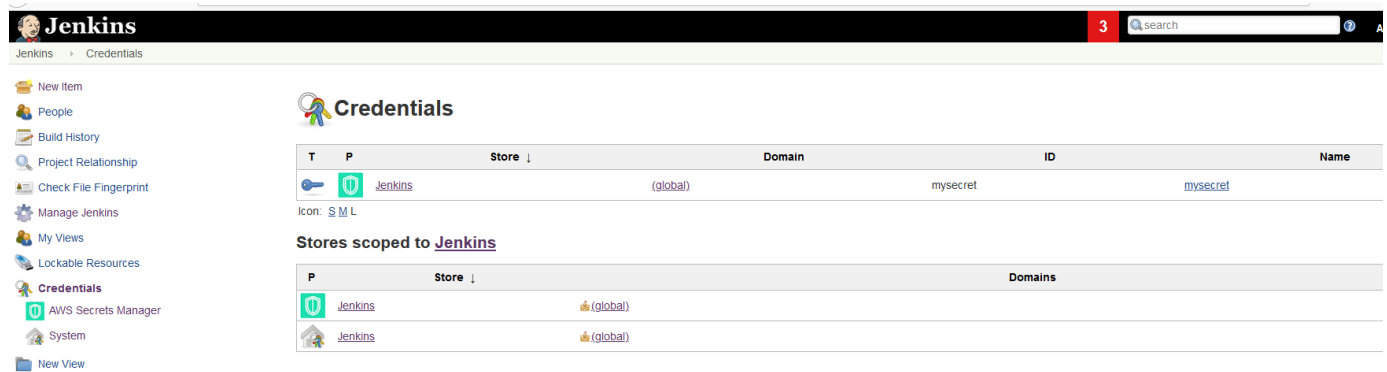


# Integration of Secrets Manager with Ci/CD

Integration of AWS Secrets Manager with Jenkins.

1. Install the Jenkins plugin, AWS Secrets Manager Credentials Provider.
2. The secrets which are stored in the Secrets manager for that particular region can be visible as below,



The screenshot shows the Jenkins web interface. The top navigation bar includes the Jenkins logo, a red notification badge with the number '3', and a search bar. The left sidebar contains a list of navigation links: New Item, People, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins, My Views, Lockable Resources, Credentials (selected), AWS Secrets Manager, System, and New View. The main content area is titled 'Credentials' and displays a table of credentials. The table has columns for 'T' (Type), 'P' (Provider), 'Store', 'Domain', 'ID', and 'Name'. A single credential is listed with a key icon for 'T', a green 'U' icon for 'P', 'Jenkins' for 'Store', '(global)' for 'Domain', 'mysecret' for 'ID', and 'mysecret' for 'Name'. Below the table, there is a section titled 'Stores scoped to Jenkins' which lists two stores: 'Jenkins' (with a green 'U' icon) and 'Jenkins' (with a house icon), both associated with the '(global)' domain.

T	P	Store	Domain	ID	Name
		Jenkins	(global)	mysecret	mysecret

Icon: S M L

**Stores scoped to Jenkins**

P	Store	Domains
	Jenkins	(global)
	Jenkins	(global)

3. To retrieve the secrets in the pipeline, below is the sample pipeline code which can be used in our pipeline.

```
pipeline {
  agent any
  environment {
    MY_KEY = credentials('mysecret')
  }
  stages {
    stage ('Foo') {
      steps {
        echo 'Hello'
      }
    }
  }
}
```