Running AWS commands using Jenkins pipelines

February 27, 2021

Jenkins is a well known tool used in the DevOps world to automate processes. Typically, it's mostly used to build and deploy software as part of a CI/CD process, including cloning code from git, running a build job, running tests and deploying the resulting artifacts. However, Jenkins pipelines can be used to automate anything at all. Because of its built-in credentials manager, multi-node architecture and multitude of plugins, it can be worth it to centralize a lot of the repeated tasks you may have inside of Jenkins, rather than having scripts resting on a server somewhere. In this post we'll see how to use a Jenkins pipeline to connect to AWS and retrieve a list of S3 buckets available.

Storing credentials

The first thing you should do is securely store your credentials. One of the oldest security issue that IT people have had to deal with is the management of credentials. If you use a shell script to run your command, then you need credentials to be stored inside the script, or possibly inside of a configuration file. In either case, those credentials are available in plain text. By using Jenkins Credentials Manager, you can store them securely.

For this task, simply create an IAM user in your AWS account, granting it read access to S3, and gathering the access key and secret. By going to the *Manage Jenkins* link in the Jenkins interface, you can then click on *Manage Credentials* and add new secure strings. Name them *AWS_ACCESS_KEY* and *AWS_ACCESS_SECRET* respectively.

Designing the pipeline

Once the credentials are stored, we need to design our pipeline. The end result will have 3 steps:

1. First we'll install the AWS CLI.
2. Then we'll store the credentials for the CLI to use from the Credentials Manager.
3. Finally we'll run our command.

Final result

Here is the final code for the pipeline:

```
node('jenkins-slave-python') {

 stage('Installing AWS CLI') {

  sh 'python -m pip install awscli'

 }
 stage('Saving AWS cedentials') {
  withCredentials([string(credentialsId: "AWS_ACCESS_KEY", variable: "KEY"),string(credentialsId: "AWS_ACCESS_SECRET", variable: "SECRET")]) {
   writeFile file: '/home/jenkins/.aws/credentials', text: """[default]
aws_access_key_id=$KEY
aws_secret_access_key=$SECRET
"""
  }
 }
 stage('Listing buckets') {
  sh '/home/jenkins/.local/bin/aws s3api list-buckets'
 }
}
```