**Security measures implemented in Jenkins pipeline**

* **Role-Based Access Control (RBAC):** Jenkins provides role-based access control to assign specific roles and permissions to users or groups. Ensure that only authorized users have access to the pipeline configurations.
* **Jenkins Credentials Plugin:** Use the Jenkins Credentials Plugin to securely manage and encrypt sensitive credentials (API keys, SSH keys, passwords, etc.). Do not hard-code them in pipeline scripts.

When you see the properties document is the place where we can store values of the variables passing through the Jenkins script.for example I uses aws count id passing through the variable document named properties instead of hardcoding the aws account id in the pipeline script.

sh "docker tag devloot:latest${AWS\_Account}.dkr.ecr.us-west-1.amazonaws.com/devloot:latest"

* **Use Declarative Pipelines:** Use Jenkins' declarative pipelines as they are easier to read and more secure compared to script-based (imperative) pipelines.