PROJECT-4

MASTER AND SLAVE CONFIGURATION

TASK – 1

Deploy wordpress web application on master – slave in jenkins

Slave – 5 (vamsi krishna)

Wordpress : **What is WordPress?**

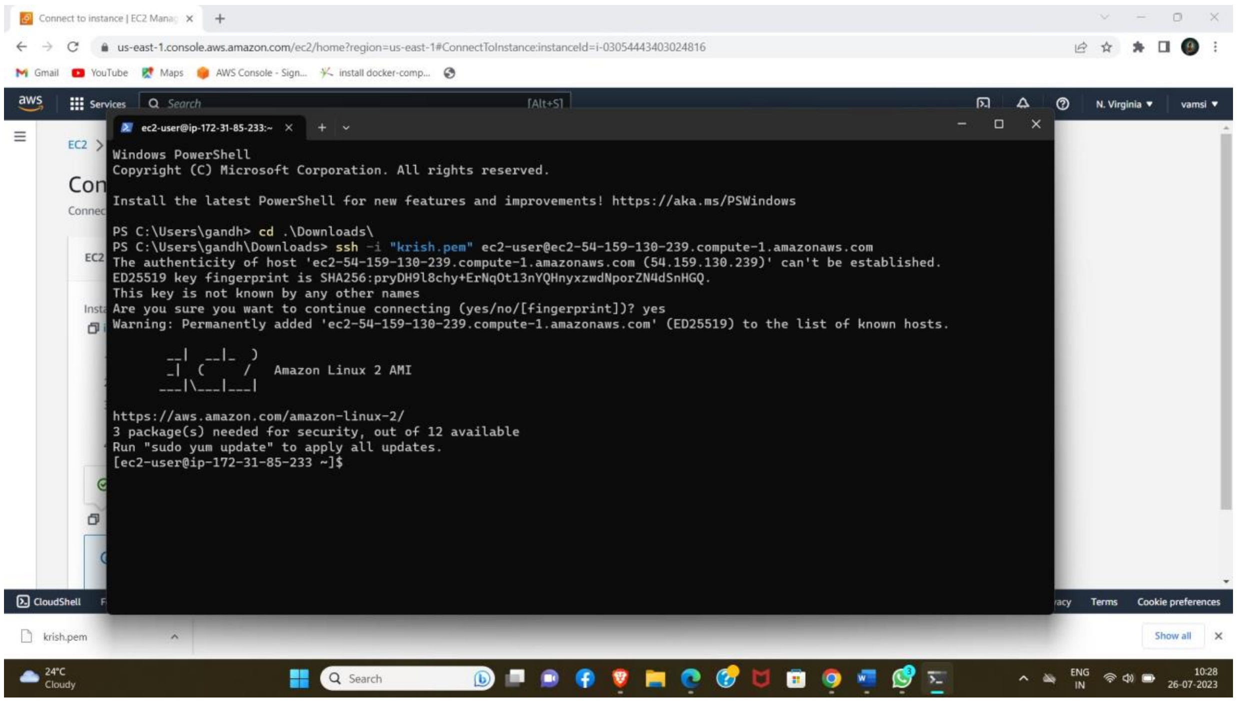
At its core, **WordPress is the simplest, most popular way to create your own website or blog.** In fact, WordPress powers over 43.3% of all the websites on the Internet. Yes – more than one in four websites that you visit are likely powered by WordPress.

On a slightly more technical level, WordPress is an open-source content management system licensed under GPLv2, which means that anyone can use or modify the WordPress software for free. A content management system is basically a tool that makes it easy to manage important aspects of your website – like content – without needing to know anything about programming.

The end result is that WordPress makes building a website accessible to anyone – even people who aren't developers.

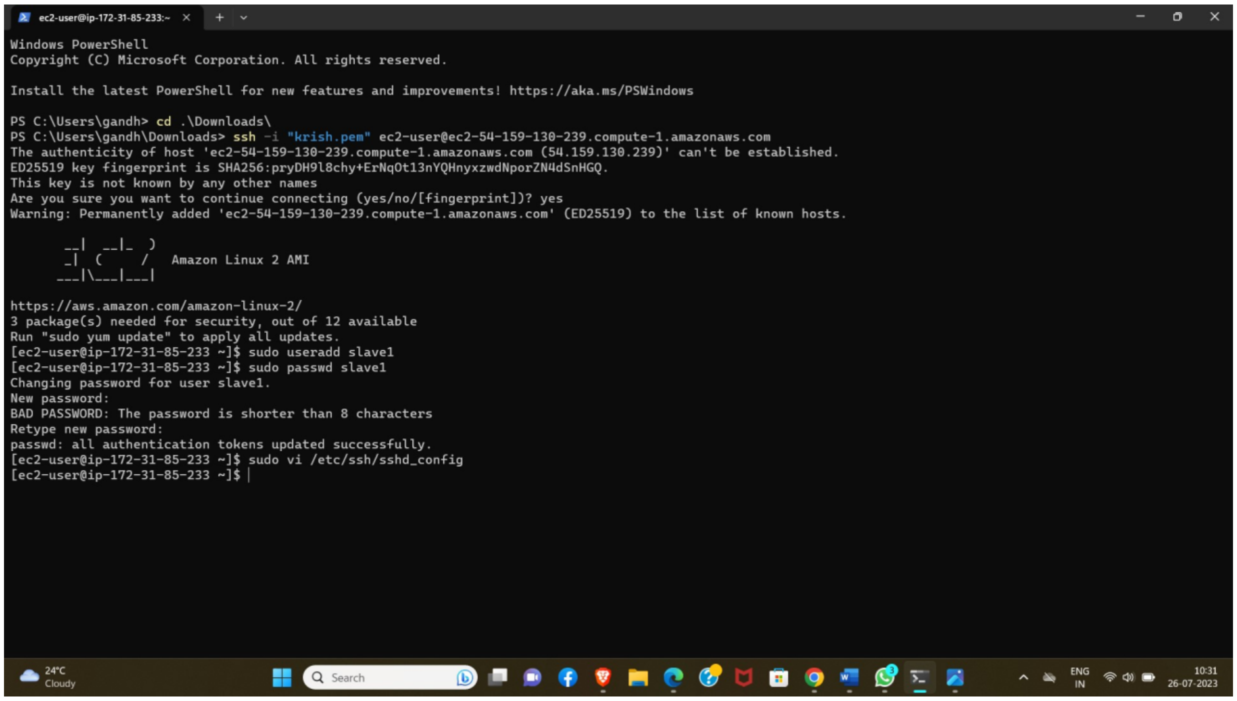
Step by step procedure:

- Create an EC2 instance for Jenkins Slavenode server and connect instance with ssh key.
-

- 

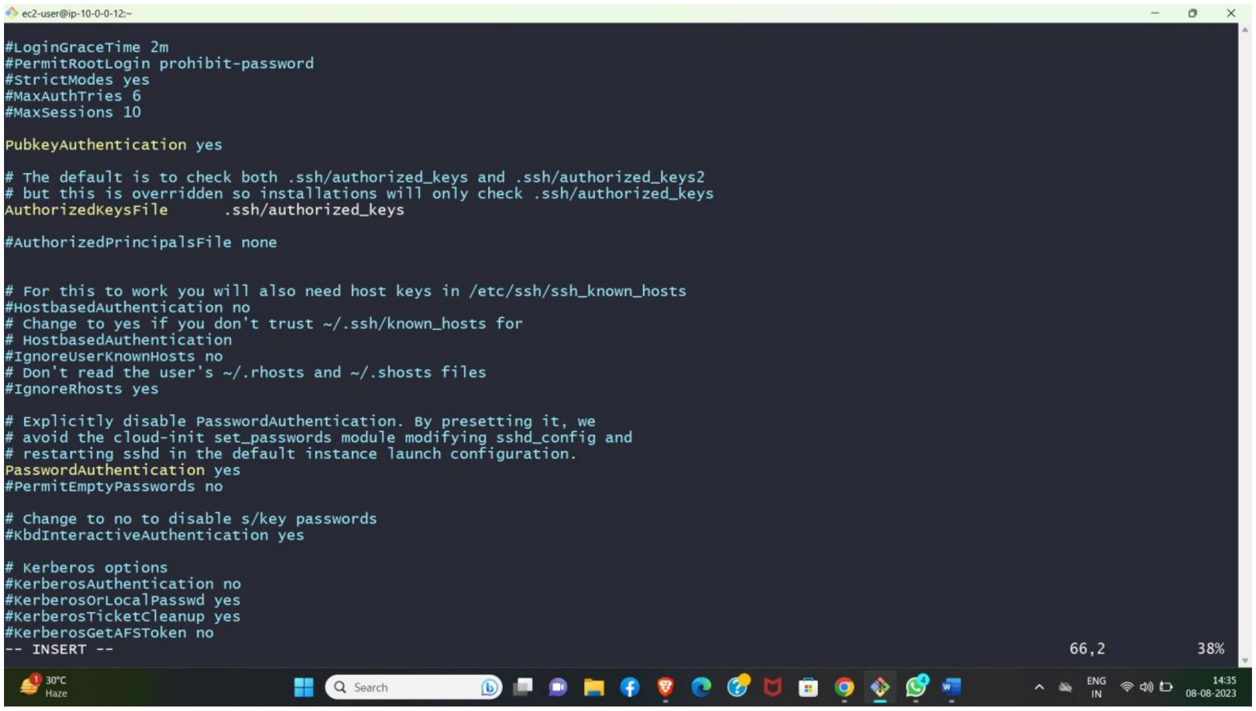
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\gandh> cd .\Downloads\
PS C:\Users\gandh\Downloads> ssh -i "krish.pem" ec2-user@ec2-54-159-130-239.compute-1.amazonaws.com
The authenticity of host 'ec2-54-159-130-239.compute-1.amazonaws.com (54.159.130.239)' can't be established.
ED25519 key fingerprint is SHA256:pryDH9l8chy+ErNqOt13nYQHnyxzwdNporZN4dSnHGQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-159-130-239.compute-1.amazonaws.com' (ED25519) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 12 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-85-233 ~]$
```

- Add user for slave using useradd/passwd



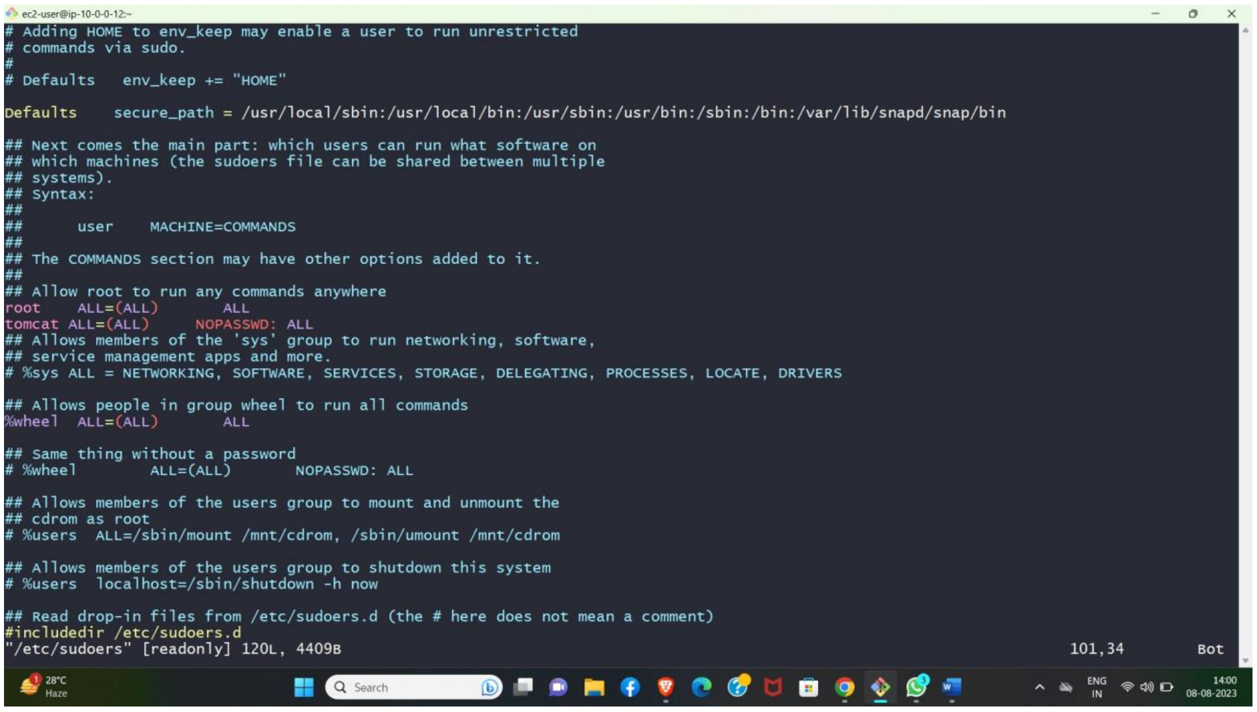
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\gandh> cd .\Downloads\
PS C:\Users\gandh\Downloads> ssh -i "krish.pem" ec2-user@ec2-54-159-130-239.compute-1.amazonaws.com
The authenticity of host 'ec2-54-159-130-239.compute-1.amazonaws.com (54.159.130.239)' can't be established.
ED25519 key fingerprint is SHA256:pryDH9l8chy+ErNqOt13nYQHnyxzwdNporZN4dSnHGQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-159-130-239.compute-1.amazonaws.com' (ED25519) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 12 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-85-233 ~]$ sudo useradd slave1
[ec2-user@ip-172-31-85-233 ~]$ sudo passwd slave1
Changing password for user slave1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-172-31-85-233 ~]$ sudo vi /etc/ssh/sshd_config
[ec2-user@ip-172-31-85-233 ~]$
```

- And give permissions for passwd authentication



```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none


# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# Explicitly disable PasswordAuthentication. By presetting it, we
# avoid the cloud-init set_passwords module modifying sshd_config and
# restarting sshd in the default instance launch configuration.
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
-- INSERT --                                                                    66,2          38%
```

- Edit the sudoers file to edit the file command is
- sudo vi /etc/sudoers
- add tomcat (ALL) NOPASSWD:ALL

- 

```
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/var/lib/snapd/snap/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
tomcat ALL=(ALL)     NOPASSWD: ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
"/etc/sudoers" [readonly] 120L, 4409B                                              101,34        Bot
```

-
- Add ssh for slave
-

sudo useradd jenkins-slave1

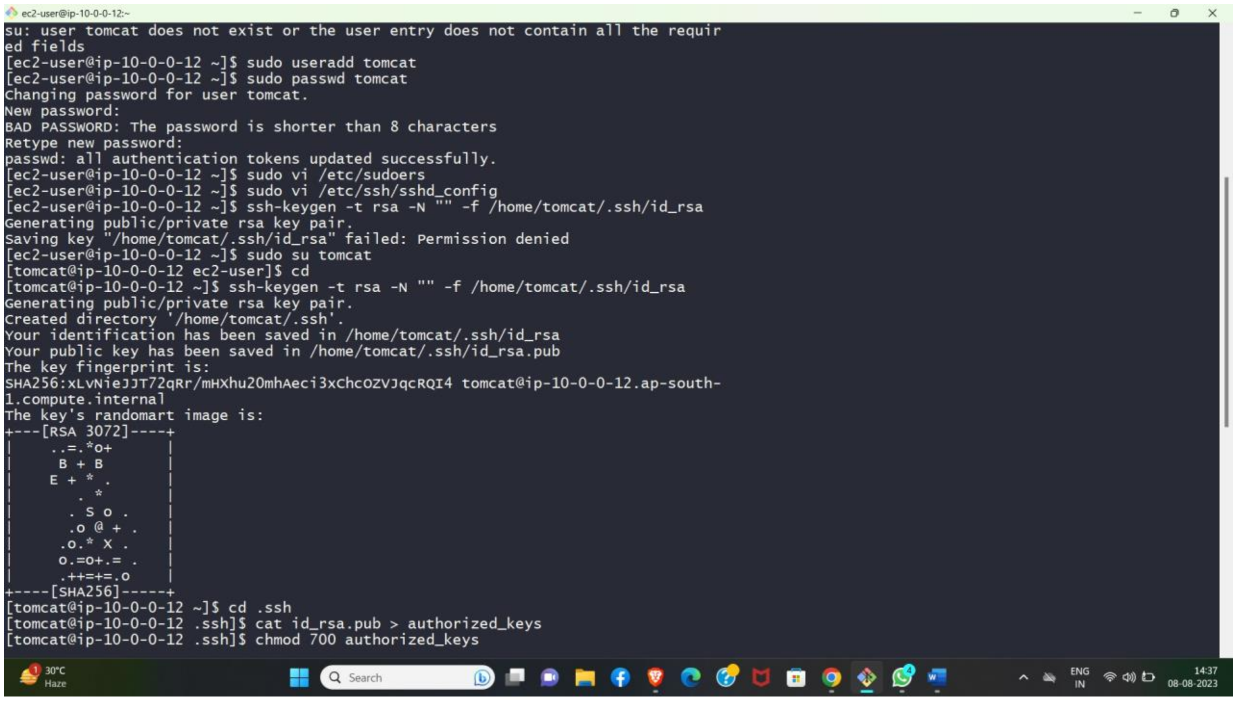
sudo su - jenkins-slave1

ssh-keygen -t rsa -N "" -f /home/jenkins-slave1/.ssh/id_rsa

cd .ssh

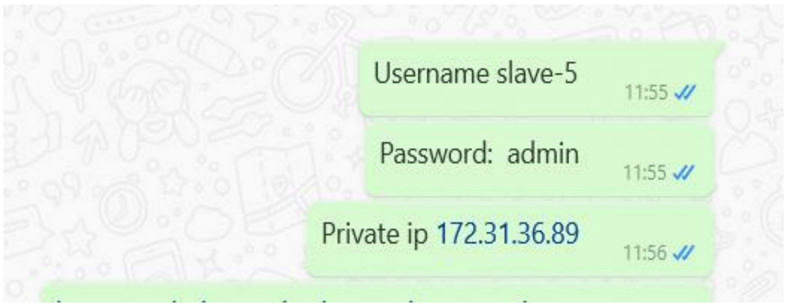
cat id_rsa.pub > authorized_keys

chmod 700 authorized_keys



```
su: user tomcat does not exist or the user entry does not contain all the requir
ed fields
[ec2-user@ip-10-0-0-12 ~]$ sudo useradd tomcat
[ec2-user@ip-10-0-0-12 ~]$ sudo passwd tomcat
Changing password for user tomcat.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[ec2-user@ip-10-0-0-12 ~]$ sudo vi /etc/sudoers
[ec2-user@ip-10-0-0-12 ~]$ sudo vi /etc/ssh/sshd_config
[ec2-user@ip-10-0-0-12 ~]$ ssh-keygen -t rsa -N "" -f /home/tomcat/.ssh/id_rsa
Generating public/private rsa key pair.
Saving key "/home/tomcat/.ssh/id_rsa" failed: Permission denied
[ec2-user@ip-10-0-0-12 ~]$ sudo su tomcat
[tomcat@ip-10-0-0-12 ec2-user]$ cd
[tomcat@ip-10-0-0-12 ~]$ ssh-keygen -t rsa -N "" -f /home/tomcat/.ssh/id_rsa
Generating public/private rsa key pair.
Created directory '/home/tomcat/.ssh'.
Your identification has been saved in /home/tomcat/.ssh/id_rsa
Your public key has been saved in /home/tomcat/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xLvNieJJT72qRr/mHXhu20mhAeci3xChcOZVJqcRQI4 tomcat@ip-10-0-0-12.ap-south-
1.compute.internal
The key's randomart image is:
+---[RSA 3072]----+
|     ..=.*o+     |
|      B + B      |
|     E + * .     |
|        . *      |
|       . S o .   |
|       .o @ + .  |
|      .o.* X .   |
|     o.=o+.= .   |
|      .++=+=.o   |
+----[SHA256]-----+
[tomcat@ip-10-0-0-12 ~]$ cd .ssh
[tomcat@ip-10-0-0-12 .ssh]$ cat id_rsa.pub > authorized_keys
[tomcat@ip-10-0-0-12 .ssh]$ chmod 700 authorized_keys
```

- Then connect to master you can give your public ip and user details on master

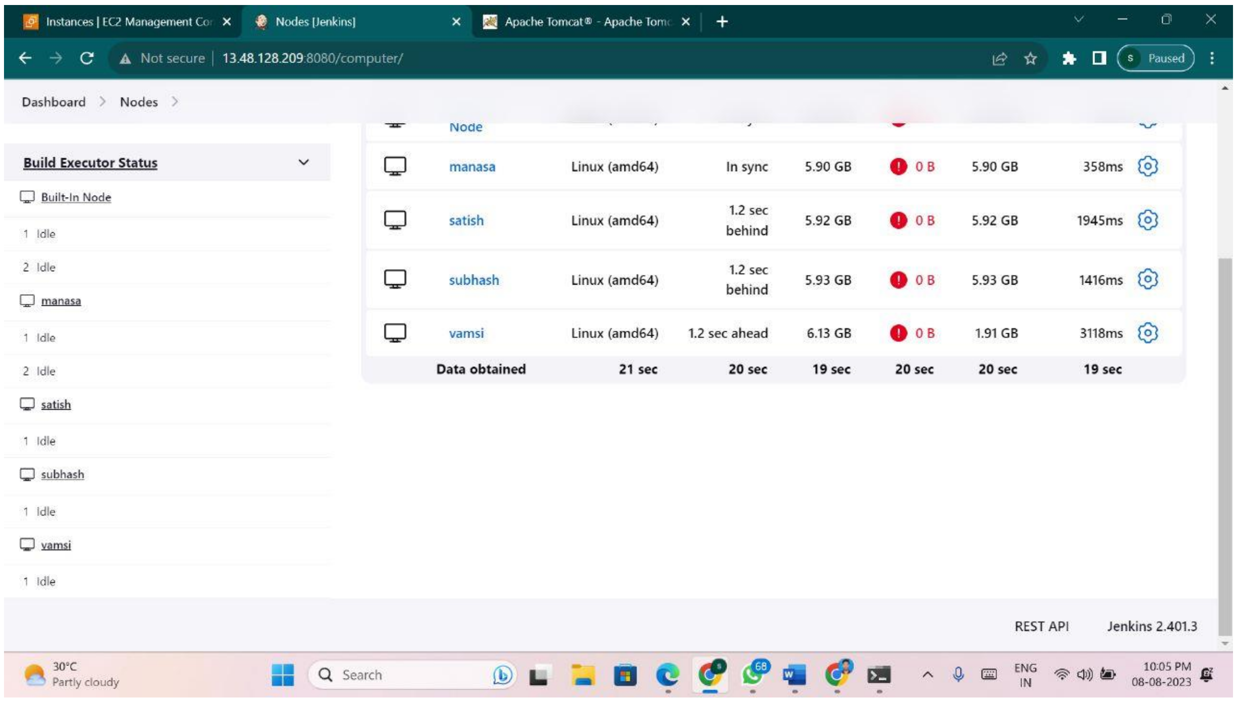


Username slave-5 11:55

Password: admin 11:55

Private ip 172.31.36.89 11:56

- Then connect to master



	Node							
	manasa	Linux (amd64)	In sync	5.90 GB	● 0 B	5.90 GB	358ms	⚙
	satish	Linux (amd64)	1.2 sec behind	5.92 GB	● 0 B	5.92 GB	1945ms	⚙
	subhash	Linux (amd64)	1.2 sec behind	5.93 GB	● 0 B	5.93 GB	1416ms	⚙
	vamsi	Linux (amd64)	1.2 sec ahead	6.13 GB	● 0 B	1.91 GB	3118ms	⚙
	Data obtained	21 sec	20 sec	19 sec	20 sec	20 sec	19 sec	

Build Executor Status

- Built-In Node
  - 1 Idle
  - 2 Idle
- manasa
  - 1 Idle
  - 2 Idle
- satish
  - 1 Idle
- subhash
  - 1 Idle
- vamsi
  - 1 Idle

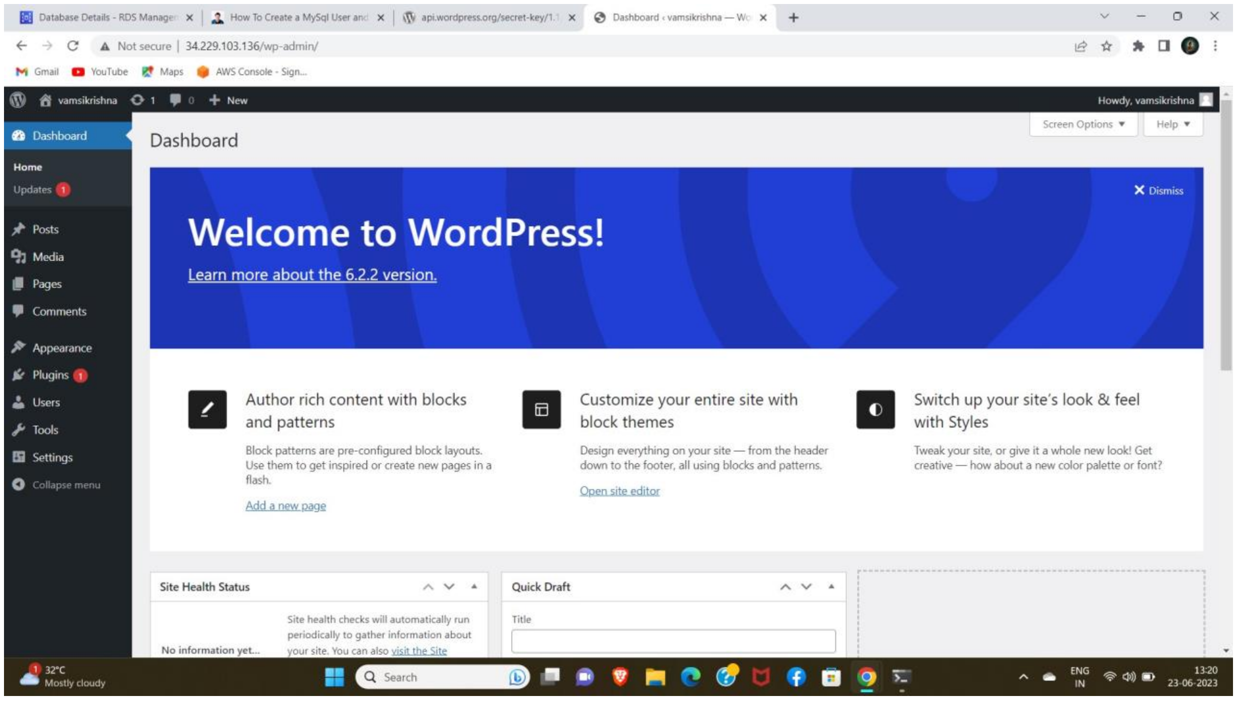
REST API Jenkins 2.401.3

- And send the wordpress git repositry and public ip and userdata commands for docker-compose for master
- Like https://github.com/krishnanaidu99/my-dc.git

- And give Commands for master like

```
sudo yum update -y
sudo amazon-linux-extras install docker
sudo yum install docker
sudo service docker start
sudo usermod -a -G docker ec2-user
sudo curl -L
https://github.com/docker/compose/releases/latest/download/docker-com
pose-$(uname -s)-$(uname -m) -o /usr/local/bin/docker-compose
sudo chmod +x /usr/local/bin/docker-compose
docker-compose version
sudo docker-compose up -d
```

- Master was deploy your project then you can browse the ip adress
-



Not secure | 34.229.103.136/wp-admin/

Dashboard

Welcome to WordPress!

Learn more about the 6.2.2 version.

Author rich content with blocks and patterns

Block patterns are pre-configured block layouts. Use them to get inspired or create new pages in a flash.

Add a new page

Customize your entire site with block themes

Design everything on your site — from the header down to the footer, all using blocks and patterns.

Open site editor

Switch up your site's look & feel with Styles

Tweak your site, or give it a whole new look! Get creative — how about a new color palette or font?

Site Health Status

No information yet...

Site health checks will automatically run periodically to gather information about your site. You can also visit the Site

Quick Draft

Title