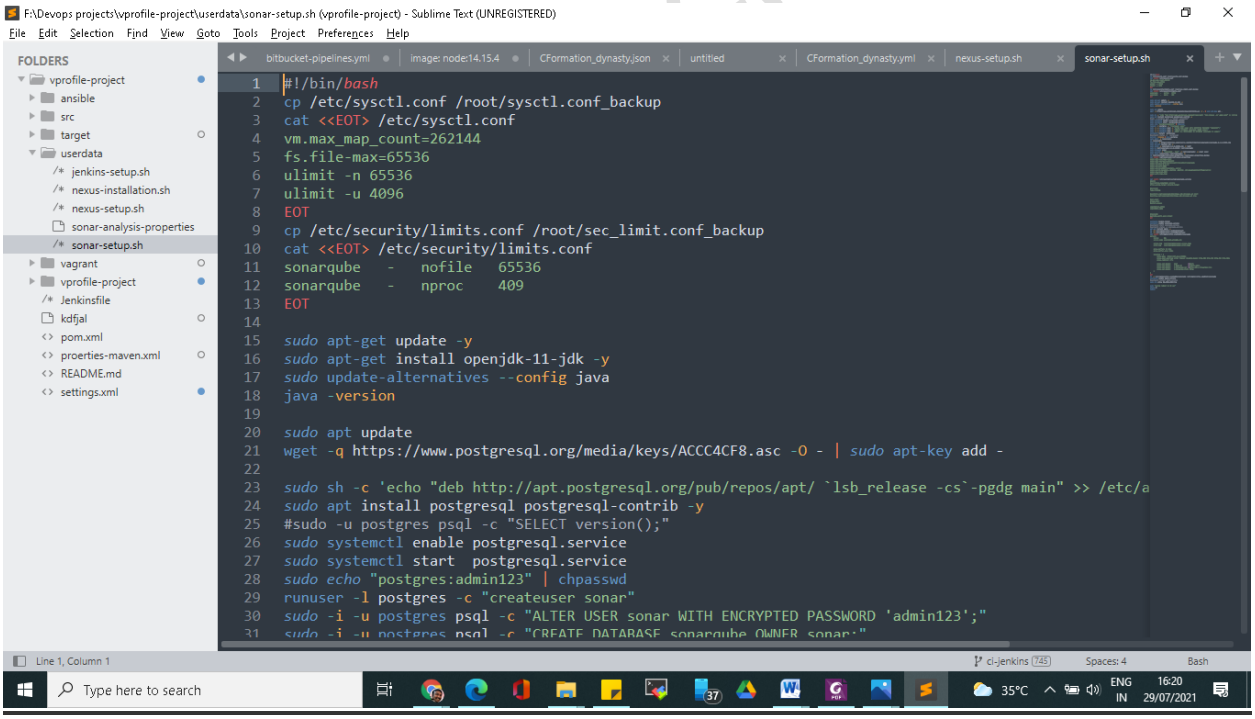

Launch instance wizard | EC2 Management Console
Step 7: Review Instance Launch
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
logic_labs_demo_keypair
I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances
Instance Details
Storage
Tags
Edit instance details
Edit storage
Edit tags
Cancel
Previous
Launch

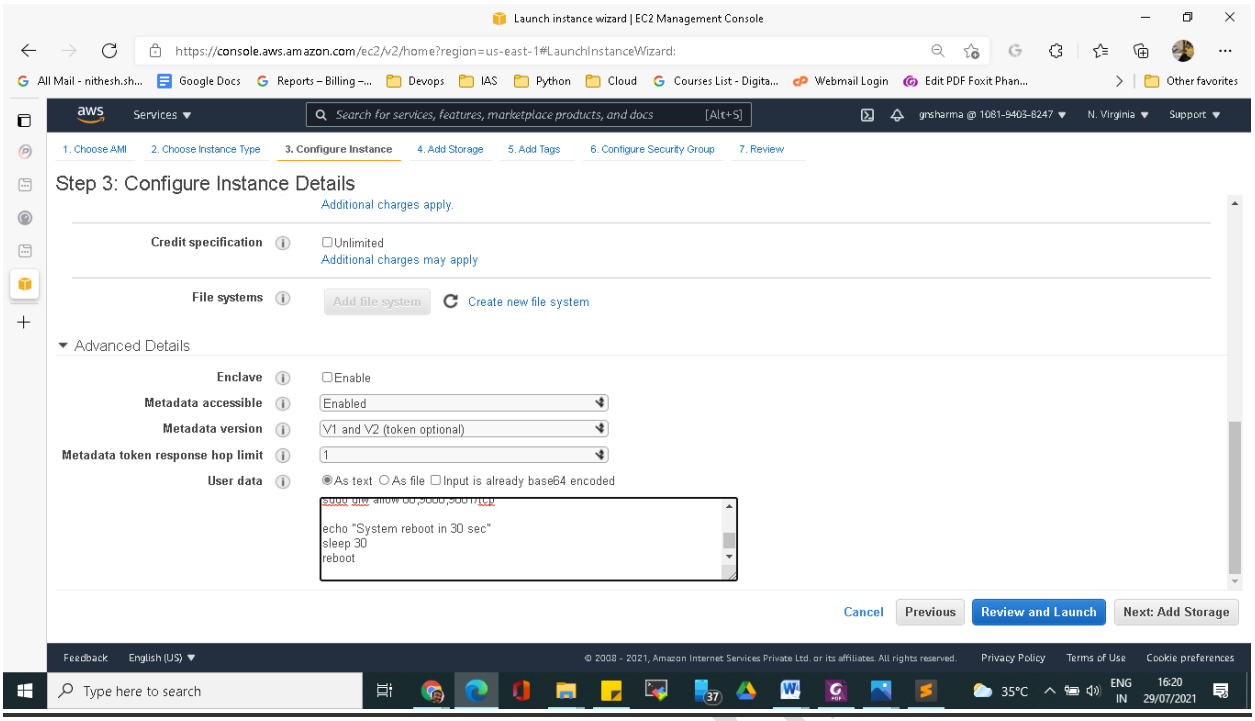
## SONARQUBE SERVER SETUP:

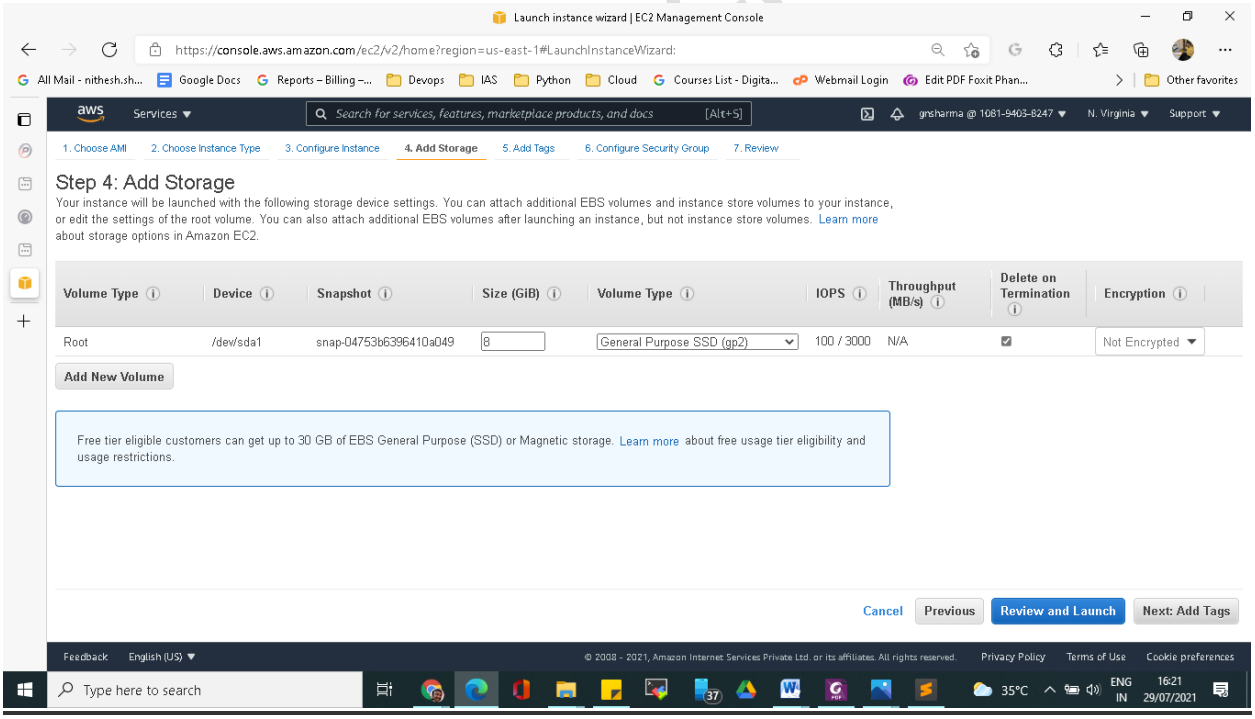
OS: Ubuntu  Instance type: t2 medium

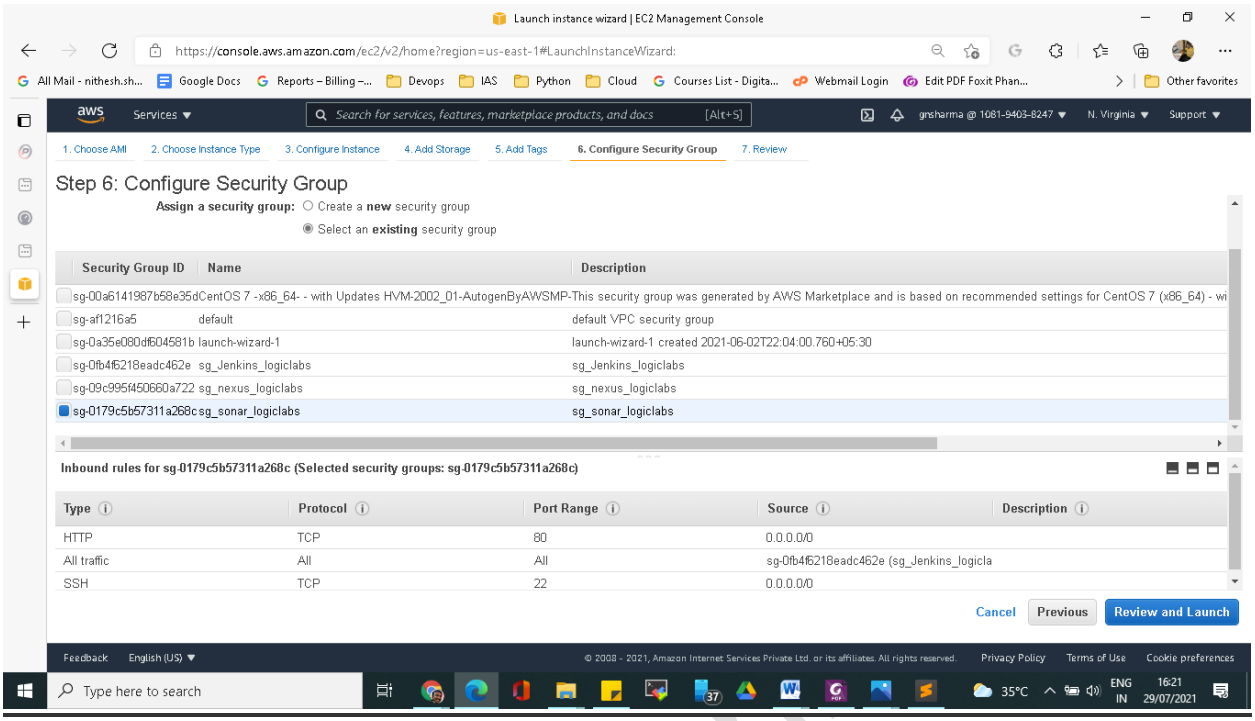


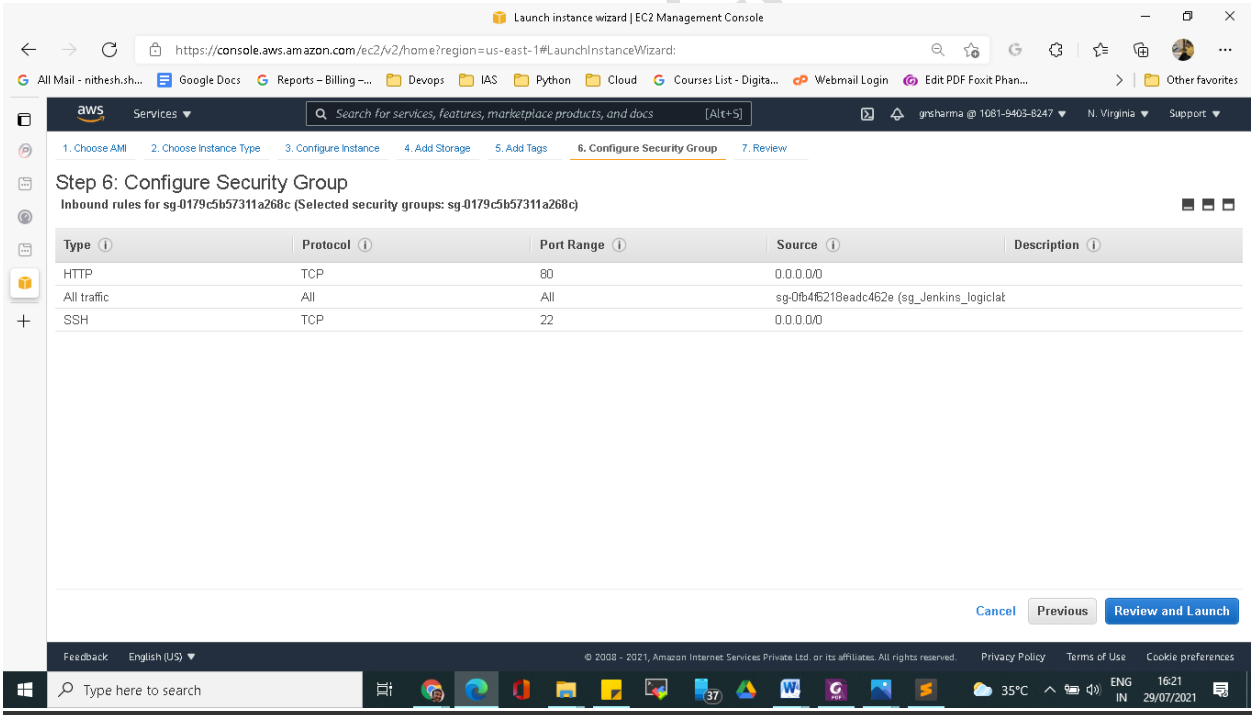

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by: All instance families Current generation Show/Hide Columns
Currently selected: t2.medium (- ECUs, 2 vCPUs, 2.3 GHz, -, 4 GiB memory, EBS only)
Family | Type | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance | IPv6 Support
t2 | t2.nano | 1 | 0.5 | EBS only | - | Low to Moderate | Yes
t2 | t2.micro Free tier eligible | 1 | 1 | EBS only | - | Low to Moderate | Yes
t2 | t2.small | 1 | 2 | EBS only | - | Low to Moderate | Yes
t2 | t2.medium | 2 | 4 | EBS only | - | Low to Moderate | Yes
t2 | t2.large | 2 | 8 | EBS only | - | Low to Moderate | Yes
t2 | t2.xlarge | 4 | 16 | EBS only | - | Moderate | Yes
t2 | t2.2xlarge | 8 | 32 | EBS only | - | Moderate | Yes
Cancel Previous Review and Launch Next: Configure Instance Details
Feedback English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy Terms of Use Cookie preferences
Type here to search
35°C ENG IN 16:19 29/07/2021

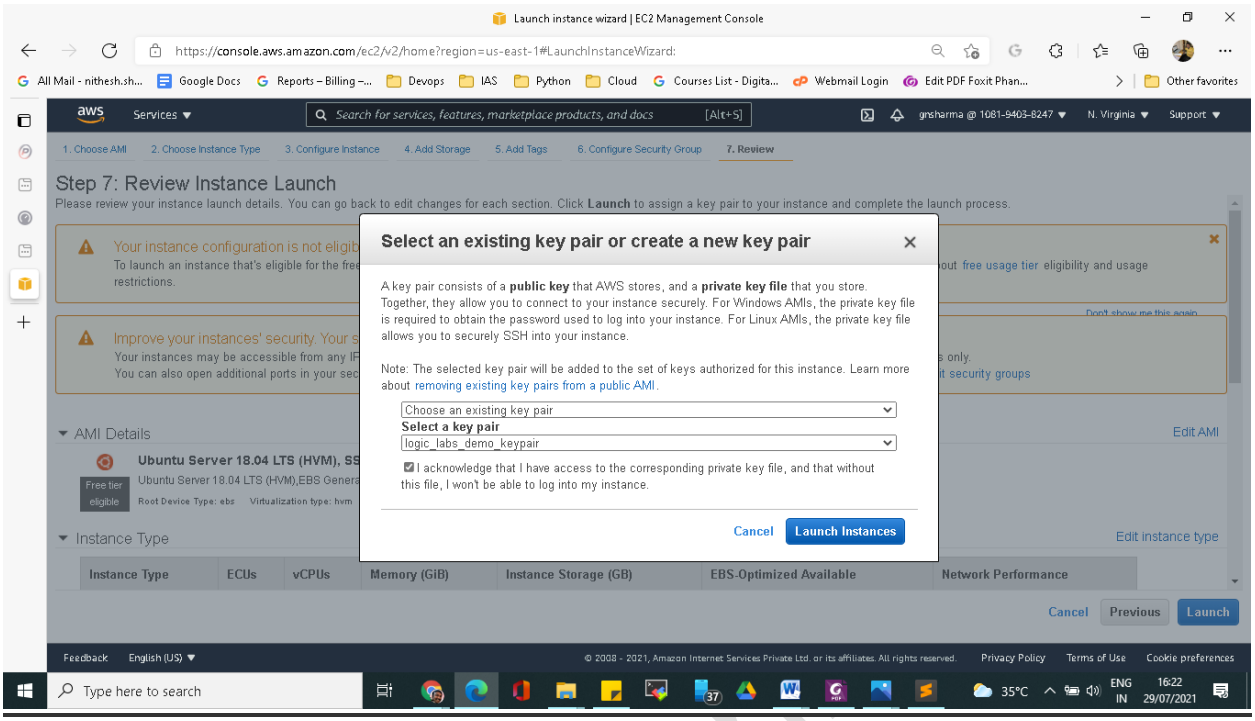

F:\Devops projects\vprofile-project\userdata\sonar-setup.sh (vprofile-project) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
vprofile-project
ansible
src
target
userdata
jenkins-setup.sh
nexus-installation.sh
nexus-setup.sh
sonar-analysis-properties
sonar-setup.sh
vagrant
vprofile-project
Jenkinsfile
kdfjal
pom.xml
proerties-maven.xml
README.md
settings.xml
bitbucket-pipelines.yml
image: node:14.15.4
CFormation_dynasty.json
untitled
CFormation_dynasty.yml
nexus-setup.sh
sonar-setup.sh
#!/bin/bash
cp /etc/sysctl.conf /root/sysctl.conf_backup
cat <<EOT> /etc/sysctl.conf
vm.max_map_count=262144
fs.file-max=65536
ulimit -n 65536
ulimit -u 4096
EOT
cp /etc/security/limits.conf /root/sec_limit.conf_backup
cat <<EOT> /etc/security/limits.conf
sonarqube - nofile 65536
sonarqube - nproc 409
EOT
sudo apt-get update -y
sudo apt-get install openjdk-11-jdk -y
sudo update-alternatives --config java
java -version
sudo apt update
wget -q https://www.postgresql.org/media/keys/ACCC4CF8.asc -O - | sudo apt-key add -
sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt/ `lsb_release -cs`-pgdg main" >> /etc/a
sudo apt install postgresql postgresql-contrib -y
#sudo -u postgres psql -c "SELECT version();"
sudo systemctl enable postgresql.service
sudo systemctl start postgresql.service
sudo echo "postgres:admin123" | chpasswd
runuser -l postgres -c "createuser sonar"
sudo -i -u postgres psql -c "ALTER USER sonar WITH ENCRYPTED PASSWORD 'admin123';"
Line 1, Column 1
Spaces: 4
Bash
Type here to search
35°C ENG IN 16:20 29/07/2021


Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Step 3: Configure Instance Details
Additional charges apply.
Credit specification
Unlimited
Additional charges may apply
File systems
Add file system
Create new file system
Advanced Details
Enclave
Enable
Metadata accessible
Enabled
Metadata version
V1 and V2 (token optional)
Metadata token response hop limit
1
User data
As text
As file
Input is already base64 encoded
echo "System reboot in 30 sec"
sleep 30
reboot
Cancel
Previous
Review and Launch
Next: Add Storage


Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/sda1
snap-04753b6396410a049
8
General Purpose SSD (gp2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags

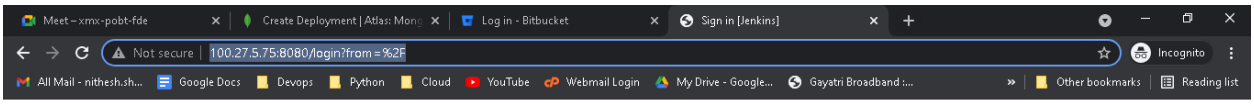

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
Assign a security group: Create a new security group
Select an existing security group
Security Group ID
Name
Description
sg-00a6141987b58e35d CentOS 7 -x86_64- - with Updates HVM-2002_01-AutogenByAWSMP- This security group was generated by AWS Marketplace and is based on recommended settings for CentOS 7 (x86_64) - wi
sg-af1216a5 default default VPC security group
sg-0a35e080df604581b launch-wizard-1 launch-wizard-1 created 2021-06-02T22:04:00.760+05:30
sg-0fb4f6218eadc462e sg_Jenkins_logiclabs sg_Jenkins_logiclabs
sg-09c995f450660a722 sg_nexus_logiclabs sg_nexus_logiclabs
sg-0179c5b57311a268c sg_sonar_logiclabs sg_sonar_logiclabs
Inbound rules for sg-0179c5b57311a268c (Selected security groups: sg-0179c5b57311a268c)
Type
Protocol
Port Range
Source
Description
HTTP TCP 80 0.0.0.0/0
All traffic All All sg-0fb4f6218eadc462e (sg_Jenkins_logicla
SSH TCP 22 0.0.0.0/0
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG IN
16:21 29/07/2021

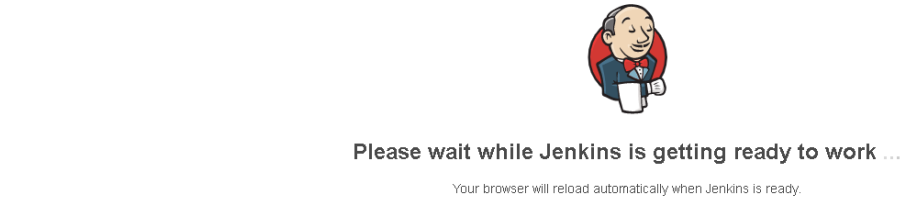

Launch instance wizard | EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
Services
Search for services, features, marketplace products, and docs [Alt+S]
gnsharma @ 1081-9403-8247
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
Inbound rules for sg-0179c5b57311a268c (Selected security groups: sg-0179c5b57311a268c)
Type
Protocol
Port Range
Source
Description
HTTP TCP 80 0.0.0.0/0
All traffic All All sg-0fb4f6218eadc462e (sg_Jenkins_logiclat
SSH TCP 22 0.0.0.0/0
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
35°C
ENG IN
16:21 29/07/2021

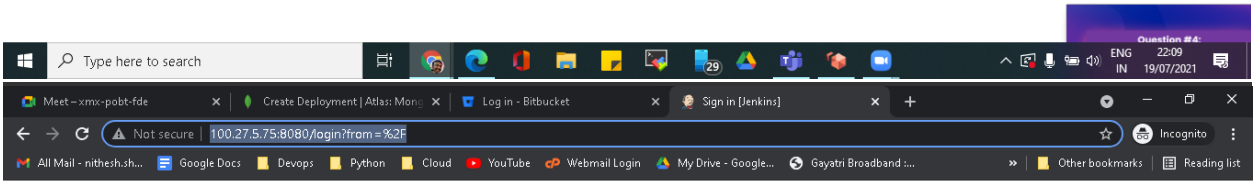


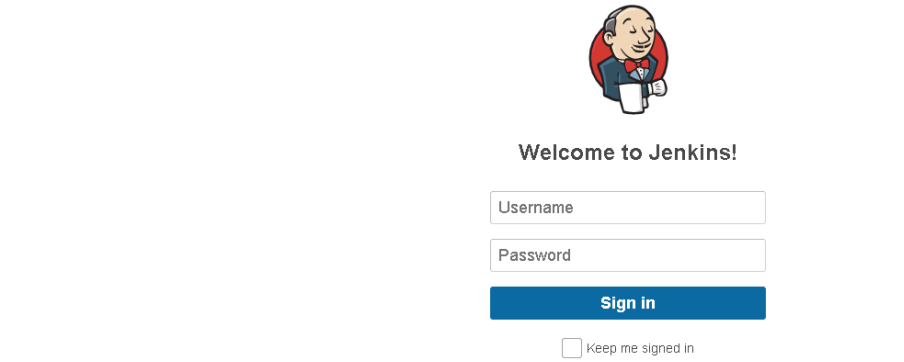

## Verifying the installation:

1. Jenkins setup verification:
    a. Login using public ip of jenkins server followed by port number Eg: 55.52.32.1:8080
    b. When the initial screen asks for Initial admin password, look into the server via ssh and copy the initial admin password
2. Sonar Setup verification
    a. Login using public ip of sonar server
    b.
3. Nexus setup Verification:
    a. Login using public ip of Nexus server followed by port number Eg: 55.52.32.1:8081


Meet – xmx-pobt-fde
Create Deployment | Atlas: Mong
Log in - Bitbucket
Sign in [Jenkins]
Not secure
100.27.5.75:8080/login?from=%2F
Incognito
All Mail - nithesh.sh...
Google Docs
Devops
Python
Cloud
YouTube
Webmail Login
My Drive - Google...
Gayatri Broadband :...
Other bookmarks
Reading list

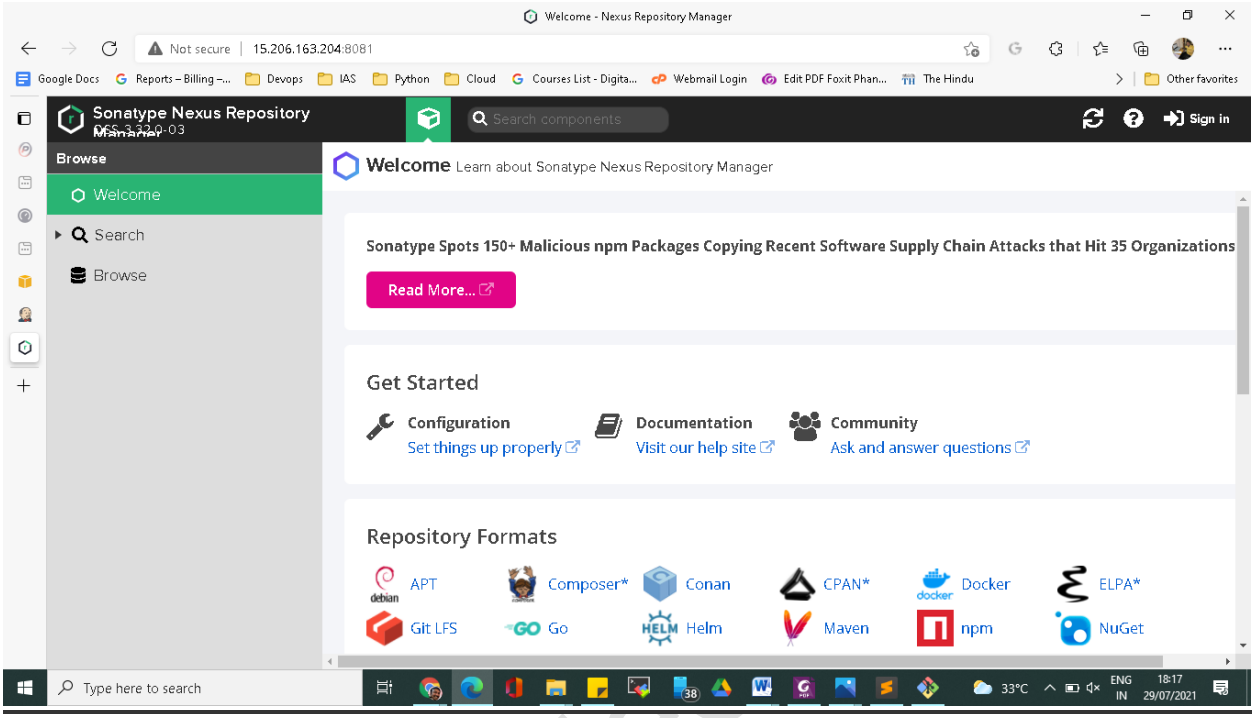

Please wait while Jenkins is getting ready to work ...
Your browser will reload automatically when Jenkins is ready.

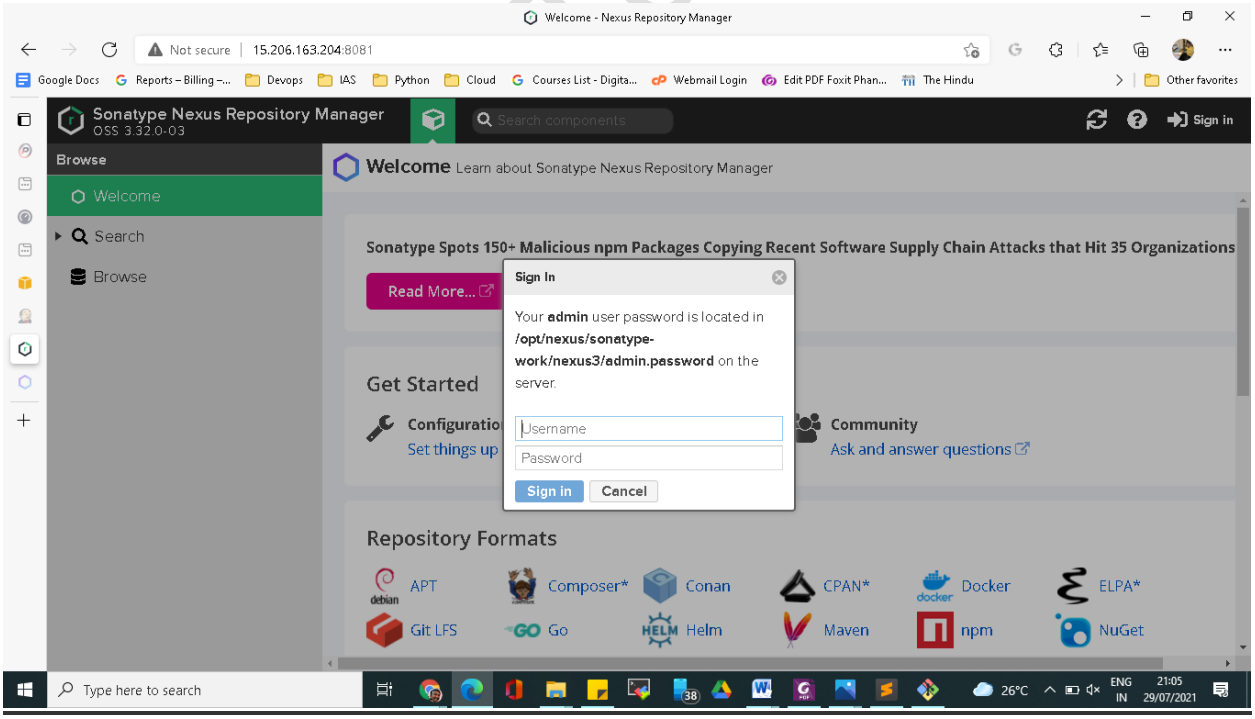

Type here to search
ENG
IN
22:09
19/07/2021
Meet – xmx-pobt-fde
Create Deployment | Atlas: Mong
Log in - Bitbucket
Sign in [Jenkins]
Not secure
100.27.5.75:8080/login?from=%2F
Incognito
All Mail - nithesh.sh...
Google Docs
Devops
Python
Cloud
YouTube
Webmail Login
My Drive - Google...
Gayatri Broadband :...
Other bookmarks
Reading list


Welcome to Jenkins!
Username
Password
Sign in
Keep me signed in

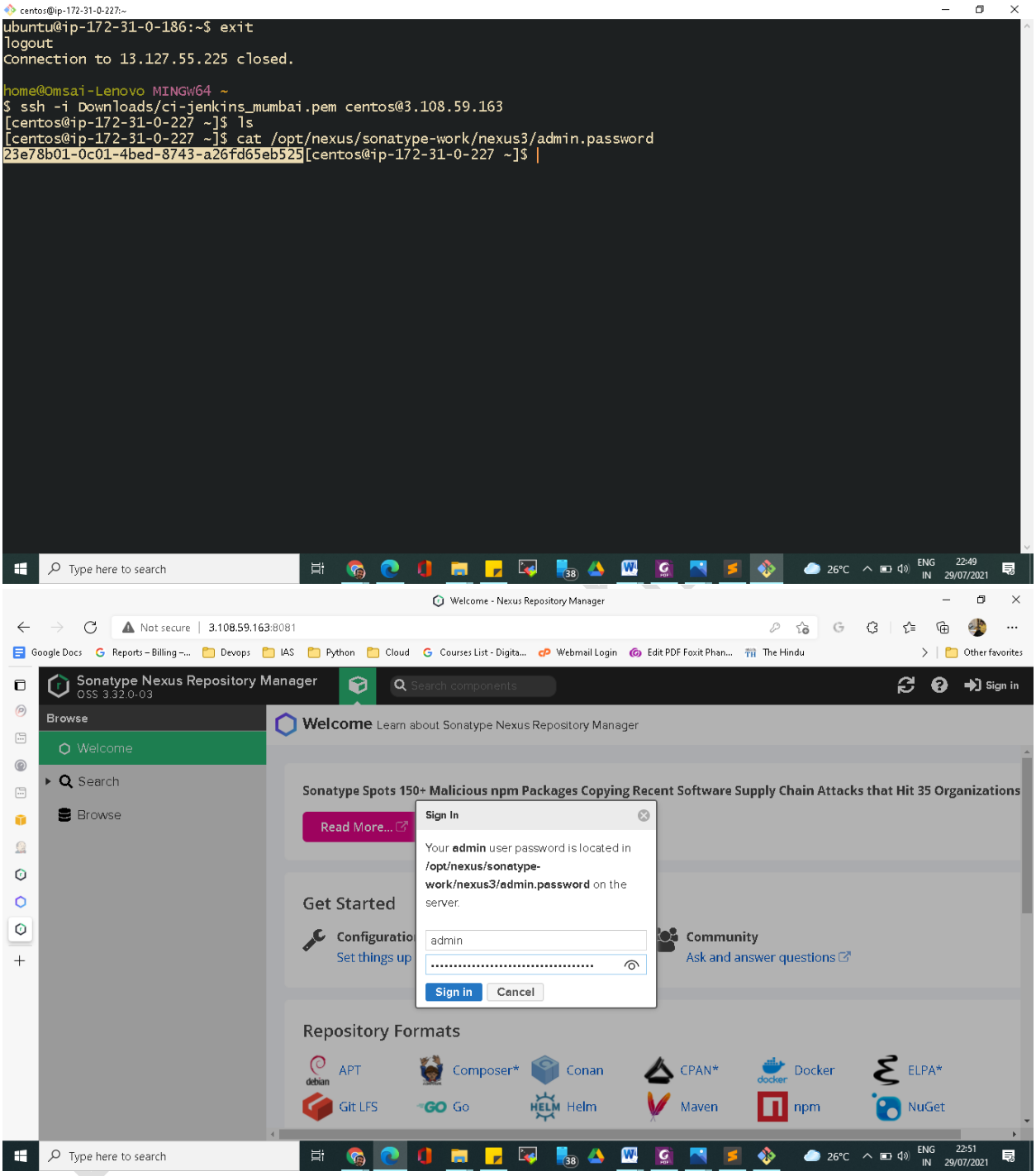

Type here to search
ENG
IN
22:09
19/07/2021

## Validating Nexus configuration:

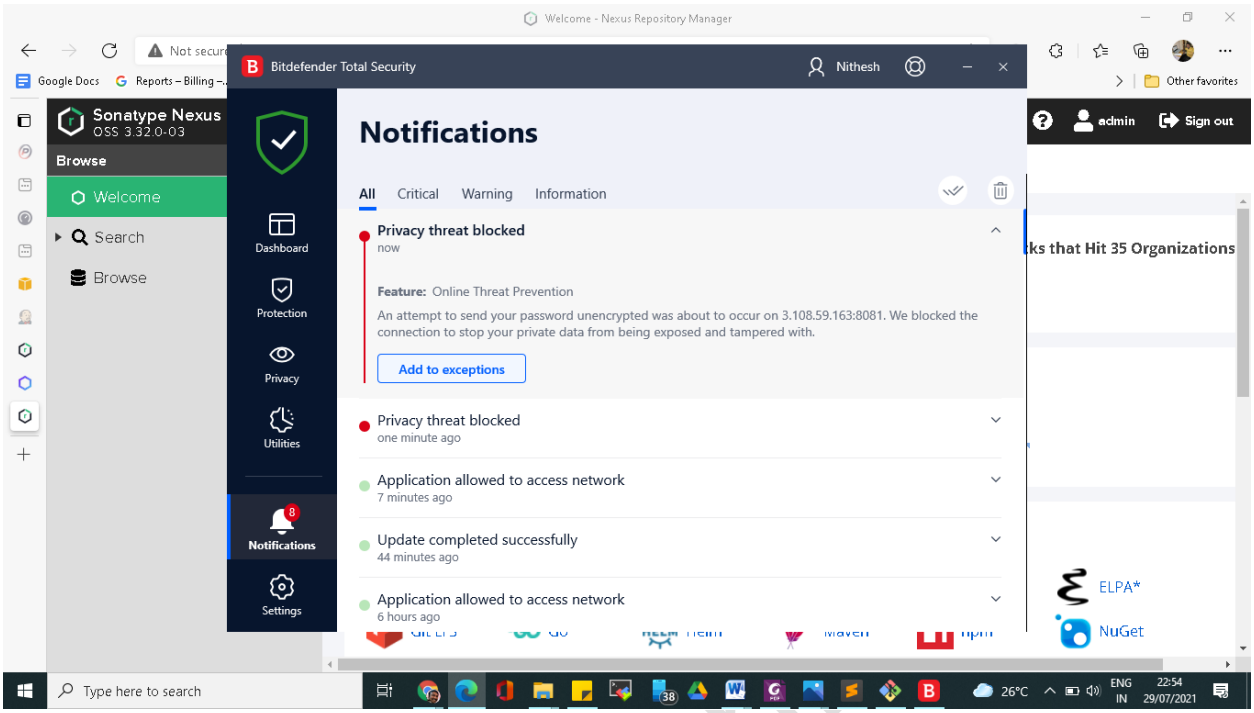


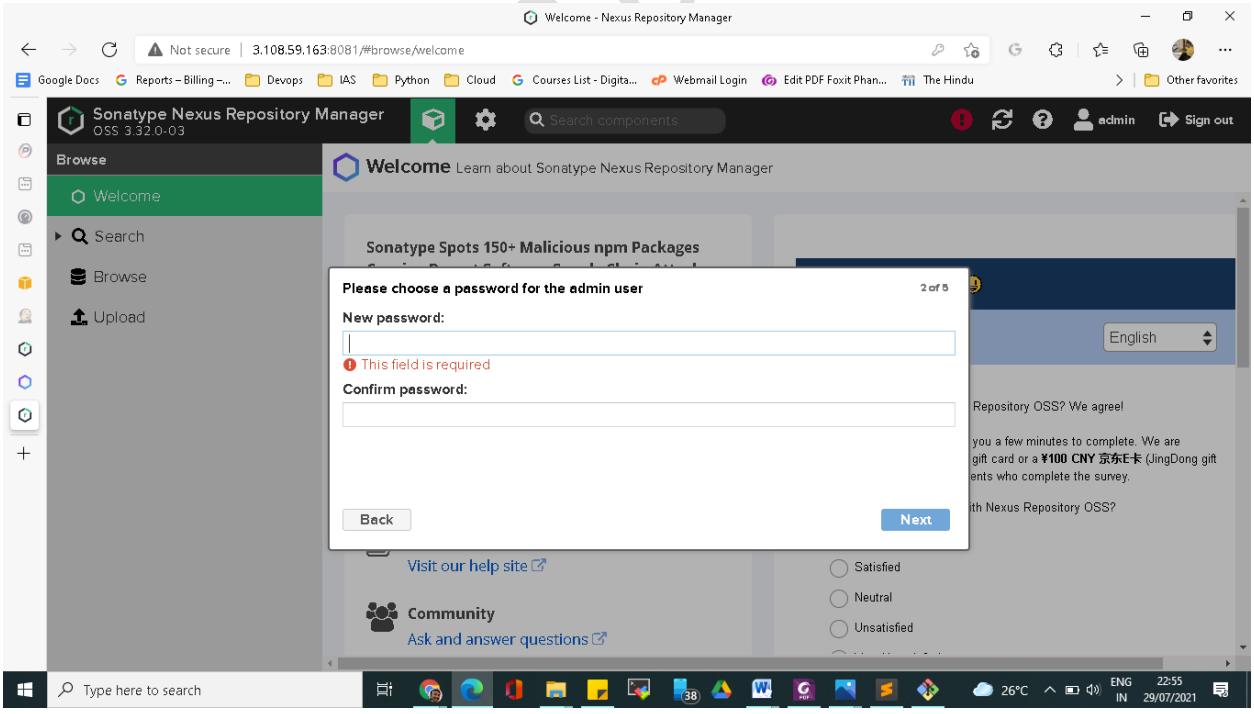

SSH into nexus server to get admin password



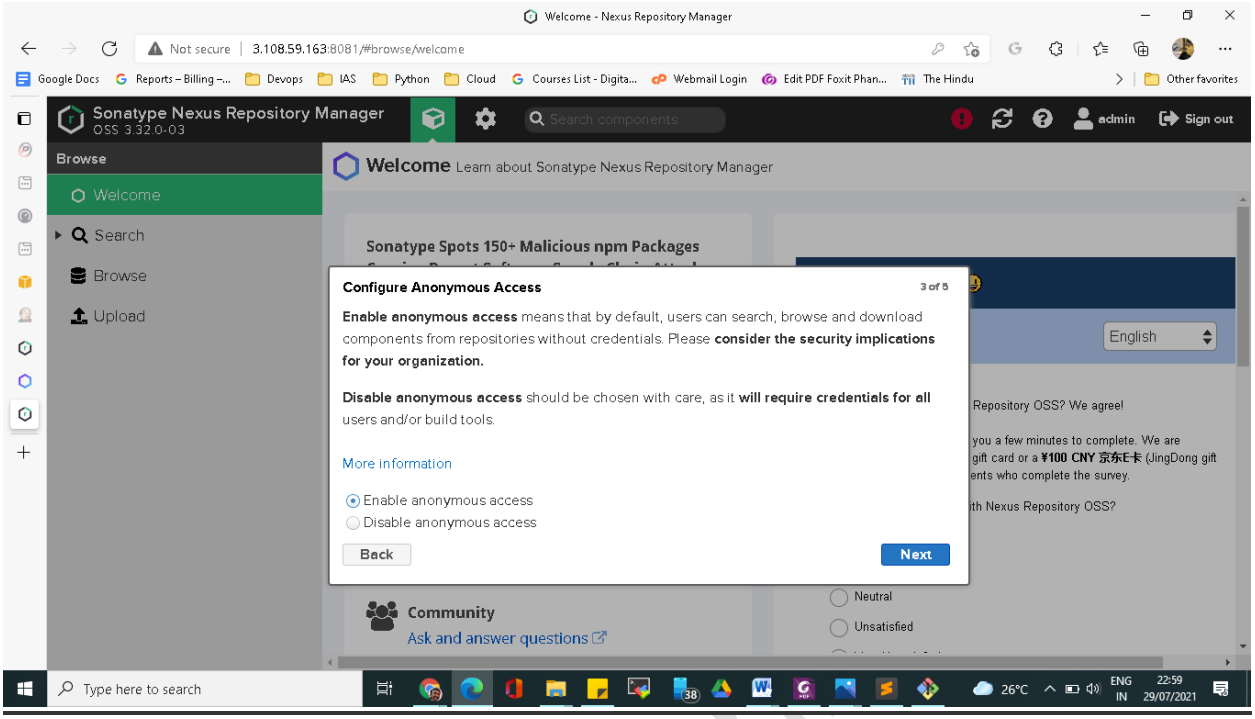

If your antivirus throws an error, please make necessary changes accordingly…

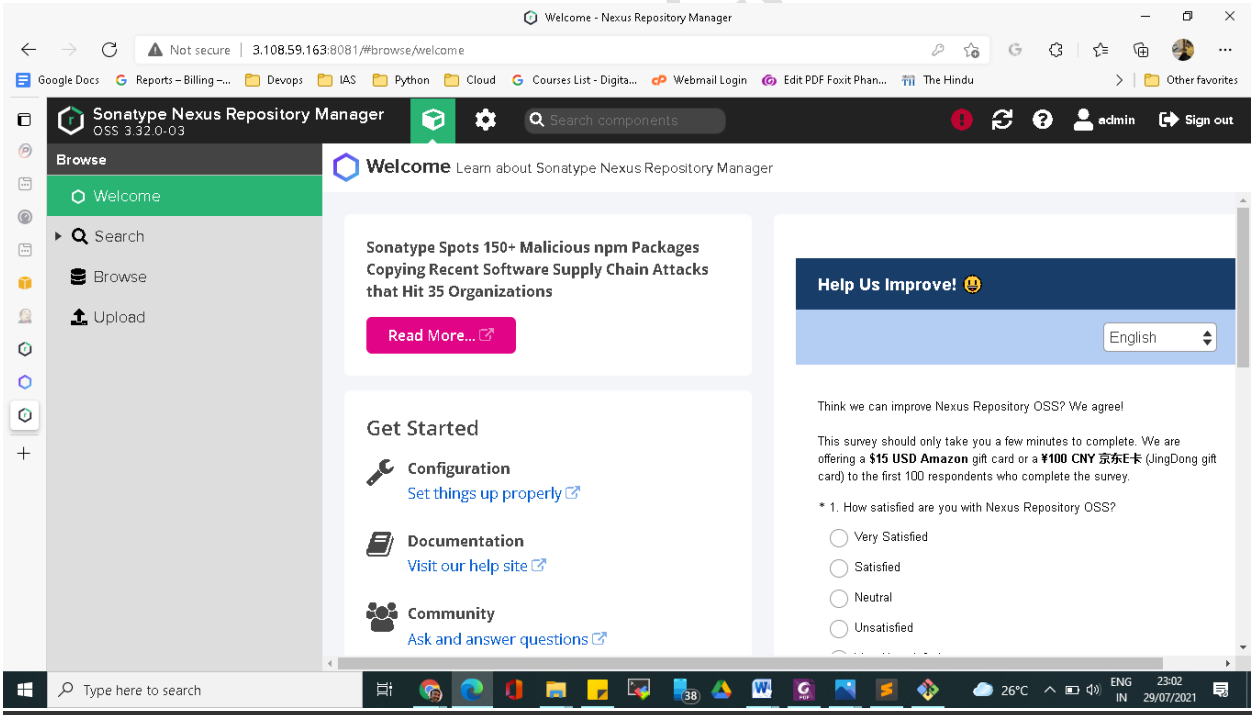



There will be option to change the default password.




Select the below given settings for anonymous access..



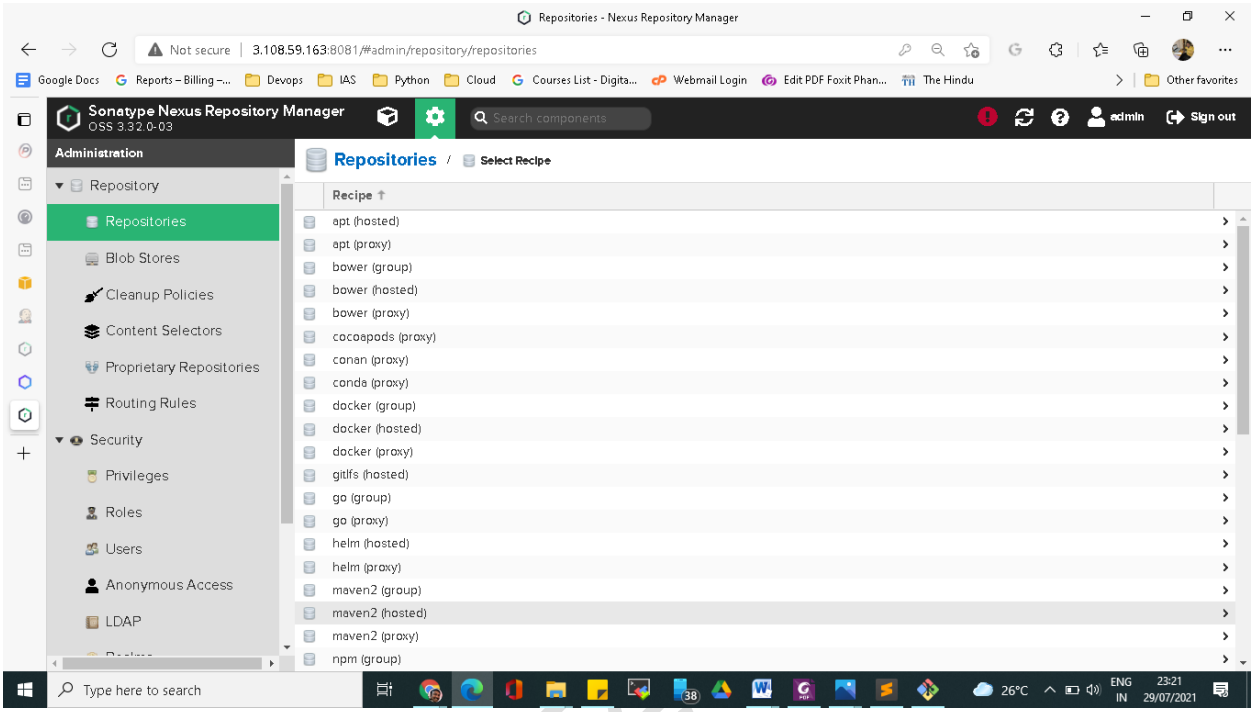



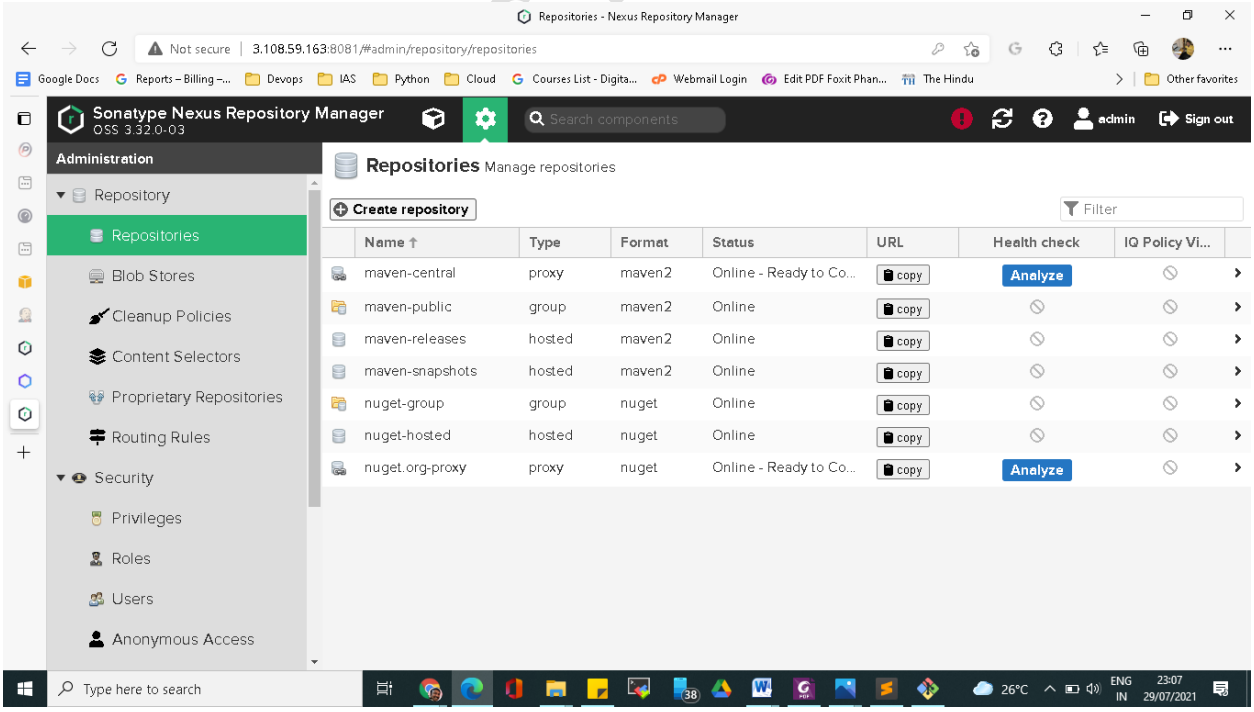

Go to browser option and create new repositories:

1. Maven release
2. Maven central

3. Maven group

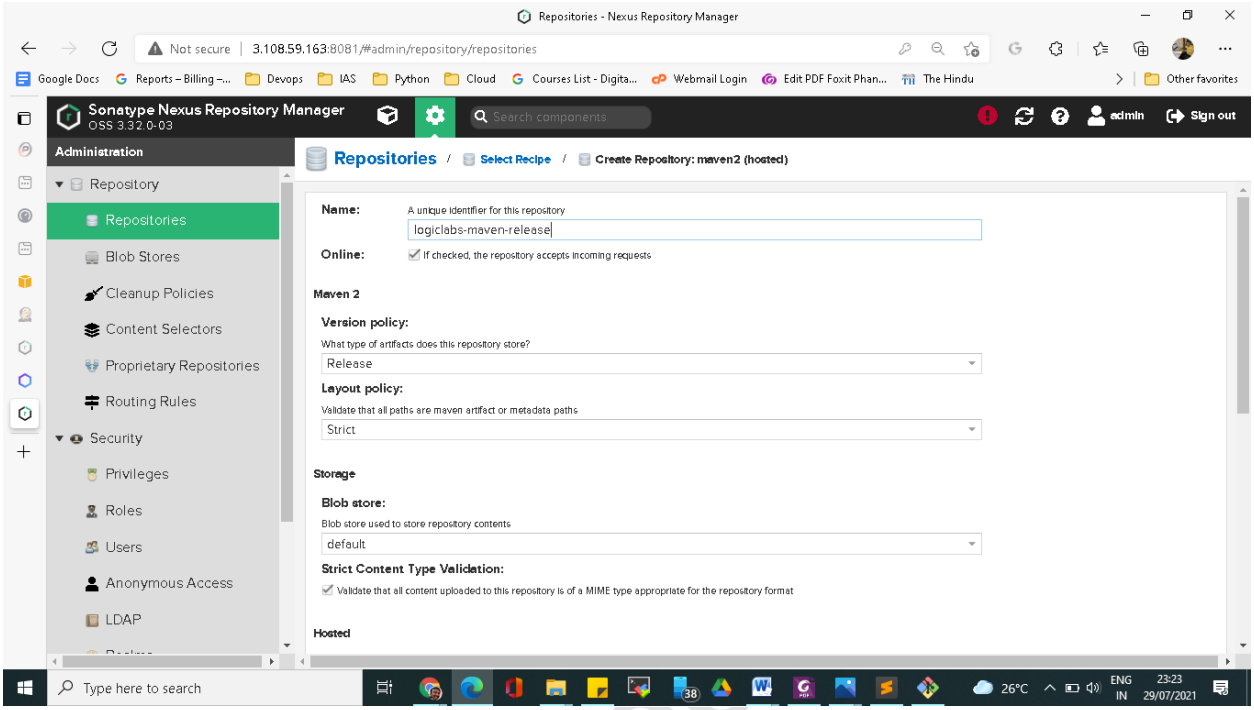
Repositories→ create new repository→ Maven2 (hosted)

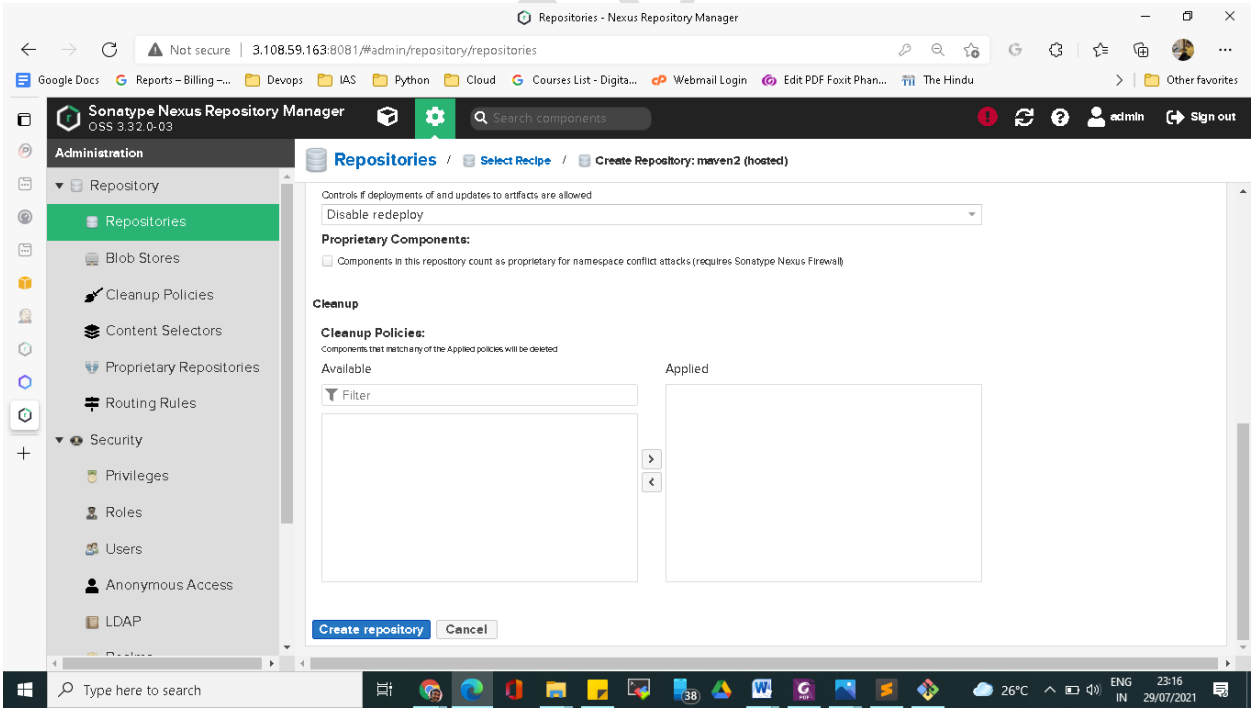


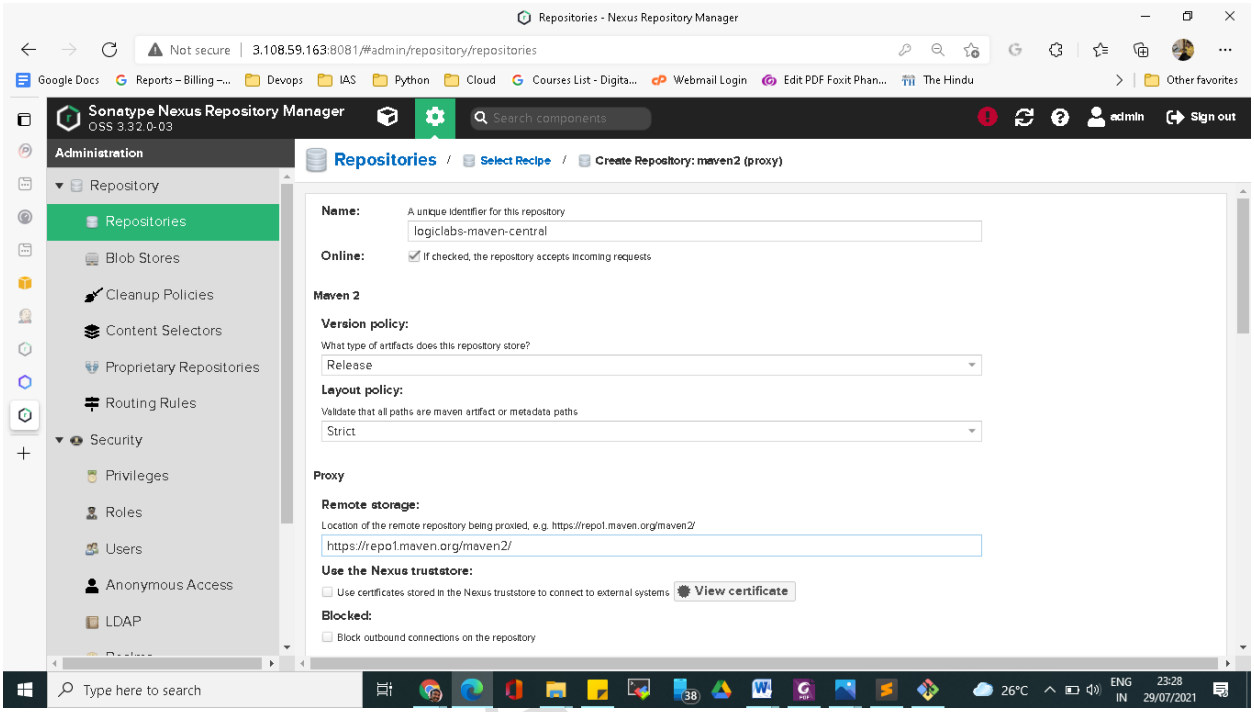




Fill in the details as given in the screenshot below.

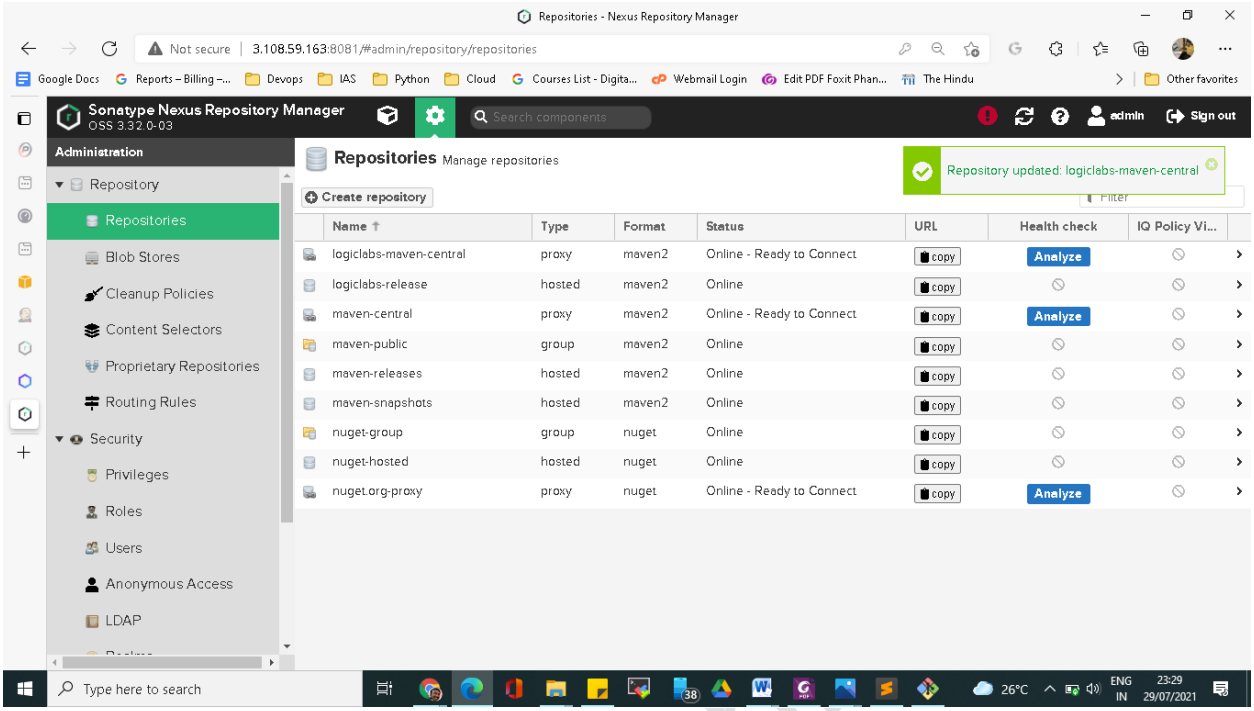
Start with the release repository, then proceed to the central repo and finally create a group repository.



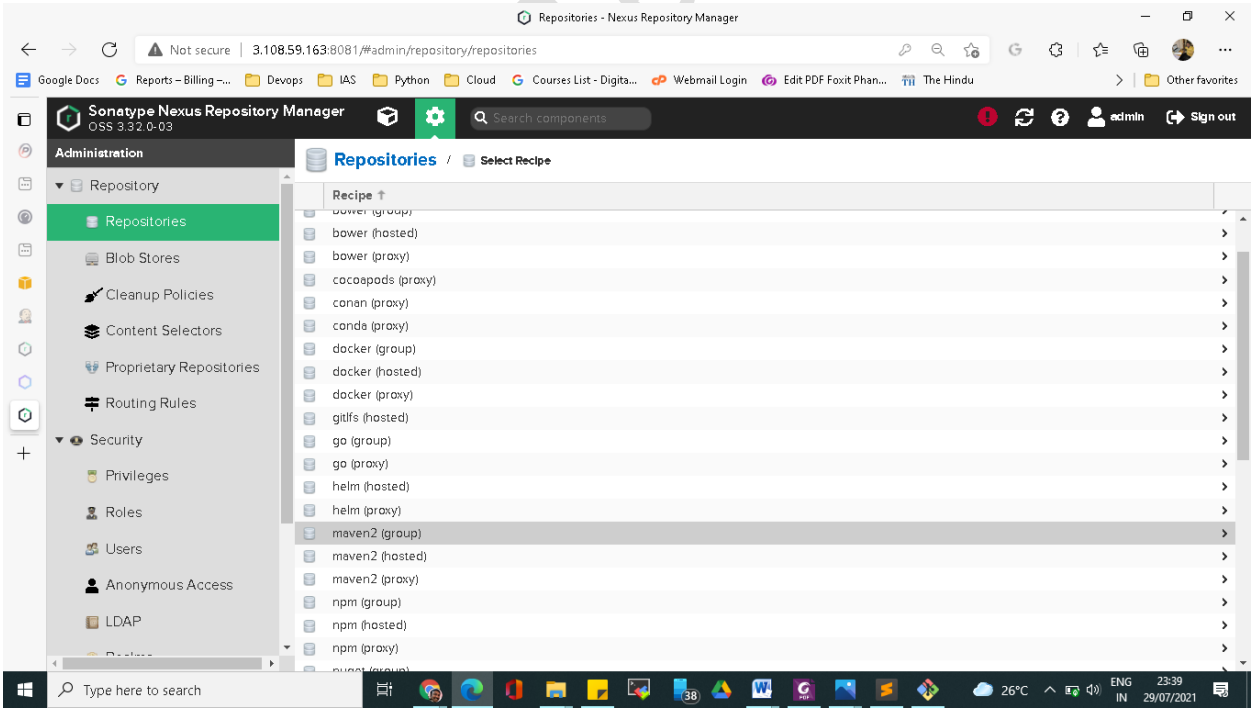



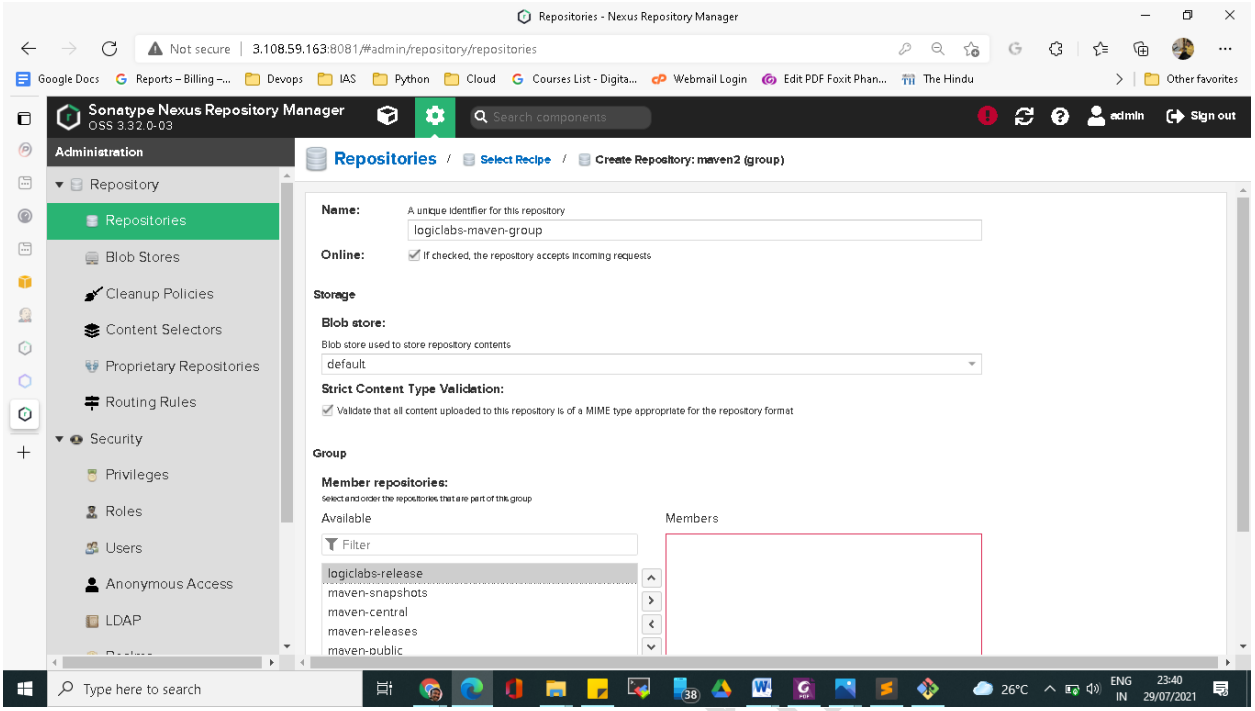


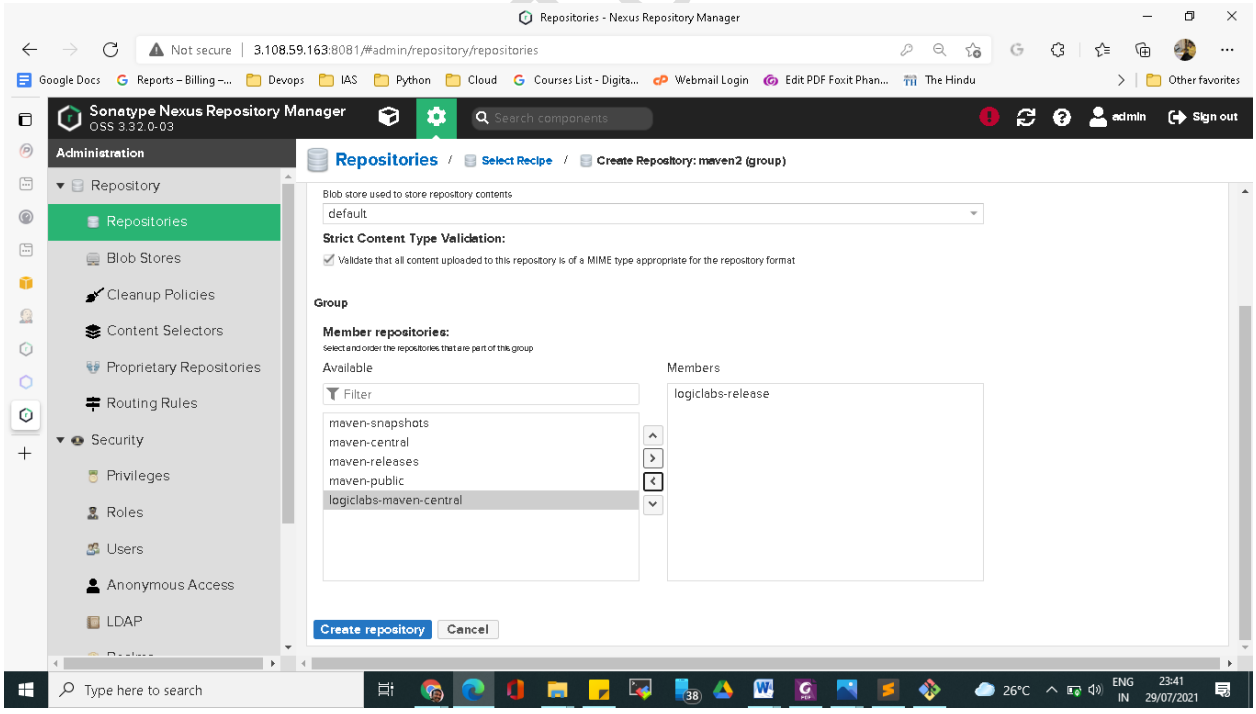

The above step is to save dependencies from maven repo to nexus repo.



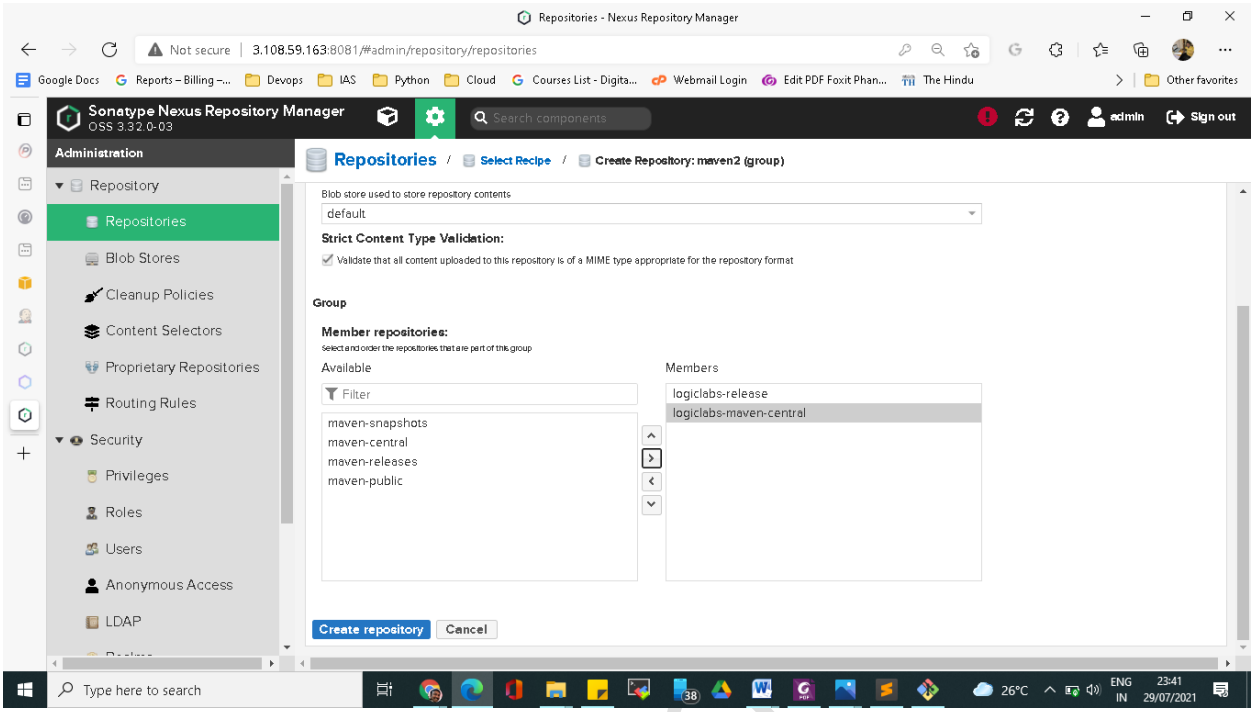

## Create a group repository





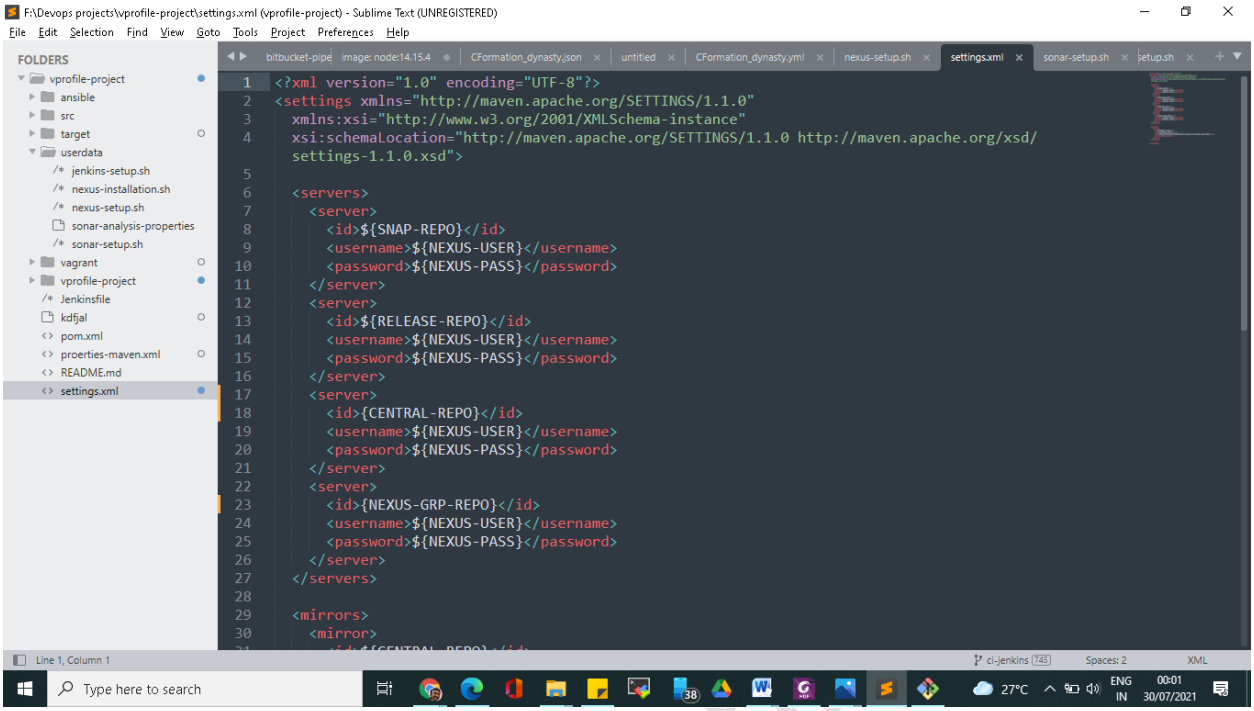

Add the relevant repositories already created to the group repository as given below.




If needed, a snapshot repository can be created from maven2(host) type and change the policy from release to snapshot...however for this demo, we aren't using a snapshot repo.

Inorder for maven to pick up dependencies from nexus repo instead of public repo, we provide necessary details in settings.xml file in our users directory.

Note: the text editor used in this demonstration is sublime text and any other alternative can be used.



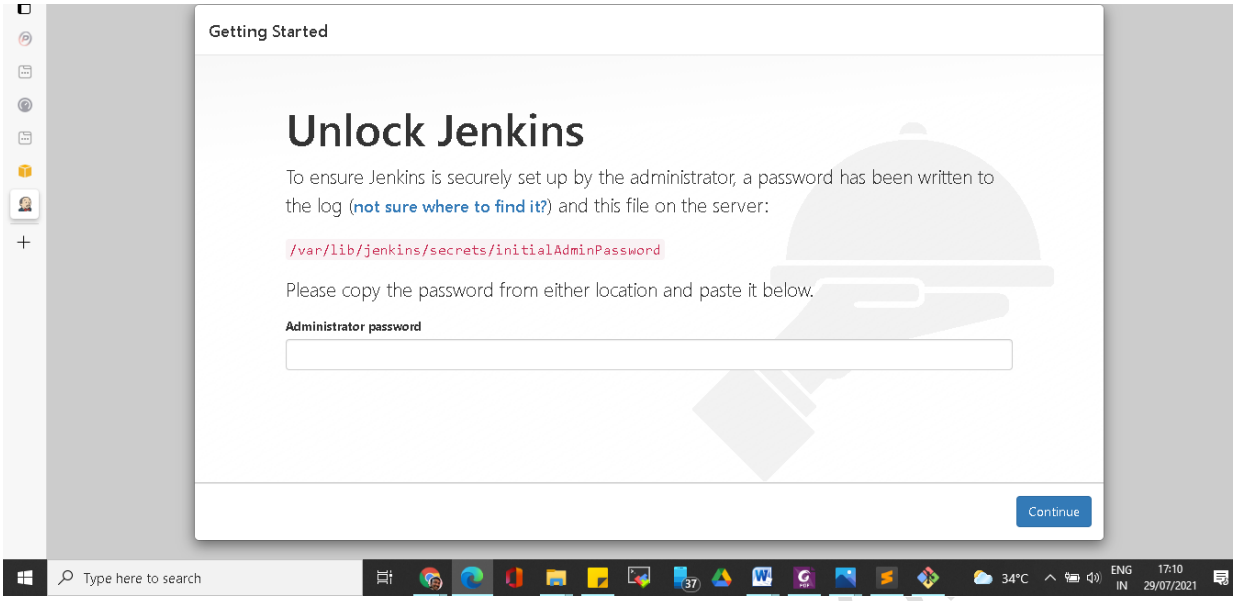

We will mention in jenkins to use this settings.xml file instead of the default one in the .m2 folder of source code.

In the settings.xml and pom.xml files, we mention the variables where the repository values and server URLs will be passed.

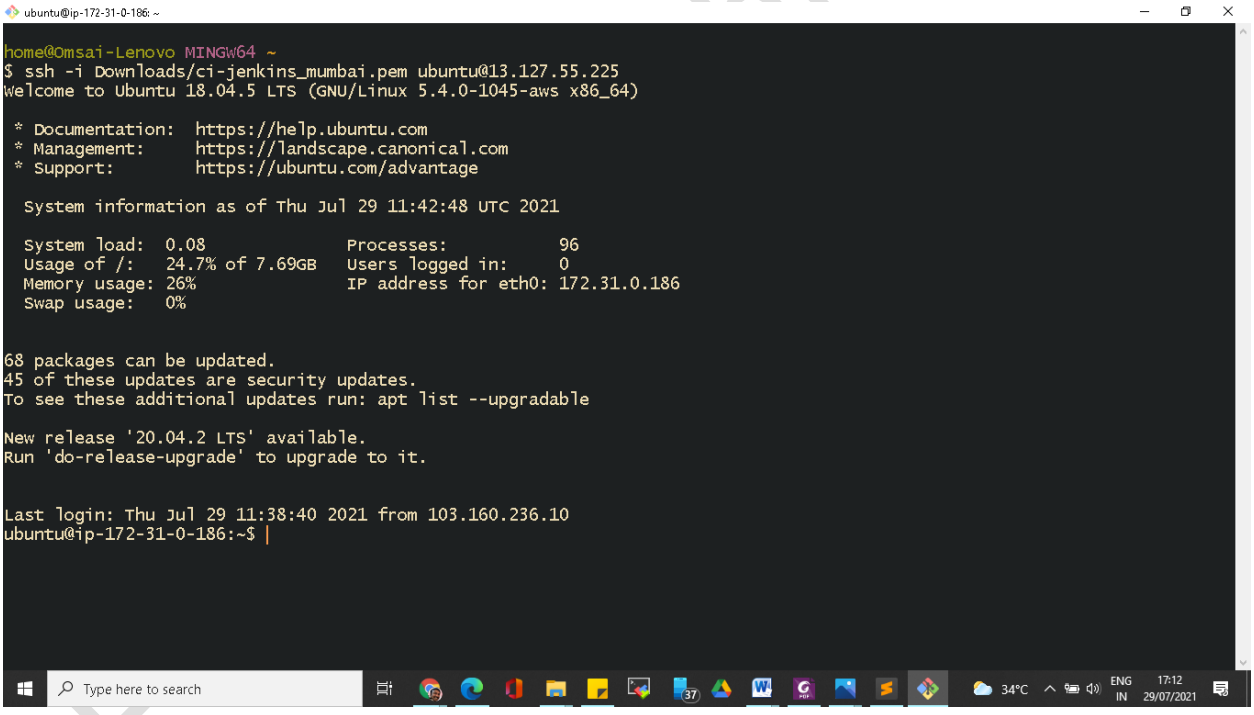
## POST INSTALLATION CONFIGURATION

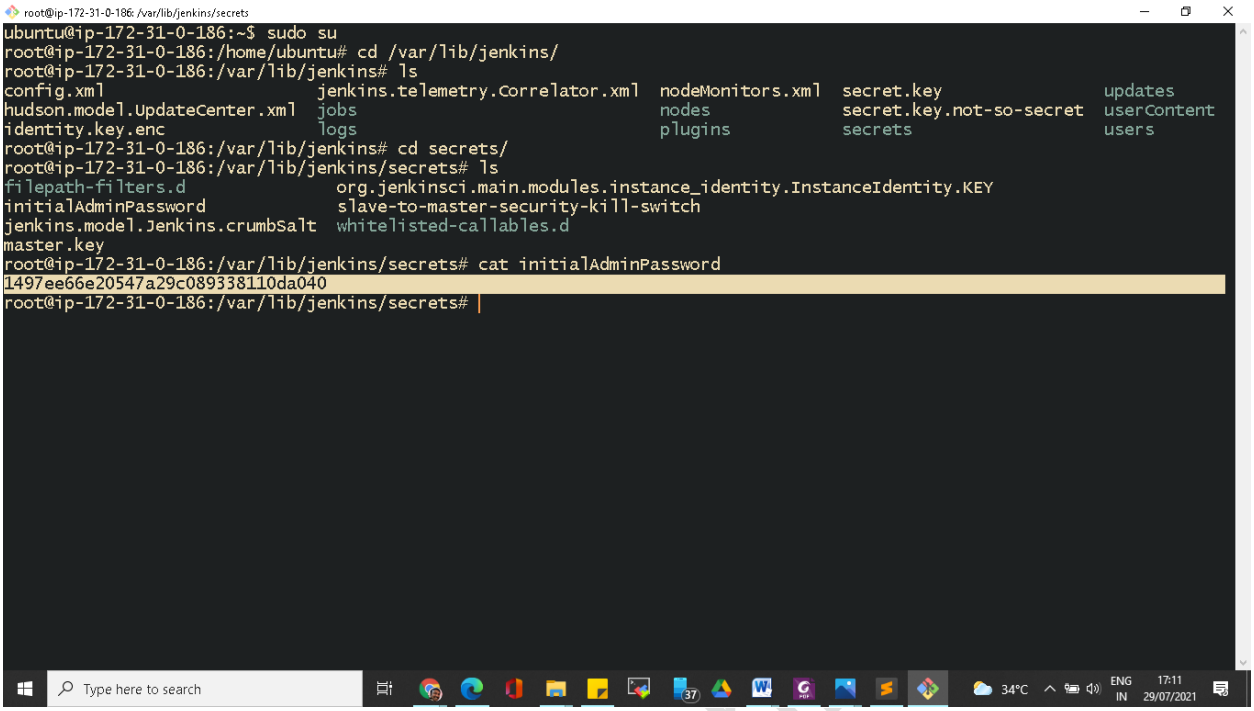
## JENKINS:

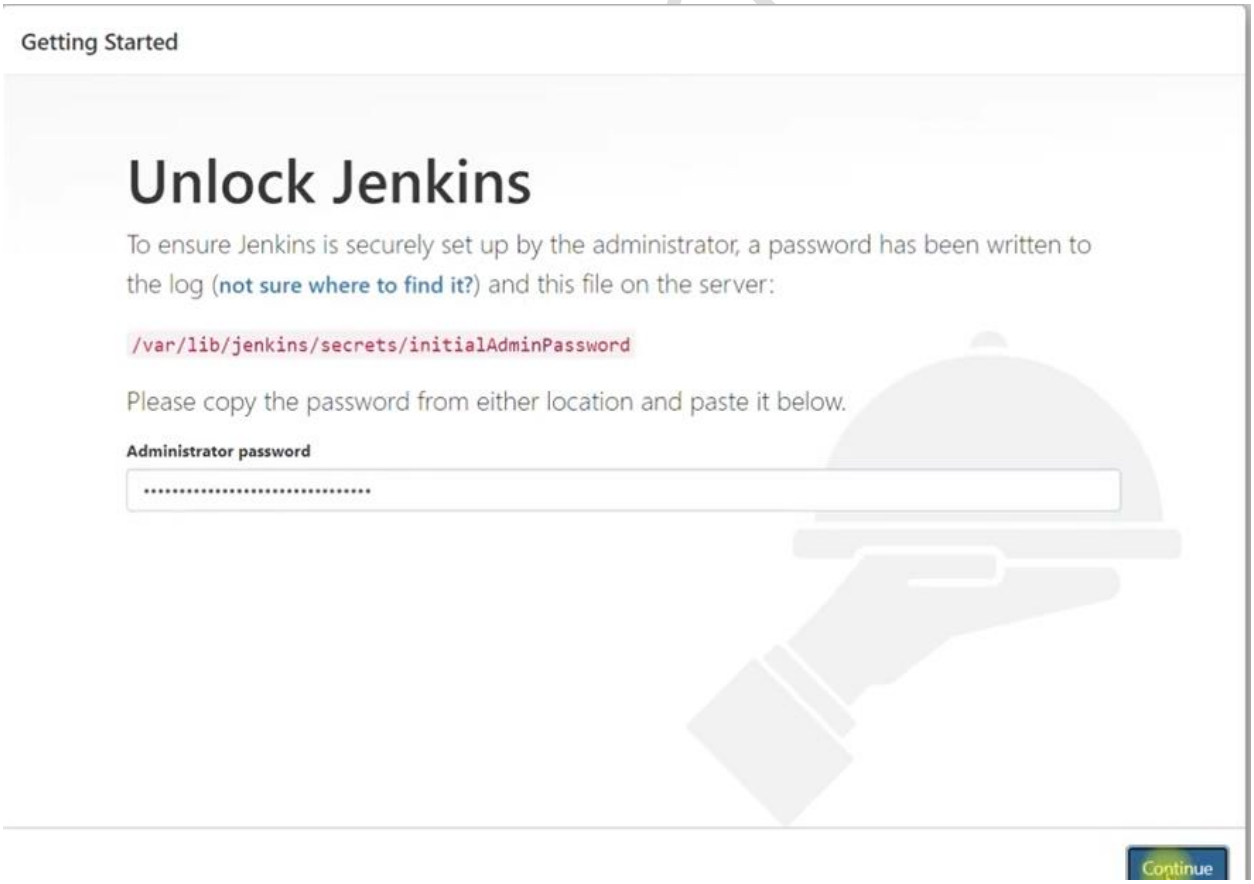
1. Initial admin password can be obtained by logging in to the jenkins ubuntu server and going to the path:
2. /var/lib/jenkins/secrets/initialadminpassword
3. Create a new admin password when prompted
4. Select install suggested plugins
5.

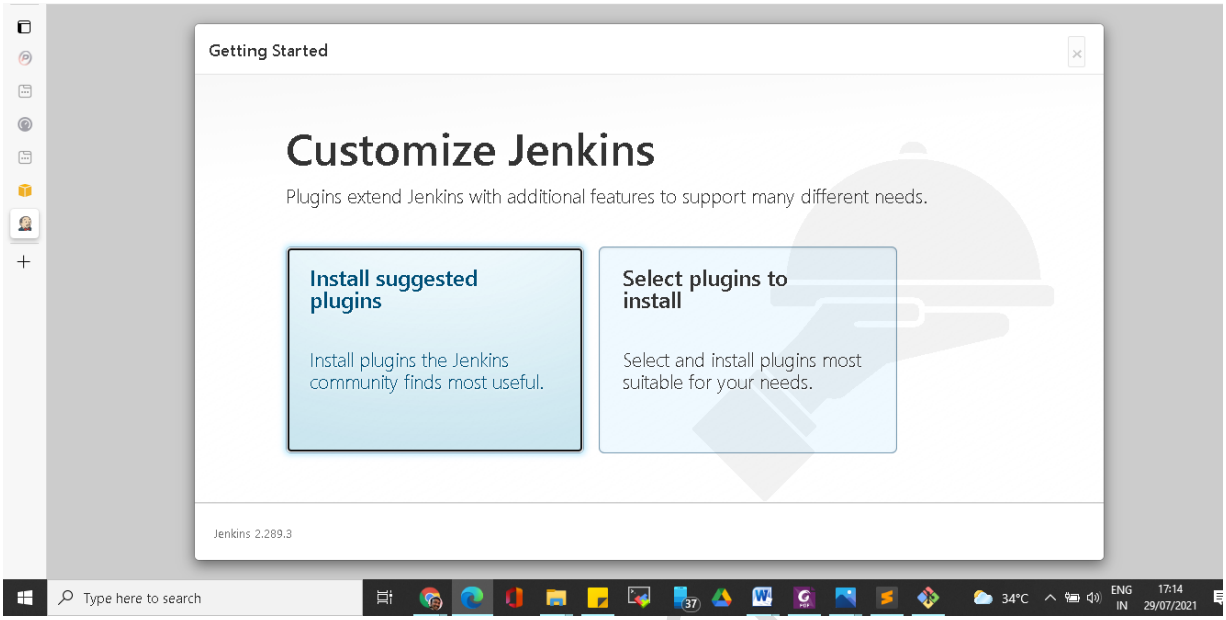



Either use putty or use git bash to ssh into the instance

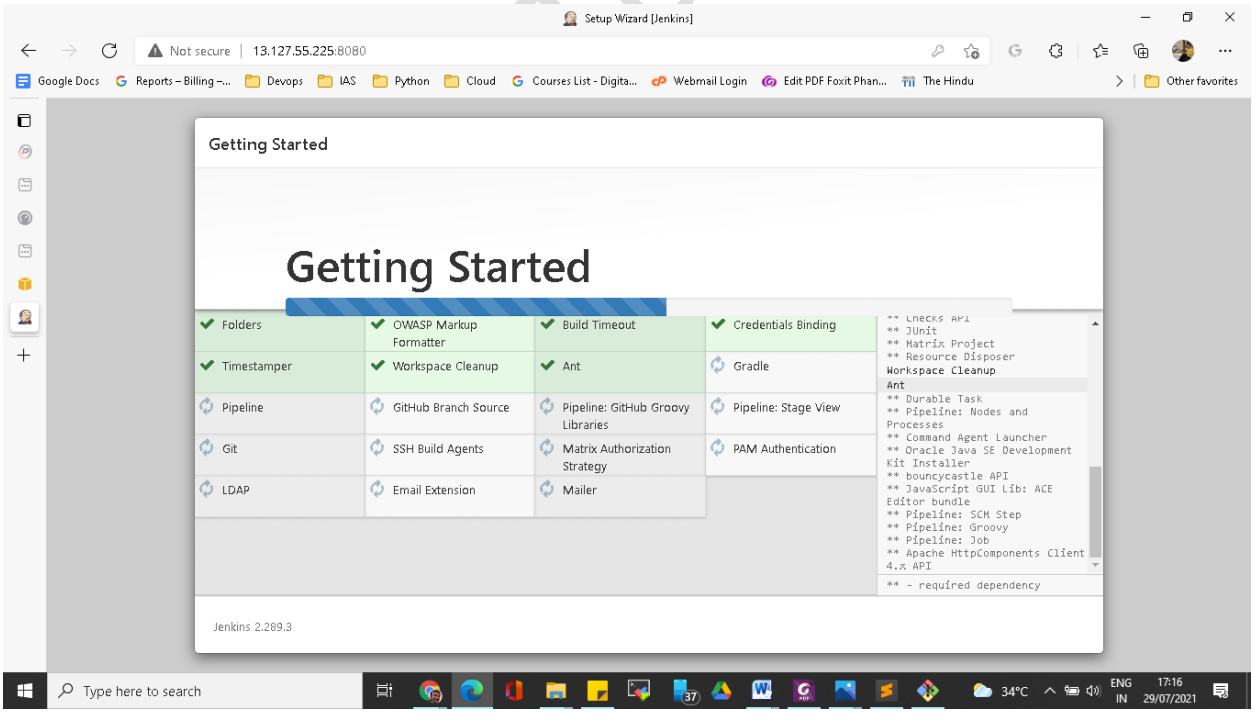


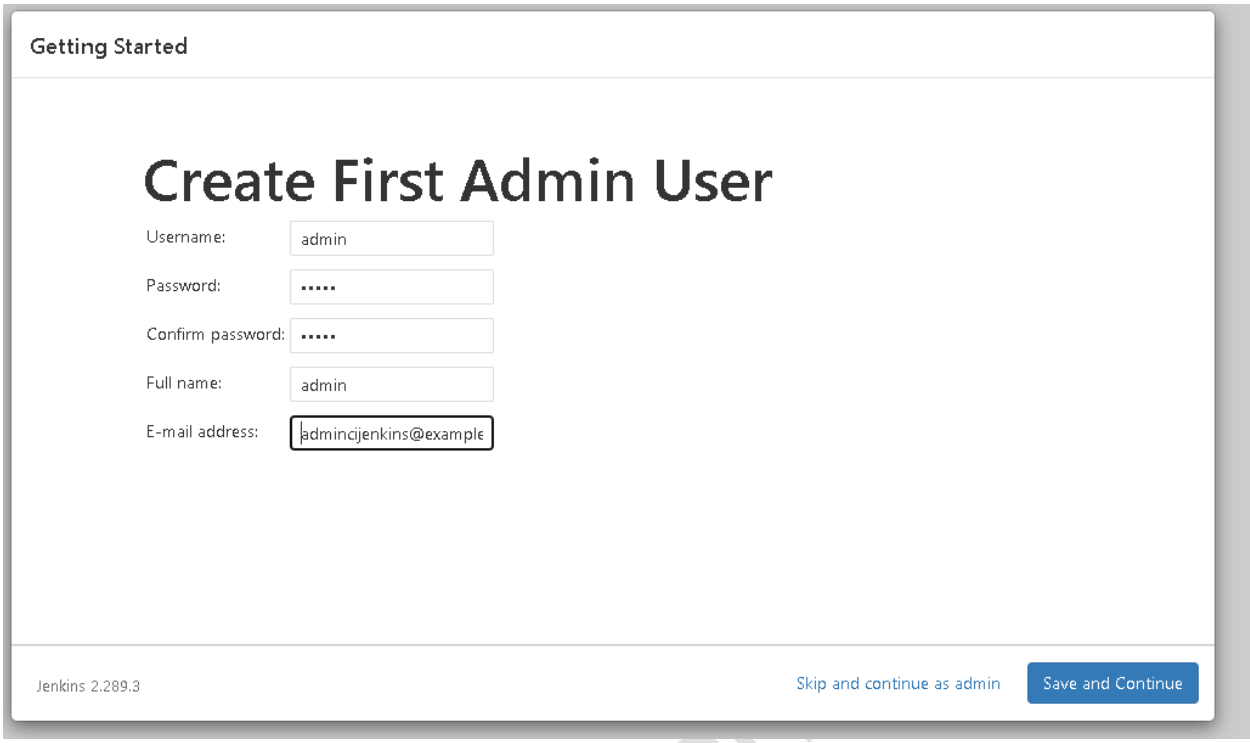

root@ip-172-31-0-186: /var/lib/jenkins/secrets
ubuntu@ip-172-31-0-186:~$ sudo su
root@ip-172-31-0-186:/home/ubuntu# cd /var/lib/jenkins/
root@ip-172-31-0-186:/var/lib/jenkins# ls
config.xml
hudson.model.UpdateCenter.xml
identity.key.enc
jenkins.telemetry.Correlator.xml
jobs
logs
nodeMonitors.xml
nodes
plugins
secret.key
secret.key.not-so-secret
secrets
updates
userContent
users
root@ip-172-31-0-186:/var/lib/jenkins# cd secrets/
root@ip-172-31-0-186:/var/lib/jenkins/secrets# ls
filepath-filters.d
initialAdminPassword
jenkins.model.Jenkins.crumbSalt
master.key
org.jenkinsci.main.modules.instance_identity.InstanceIdentity.KEY
slave-to-master-security-kill-switch
whitelisted-callables.d
root@ip-172-31-0-186:/var/lib/jenkins/secrets# cat initialAdminPassword
1497ee66e20547a29c089338110da040
root@ip-172-31-0-186:/var/lib/jenkins/secrets#
Type here to search
34°C
ENG
IN
17:11
29/07/2021


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

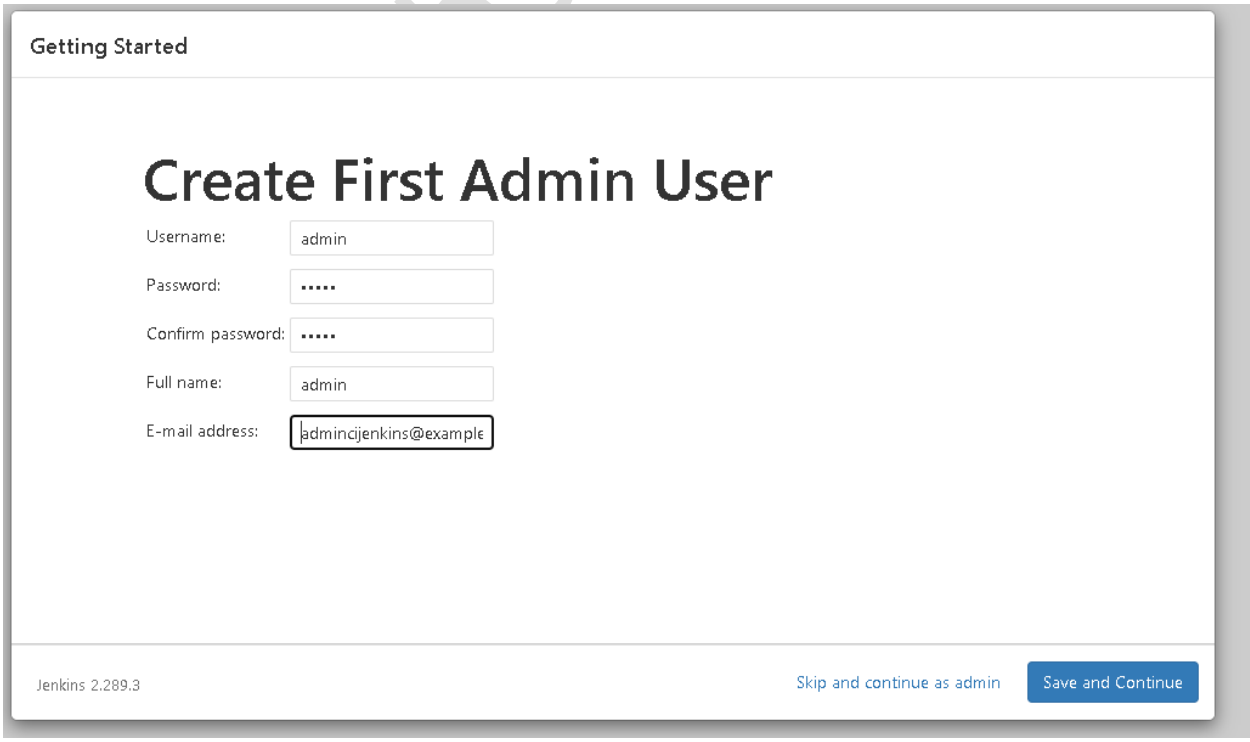



Wait till all the suggested plugins are installed





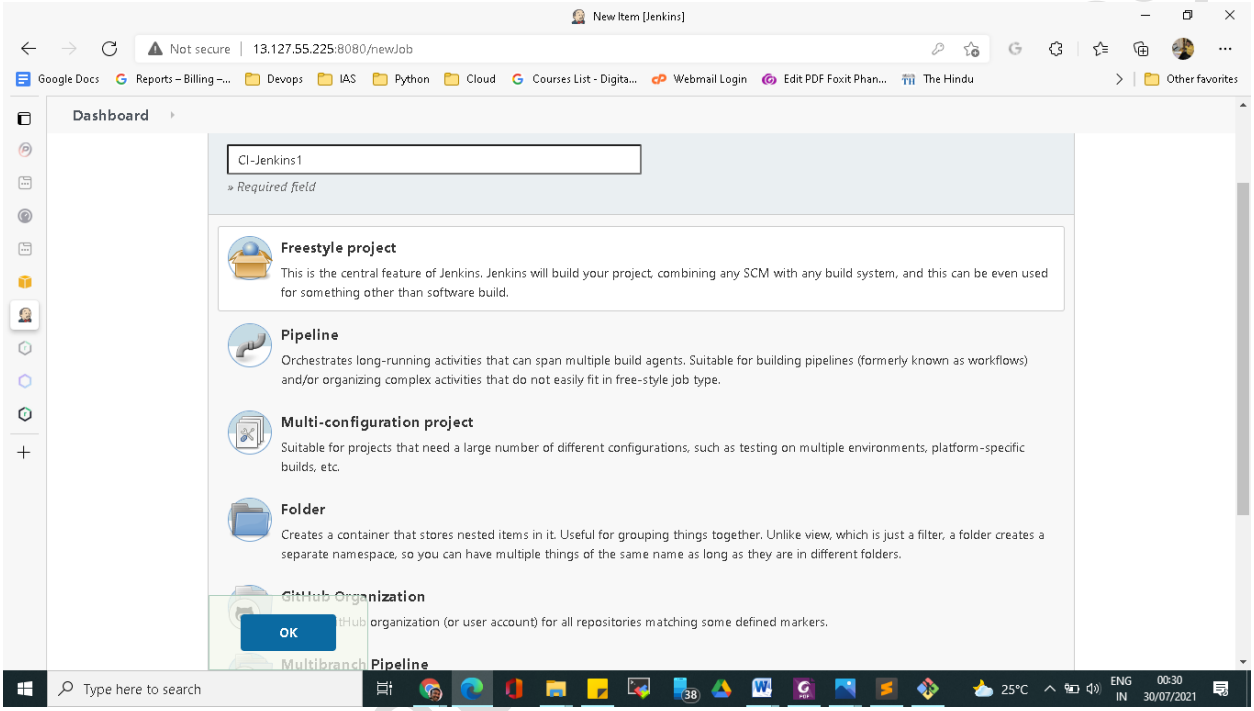

Give your desired values for username and password, select continue to configure further steps.

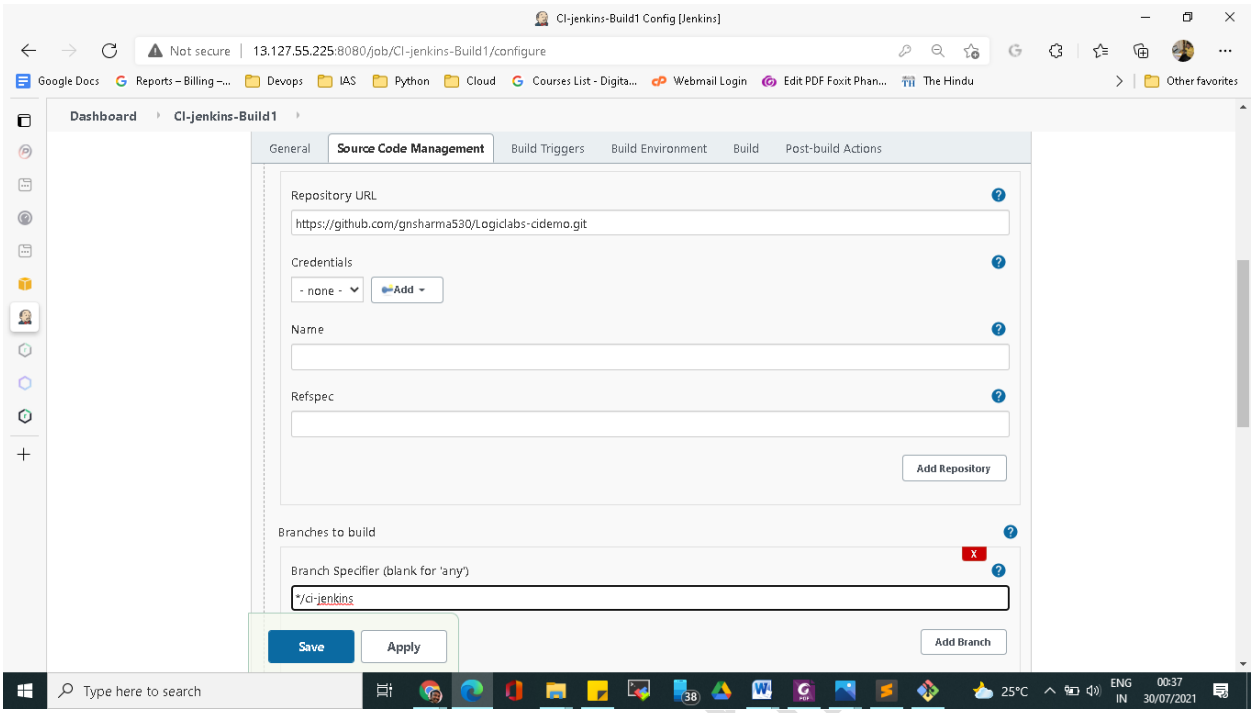


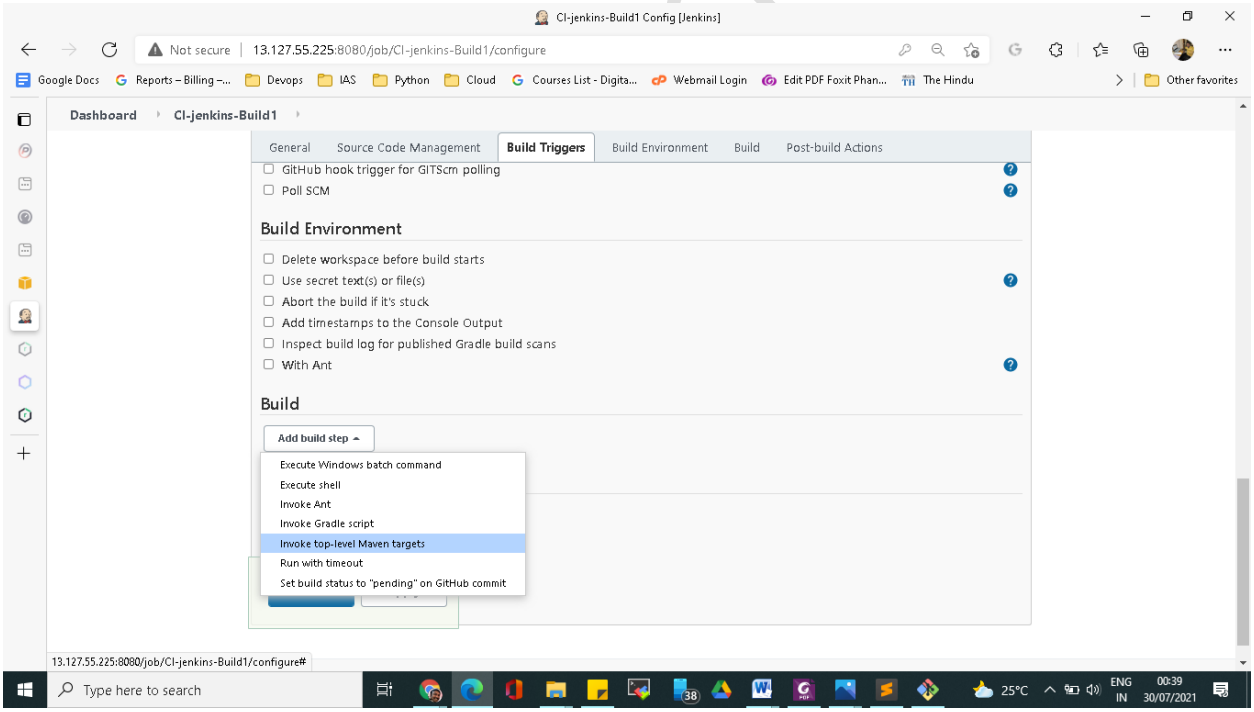
## Creating a JENKINS Job:

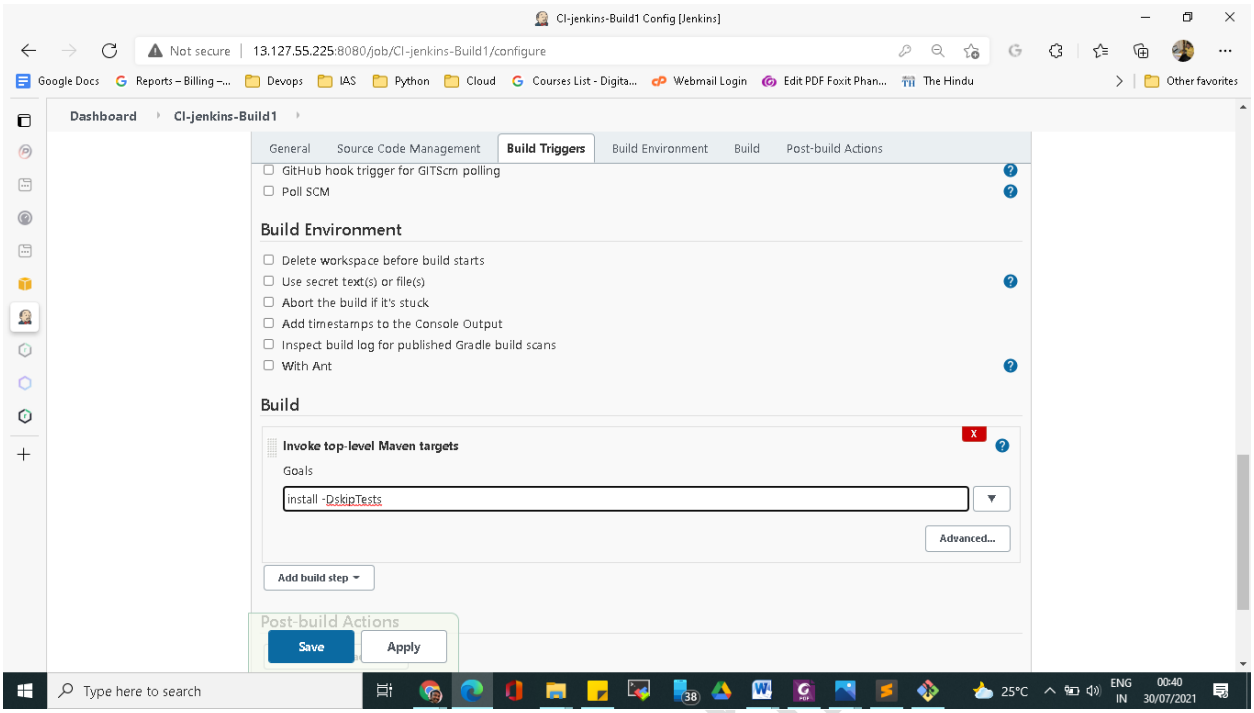
Give a proper name (eg: CI-Jenkins1) and select freestyle project and click on ok to create a new jenkins job.

1. Provide settings for the job as given in the screenshots below.




CI-jenkins-Build1 Config [Jenkins]
Not secure | 13.127.55.225:8080/job/CI-jenkins-Build1/configure
Dashboard
CI-jenkins-Build1
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Repository URL
https://github.com/gnsharma530/Logiclabs-cidemo.git
Credentials
- none -
Add
Name
Refspec
Add Repository
Branches to build
Branch Specifier (blank for 'any')
*/ci-jenkins
Save
Apply
Add Branch
Type here to search
25°C
ENG
IN
00:37
30/07/2021


CI-jenkins-Build1 Config [Jenkins]
Not secure | 13.127.55.225:8080/job/CI-jenkins-Build1/configure
Dashboard
CI-jenkins-Build1
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
GitHub hook trigger for GITScm polling
Poll SCM
Build Environment
Delete workspace before build starts
Use secret text(s) or file(s)
Abort the build if it's stuck
Add timestamps to the Console Output
Inspect build log for published Gradle build scans
With Ant
Build
Add build step
Execute Windows batch command
Execute shell
Invoke Ant
Invoke Gradle script
Invoke top-level Maven targets
Run with timeout
Set build status to "pending" on GitHub commit
13.127.55.225:8080/job/CI-jenkins-Build1/configure#
Type here to search
25°C
ENG
IN
00:39
30/07/2021

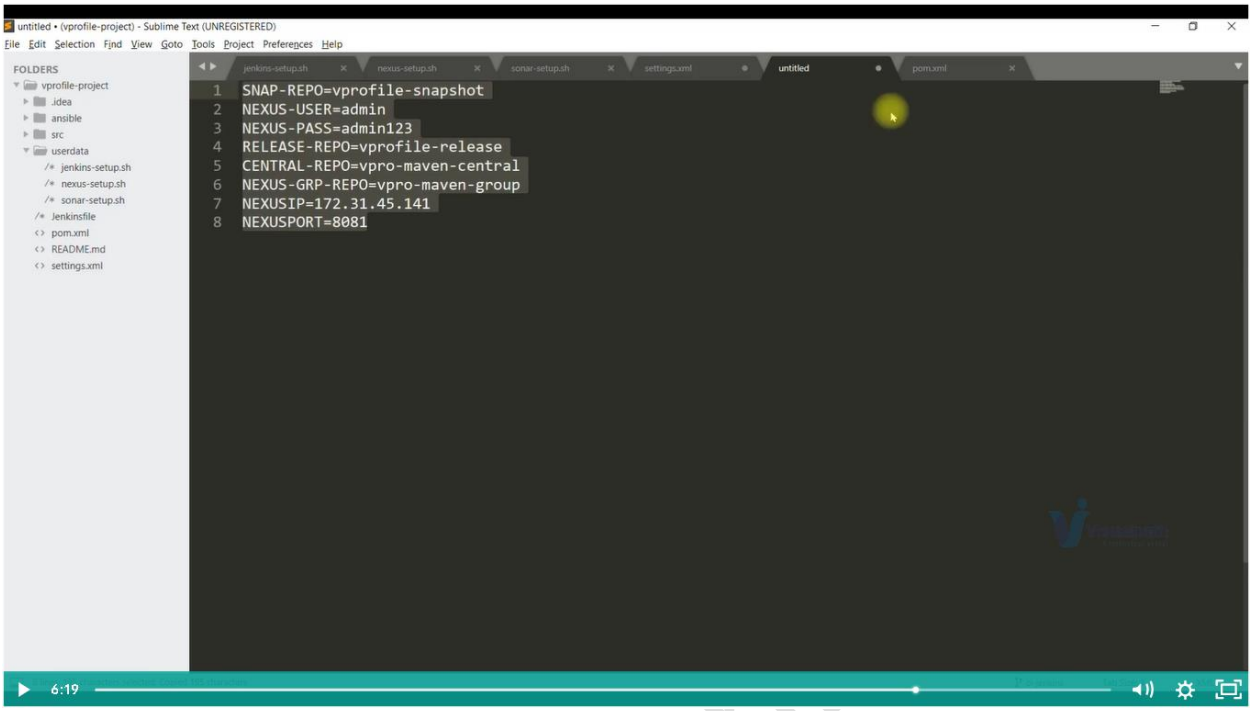



We pass the goals as *"install - DskipTests"* to skip unit test as of now and only package our source code

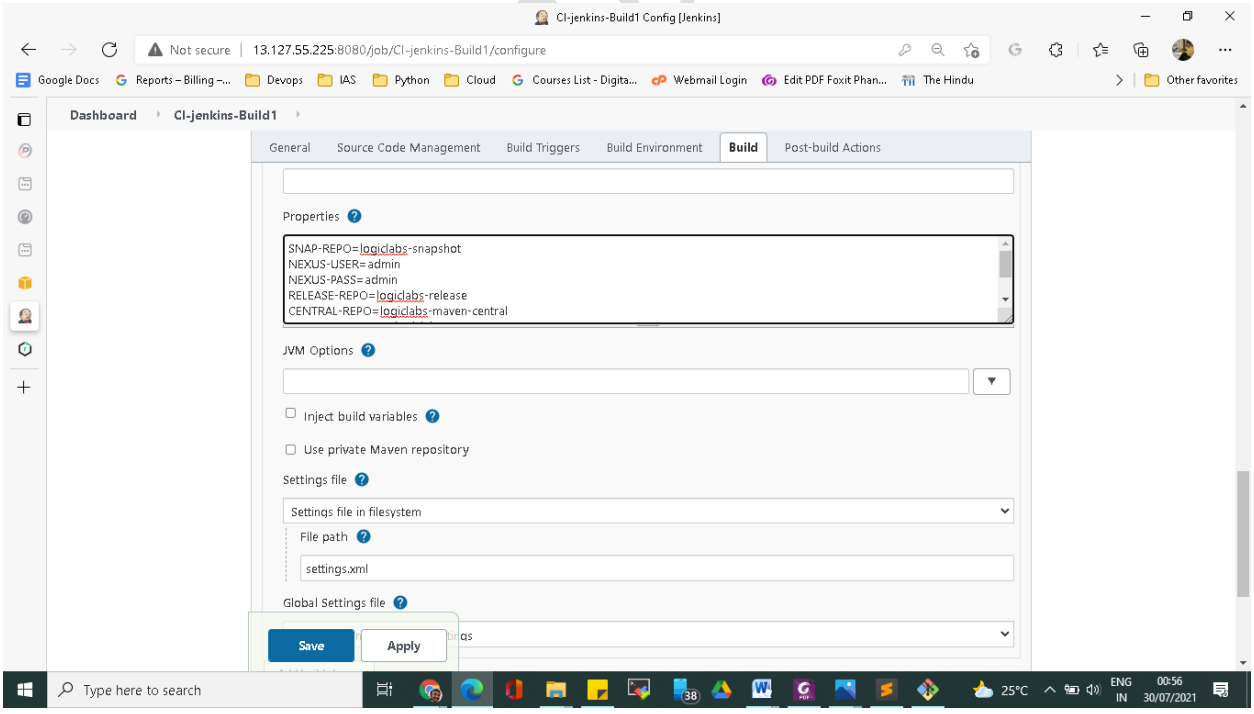
SET VARIABLES:

Create a properties file and fill in the below given details. Change the below properties as per your server configurations

We obtain the necessary details from nexus repository configurations.
Paste the same values as you have given.
The values given in below screenshots may be different from what you might have given.



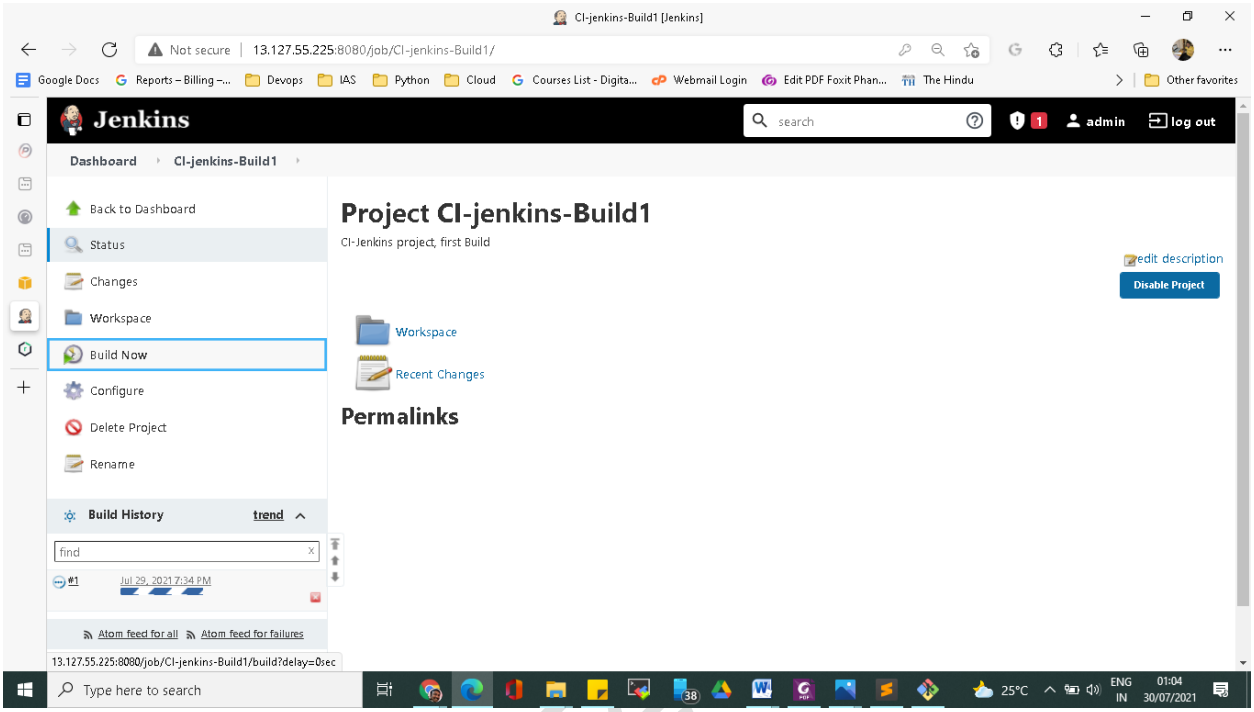

Copy these properties into the jenkins properties option;

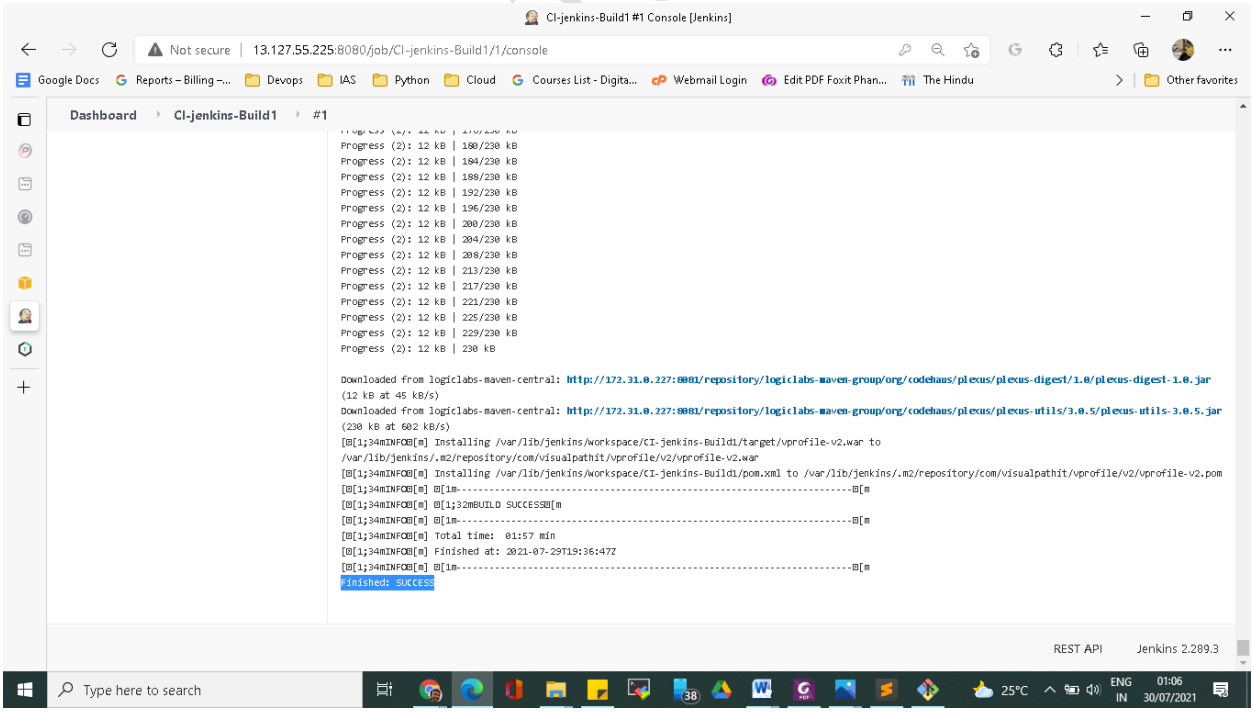


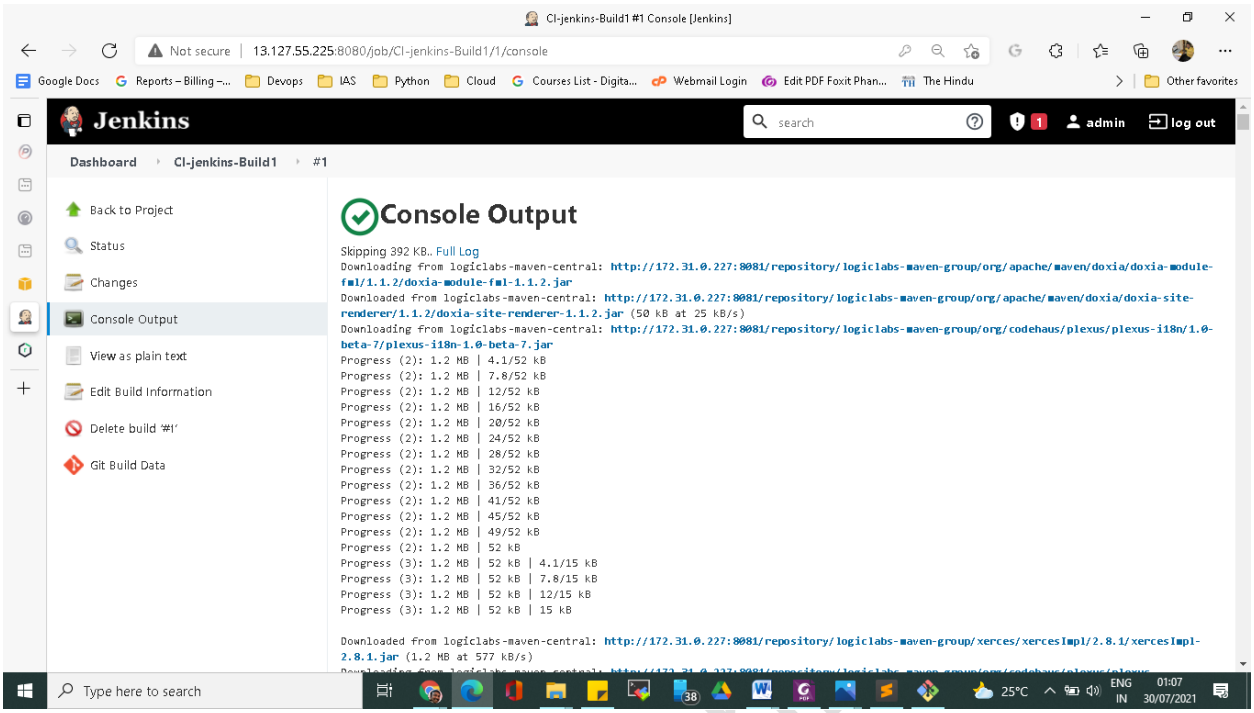

**Also provide 'File path' to settings.xml file as settings file in filesystem..**

For that, go to settings file → file path→ *type* “settings.xml”

**Save the file.. And click on build now option to test our first build job.**

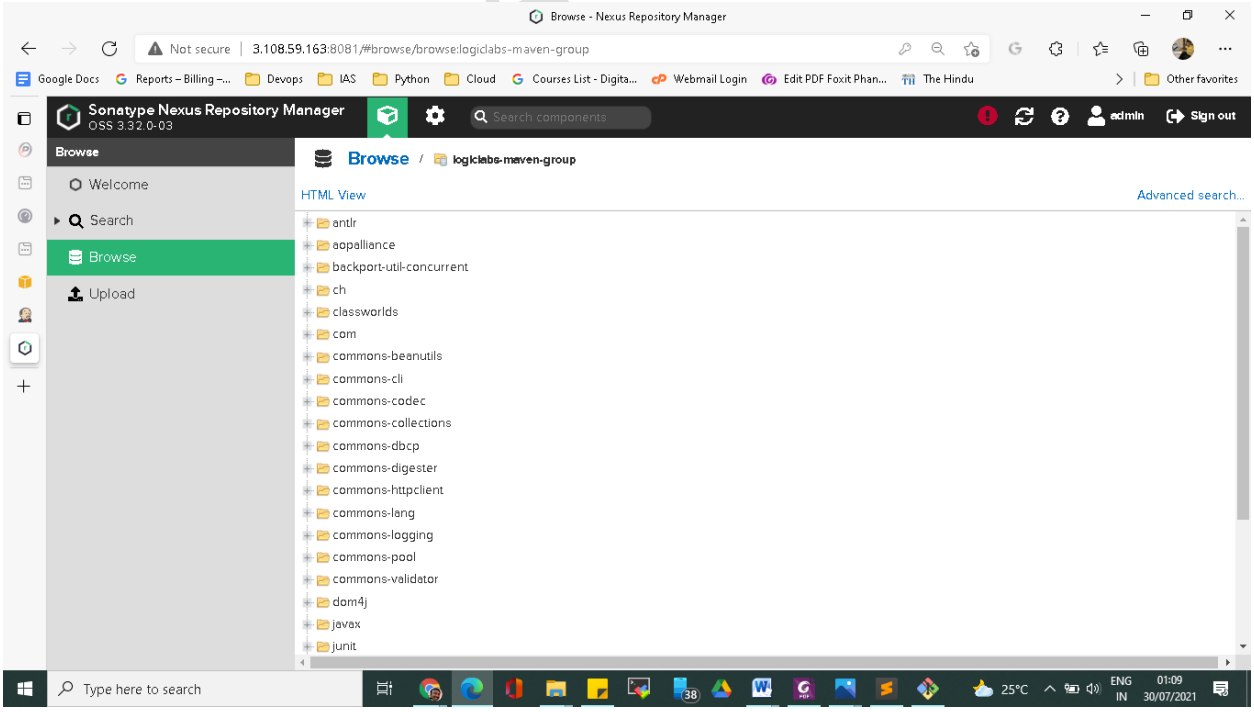




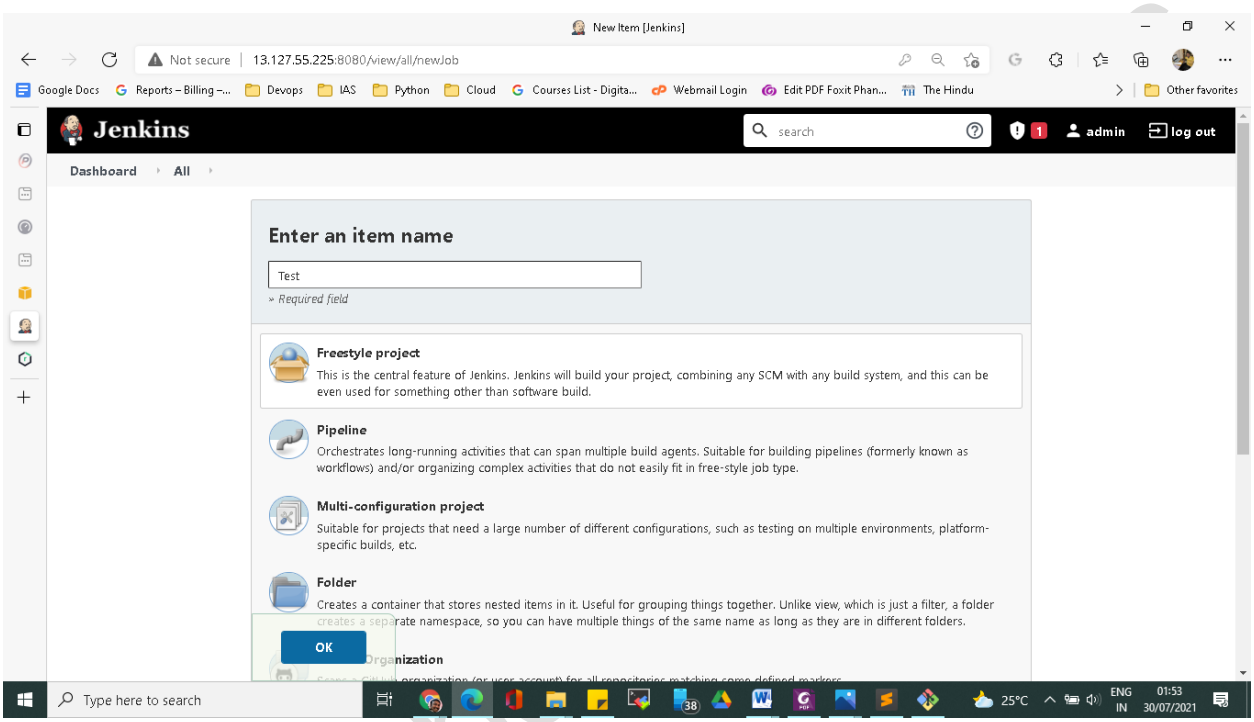

**After the build is successful, proceed to the next steps as given below.**

**Verify whether the dependencies are getting created in the nexus repo :**

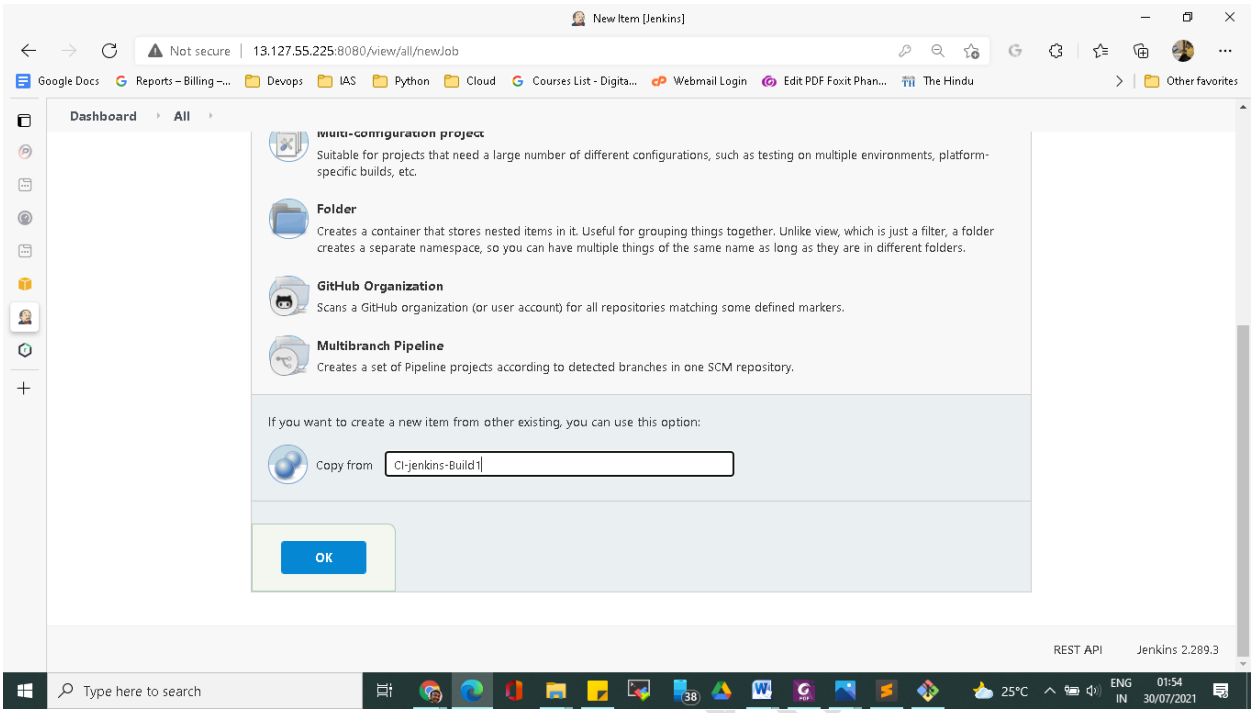


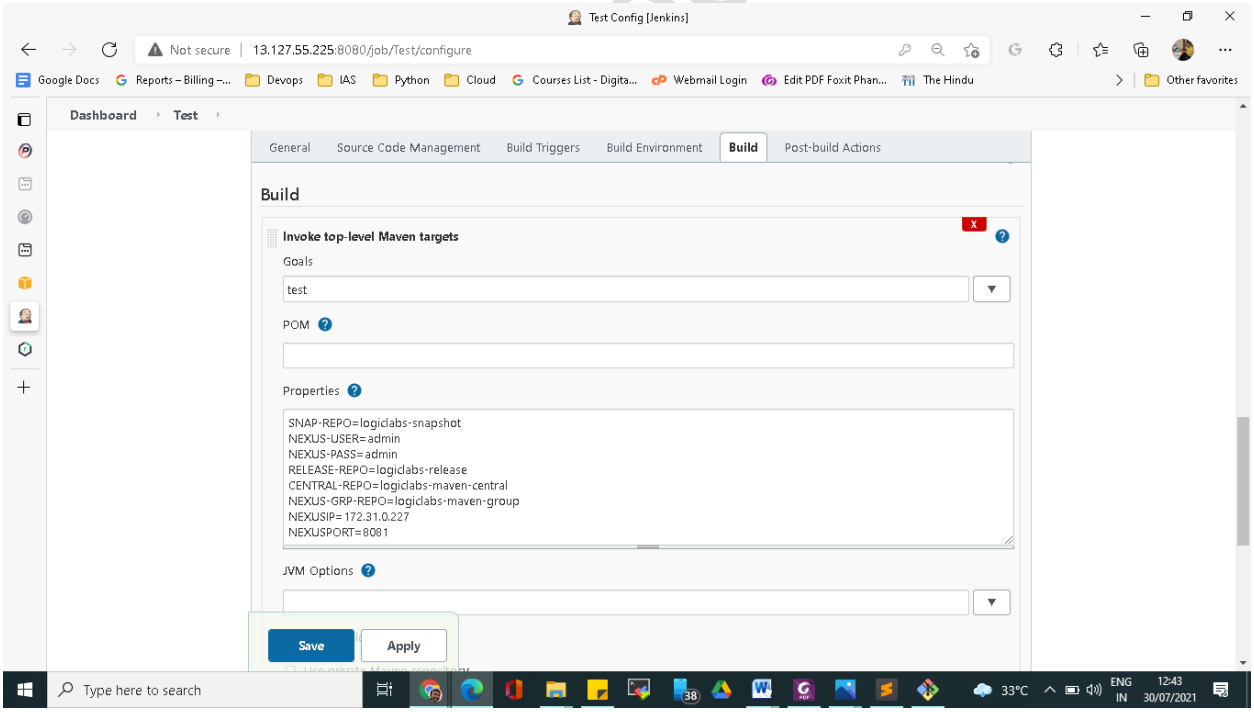
Create the second job:

Name it as “Test” or “Unit-Test”.

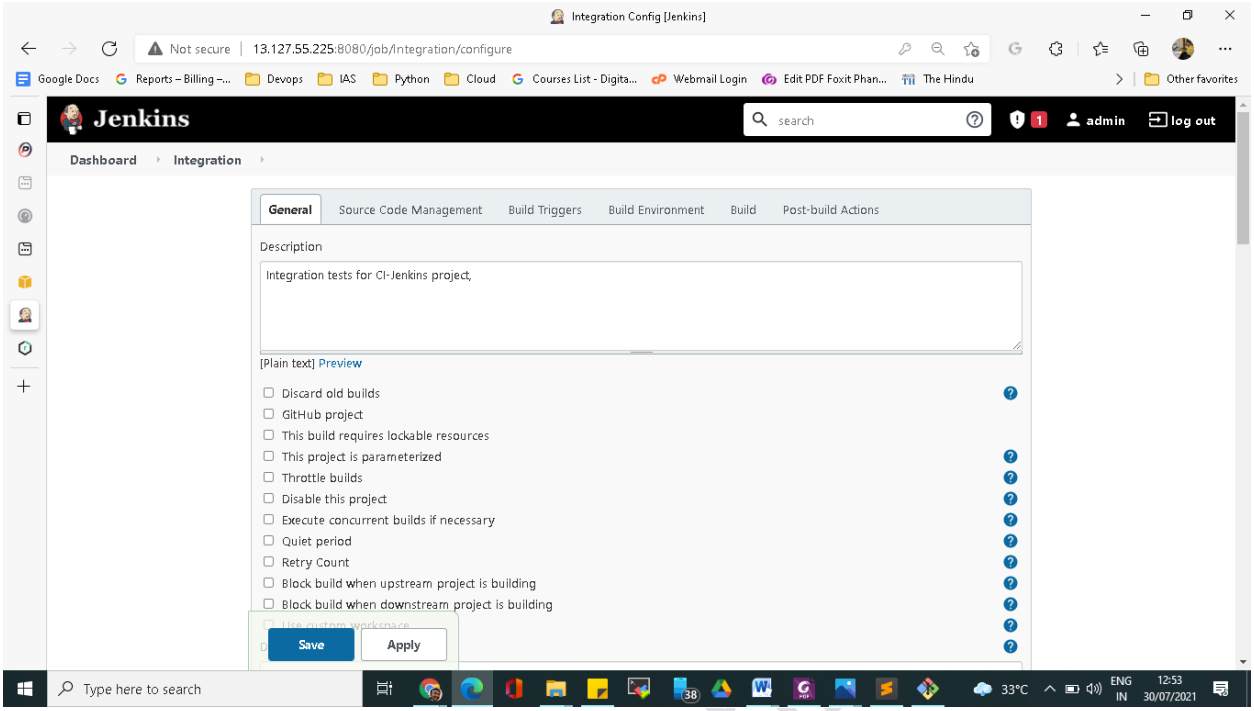


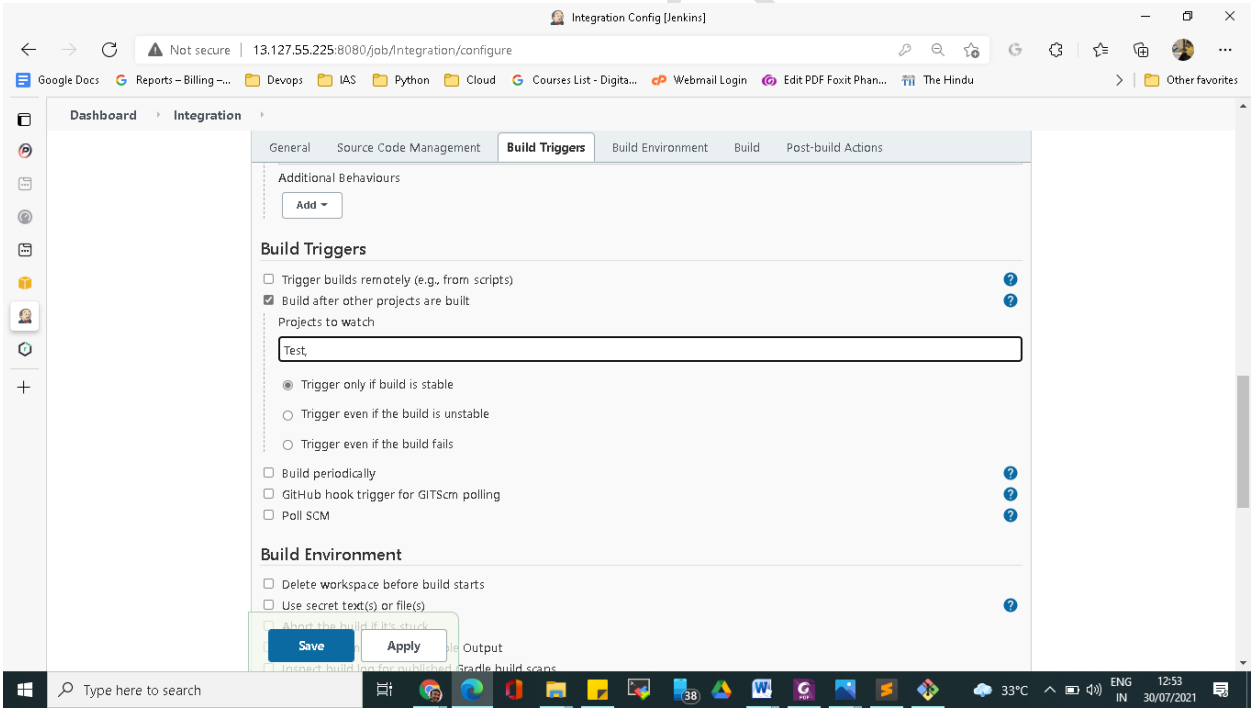

Select freestyle and copy everything from Build job. For this select the last option in the screen and give the name of the job to be copied from.



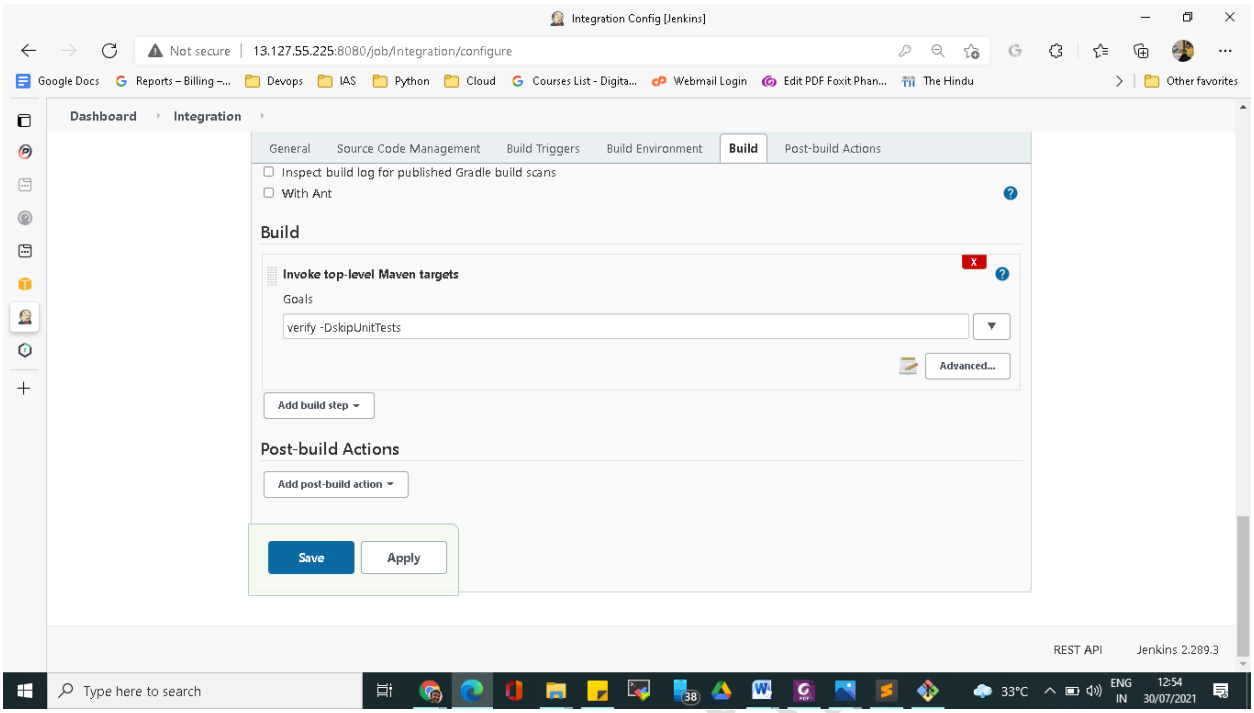

Similarly create another job for performing “integration Tests”.

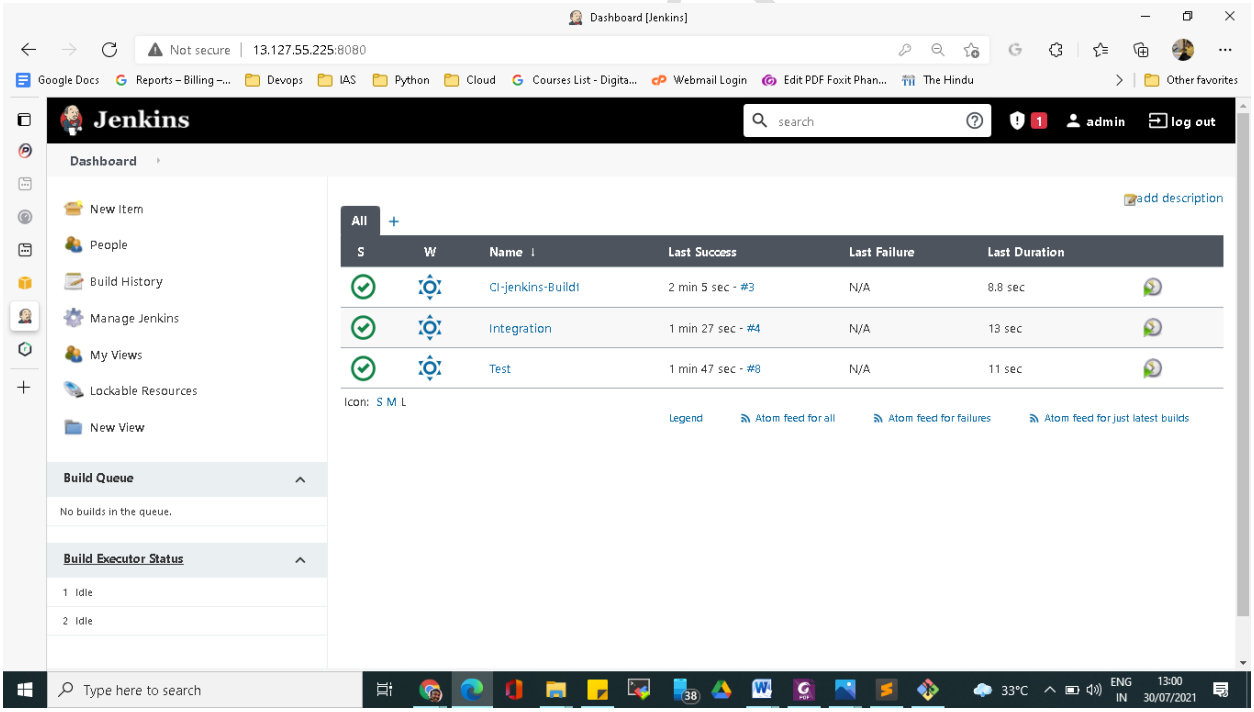


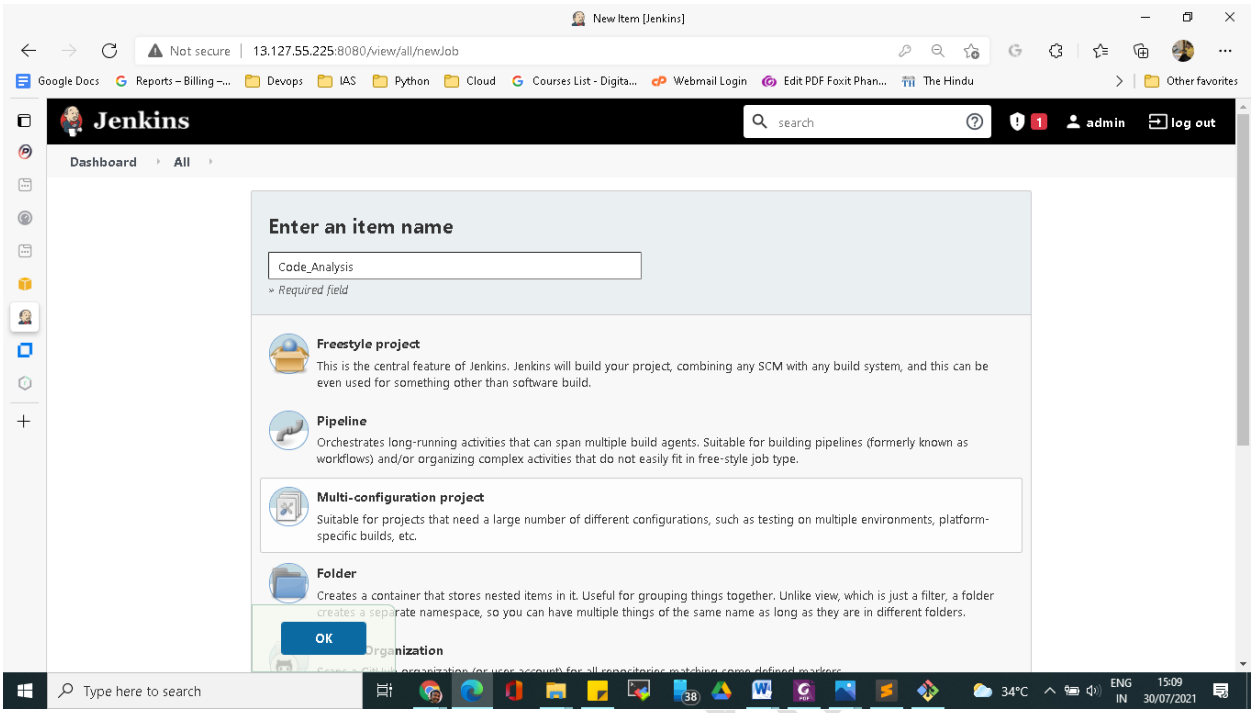

Change maven build goals as follows:

For Test job - test
For Integration -> verify -DskipUnitTests



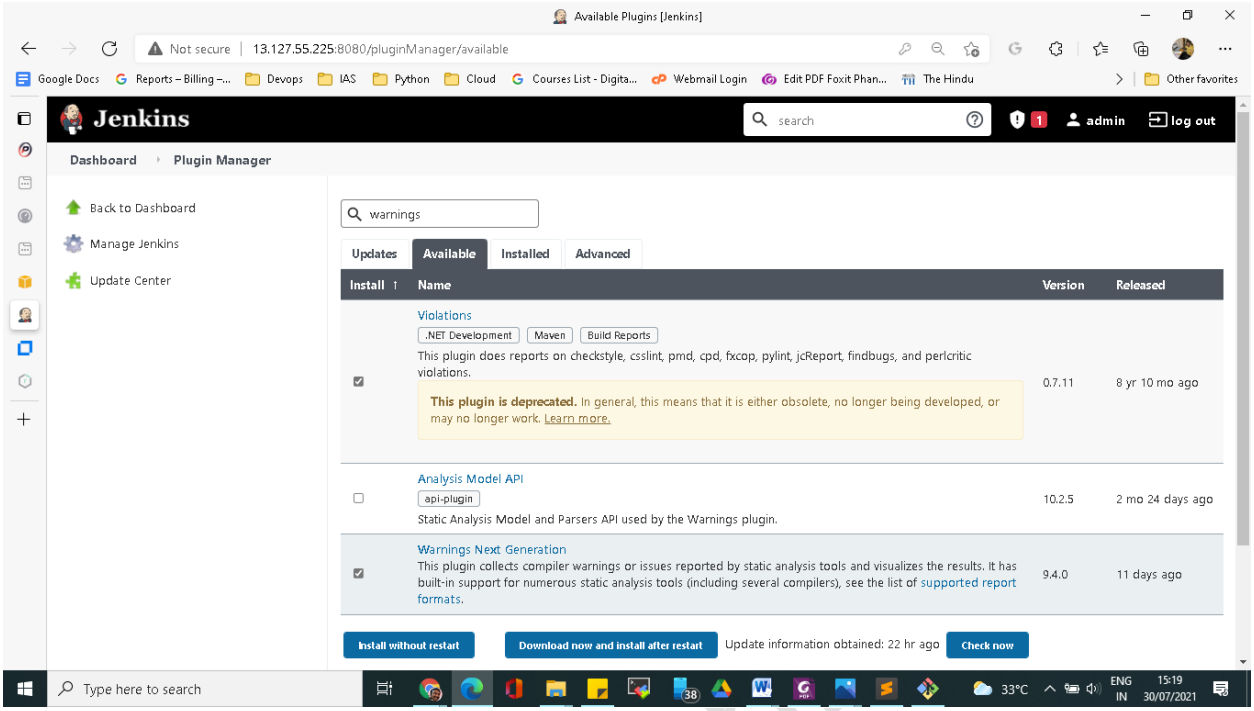

Inorder to perform static code analysis, we create a new step and name it code-analysis (you can name it as you wish).

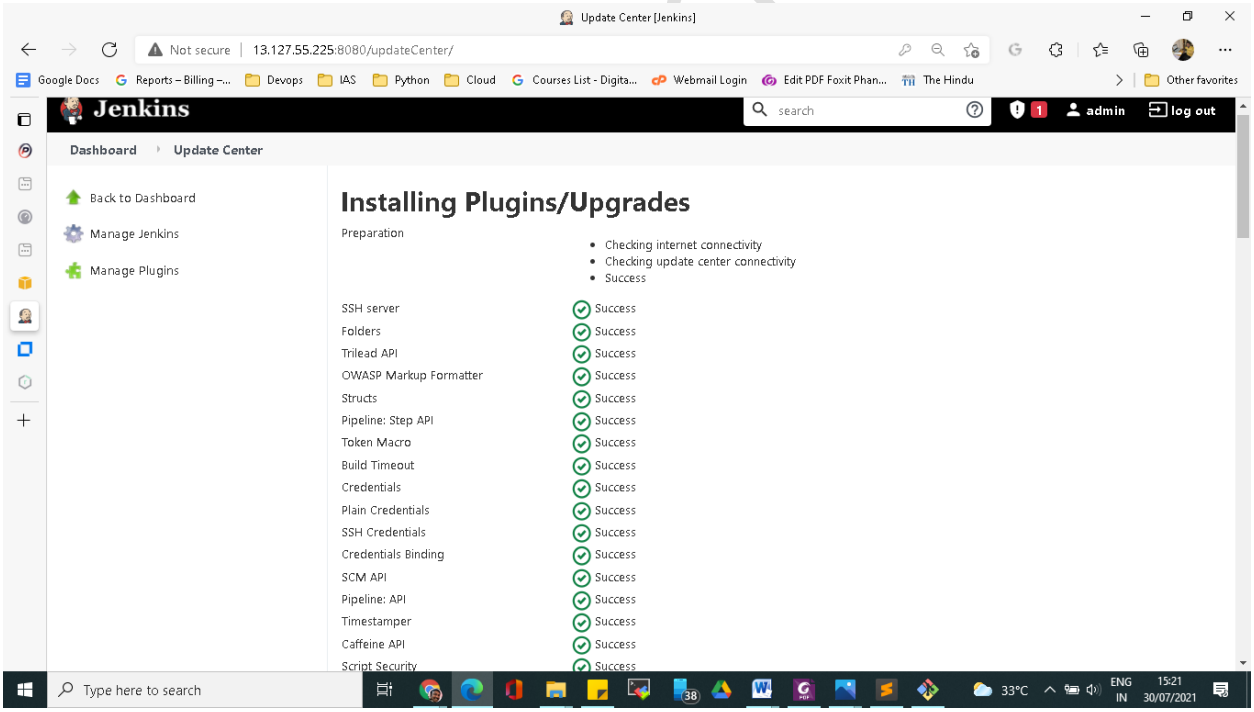



Select copying settings from build pipeline and Click on ok

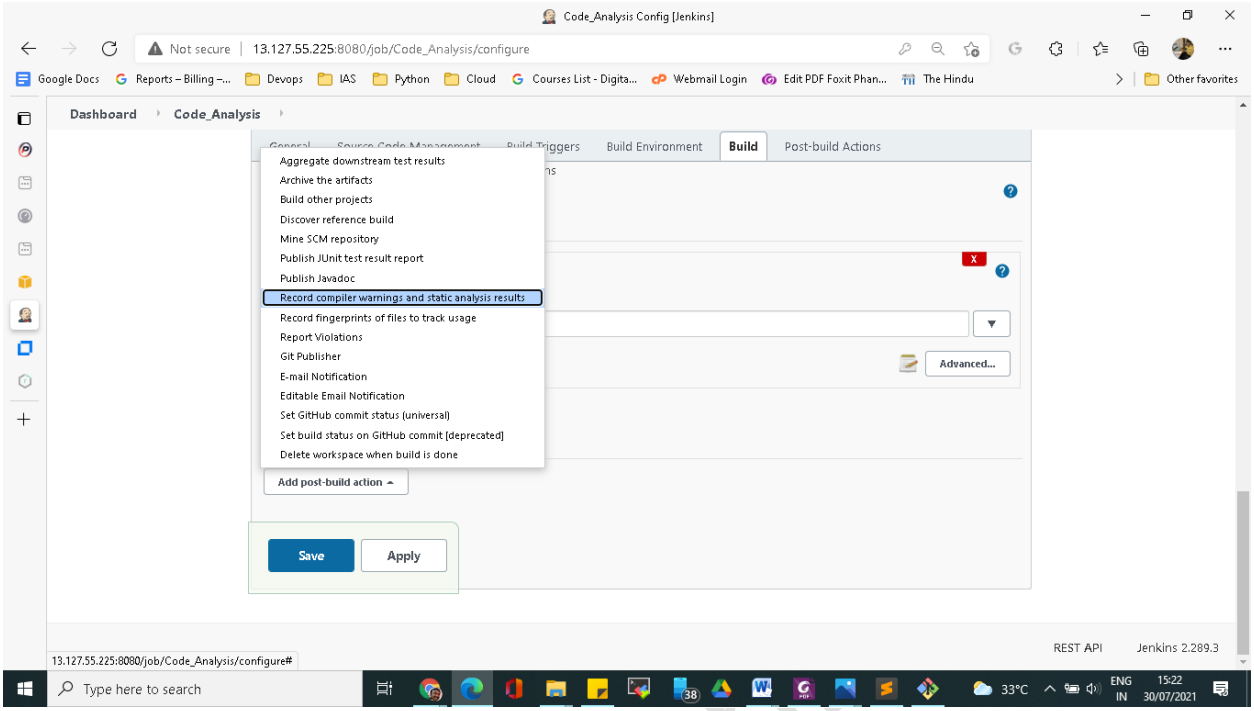
Install jenkins  plugins :

→ Warnings next generation plugin

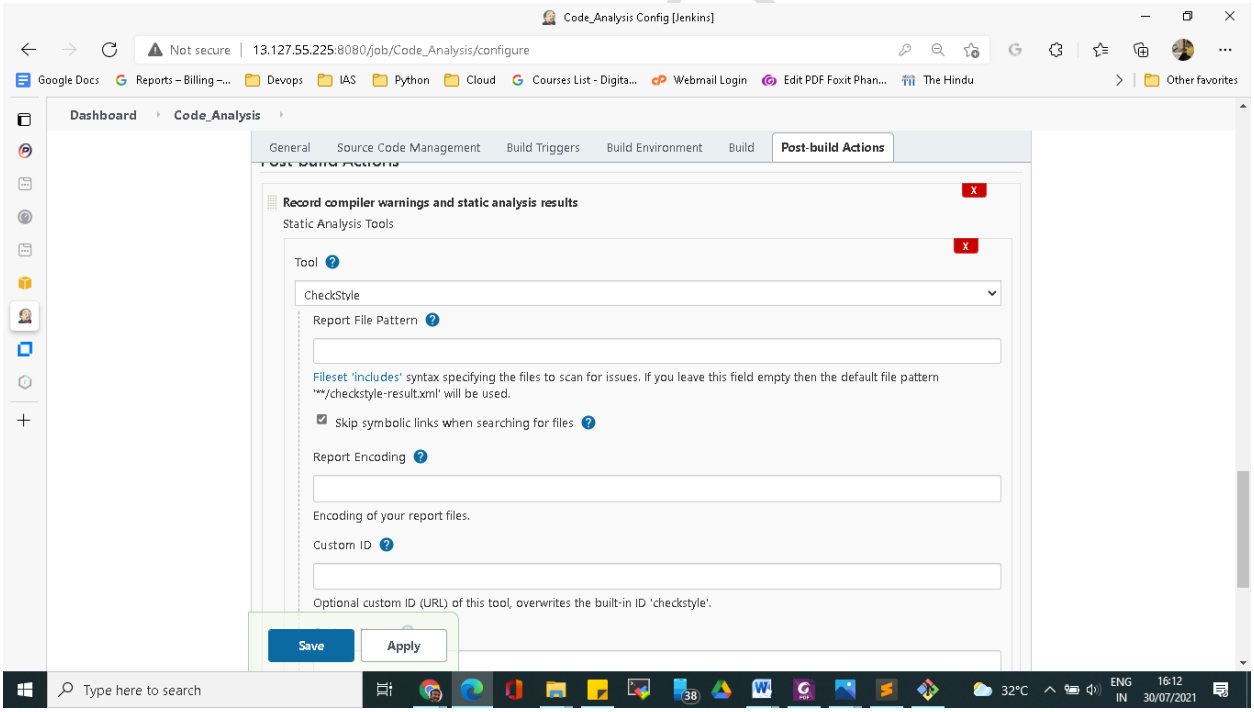


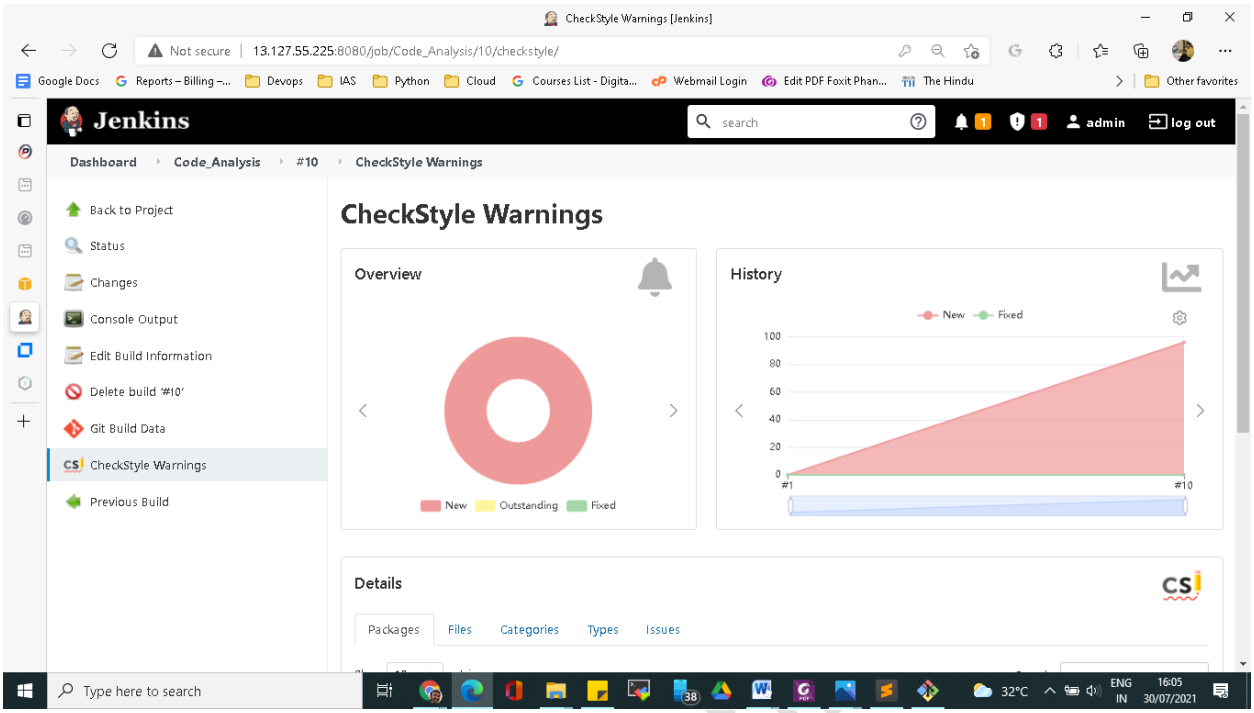

Add a post build action to record compiler warnings and static analysis results

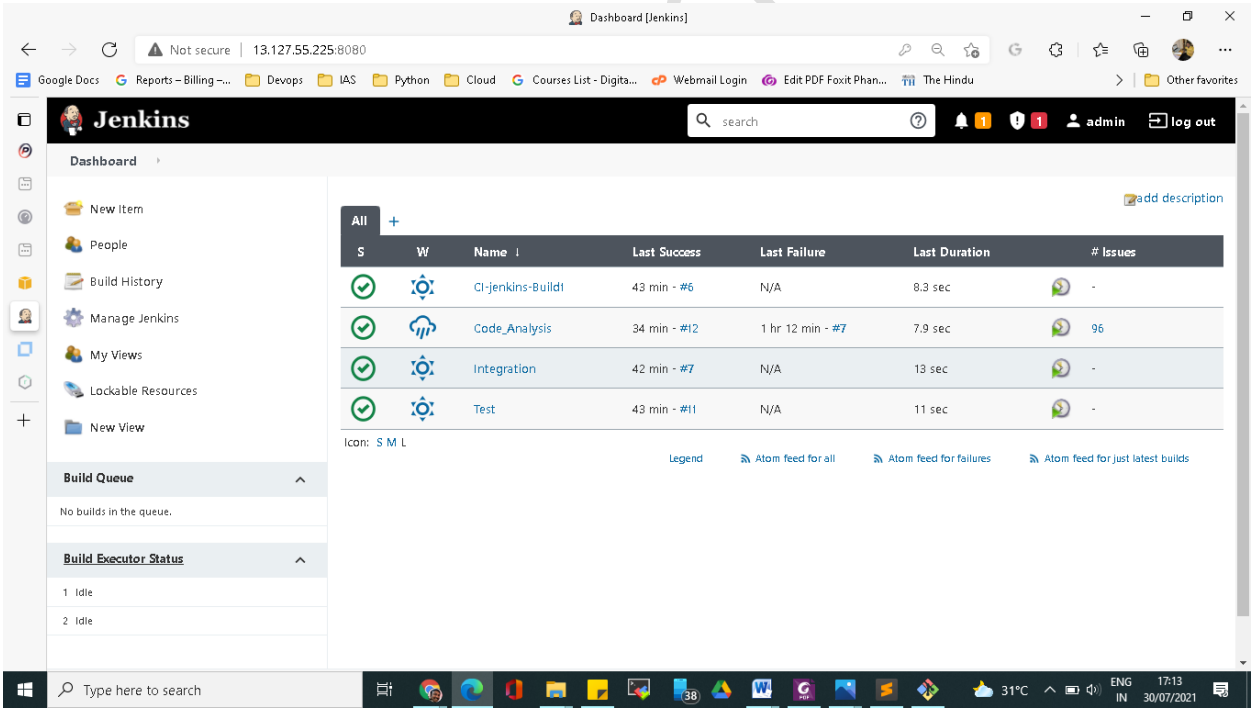



In the tools option, select Checkstyle.



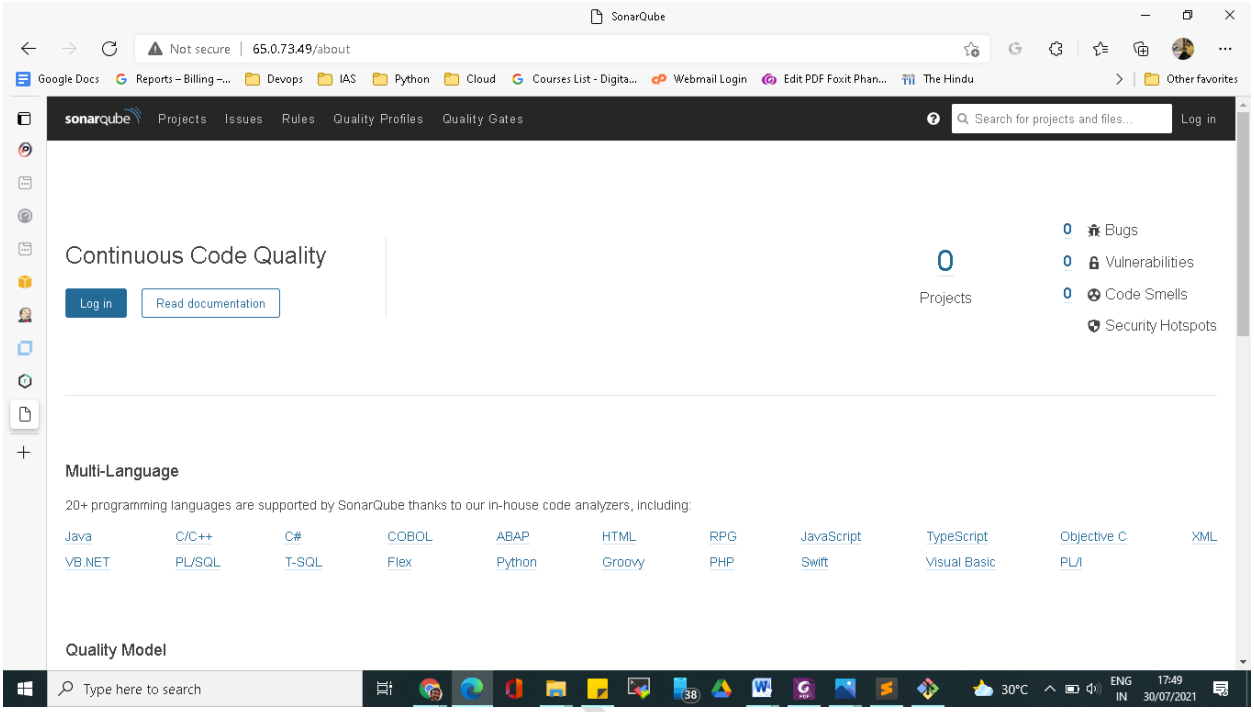

Run the job with other settings same. After success observe the checkstyle results as shown below.

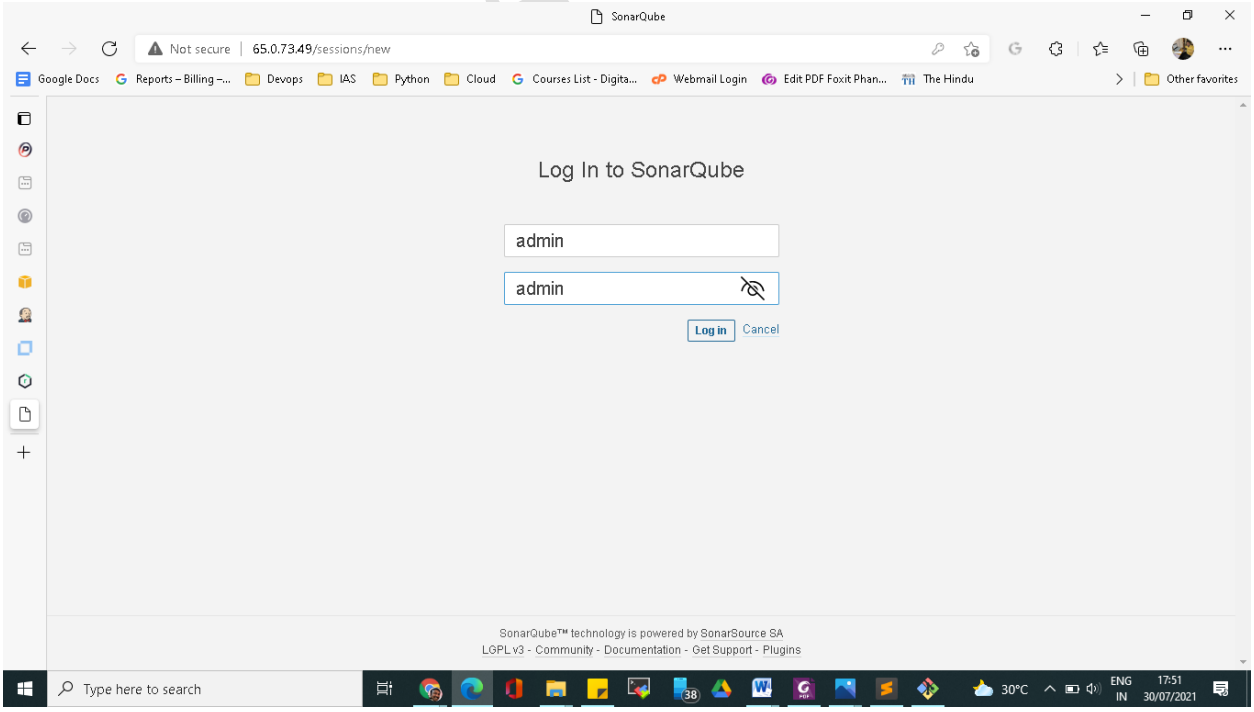

CheckStyle Warnings [Jenkins]
Not secure | 13.127.55.225:8080/job/Code_Analysis/10/checkstyle/
Jenkins
search
admin
log out
Dashboard
Code_Analysis
#10
CheckStyle Warnings
Back to Project
Status
Changes
Console Output
Edit Build Information
Delete build '#10'
Git Build Data
CheckStyle Warnings
Previous Build
CheckStyle Warnings
Overview
New
Outstanding
Fixed
History
New
Fixed
100
80
60
40
20
0
#1
#10
Details
Packages
Files
Categories
Types
Issues
Type here to search
32°C
ENG
IN
16:05
30/07/2021


Dashboard [Jenkins]
Not secure | 13.127.55.225:8080
Jenkins
search
admin
log out
Dashboard
New Item
People
Build History
Manage Jenkins
My Views
Lockable Resources
New View
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
add description
All
S
W
Name
Last Success
Last Failure
Last Duration
# Issues
CI-jenkins-Build1
43 min - #6
N/A
8.3 sec
-
Code_Analysis
34 min - #12
1 hr 12 min - #7
7.9 sec
96
Integration
42 min - #7
N/A
13 sec
-
Test
43 min - #11
N/A
11 sec
-
Icon: S M L
Legend
Atom feed for all
Atom feed for failures
Atom feed for just latest builds
Type here to search
31°C
ENG
IN
17:13
30/07/2021

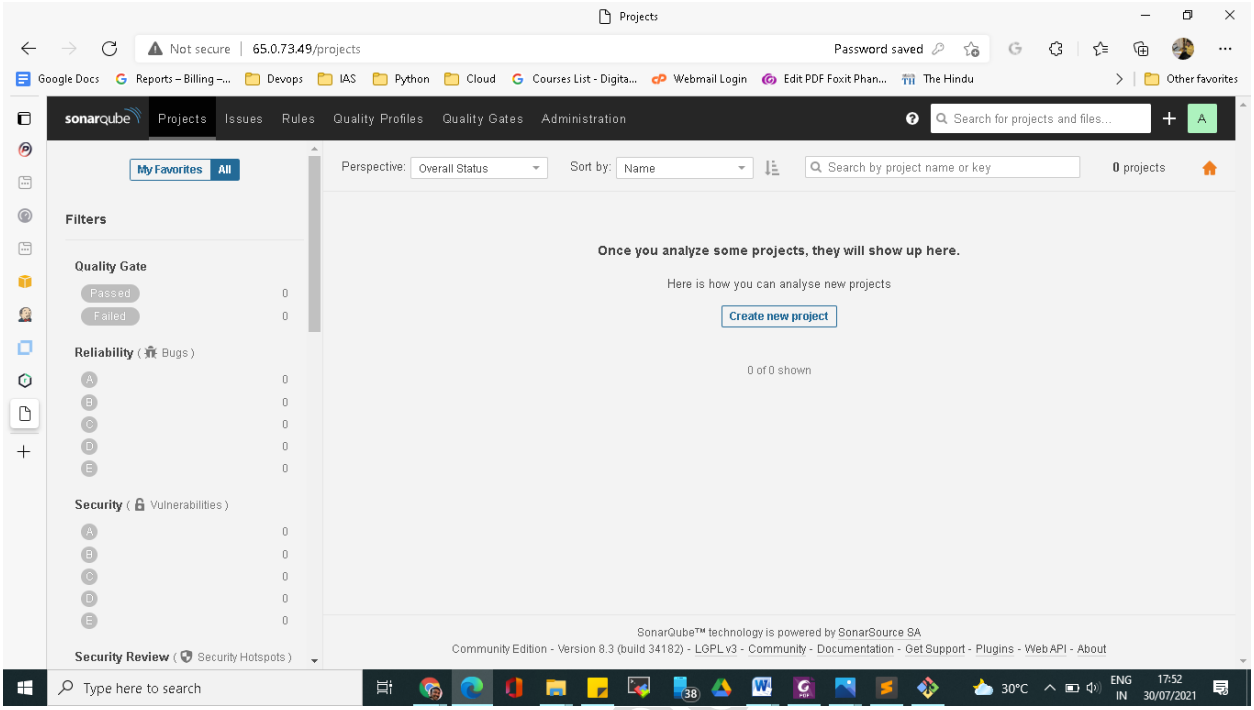
## SONAR QUBE configuration:

Login to sonarQube with public IP.Usually Sonar Qube works on port 9000, however as we are installing it along with Nginx, we need not provide any port number after public ip in the browser to access sonar.

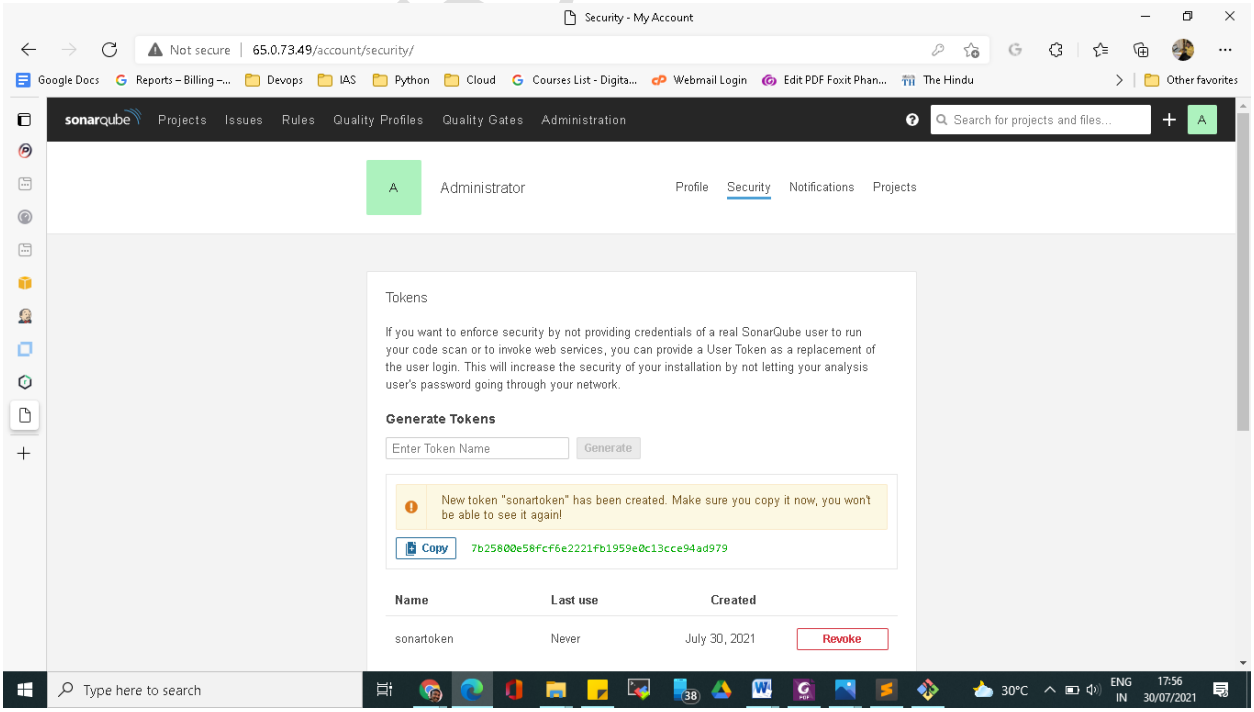


Change the default password afterwards.



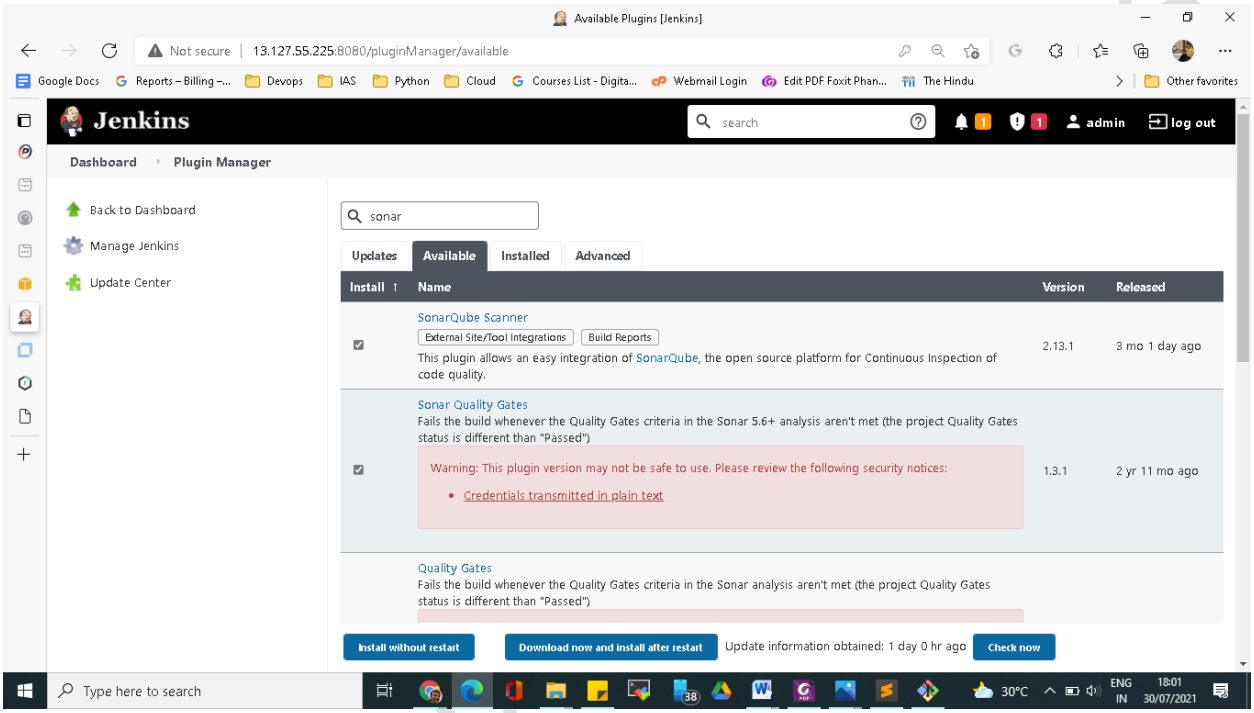

Go to Administrator → my account → security→ Generate tokens



Create a token by the name sonartoken. Copy the token and use it in jenkins.

Get sonar plugin in Jenkins:

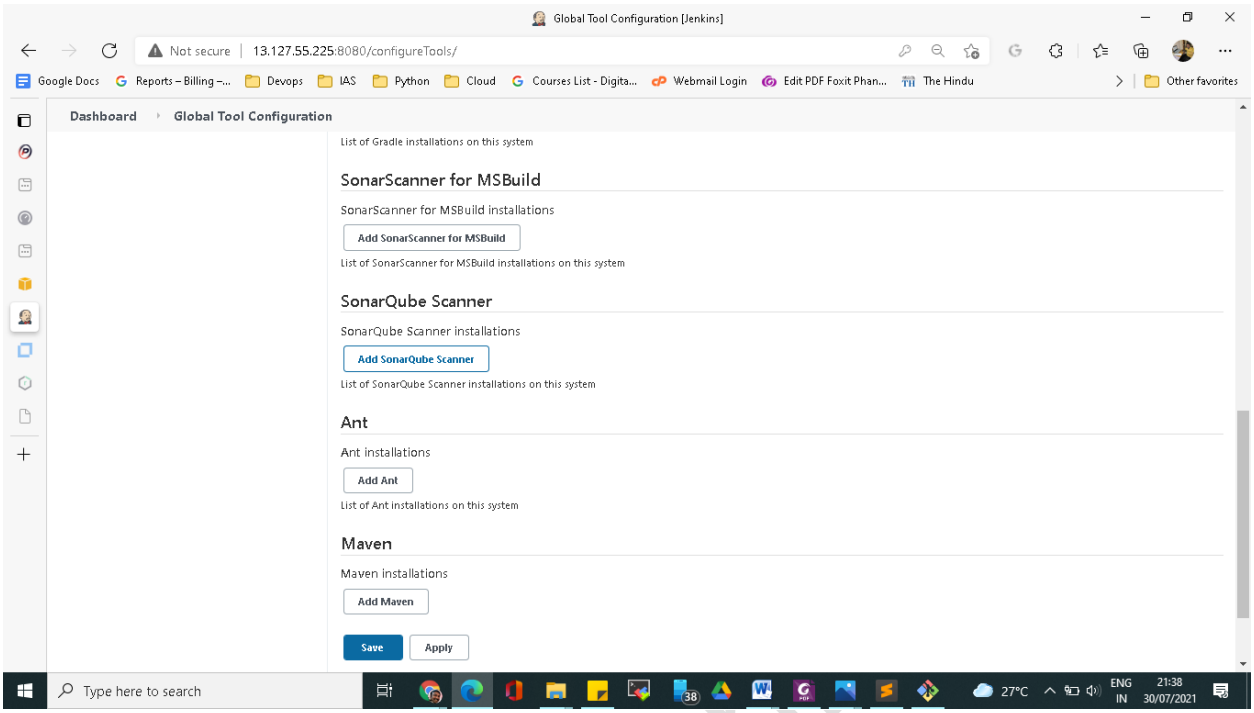
Jenkins → manage jenkins → manage plugins → Available

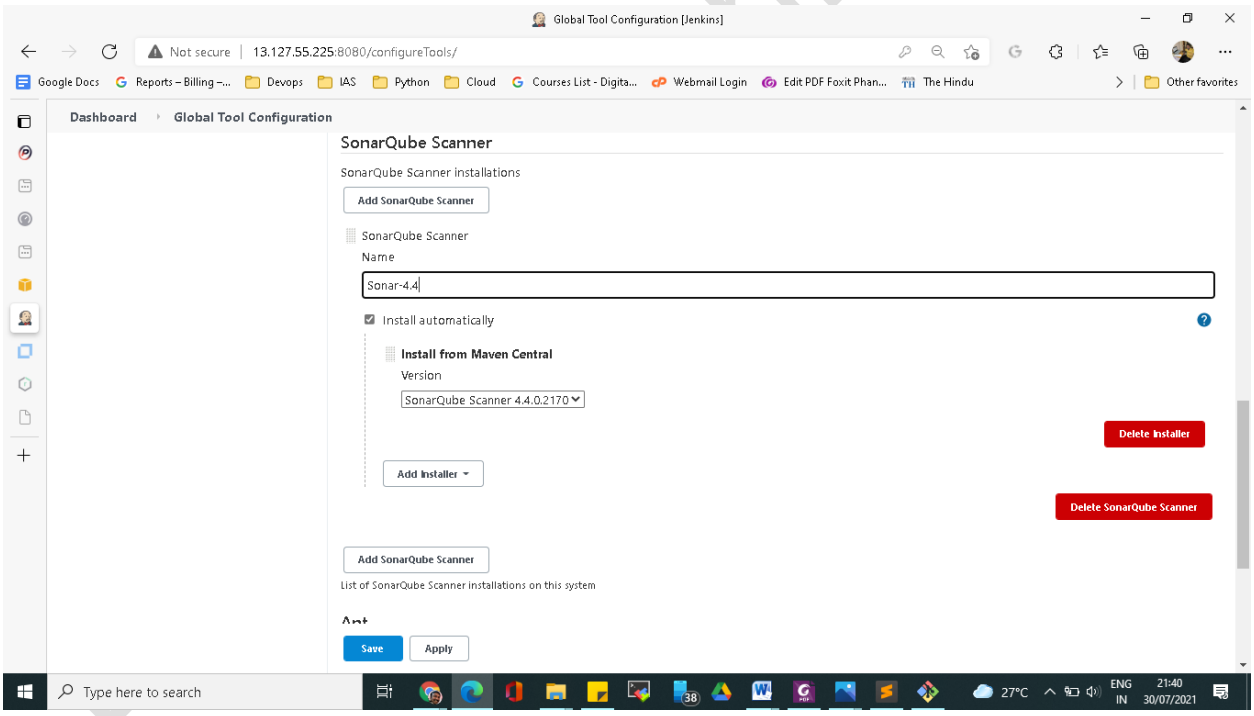



Note: If these plugins are deprecated by the time this document is used, please look for alternatives…

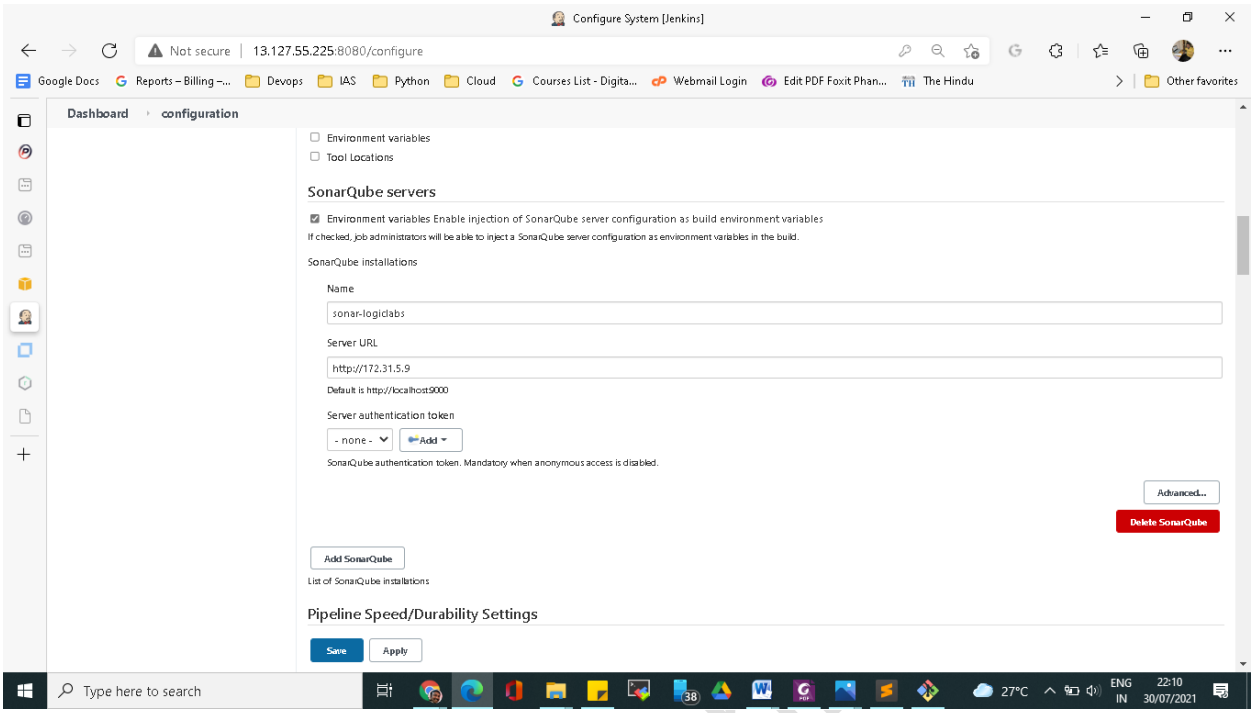
Configure sonar in jenkins:

Global tool configuration→

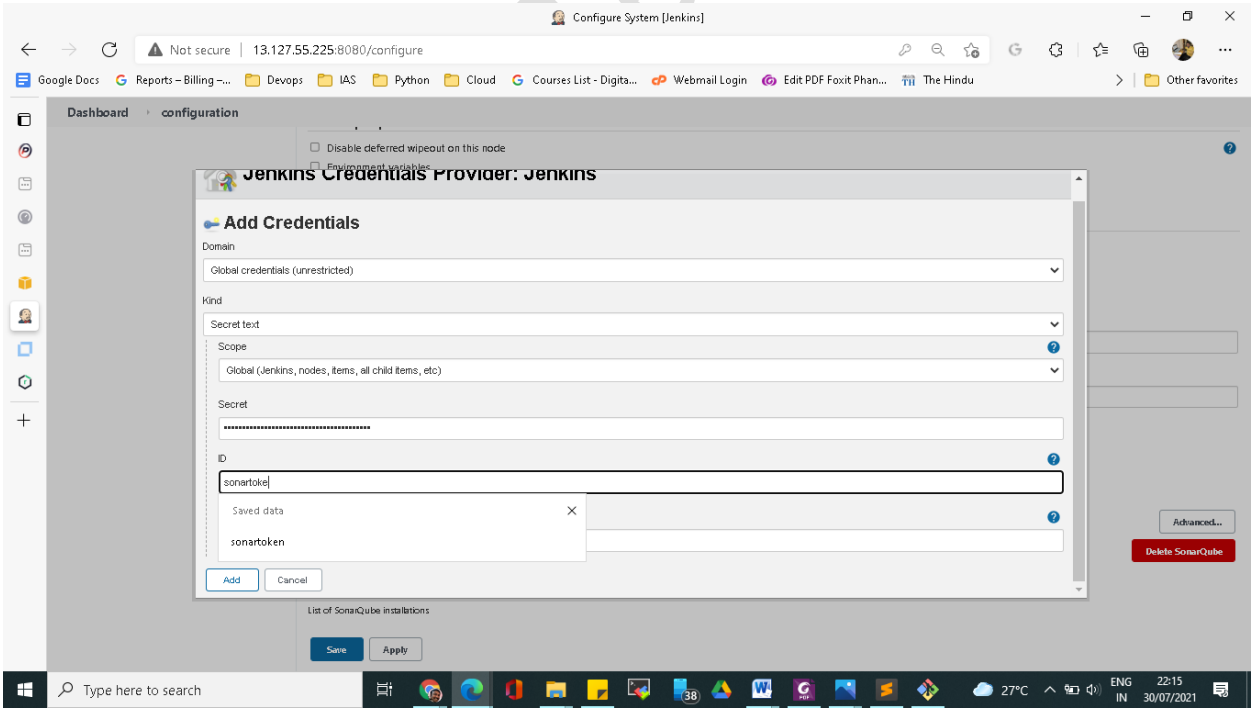



Goto jenkins→ configuration→ add sonar and enable environmental variables



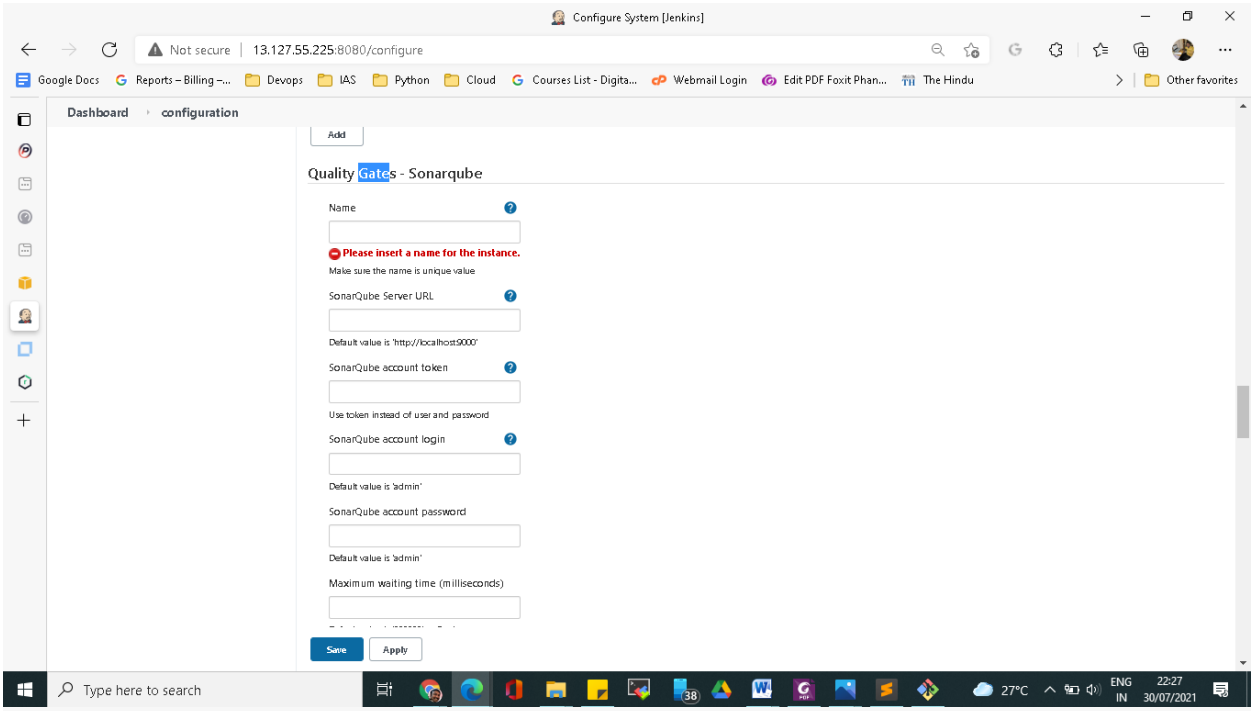

Select add credentials to add sonar token. If it doesn't open, save without adding a token and later reopen the configuration page and check again.

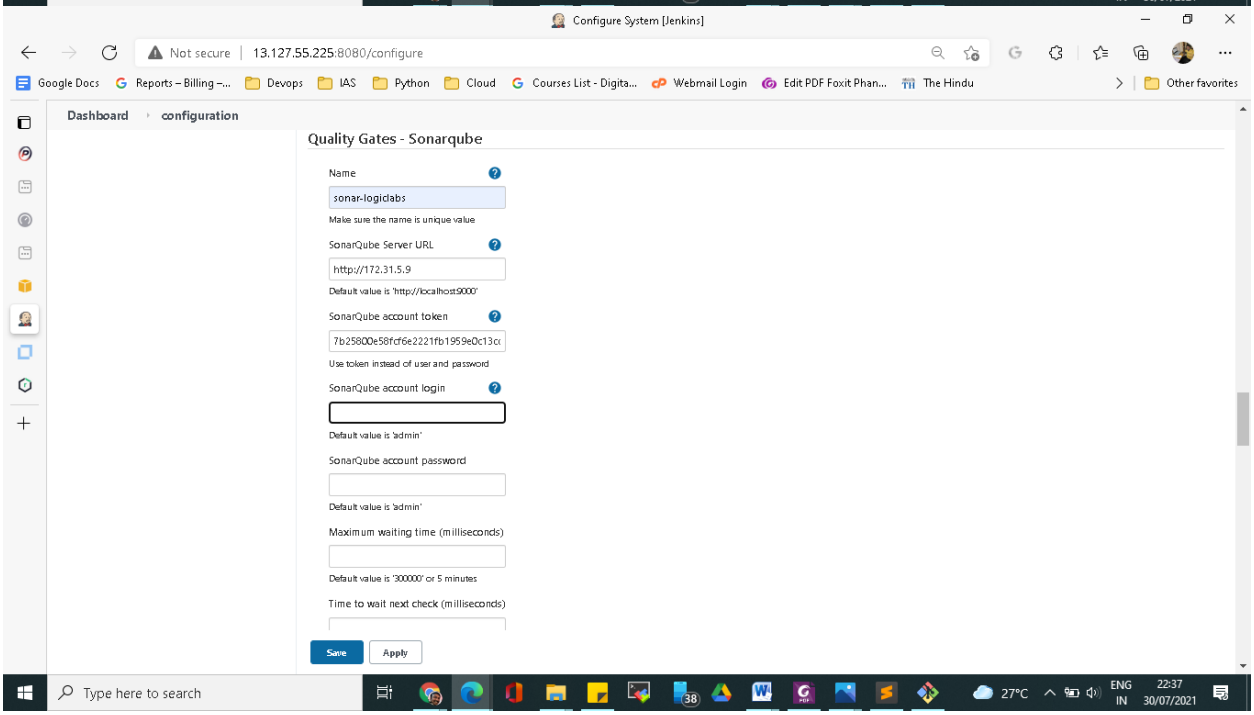



save the configuration after adding the sonar token at the sonar authentication token.

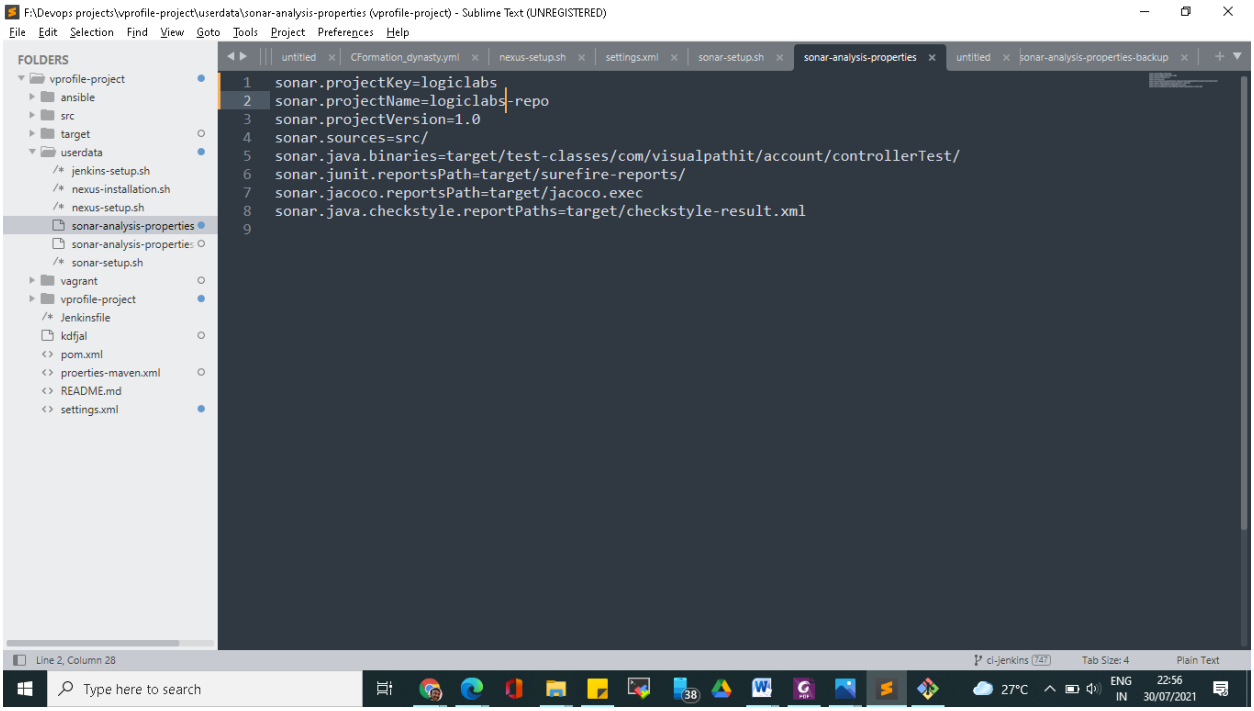
Quality gates give us the option to pass the build to next stages if only certain criteria are fulfilled.

Sample Quality Gate configuration is given below.



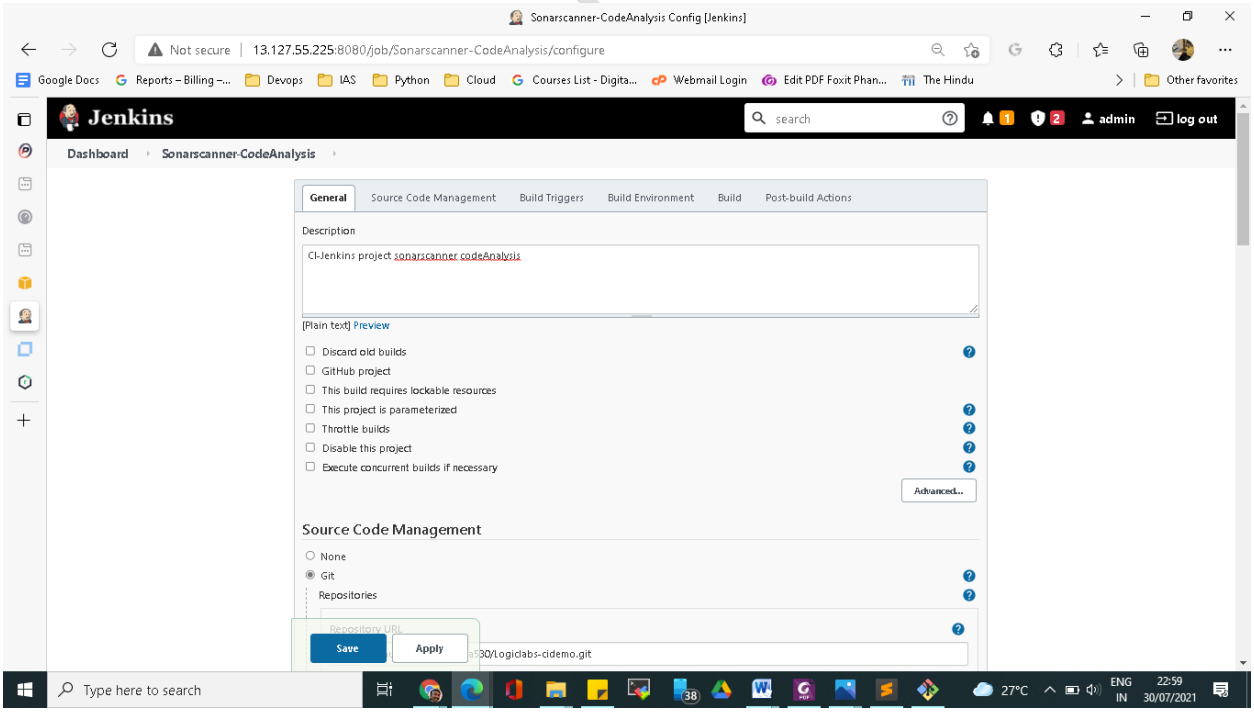



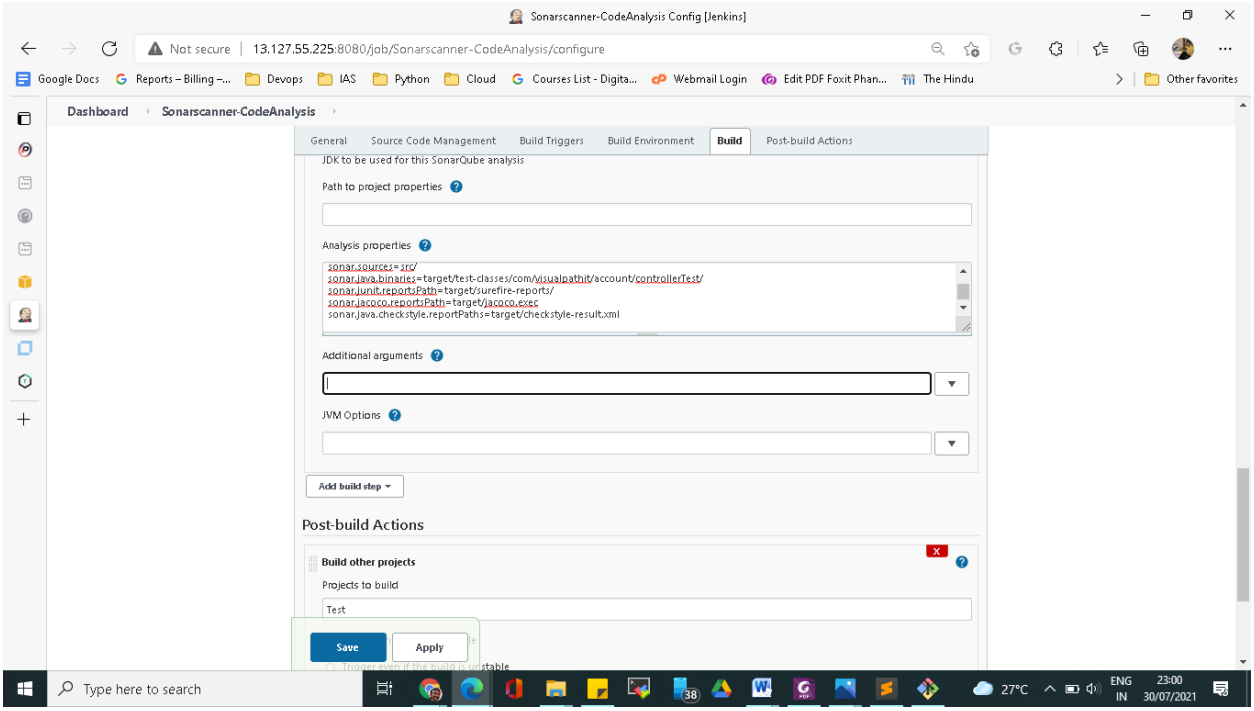

Save quality gates configuration



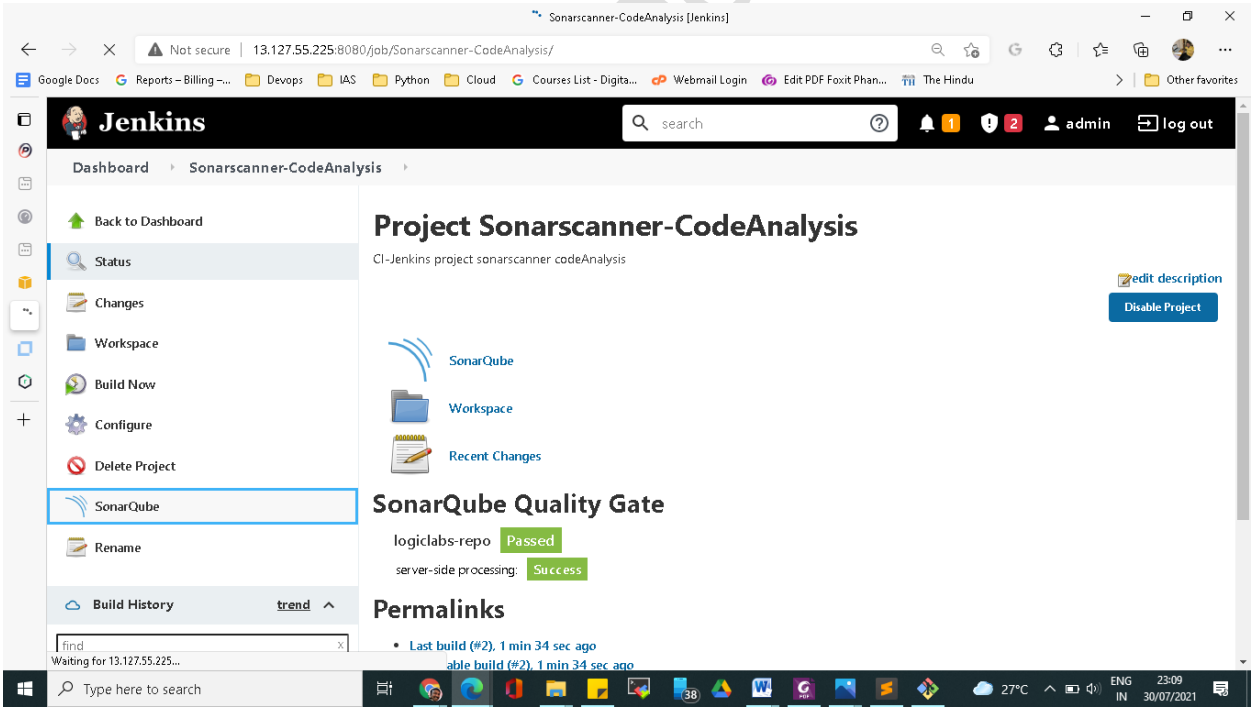

copy the sonar analysis properties from the file in the source directory with name ‘sonar-analysis-properties’.

Add a new job in jenkins for sonar scanner code analysis.





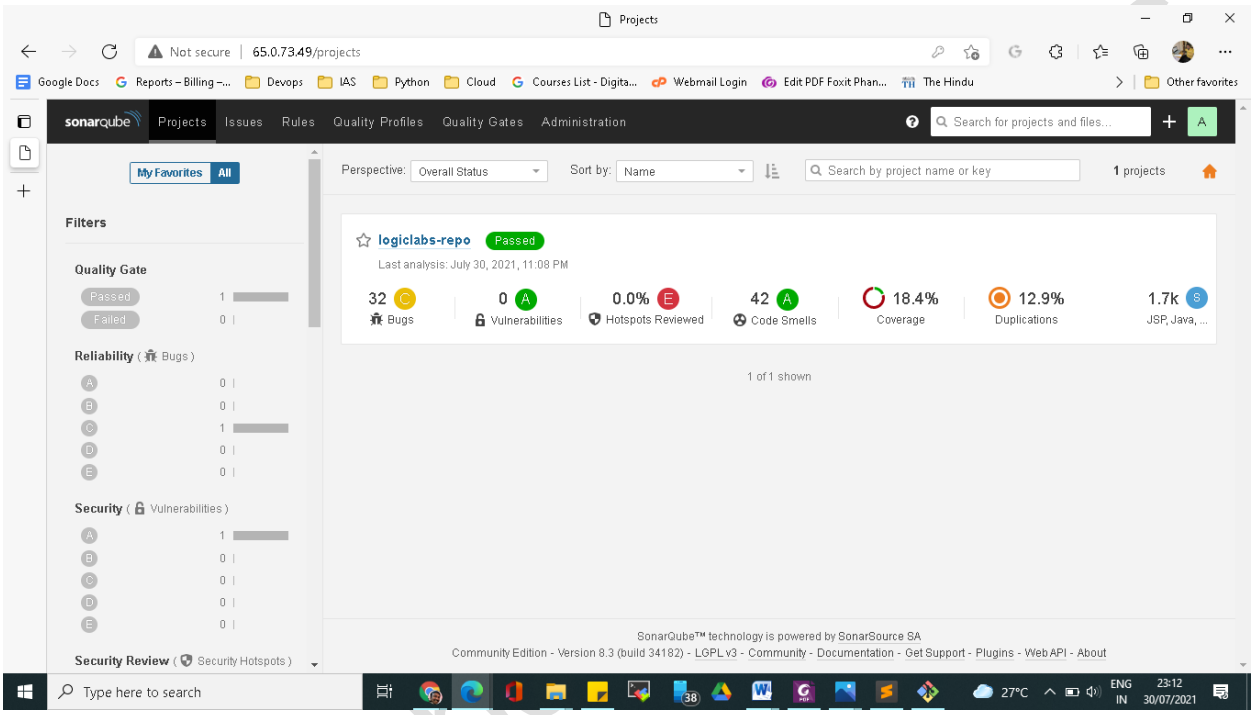

copy paste the variables from the file above mentioned.



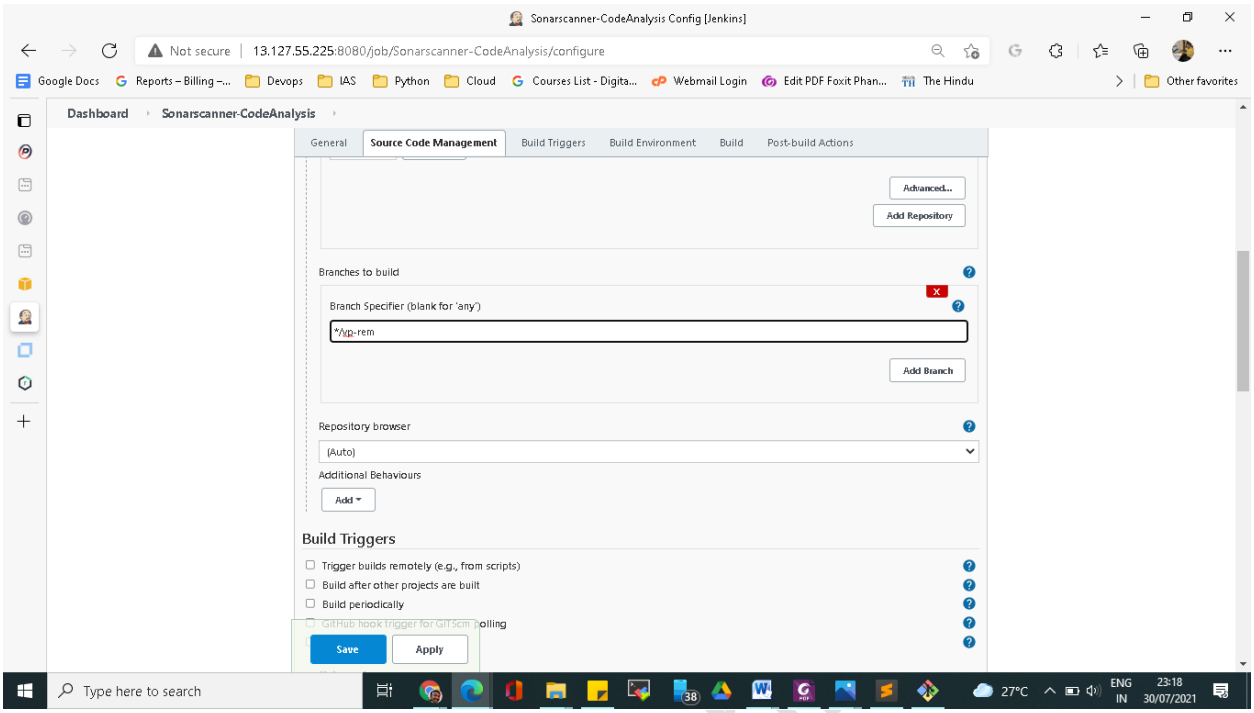

If the build fails because of checkstyle issues, it can be removed from maven targets step for this demonstration.

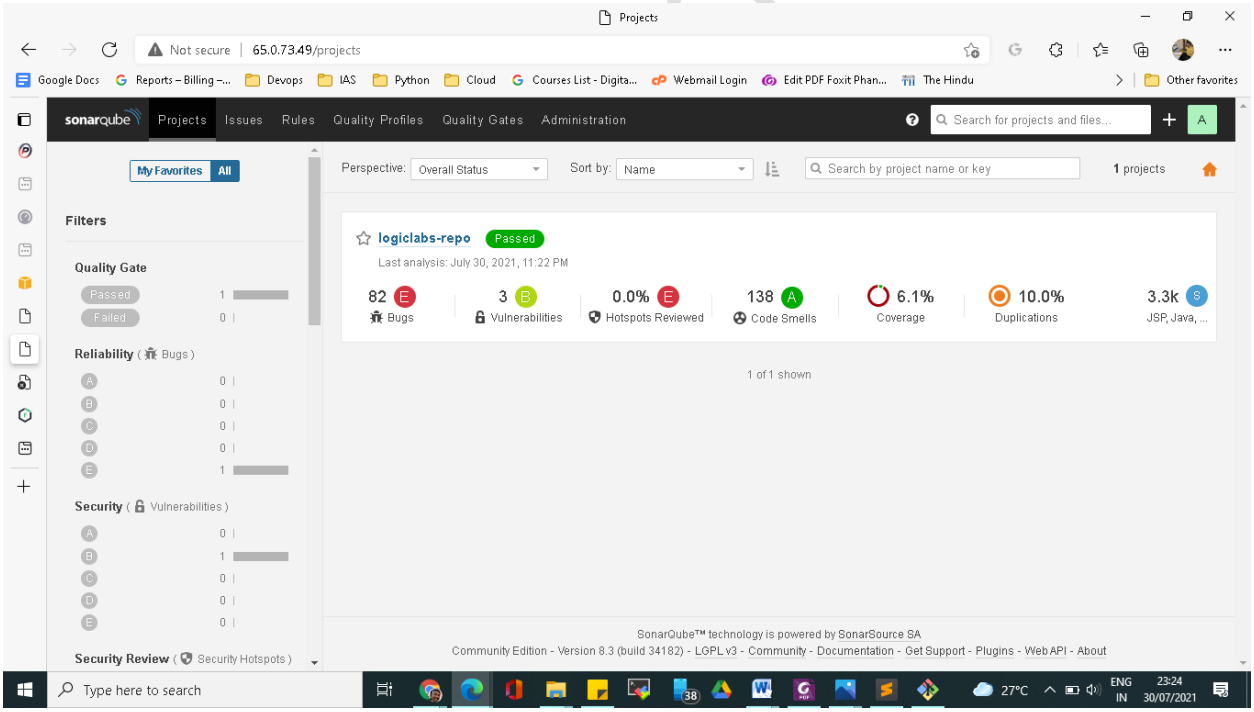
Verification of Static code Analysis from sonar server:

After Jenkins job is complete, login to sonar server to verify and obtain the static code analysis results.



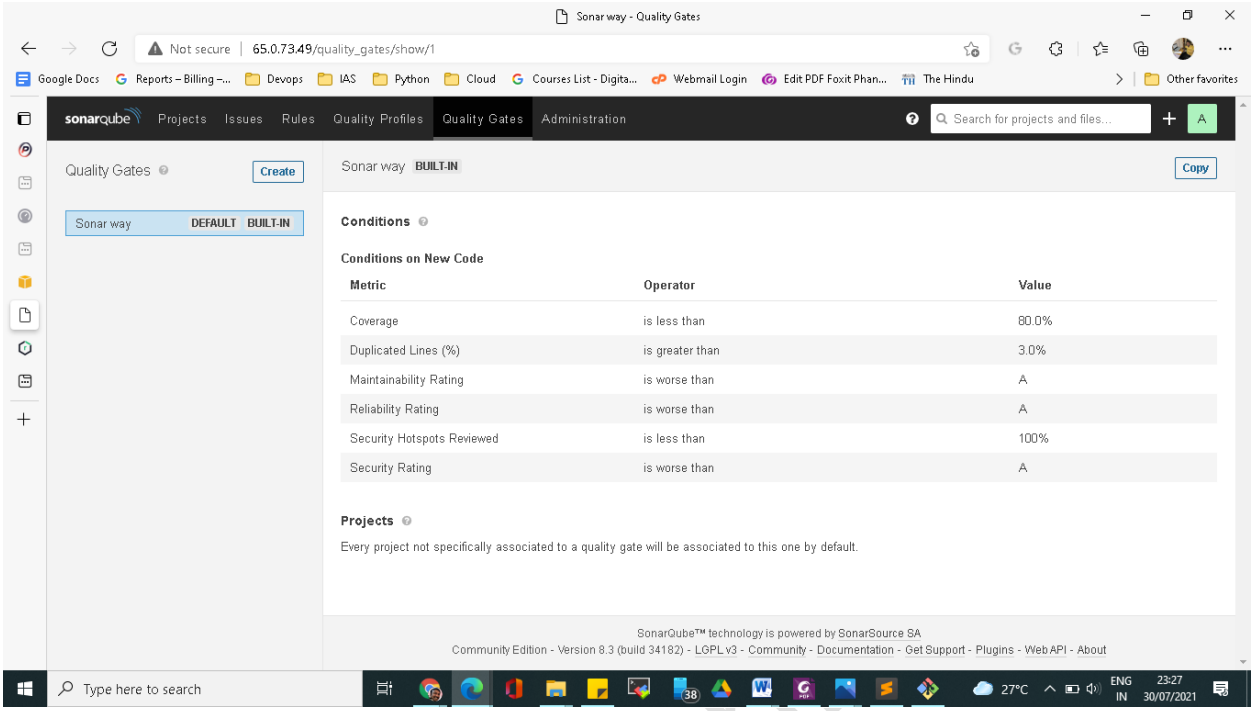

(Optional)For experimentation purposes, the name of the branch in the jenkins job can be changed to vp-rem and check the sonar results after running the job.

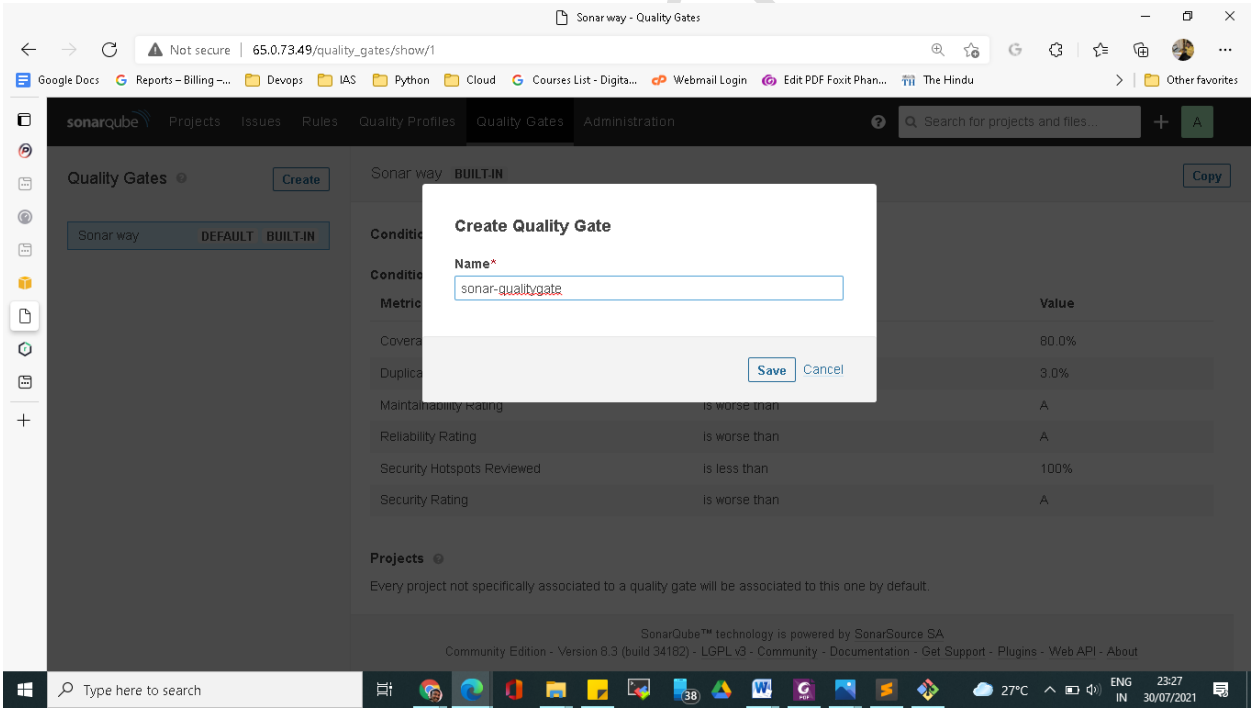


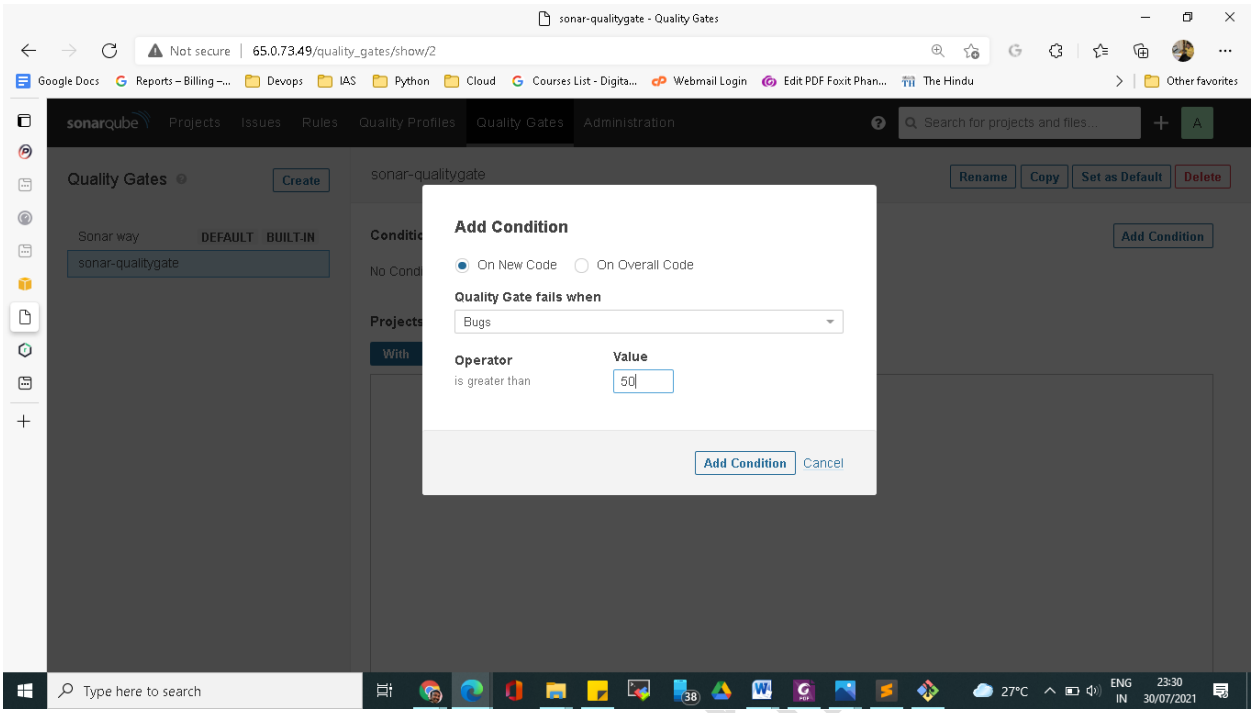



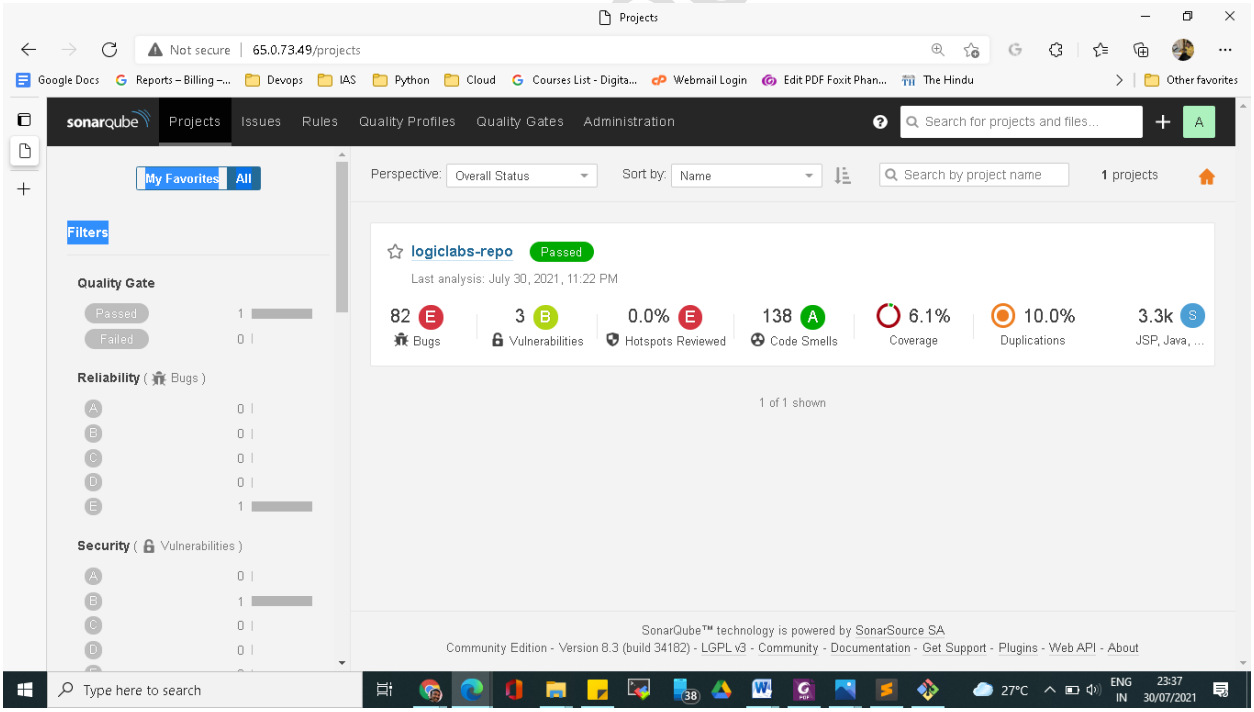

Creating Quality Gates:

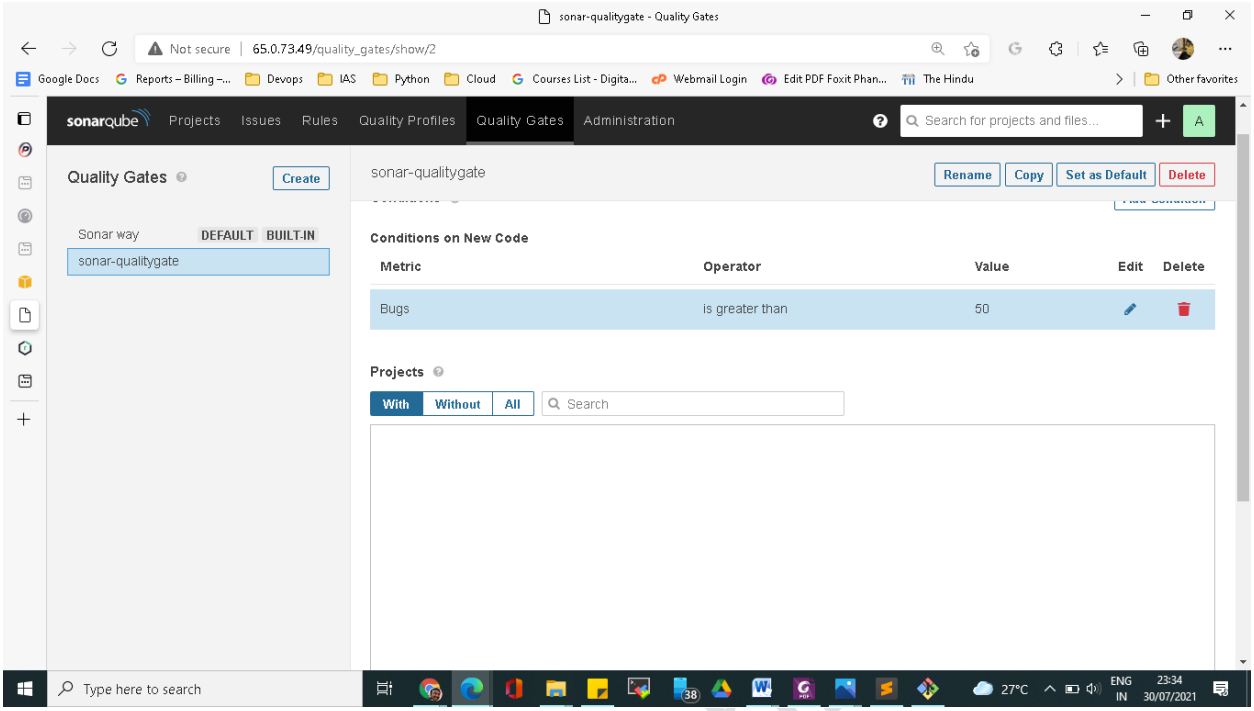
The below screenshot shows how to configure Quality gates.


Sonar way - Quality Gates
Not secure | 65.0.73.49/quality_gates/show/1
sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
Quality Gates
Create
Sonar way DEFAULT BUILT-IN
Sonar way BUILT-IN
Copy
Conditions
Conditions on New Code
Metric
Operator
Value
Coverage
is less than
80.0%
Duplicated Lines (%)
is greater than
3.0%
Maintainability Rating
is worse than
A
Reliability Rating
is worse than
A
Security Hotspots Reviewed
is less than
100%
Security Rating
is worse than
A
Projects
Every project not specifically associated to a quality gate will be associated to this one by default.
SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 8.3 (build 34182) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About
Type here to search
27°C
ENG
IN
23:27
30/07/2021


Sonar way - Quality Gates
Not secure | 65.0.73.49/quality_gates/show/1
sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
Quality Gates
Create
Sonar way DEFAULT BUILT-IN
Sonar way BUILT-IN
Copy
Create Quality Gate
Name*
sonar-qualitygate
Save
Cancel
Value
80.0%
3.0%
A
is worse than
A
Reliability Rating
is worse than
A
Security Hotspots Reviewed
is less than
100%
Security Rating
is worse than
A
Projects
Every project not specifically associated to a quality gate will be associated to this one by default.
SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 8.3 (build 34182) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About
Type here to search
27°C
ENG
IN
23:27
30/07/2021


sonar-qualitygate - Quality Gates
Not secure | 65.0.73.49/quality_gates/show/2
sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
Quality Gates
Create
Sonar way
DEFAULT
BUILT-IN
sonar-qualitygate
Rename
Copy
Set as Default
Delete
Add Condition
Add Condition
On New Code
On Overall Code
Quality Gate fails when
Bugs
Operator
is greater than
Value
50
Add Condition
Cancel
Type here to search
27°C
ENG
IN
23:30
30/07/2021

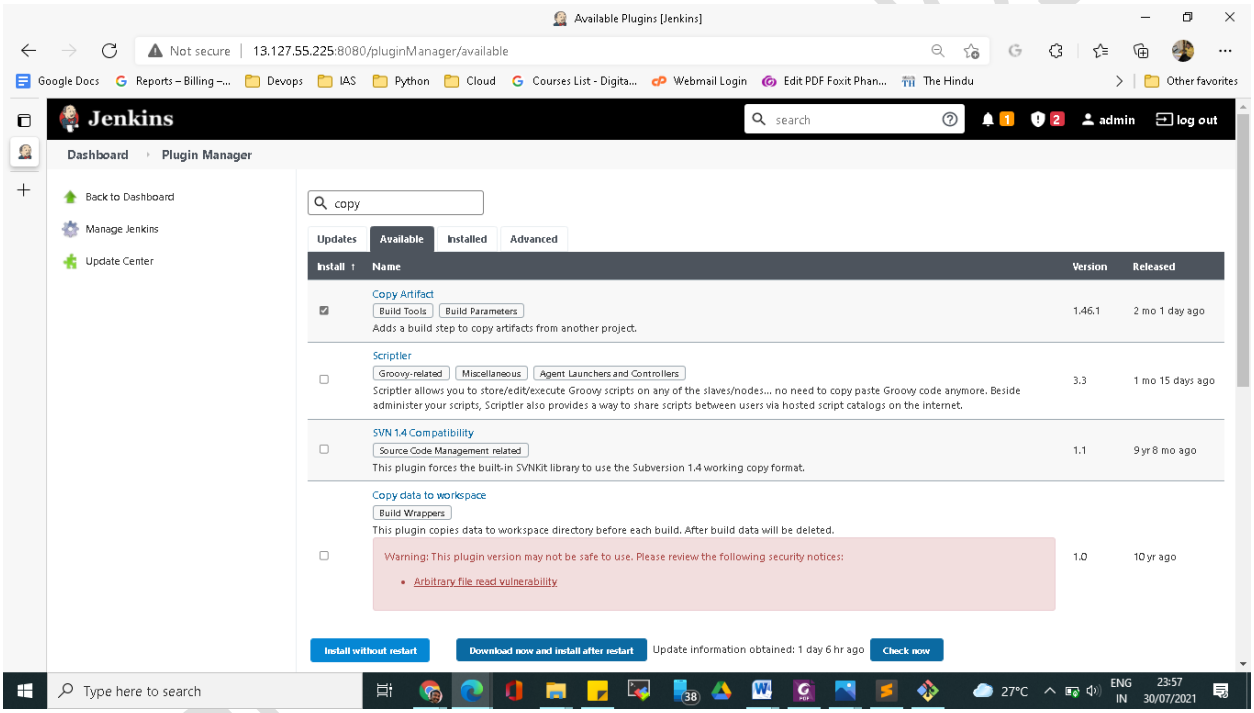

Projects
Not secure | 65.0.73.49/projects
sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
My Favorites
All
Perspective:
Overall Status
Sort by:
Name
Search by project name
1 projects
Filters
Quality Gate
Passed
Failed
Reliability ( Bugs )
Security ( Vulnerabilities )
logiclabs-repo
Passed
Last analysis: July 30, 2021, 11:22 PM
82 Bugs
3 Vulnerabilities
0.0% Hotspots Reviewed
138 Code Smells
6.1% Coverage
10.0% Duplications
3.3k JSP, Java, ...
1 of 1 shown
SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 8.3 (build 34182) - LGPL v3 - Community - Documentation - Get Support - Plugins - Web API - About
Type here to search
27°C
ENG
IN
23:37
30/07/2021

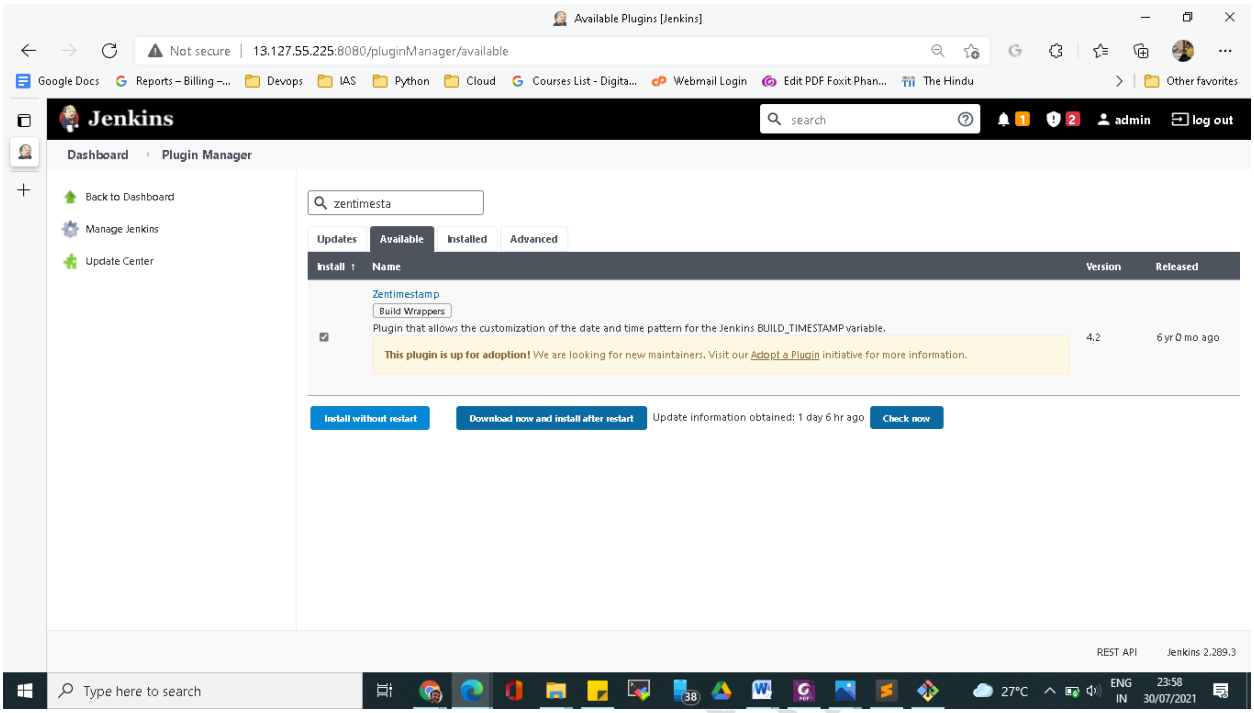


Copying Artifact Stage:

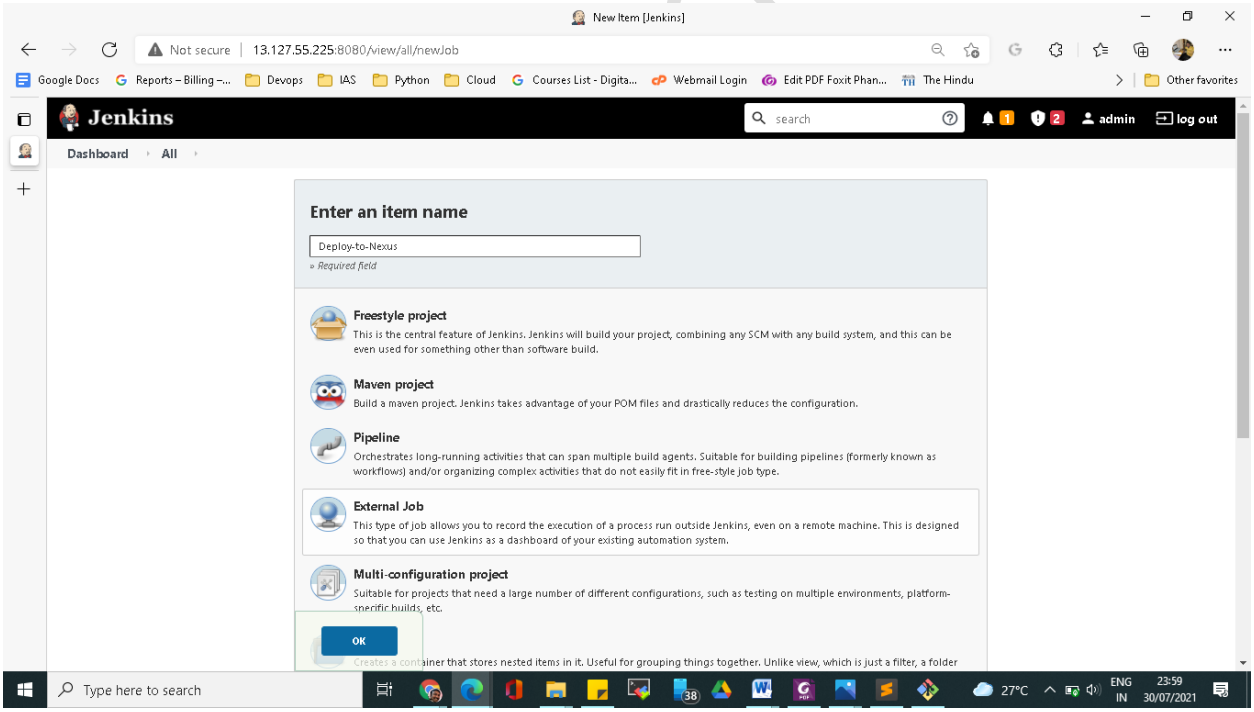
The build which passes through these stages and ready to be deployed is called an Artifact in SDLC lifecycle.
The artifacts are stored and versioned using Artifacts repository.
For this demonstration purpose, **Sonatype Nexus-3** is being used.

Before that let's install a relevant plugin in the Jenkins .
1. Copy Artifact plugin
2. Zentimestamp plugin

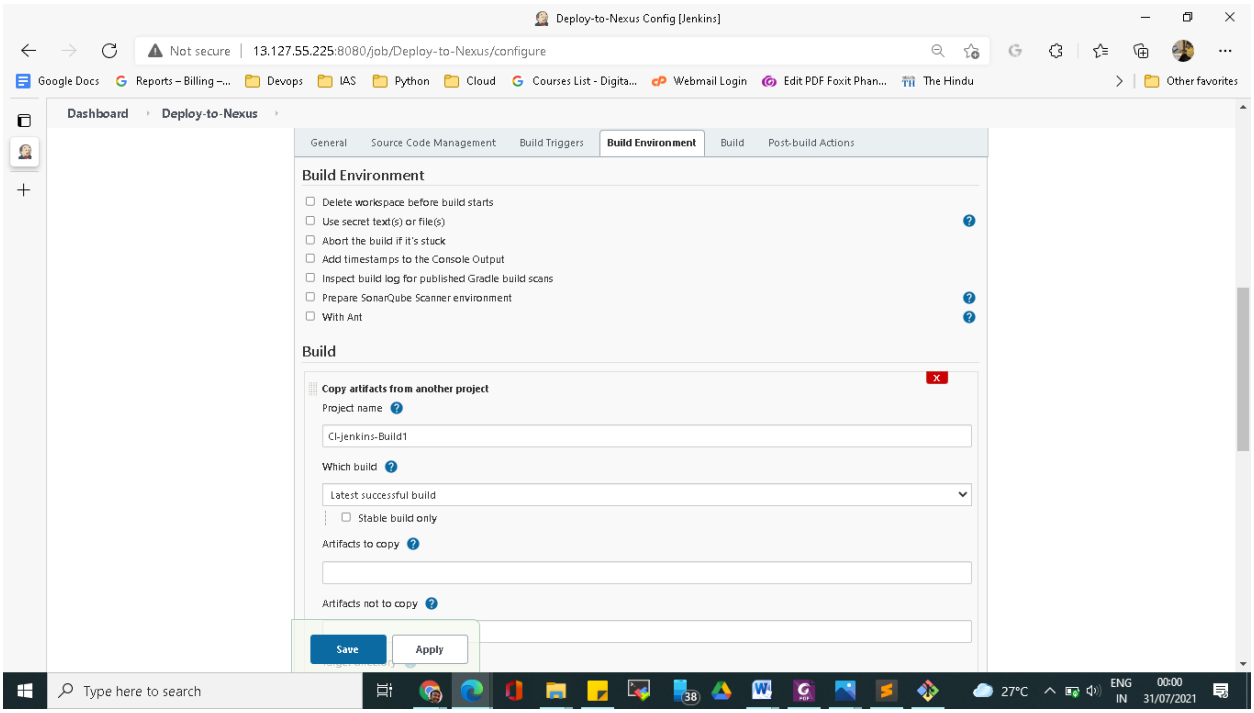





Create a new step in Jenkins for Deploying artifact to nexus.

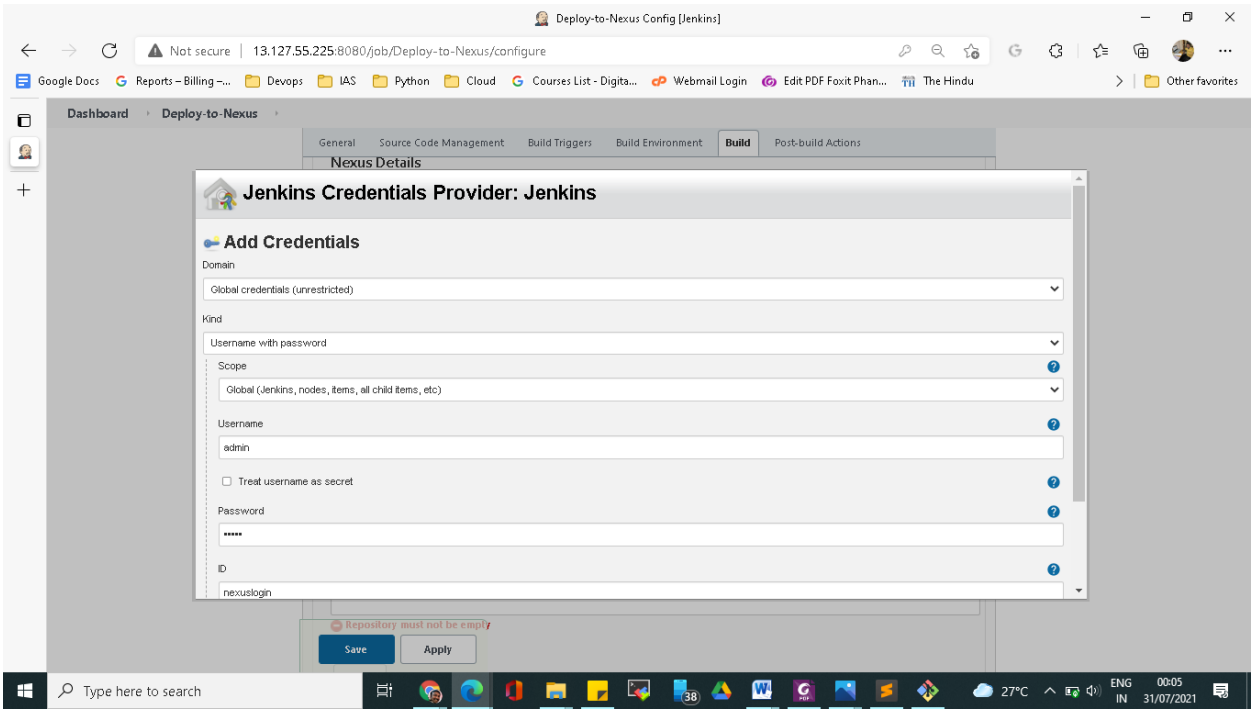


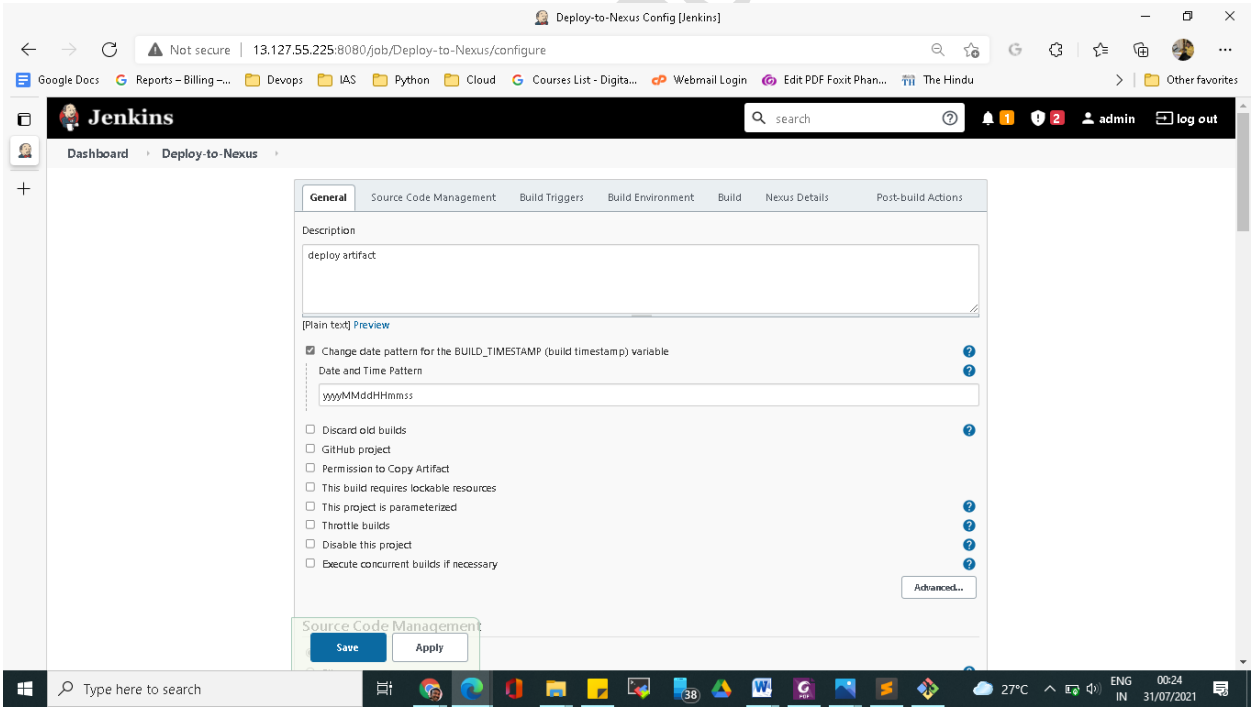

click on add build step and select artifact upload option to give artifact details

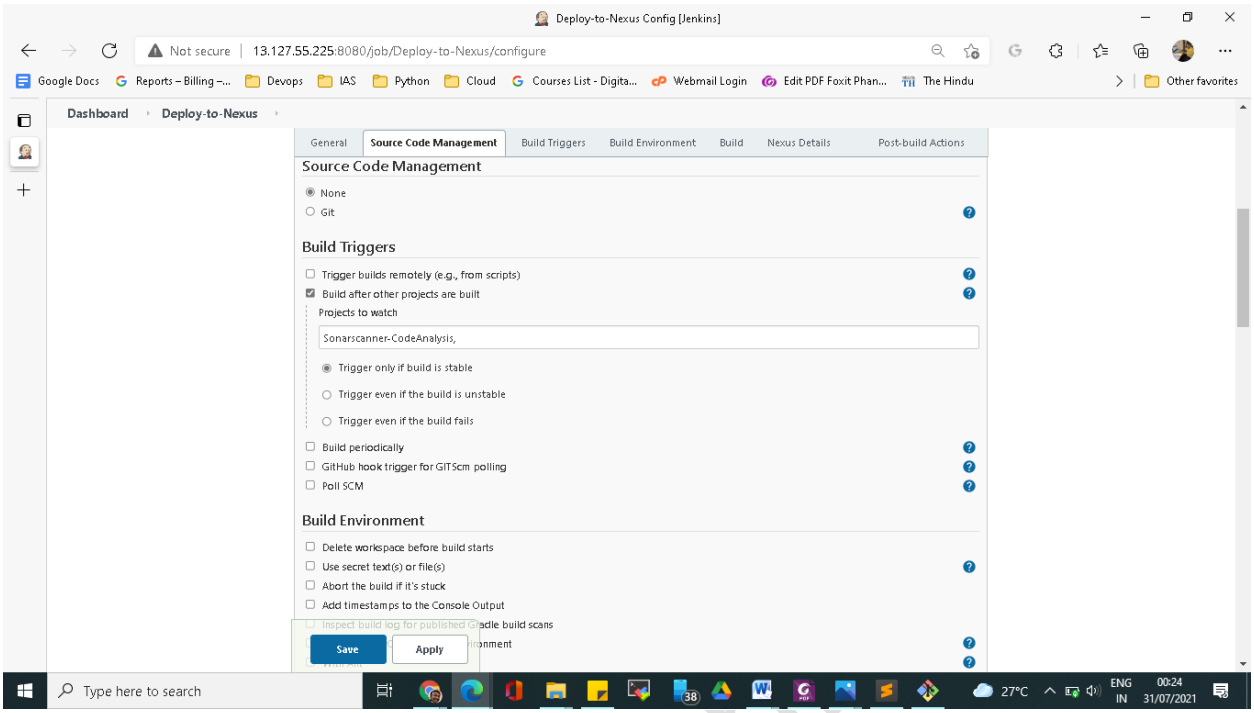


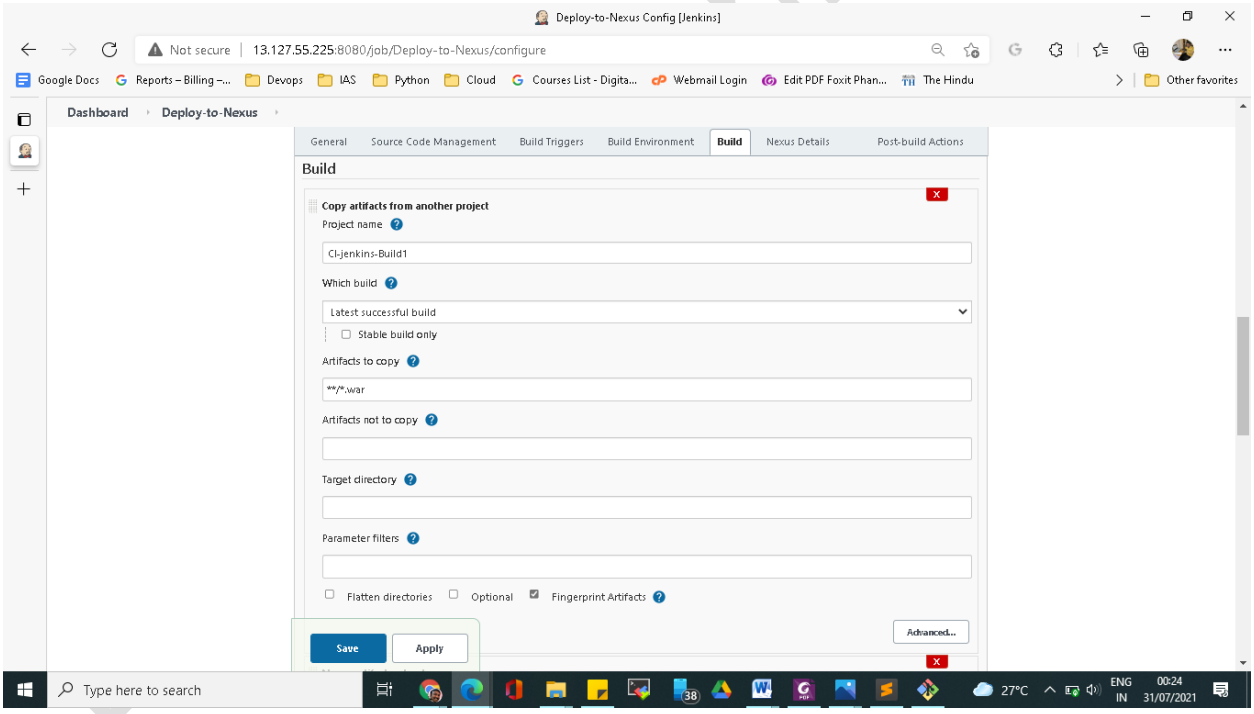

click on add build step and select nexus artifact uploader option to give artifact details

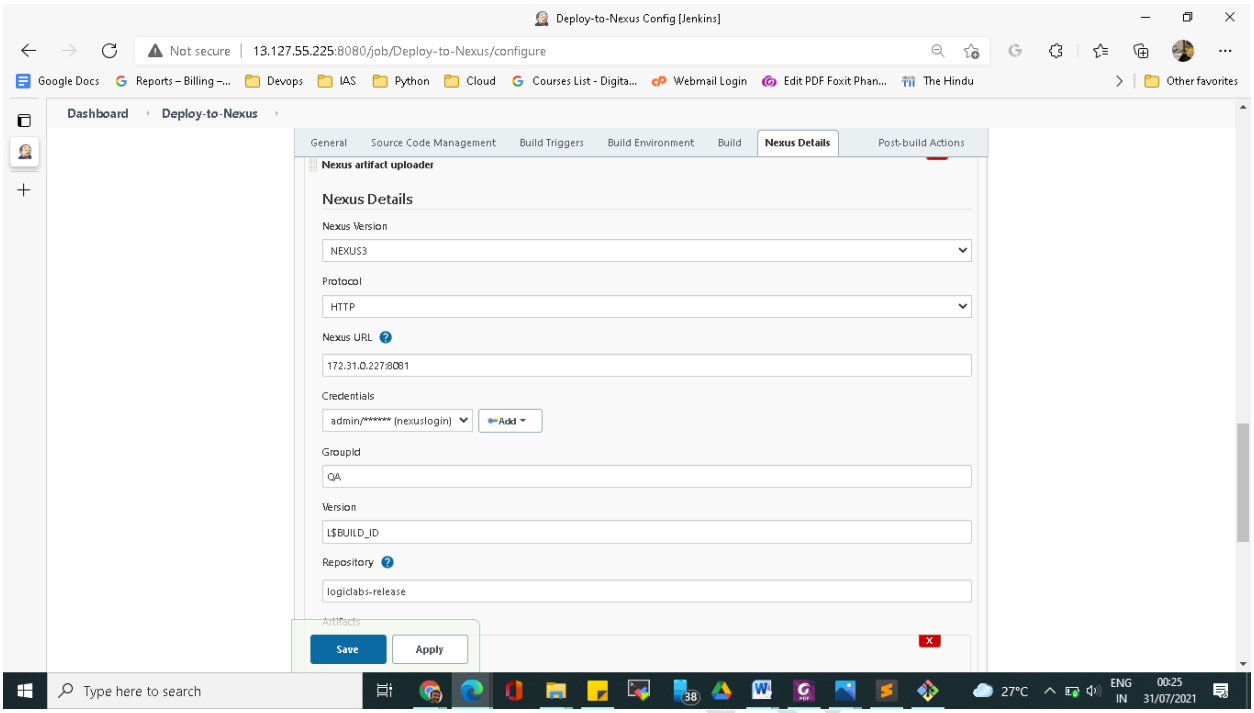
Add the credentials of Nexus server in the Jenkins credentials provider.


Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Nexus Details
Jenkins Credentials Provider: Jenkins
Add Credentials
Domain
Global credentials (unrestricted)
Kind
Username with password
Scope
Global (Jenkins, nodes, items, all child items, etc)
Username
admin
Treat username as secret
Password
ID
nexuslogin
Repository must not be empty
Save
Apply
Type here to search


Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Jenkins
search
admin
log out
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Nexus Details
Post-build Actions
Description
deploy artifact
[Plain text] Preview
Change date pattern for the BUILD_TIMESTAMP (build timestamp) variable
Date and Time Pattern
yyyyMMddHHmmss
Discard old builds
GitHub project
Permission to Copy Artifact
This build requires lockable resources
This project is parameterized
Throttle builds
Disable this project
Execute concurrent builds if necessary
Advanced...
Source Code Management
Save
Apply
Type here to search

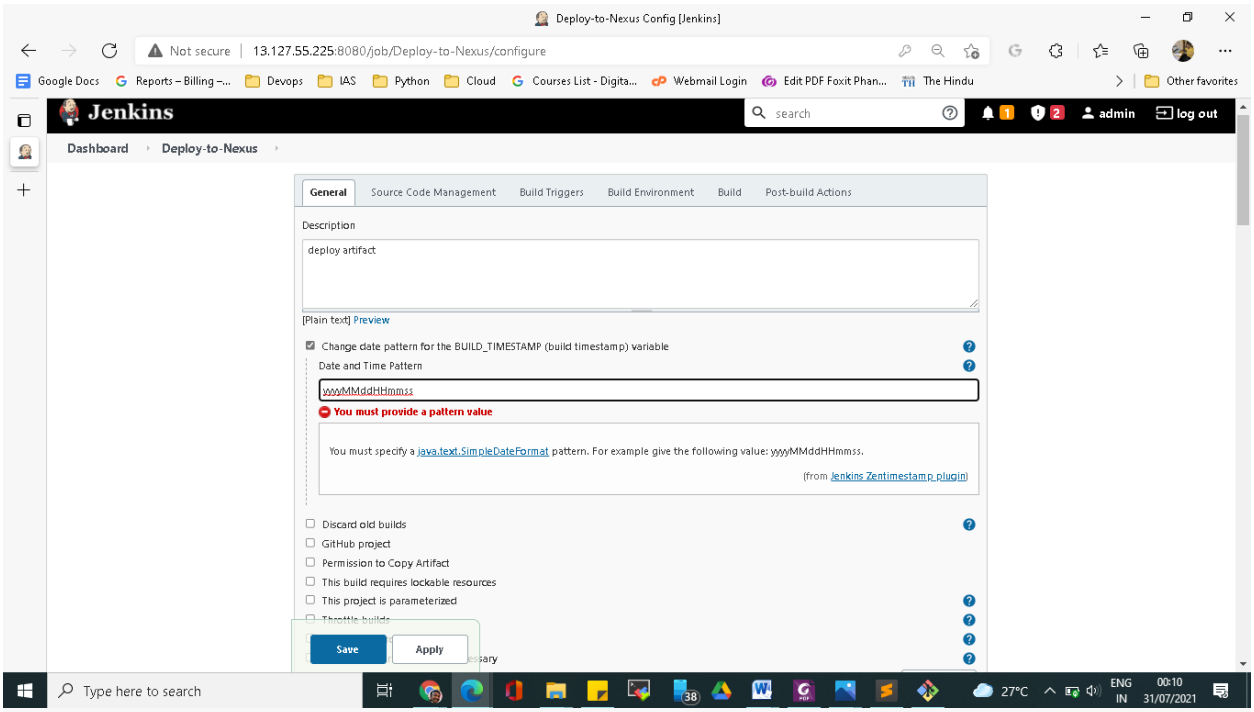

Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Nexus Details
Post-build Actions
Source Code Management
None
Git
Build Triggers
Trigger builds remotely (e.g., from scripts)
Build after other projects are built
Projects to watch
Sonarscanner-CodeAnalysis,
Trigger only if build is stable
Trigger even if the build is unstable
Trigger even if the build fails
Build periodically
GitHub hook trigger for GITScm polling
Poll SCM
Build Environment
Delete workspace before build starts
Use secret text(s) or file(s)
Abort the build if it's stuck
Add timestamps to the Console Output
Save
Apply
Type here to search
27°C
ENG
IN
00:24
31/07/2021

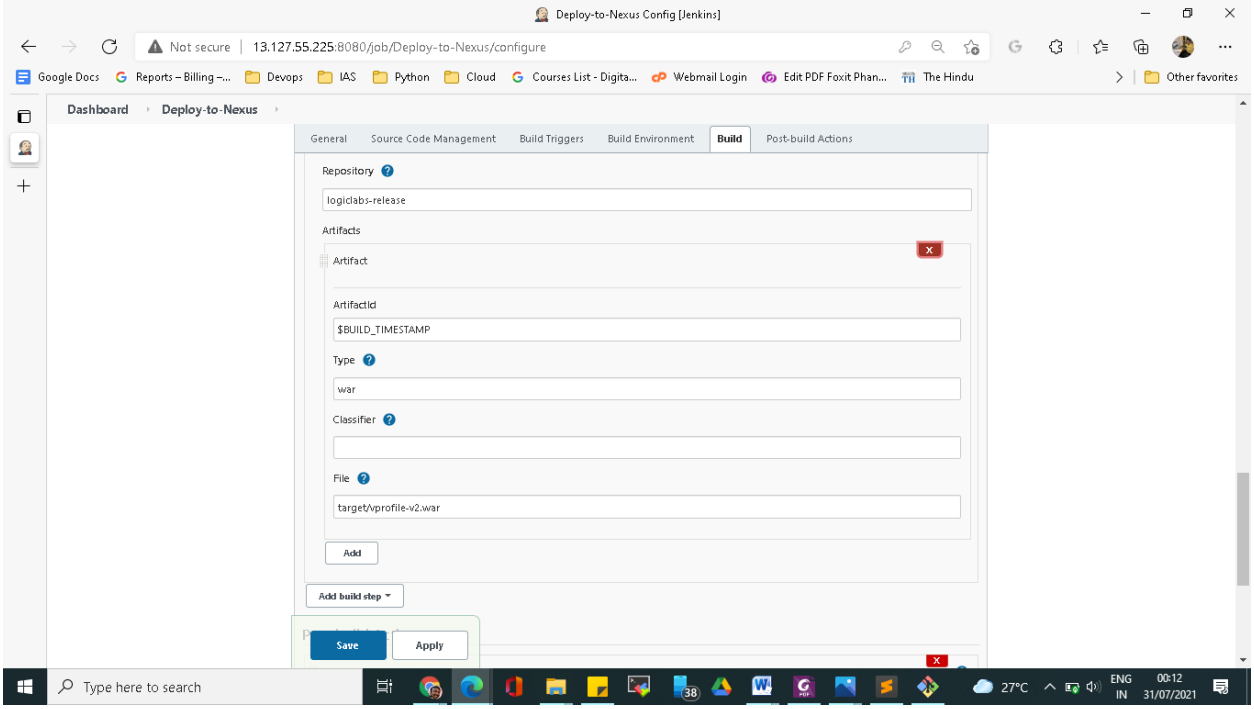

Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Nexus Details
Post-build Actions
Build
Copy artifacts from another project
Project name
CI-jenkins-Build1
Which build
Latest successful build
Stable build only
Artifacts to copy
**/*.war
Artifacts not to copy
Target directory
Parameter filters
Flatten directories
Optional
Fingerprint Artifacts
Advanced...
Save
Apply
Type here to search
27°C
ENG
IN
00:24
31/07/2021

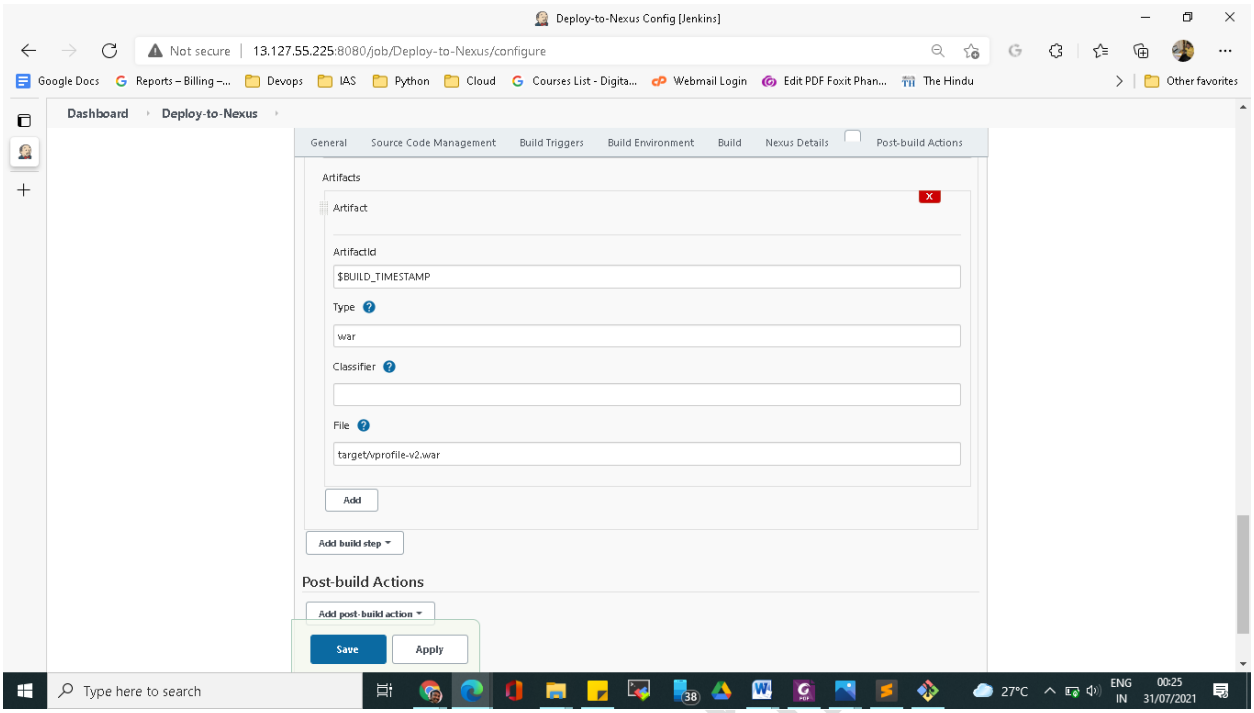



Note: Make sure you don't repeat http while giving the nexus pvt URL.

Give the time format as given in the screenshot below.

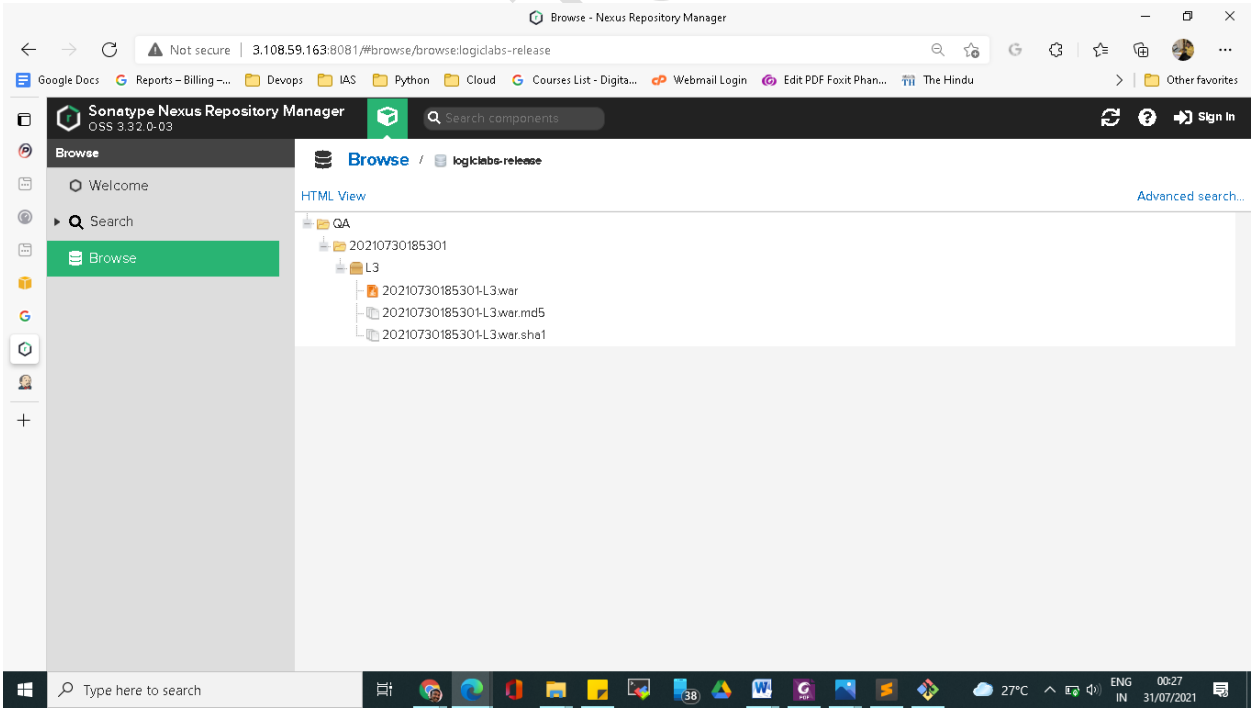

Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Jenkins
admin
log out
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Description
deploy artifact
[Plain text] Preview
Change date pattern for the BUILD_TIMESTAMP (build timestamp) variable
Date and Time Pattern
yyyyMMddHHmmss
You must provide a pattern value
You must specify a java.text.SimpleDateFormat pattern. For example give the following value: yyyyMMddHHmmss.
(from Jenkins Zentimestamp plugin)
Discard old builds
GitHub project
Permission to Copy Artifact
This build requires lockable resources
This project is parameterized
Save
Apply
Type here to search


Deploy-to-Nexus Config [Jenkins]
Not secure | 13.127.55.225:8080/job/Deploy-to-Nexus/configure
Dashboard
Deploy-to-Nexus
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Repository
logiclabs-release
Artifacts
Artifact
ArtifactId
$BUILD_TIMESTAMP
Type
war
Classifier
File
target/vprofile-v2.war
Add
Add build step
Save
Apply
Type here to search



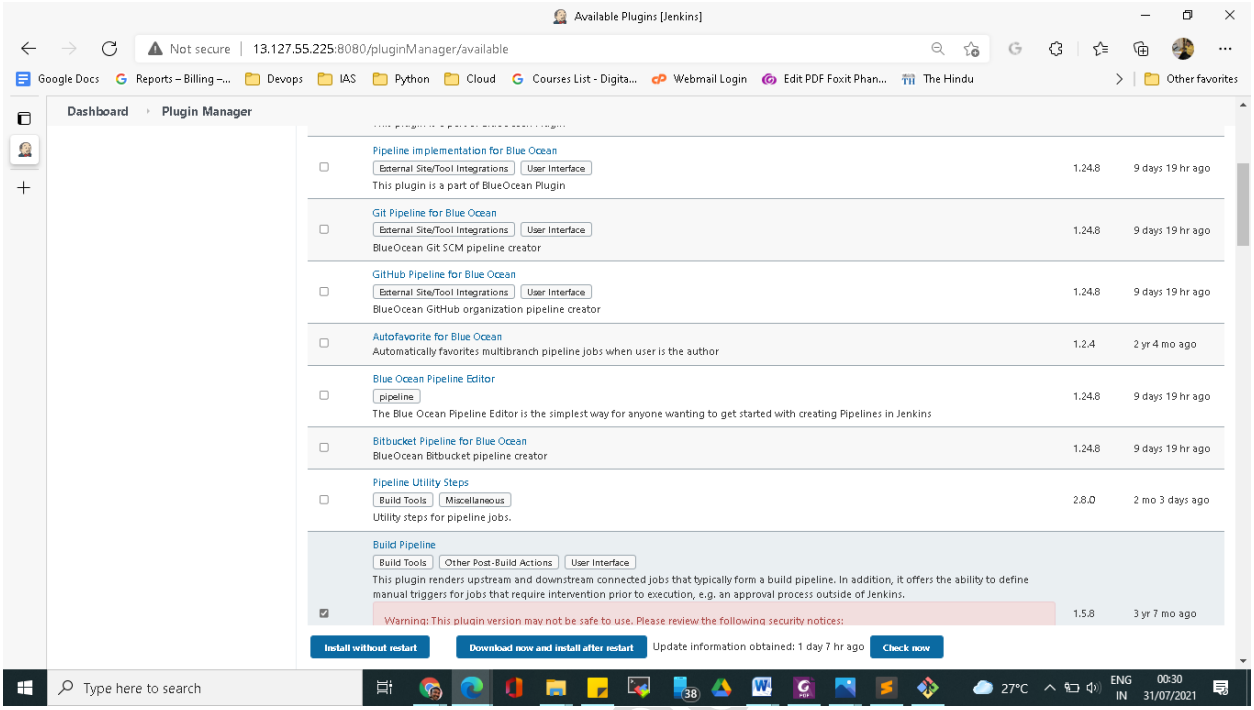

VALIDATE Artifact Deployment to Nexus repository:

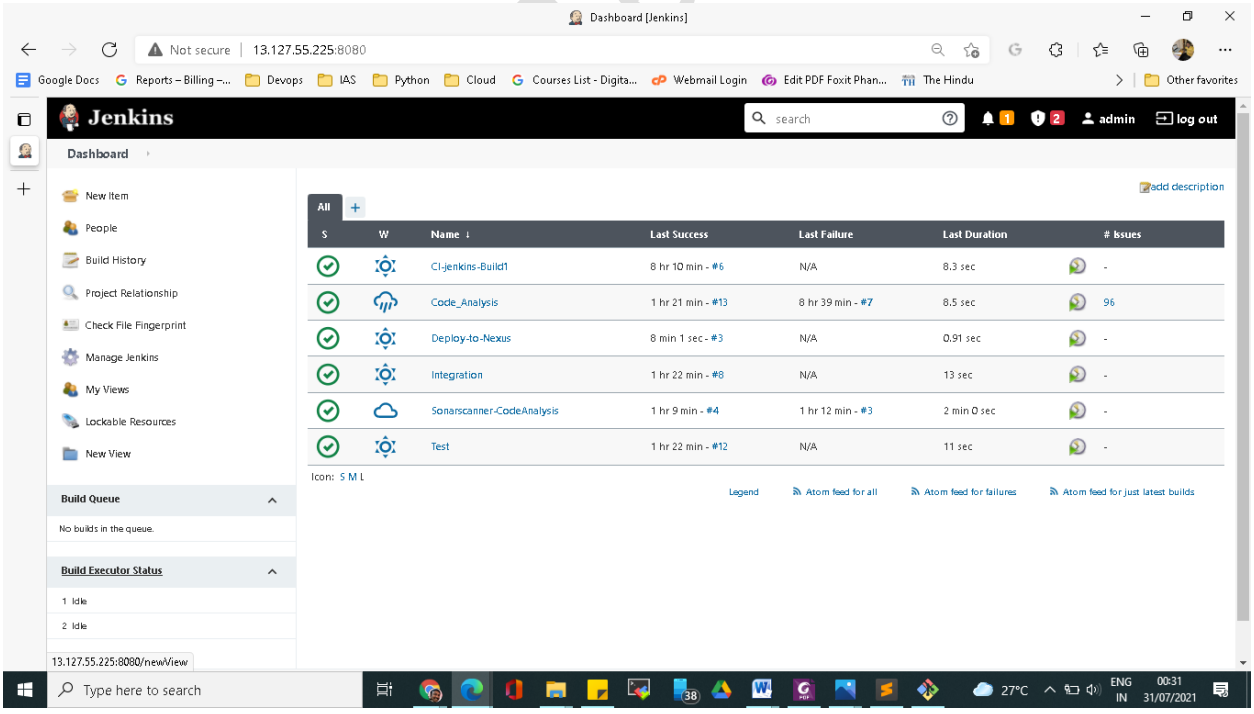
Goto Nexus server→ Browse repo → release repository



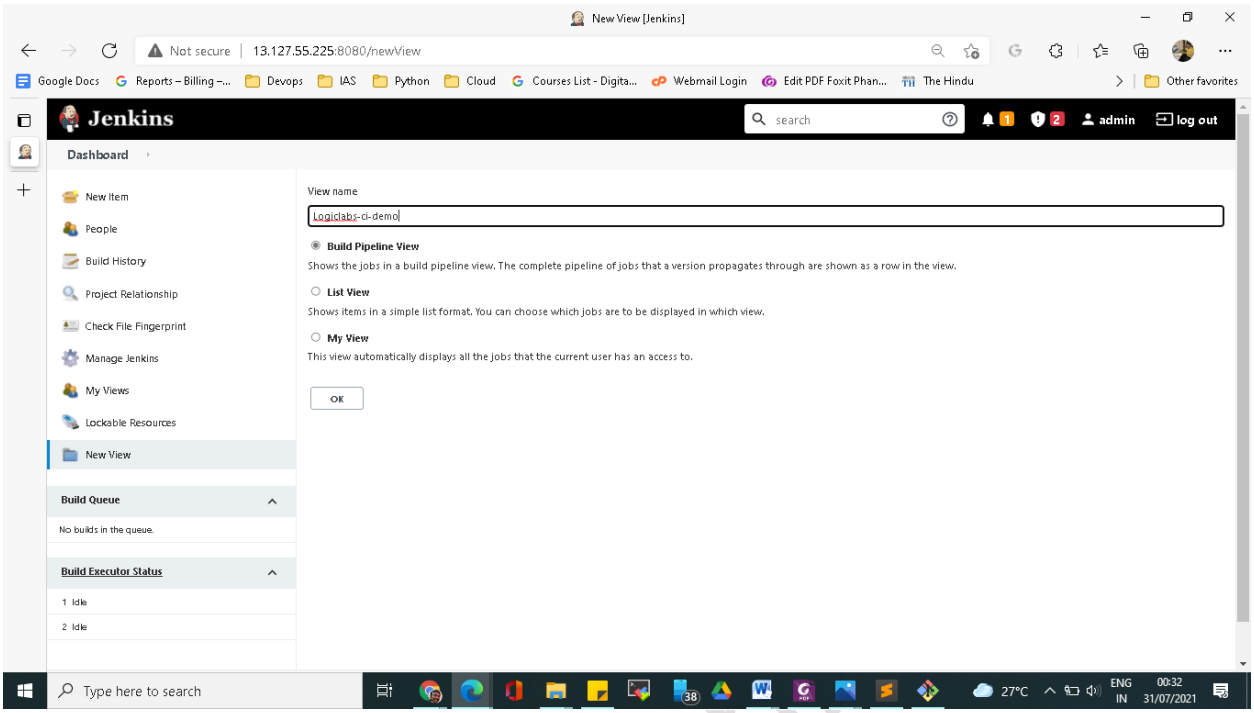

BUILDING Pipeline:

In jenkins install the pipeline plugin as shown below. It helps in visually appealing pipeline view in Jenkins.

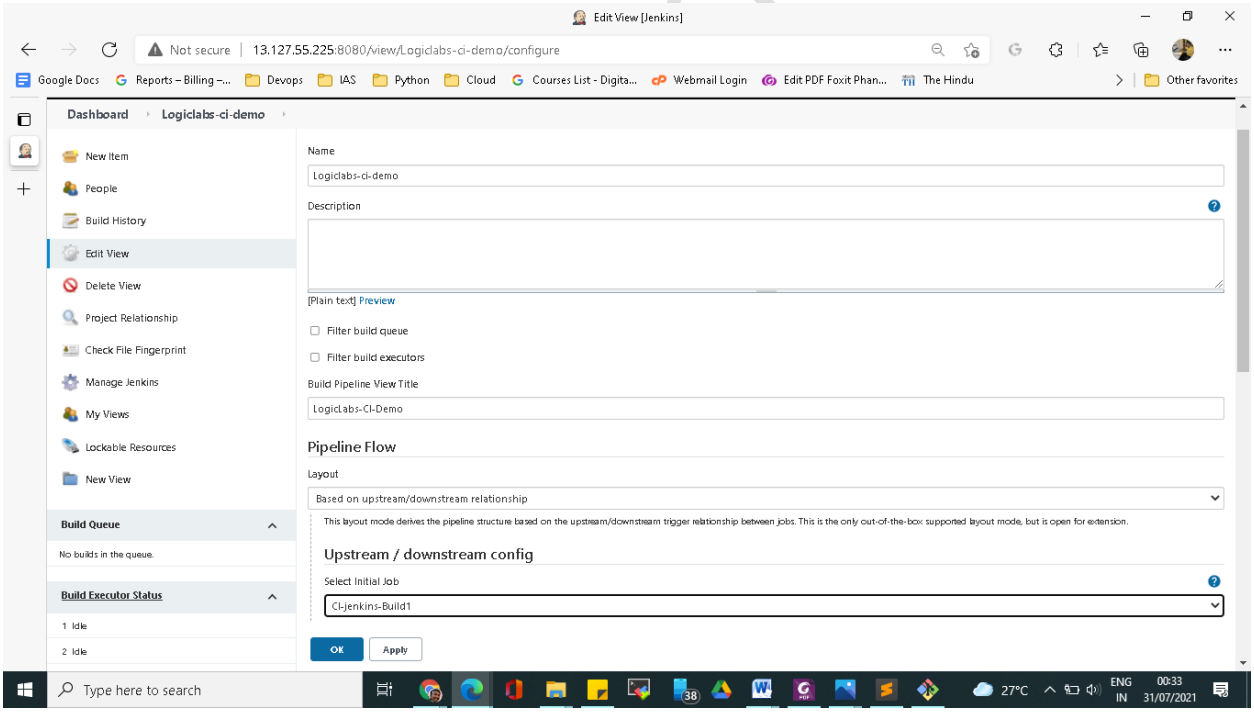


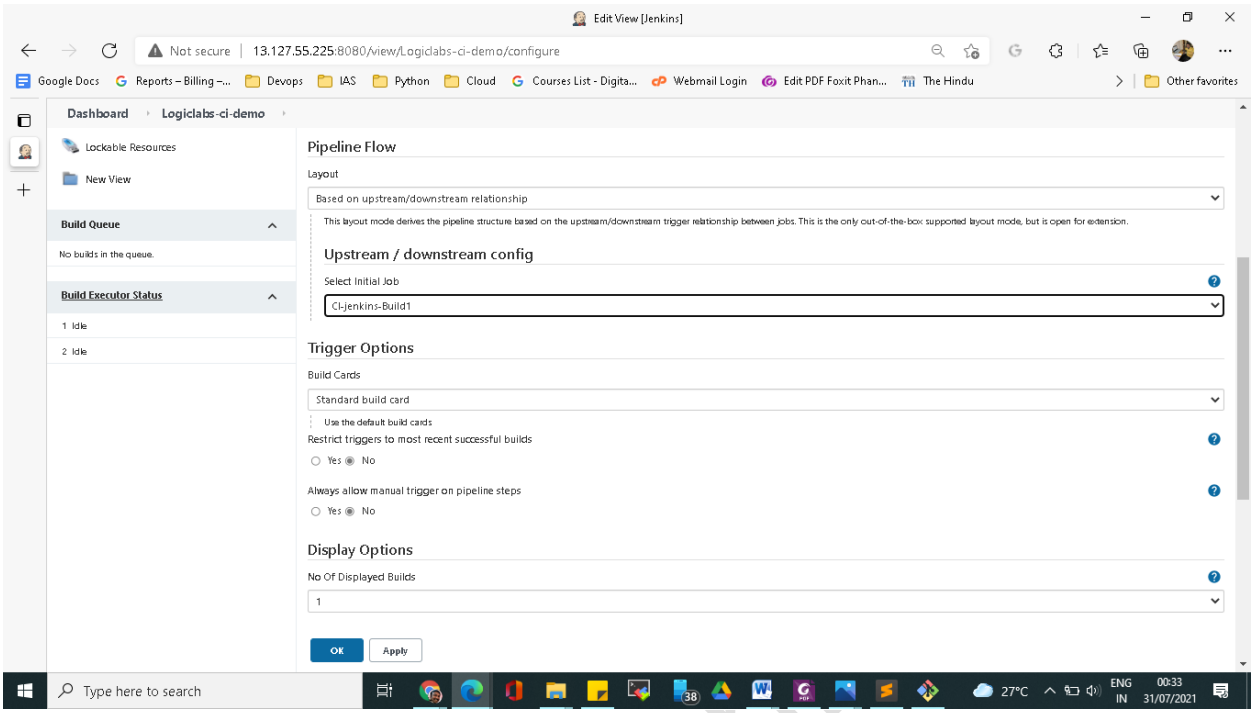



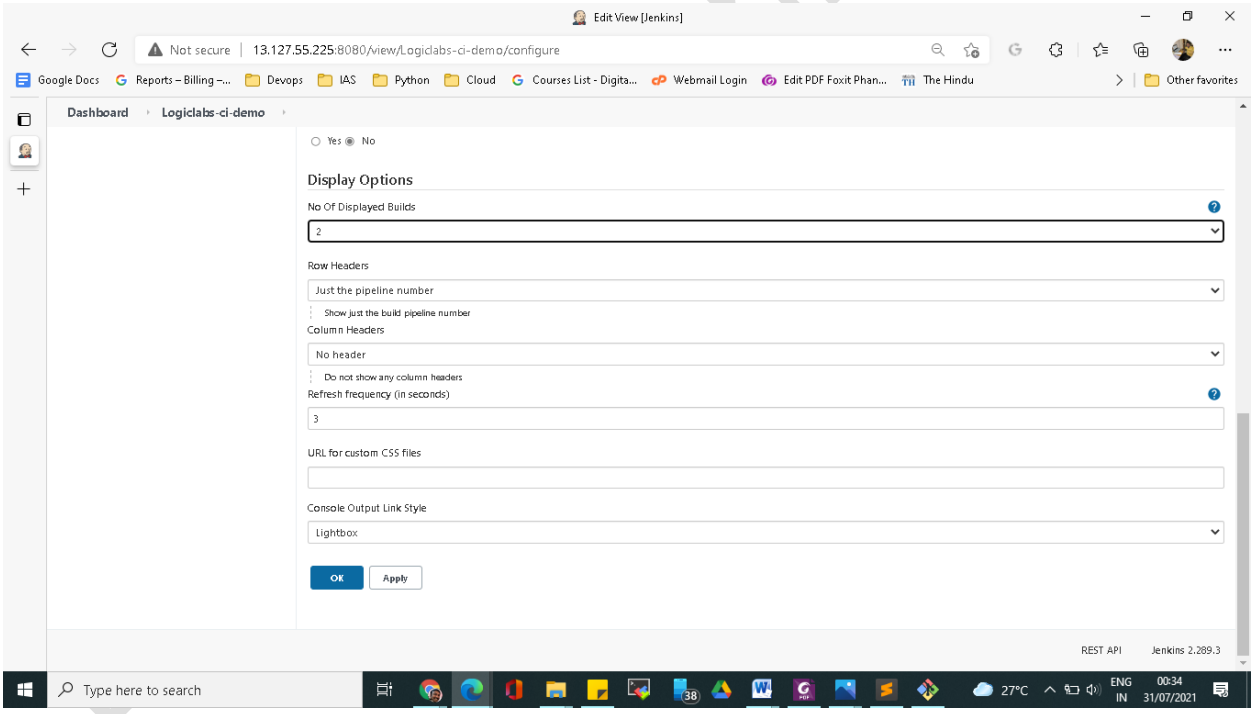

Click on the + symbol besides All in the jobs dashboard to add a new view.




Give the name of the first job to be started .





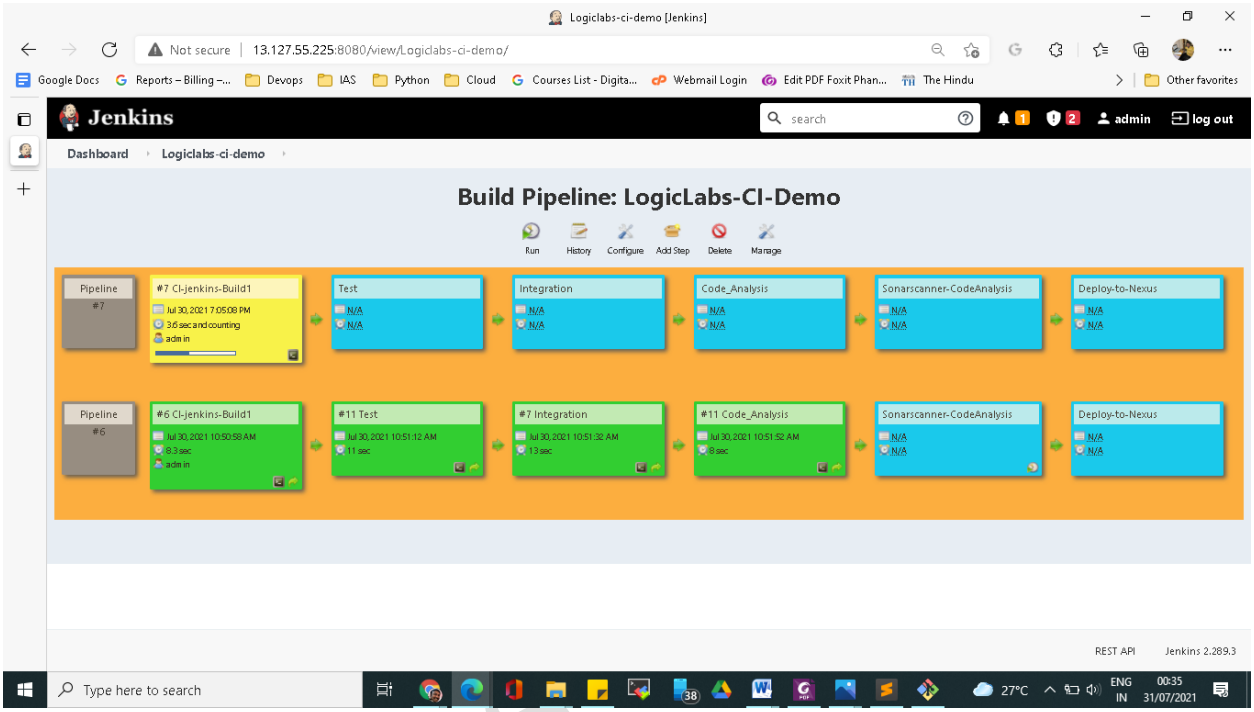



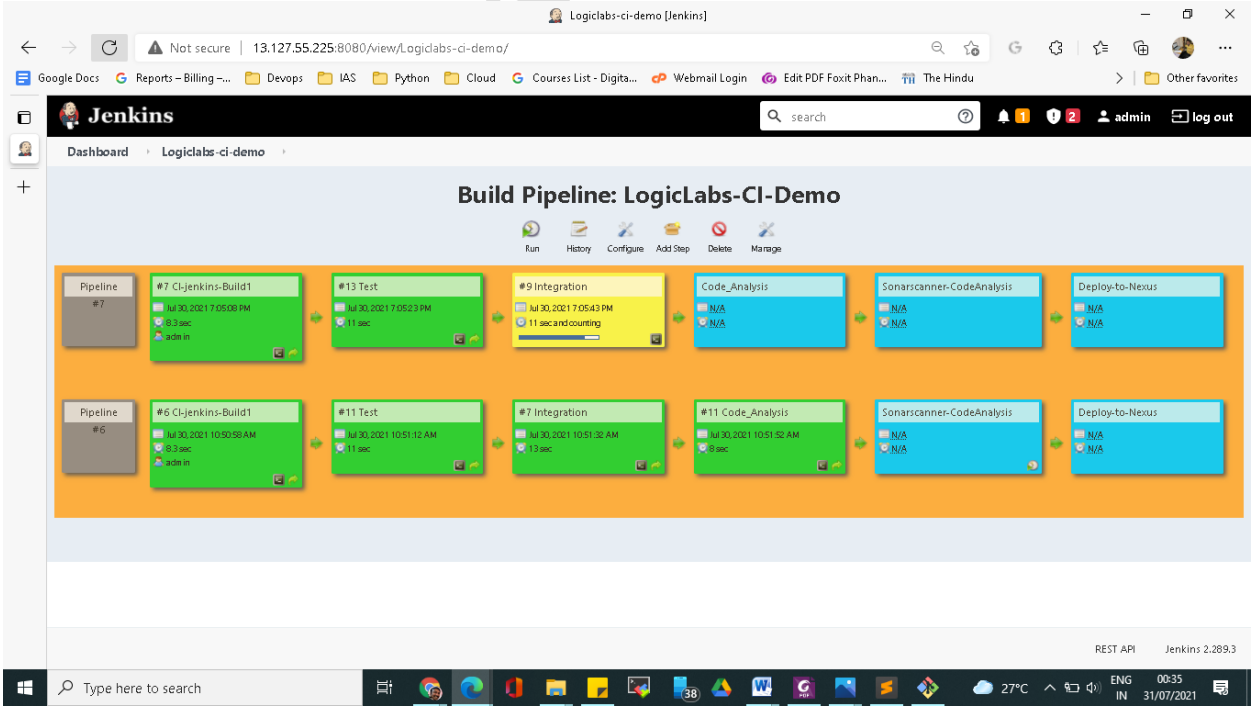

Click on Run  to start the pipeline. Observe that all the downstream Jobs are performed sequentially.

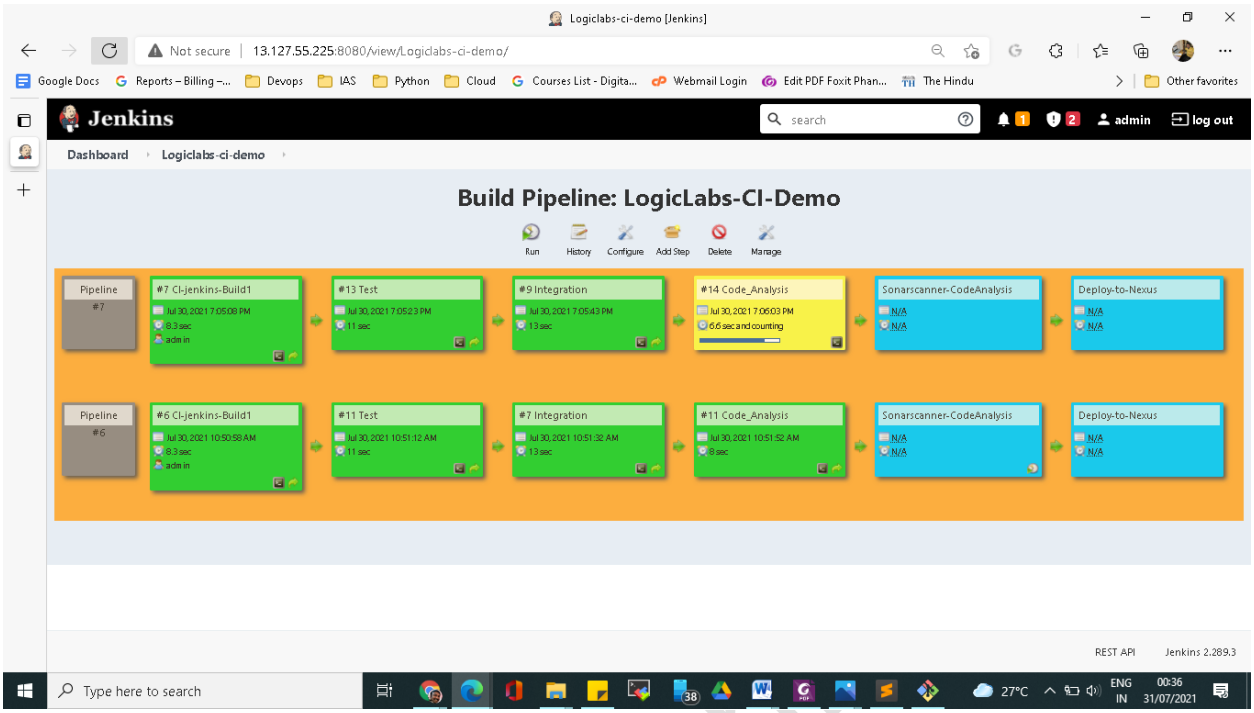
Verify that all the jobs are properly configured for downstream jobs/upstream jobs.

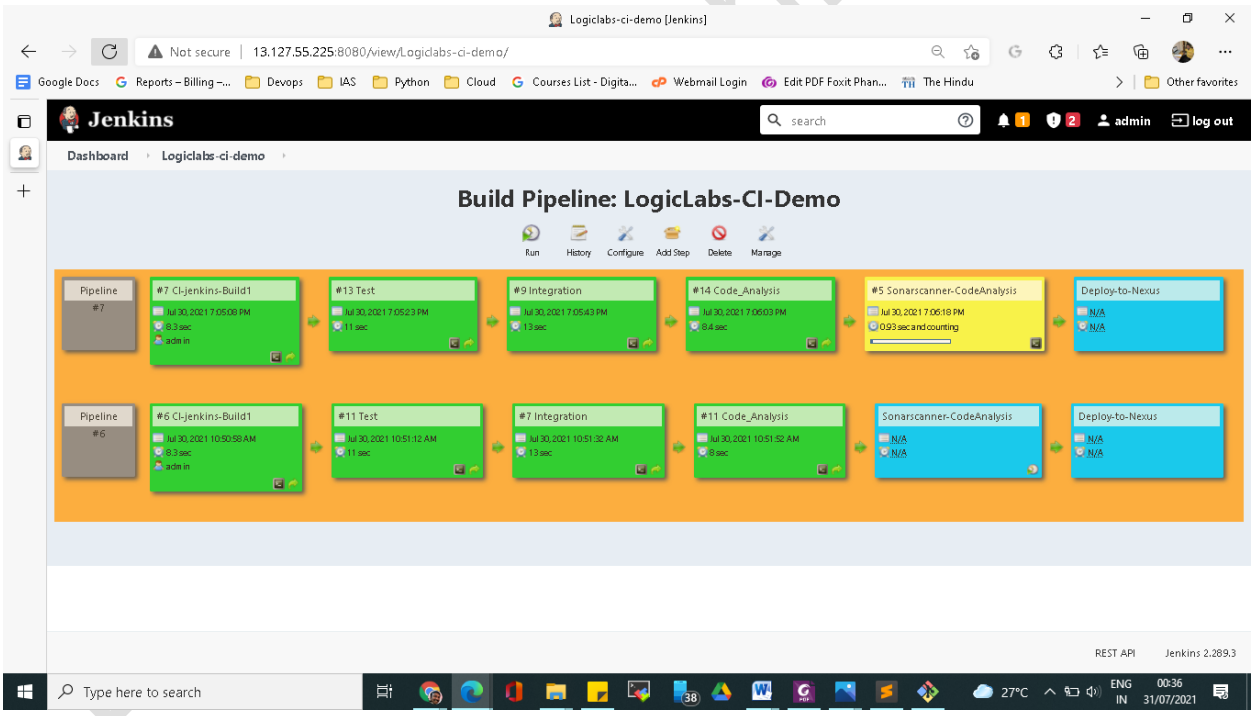
Please make sure the pipeline flow is as shown below.

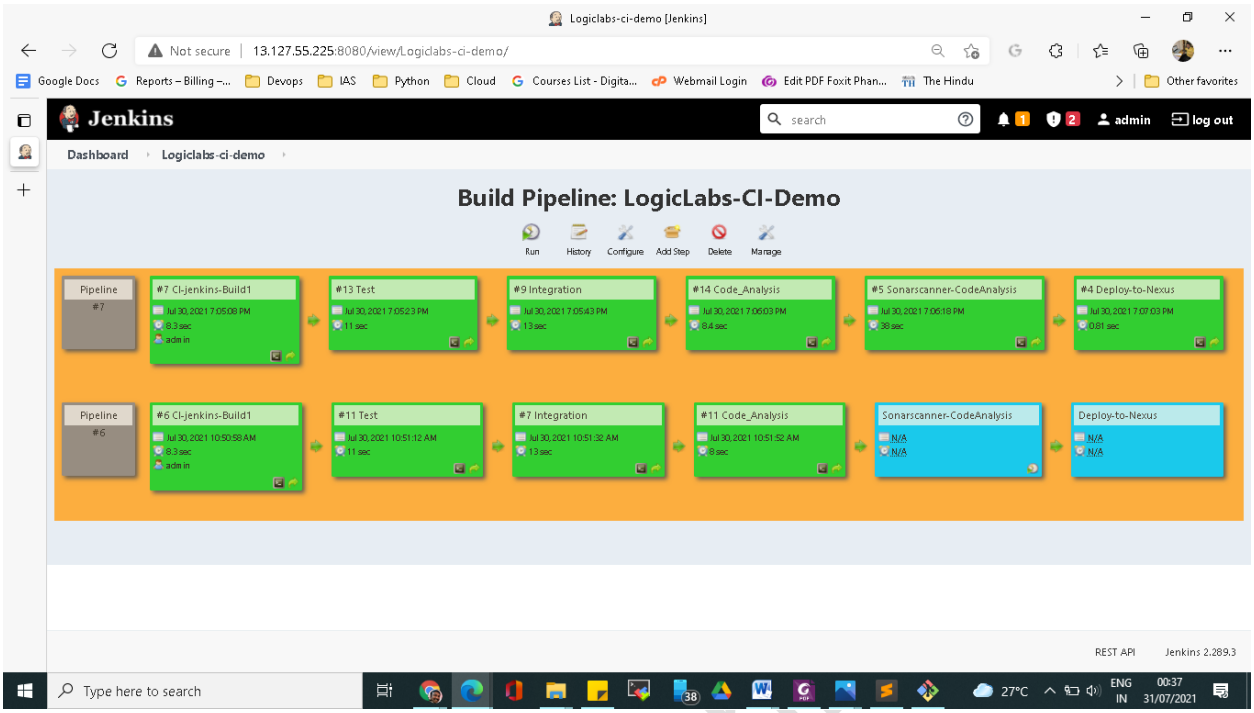
CI jenkins Build → UnitTest→ Integration Test→ CodeAnalysis → SonarScanner Code Analysis → Deploy to Nexus



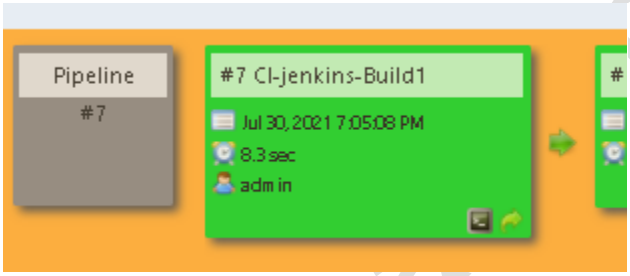



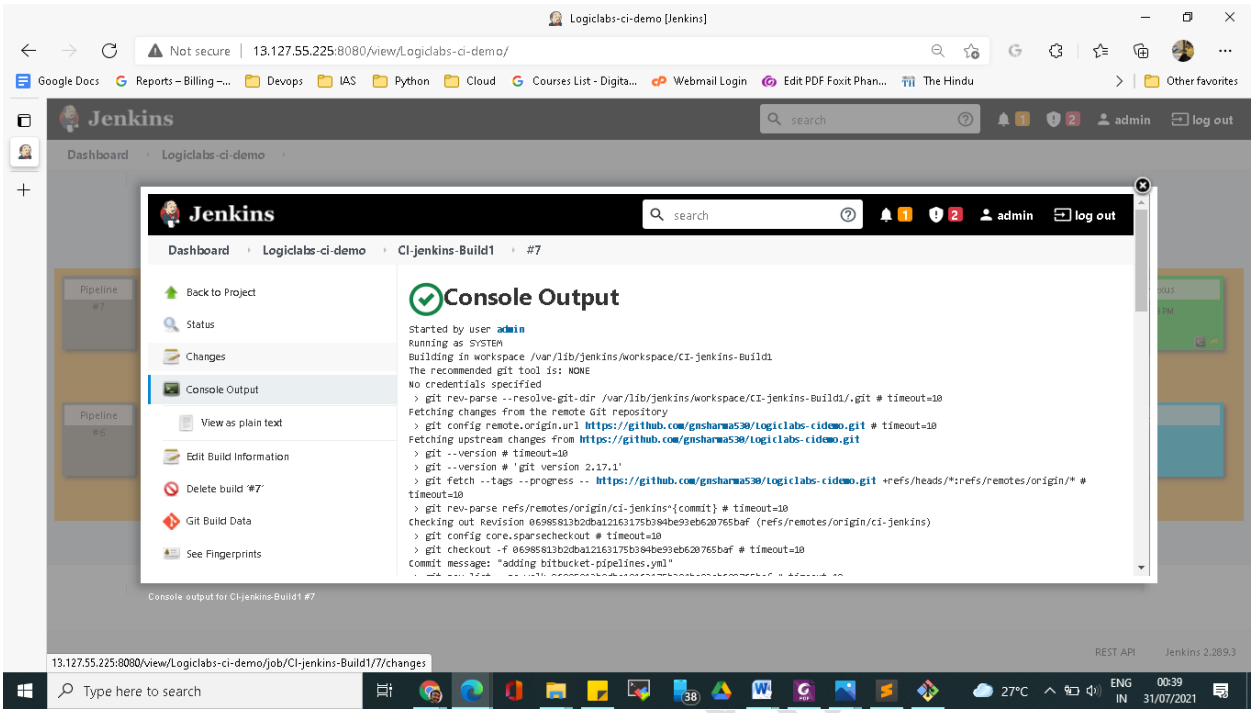

Logiclabs-ci-demo [Jenkins]
Not secure | 13.127.55.225:8080/view/Logiclabs-ci-demo/
Jenkins
search
admin
log out
Dashboard
Logiclabs-ci-demo
Build Pipeline: LogicLabs-CI-Demo
Run
History
Configure
Add Step
Delete
Manage
Pipeline #7
#7 CI-Jenkins-Build1
#13 Test
#9 Integration
#14 Code_Analysis
Sonarscanner-CodeAnalysis
Deploy-to-Nexus
Pipeline #6
#6 CI-Jenkins-Build1
#11 Test
#7 Integration
#11 Code_Analysis
Sonarscanner-CodeAnalysis
Deploy-to-Nexus
REST API
Jenkins 2.289.3
Type here to search
27°C
ENG
IN
00:36
31/07/2021


Logiclabs-ci-demo [Jenkins]
Not secure | 13.127.55.225:8080/view/Logiclabs-ci-demo/
Jenkins
search
admin
log out
Dashboard
Logiclabs-ci-demo
Build Pipeline: LogicLabs-CI-Demo
Run
History
Configure
Add Step
Delete
Manage
Pipeline #7
#7 CI-Jenkins-Build1
#13 Test
#9 Integration
#14 Code_Analysis
#5 Sonarscanner-CodeAnalysis
Deploy-to-Nexus
Pipeline #6
#6 CI-Jenkins-Build1
#11 Test
#7 Integration
#11 Code_Analysis
Sonarscanner-CodeAnalysis
Deploy-to-Nexus
REST API
Jenkins 2.289.3
Type here to search
27°C
ENG
IN
00:36
31/07/2021



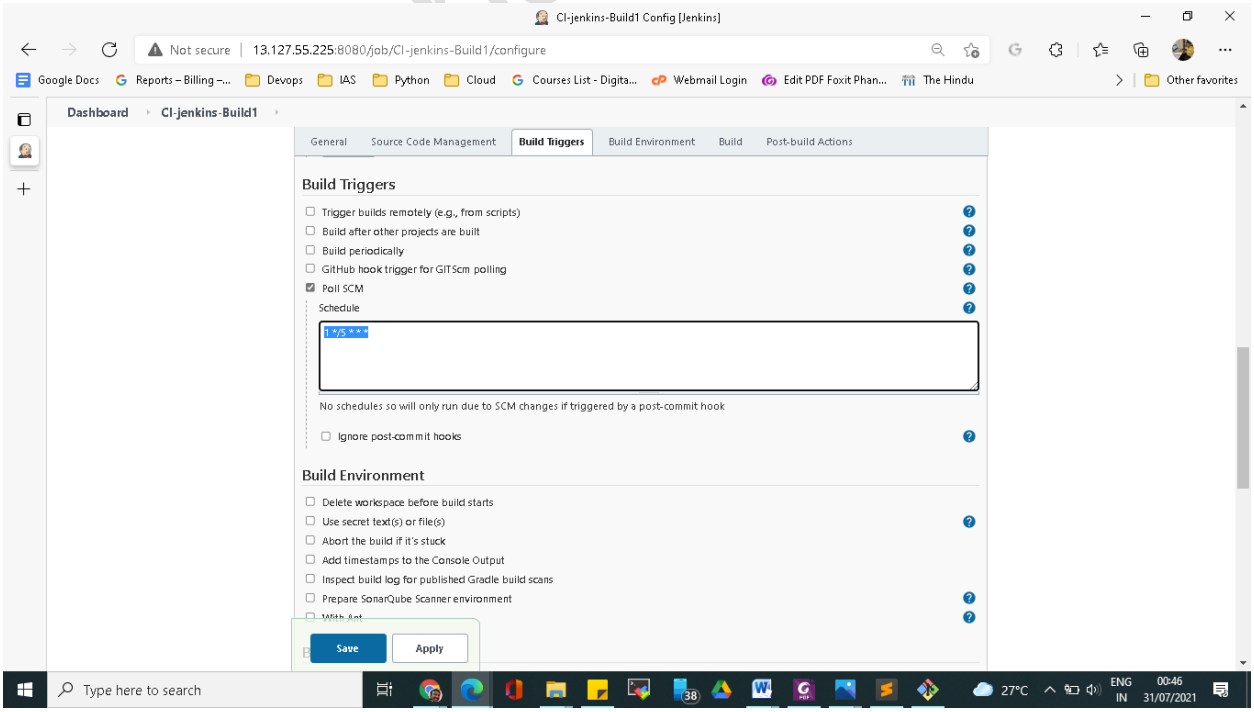

Click on the console button on each of the jobs to see the logs






Automating the build pipeline triggering:

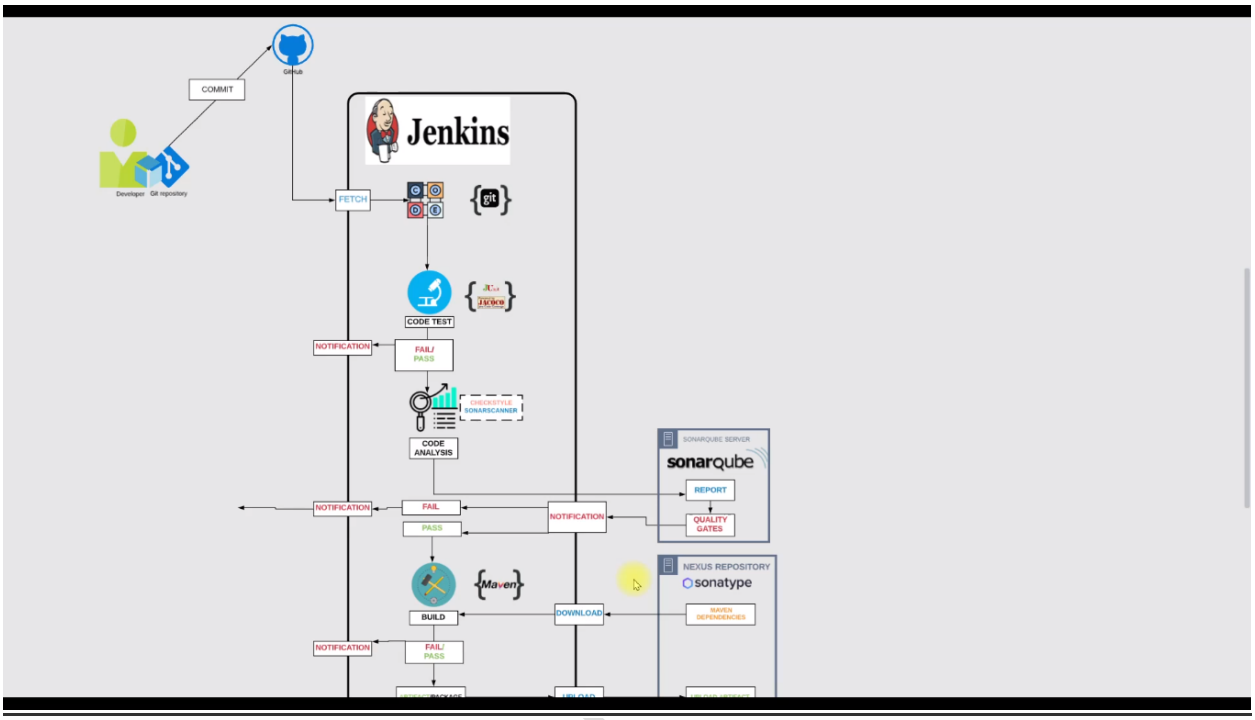
Enable poll scm or github webhooks and observe that the pipeline is triggered automatically whenever any commit happens in the SCM tool (Github)



Eg: 1 */5 * * *  = check for commits and start building at every 5 hour interval of every day.

Note: Inorder to verify, create your own repo which is cloned from the original repo and experiment with this automated pipeline triggering mechanism.

# Summary:




In this Demonstration, we have witnessed how a C.I. pipeline can be built using tools such as jenkins, sonarQube and Nexus. We have observed how the source code commit by developer triggers a pipeline which starts with build job followed by Unit test, Integration test, Code analysis using SonarQube scanner and finally a well tested artifact is uploaded into Nexus repository.