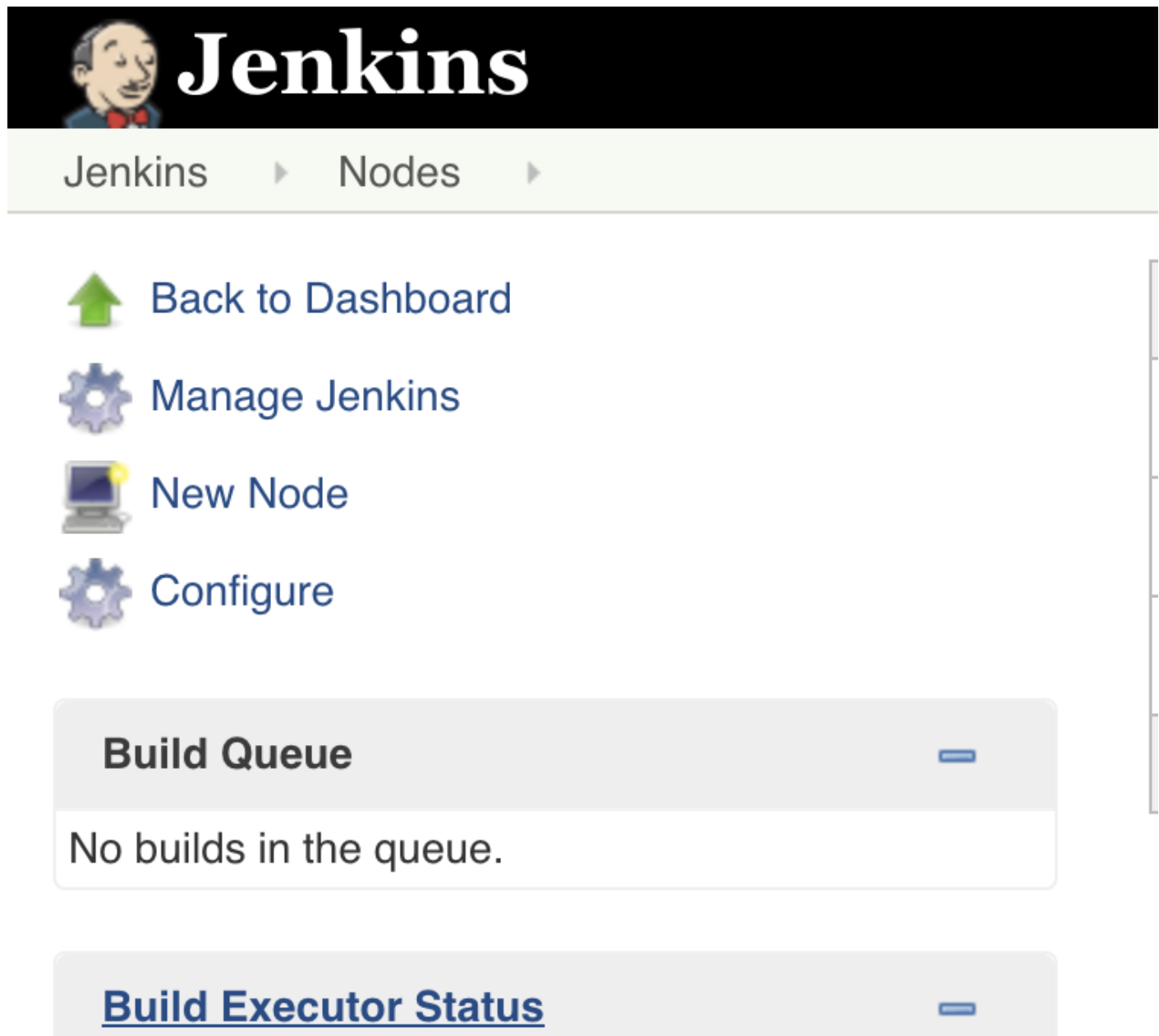


# JENKINS MASTER SLAVE SETUP IN AWS EC2

Adding the slave node to the master

Log in to the Jenkins console via the browser and click on "Manage Jenkins" and scroll down to the bottom. From the list click on "Manage Nodes". In the new window click on "New Node".



Give a name to the node, select "Permanent Agent" and click on OK

Node name

☒ **Permanent Agent**  
Adds a plain, permanent agent to Jenkins. This is called "permanent" because Jenkins doesn't provide higher level of integration with these agents, such as dynamic provisioning. Select this type if no other agent types apply — for example such as when you are adding a physical computer, virtual machines managed outside Jenkins, etc.

☐ **Copy Existing Node**  
Copy from

In the remote root directory field enter a path in the slave node. Note that ssh user **must have read/write access** to this directory path. Here I use the ssh user's home directory.

Enter the slave nodes IP address in the field.

Name

Description

# of executors

Remote root directory

Labels

Usage

Launch method

Host

Credentials

Host Key Verification Strategy

Availability

**Node Properties**

☐ Disable deferred wipeout on this node

☐ Environment variables

☐ Tool Locations

Click on the "Add" button near the credentials field. Jenkins will popup a new window to add credentials. Select the kind as "SSH Username with private key" from the drop-down. Enter the user name of the slave node. In the private key field add the Jenkins masters private key. You can find the private key with the below command,

Generated private key by following steps:

On the agent machine:

1. Log in to the agent machine
2. Create private and public SSH keys. The following command creates the private key `jenkinsAgent_rsa` and the public key `jenkinsAgent_rsa.pub`. It is recommended to store your keys under `~/.ssh/` so we move to that directory before creating the key pair.

```
mkdir ~/.ssh; cd ~/.ssh/ && ssh-keygen -t rsa -m PEM -C "Jenkins agent key" -f "jenkinsAgent_rsa"
```
3. Add the public SSH key to the list of authorized keys on the agent machine


```
cat jenkinsAgent_rsa.pub >> ~/.ssh/authorized_keys
```
4. Ensure that the permissions of the `~/.ssh` directory is secure, as most ssh daemons will refuse to use keys that have file permissions that are considered insecure:


```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys ~/.ssh/jenkinsAgent_rsa
```
5. Copy the private SSH key (`~/.ssh/jenkinsAgent_rsa`) from the *agent machine* to your OS clipboard (eg: `xclip`, `pbcopy`, or `ctrl-c`).

```
cat ~/.ssh/jenkinsAgent_rsa
```

The output should be similar to this:

```
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```


**Jenkins Credentials Provider: Jenkins**


**Add Credentials**

Domain

Kind

Scope

ID

Description

Username

Private Key ☒ Enter directly

Key 

Enter New Secret Below

Passphrase

Add Cancel

Click on add and select the credentials we created from the drop-down. Click on save. If you did all the correct slave node will come to live state within a few seconds.

Note:

1. In case if you unable to connect change the **Host Key Verification Strategy** to

Non verifying verification strategy and Save it and click on Relaunch agent.

2. Make sure u have install Java in the agent server



