Jenkins Nodes

Types of Nodes

- **Master Node:**
    - The central instance of Jenkins is called the Master Node.
    - It handles tasks such as scheduling builds, monitoring agents, and serving the Jenkins web interface.
- **Agent (or Slave) Node:**
    - A node that is set up to offload tasks from the master node.
    - Agents can run on the same machine as the master or on separate machines.

Setting up Nodes

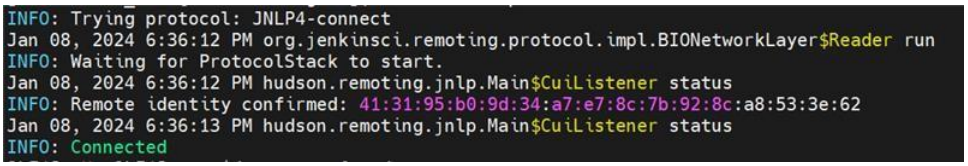
- **Adding Nodes:**
    - Go to Jenkins Dashboard -> Manage Jenkins -> Manage Nodes and Clouds.
    - Click on "New Node" to add a new agent node.
    - Provide a name, choose the type (permanent or a one-time agent), and configure other settings.
- **Configuring Agents:**
    - Agents can be configured using Java Web Start or by connecting them with a secret key.
    - For permanent agents, install the Jenkins agent software on the machine and configure it with the master.
- **Usage:**
    - Jobs in Jenkins can be configured to run on specific nodes, ensuring the workload is distributed across multiple machines.

Agents Connectivity Issue Standard Operating Procedure

Agent Name: Onprem_Agent_Main

If onpremjenkins_agent goes down pls follow the below to bring up the agent again

- connect to the agent server using the credentials
- 192.168.0.28
  username - Automation_Prod
  password - Welcome#1
- go to below path
- cd /home/Automation_Prod/jenkins/agent
- and run the startagent.sh file
- ./startagent.sh
- check the logs if the agent gets connected or not using the below command
- tail -f nohup.out
- If you see connected in the output, then agent is connected.

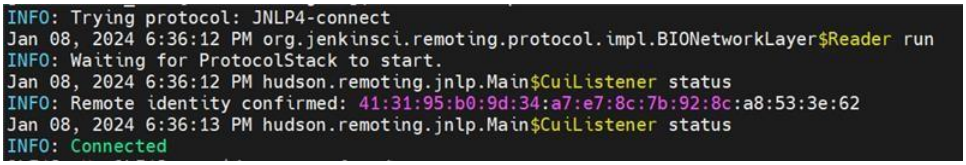


Agent Name: Scans_Agent

If Scans_Agent goes down pls follow the below to bring up the agent again

- connect to the agent server using the credentials
- 192.168.0.33
  username - anil
  password - Welcome1
- Go to below path
- cd /home/anil/jenkins_agent
- and run the startagent.sh file

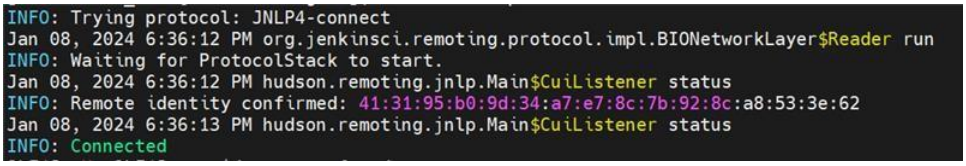
- ./startagent.sh
- check the logs if the agent gets connected or not using the below command
- tail -f nohup.out
- If you see connected in the output, then agent is connected.



Agent Name: FileGPS_Onprem_Agent

If FileGPS_Onprem_Agent goes down pls follow the below to bring up the agent again

- connect to the agent server using the credentials
- 192.168.0.35
  username - filegps
  password – Pragma@07
- Go to below path
- cd /home/filegps/jenkins_agent
- and run the startagent.sh file
- ./startagent.sh
- check the logs if the agent gets connected or not using the below command
- tail -f nohup.out
- If you see connected in the output, then agent is connected.

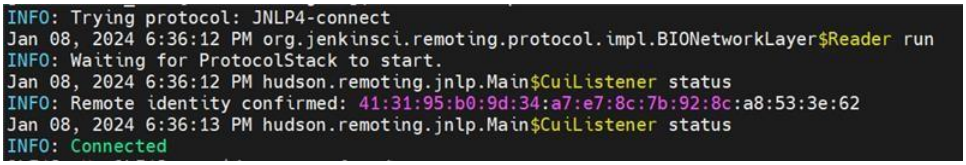


Agent Name: PCM_Cloud_CICD_Agent

If PCM_Cloud_CICD_Agent goes down pls follow the below to bring up the agent again

- connect to the agent server using the credentials

- 52.0.121.130
  username - ubuntu
  pem key – for pem key reach out cloud team
- Go to below path
- cd /jenkins
- and run the startagent.sh file
- ./startagent.sh
- check the logs if the agent gets connected or not using the below command
- tail -f nohup.out
- If you see connected in the output, then agent is connected.



Agent Name: Jarvis_Cloud_Agent

If Jarvis_Cloud_Agent goes down pls follow the below to bring up the agent again

- connect to the agent server using the credentials
- 54.235.246.73
  username – jenkins
  password – Pragma@123#
- Go to below path
- cd /opt/jenkins_agent
- and run the startagent.sh file
- ./startagent.sh
- check the logs if the agent gets connected or not using the below command
- tail -f nohup.out
- If you see connected in the output, then agent is connected.

Access Management

Access management in Jenkins involves controlling who can access the Jenkins server, what actions they can perform, and which resources they can access.

Authentication

- **Jenkins Authentication:**
    - Jenkins supports various authentication methods, including its built-in database, LDAP, Active Directory, GitHub, and more.
    - Configure authentication in Jenkins Dashboard -> Manage Jenkins -> Configure Global Security.

Authorization

- **Authorization Strategies:**
    - Define who has access to Jenkins and what permissions they have.
    - Common strategies include matrix-based security, role-based access control (RBAC), and Project-based Matrix Authorization Strategy.
- **Matrix-based Security:**
    - Assign permissions to users or groups based on a matrix.
    - Specify permissions like Overall, Job, Run, and other global and specific actions.
- **RBAC:**
    - Define roles with specific permissions and assign users or groups to these roles.
    - Useful for more granular control over access.