

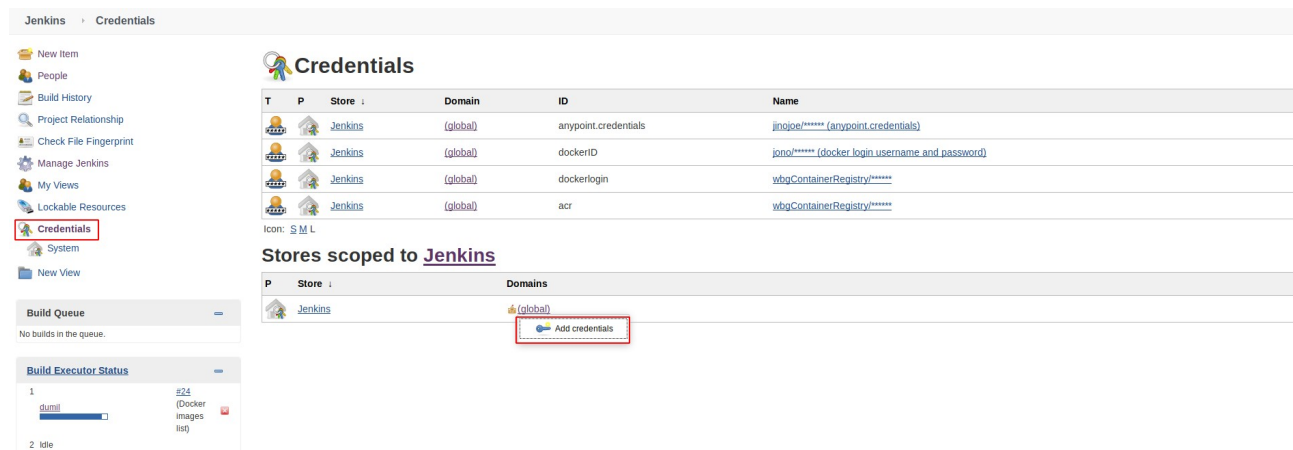
Method one:

Docker image build and push use jenkins (Run as jenkins)

Dependencies:

```
sudo apt update
sudo apt install docker.io -y
sudo systemctl start docker
sudo systemctl enable docker
usermod -aG docker [jenkinsuser]
```

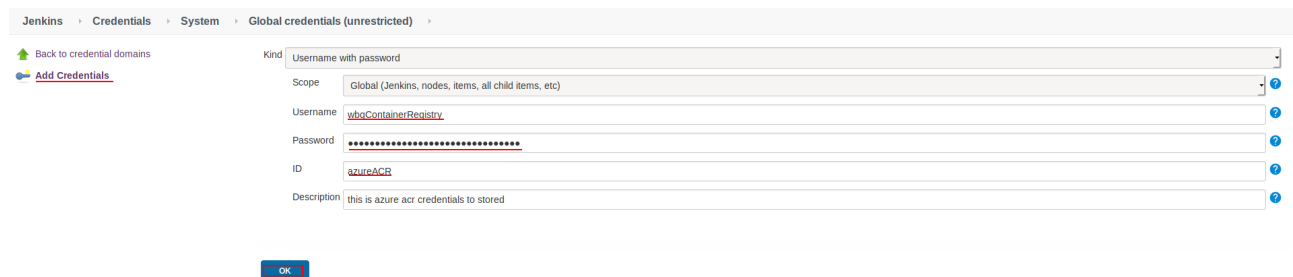
create credentials in jenkins server:



The screenshot shows the Jenkins 'Credentials' page. On the left is a sidebar with navigation links: 'New Item', 'People', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins', 'My Views', 'Lockable Resources', 'Credentials' (highlighted with a red box), 'System', and 'New View'. Below the sidebar are sections for 'Build Queue' (showing 'No builds in the queue.') and 'Build Executor Status' (showing two executors: 'dumil' and 'Idle'). The main content area is titled 'Credentials' and contains a table of existing credentials:

T	P	Store	Domain	ID	Name
		Jenkins	(global)	anypoint.credentials	injoje/***** (anypoint.credentials)
		Jenkins	(global)	dockerID	ijonj/***** (docker login username and password)
		Jenkins	(global)	dockerlogin	wbgContainerRegistry/*****
		Jenkins	(global)	acr	wbgContainerRegistry/*****

Below the table is a section 'Stores scoped to Jenkins' with a table showing the 'Jenkins' store and a button to 'Add credentials' (highlighted with a red box).

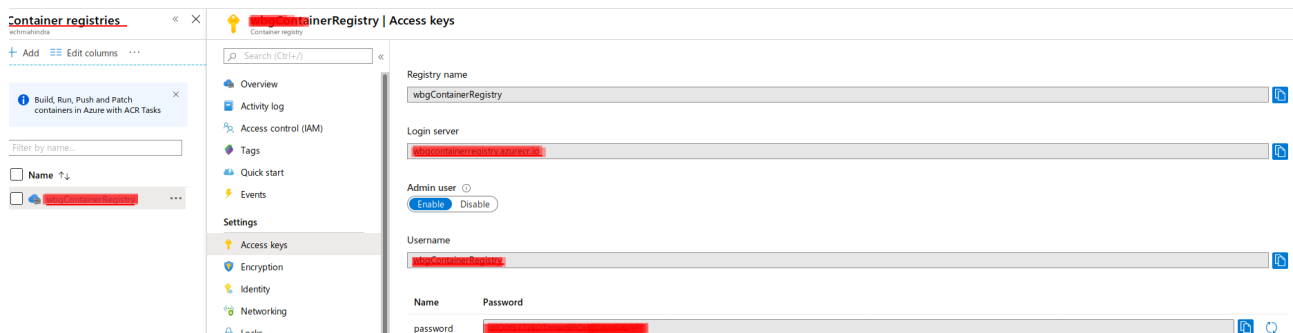


The screenshot shows the 'Add Credentials' form in Jenkins. The breadcrumb trail is 'Jenkins > Credentials > System > Global credentials (unrestricted)'. The form has a left sidebar with 'Back to credential domains' and 'Add Credentials' (highlighted with a red box). The main form fields are:

- Kind: Username with password
- Scope: Global (Jenkins, nodes, items, all child items, etc)
- Username: wbgContainerRegistry
- Password: [Redacted]
- ID: azureACR
- Description: this is azure acr credentials to stored

At the bottom is an 'OK' button.

how to get acr details → login portal.azure.com → go to container registries



The screenshot shows the 'Container registries' page in the Azure Portal. The breadcrumb trail is 'Container registries > wbgContainerRegistry | Access keys'. The left sidebar shows navigation links: 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Quick start', 'Events', 'Settings', 'Access keys' (selected), 'Encryption', 'Identity', 'Networking', and 'Locks'. The main content area shows the 'Access keys' for the 'wbgContainerRegistry' registry. It includes fields for 'Registry name', 'Login server', 'Admin user' (with 'Enable' and 'Disable' buttons), 'Username', and a table of access keys with columns 'Name' and 'Password'.

create Jenkinsfile

```
pipeline {
  agent any
  environment {
    dockerhost = 'containerregistry.azurecr.io'
  }

  stages {

    stage('docker login process') {
      steps {
        script {
          withCredentials([
            usernamePassword(credentialsId: 'azureACR',
              usernameVariable: 'username',
              passwordVariable: 'password')
          ]) {
            sh '''
              docker login $dockerhost -u $username -p $password
            '''
          }
        }
      }
    }

    stage('Docker image build') {
      steps {
        sh 'docker build -t $dockerhost/test:latest .'
      }
    }

    stage('Docker images list') {
      steps {
        sh 'docker push $dockerhost/test:latest '
        sh 'docker logout $dockerhost '
      }
    }
  }

  post {
    always {
      echo 'One way or another, I have finished'
      deleteDir() /* clean up our workspace */
    }
    success {
      echo 'I succeeeded!'
    }
    unstable {
      echo 'I am unstable :/'
    }
    failure {
      echo 'I failed :('
    }
    changed {
      echo 'Things were different before...'
    }
  }
}
```
