Master-Agent Architecture Setup

**SSH Key Setup (Master → Agent)**

On **master node**:

*cd ~/.ssh*

*ssh-keygen*

*cat ~/.ssh/id\_rsa.pub*

*No passphrase needed during generation.*

On **agent node**:

*cd ~/.ssh*

*vim authorized\_keys*

*# Paste the public key from master node into new line*

On **master node:**

sudo cat /var/lib/jenkins/secrets/initialAdminPassword

Copy the password and paste in Jenkins

**Add Agent in Jenkins UI**

* Go to **Manage Jenkins** → **Nodes**
* Click **New Node**
* Name the node (e.g., *k8s*)
* Type: **Permanent Agent**

Fill these details:

* *Remote root directory*: /home/ubuntu
* *Labels*: k8s
* *Launch method*: **Launch agent via SSH**
* *Host*: <agent-node-public-ip>
* *Credentials*: Choose or create SSH username with private key:
  + Username: *ubuntu*
  + Paste private key from master node (~/.ssh/id\_rsa)
  + Verification strategy: *No Verification*

Save and **Launch Agent**  
Check connection logs to ensure it's online.

**Update Jenkinsfile to Target Agent**

Replace agent any with labeled agent:

*pipeline {*

*agent { label 'k8s' }*

*stages {*

*stage('Hello') {*

*steps {*

*echo 'Hello World'*

*}*

*}*

*stage('Create Folder') {*

*steps {*

*sh "mkdir -p devops1"*

*}*

*}*

*stage('Demo') {*

*steps {*

*sh "mkdir -p devops2"*

*}*

*}*

*}*

*}*

**Notes & Clarifications**

* Ran *sudo apt update* twice—one is enough unless it’s after adding new repositories.
* For SSH key-based agent setup, both nodes need inbound SSH access and correct user permissions.
* Ensure Jenkins master can resolve the agent’s IP and the port isn’t blocked by security groups.
* If managing multiple agents, label naming conventions matter for easy pipeline targeting.
* To clean old builds, add a **Build Discarder** property with rules like *daysToKeepStr: 3*, *numToKeepStr: 4*.