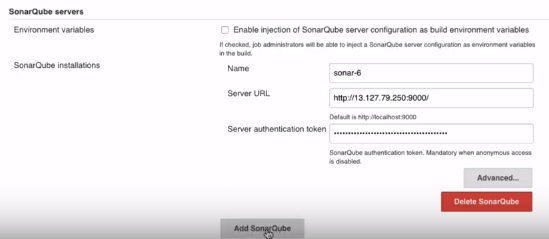
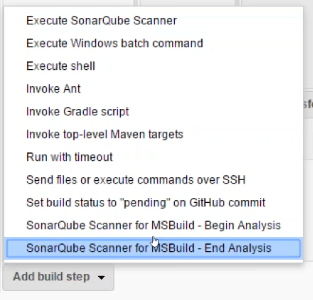
**Code analysis from Jenkins:**

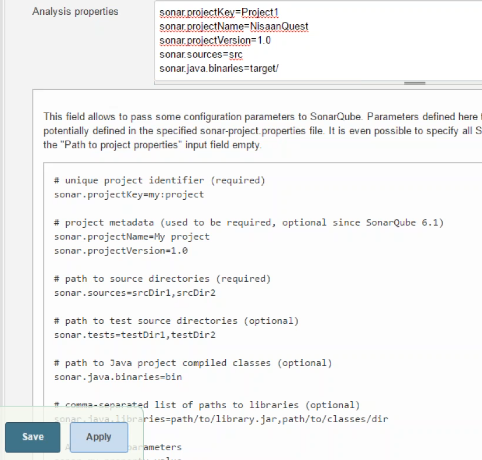
* Generate a token in SonarQube which acts like a username and password, using this token Jenkins connects to SonarQube and publishes the code
* We need to keep this token safe
* Go to configure system settings and set sonar server as below



* We can also multiple sonar servers



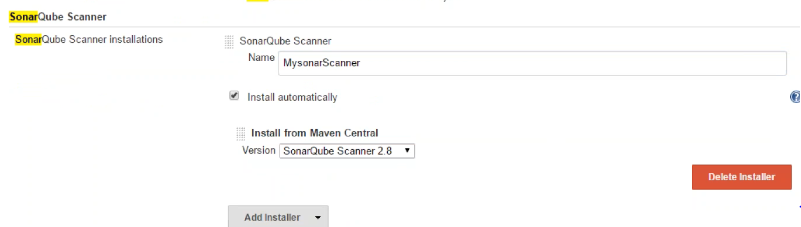
* Select execute sonarqube scanner
* Add analysis properties



* We can mention task to run, we can bring any project related properties to path to project properties, and otherwise we can configure analysis properties
* Sonar.projectname, we can mention any name we want
* Sonar.version, we can mention whatever the version
* Sonar.sources, we can mention the directories of code. If we have more than one, we can separate it by ,
* Sonar.tests, for test file
* Sonarsrc is the directory of code
* Proxy in the browser and the proxy in Jenkins under plugin manager should match



* We need to add sonar scanner in global build tools also



* Add sonar.scm.disabled=true in analysis properties of job
* Once we successfully run the job, we can see the project details in sonar dashboard
* We can provide the link to developers, they can verify the violations in that
* We may can add PMD or security checks etc inside sonar if the plugins are available

We can integrate SonarQube with Jira to trigger a ticket automatically where developer can solve it

We can generate authentication token and change the admin password inside account settings as below

