Automating your CI/CD Stack   
with Java and Groovy

Jeanne Boyarsky & Scott Selikoff

Tuesday Oct 23, 2018

Oracle Code One – HOL4957

Table of Contents

Step 0: Perquisite and Tools 4

0.1 Basic Requirements – PLEASE READ! 4

0.2 - Docker 4

0.3 - Docker Images 5

0.4 - The ability to run curl 6

0.5 – Optional: Groovy 6

Step 1: Start Nexus and Jenkins 8

1.1 - Create network bridge 8

1.2 - Install Nexus 8

1.3 - Install Jenkins 8

1.4 – Verify Jenkins is Running 8

1.5 - Unlock Jenkins 9

1.6 – Add additional plugins 10

Step 2: Basic Jenkins Scripting 12

2.1 - Run your first Groovy script in Jenkins 12

2.2 - Run your first job containing Groovy scripting 12

2.3 - Writing your own script in Jenkins 14

Step 3: Basic Nexus Scripting 15

3.1 - Run your first Groovy script in Nexus 15

3.2 - Looking in the task log on the command line 16

3.3 - Writing your own script in Nexus 16

3.4 - log vs println 17

Step 4: Jenkins System Scripting 18

4.1 - Tools for finding methods 18

4.2 - Creating a user 19

4.3 - Setting up the authorization strategy 20

Step 5: Nexus System Scripting 22

5.1 - Learn what objects are available 22

5.2 - Create global access and Jenkins access 22

5.3 - Setup Nexus Access 23

Step 6 – Create a Jenkins pipeline 24

6.1 - Setup Nexus Credentials in Jenkins 24

6.2 - Create a job to setup jobs with proper configuration 24

6.3 - Testing Access and Running Jenkins Jobs 25

6.4 - Testing access and Viewing Nexus artifacts 26

6.6 - Editing a pipeline job 27

Step 7 – Switch services (Optional) 28

7.1 - Download and Build sea-lion Project 28

7.2 - Stop Nexus and Jenkins to free up some resources 28

7.3 - Install SonarQube 29

Step 8 – Creating a custom SonarQube rule 30

8.1 - Deploying a custom rule 30

8.2 - Add this rule to the default quality profile 30

8.3 - Run a scan with this custom rule 32

Step 9 – Extra credit in Jenkins (Optional) 34

Appendix I: Cleanup 35

I.1 Stop containers: 35

II.2 Reclaiming Disk Space 35

Appendix II: Corrupted Jenkins Roles 36

II.1 Faster way – install your favorite text editor 36

II.2 lower way – delete your docker container/image and start over 36

Appendix III: Useful References 37

## Step 0: Prequisite and Tools

This lab requires the following:

1. Docker
2. Docker images
3. Groovy
4. The ability to run curl

### 0.1 Basic Requirements – PLEASE READ!

#### Space Requirements

For this lab, you will need approximately **2 gigabytes** of space. So as not to tax the conference network, please pull them in advance. See Appendix I at the end of this lab for instructions on how to reclaim disk space after you have completed the lab.

#### Ports Requirements

For this lab, we will be using default ports of **8080**, **8081**, **9000**. If you already have services running on your computer, you will either need to stop those services or change the ports you use to install the various services throughout this lab.

#### Docker ID Requirements

In order to download Docker from the Docker Store and install the software, you will need to have a Docker ID account. If you do not have one, you can create one for free at:

<https://store.docker.com/signup>

Please create a Docker ID account now if you do not already have one.

### 0.2 - Docker

To install Docker, follow the instructions at using your Docker ID account:

<https://docs.docker.com/install>

If your OS doesn't support Docker, you won't be able to do the lab on your machine. You can ask another attendee to pair with you.

*Validation:*

At the command line, run **docker –version** (Small version differences are ok in the output)

$ **docker --version**

Docker version 18.06.0-ce, build 0ffa825

### 0.3 - Docker Images

This will also let you deal with any corporate internet proxies while you are still at work and can ask for help.

At the command line run:

**docker pull sonatype/nexus3:3.13.0**

**docker pull jenkins/jenkins:2.146**

**docker pull sonarqube:7.1**

**Note: “latest” will probably work. These version numbers are the ones we tested with.**

**$ docker pull sonatype/nexus3:3.13.0**

3.13.0: Pulling from sonatype/nexus3

256b176beaff: Pull complete

18d124afa1e9: Pull complete

9bb412307f82: Pull complete

Digest: sha256:19d186d5bc8be1ea4f7bae72756baa830e79bf20aae0e9e7b1a0c7d3ce7ac136

Status: Downloaded newer image for sonatype/nexus3:3.13.0

**$ docker pull jenkins/jenkins:2.146**

2.146: Pulling from jenkins/jenkins

55cbf04beb70: Pull complete

1607093a898c: Pull complete

9a8ea045c926: Pull complete

d4eee24d4dac: Pull complete

c58988e753d7: Pull complete

794a04897db9: Pull complete

70fcfa476f73: Pull complete

806029475e0c: Pull complete

67959b355155: Pull complete

4d217ccd3d4c: Pull complete

0261bb88a4a5: Pull complete

96f2a3ae5539: Pull complete

f6bf99db32d5: Pull complete

bb47d4bbb0e1: Pull complete

4b48ec5d60cf: Pull complete

7280a8dfb767: Pull complete

91091f8d44ca: Pull complete

8ca02cad320f: Pull complete

46009bfec329: Pull complete

f9860b79812e: Pull complete

89ac8103ea67: Pull complete

Digest: sha256:161cb25fbb23a1c5ac5fdd0feebd713edd62c235e199e68b34d1a78205a42da7

Status: Downloaded newer image for jenkins/jenkins:2.146

**$ docker pull sonarqube:7.1**

7.1: Pulling from library/sonarqube

55cbf04beb70: Already exists

1607093a898c: Already exists

9a8ea045c926: Already exists

d4eee24d4dac: Already exists

c58988e753d7: Already exists

794a04897db9: Already exists

70fcfa476f73: Already exists

806029475e0c: Already exists

67959b355155: Already exists

1e6b3af7f55a: Pull complete

e0b67c57c8e1: Pull complete

ce12e009fbe7: Pull complete

3edf8e47f9c4: Pull complete

Digest: sha256:4438a37735caa24d80da31ee29e72d686abdaa8f5009746ec60e0d43519e1a57

Status: Downloaded newer image for sonarqube:7.1

If you get an illegal access error, try placing Java 8 on your path instead of Java 9

### 0.4 - The ability to run curl

If you are running Mac, Linux or Windows 10, you don’t need to do anything. If you are running an older version of Windows, you can install <https://www.cygwin.com>.

*Validation:*

At the command line, run

**curl https://www.oracle.com/code-one/index.html**

and ensure the output isn’t an error message.

### 0.5 – Optional: Groovy

If you want to use Groovy in this lab (vs running everything on the server), ensure JDK 8 is on your path and then follow the instructions at: <http://groovy-lang.org/install.html>

Note: Please download Groovy 2.X rather than 3.X. Version 3.X is in alpha at the time of writing this lab.

Validation:

At the command line, run **groovy –version** (Small version differences are ok in the output)

$ **groovy -version**

Groovy Version: 2.5.2 JVM: 1.8.0\_45 Vendor:

Oracle Corporation OS: Mac OS X

## Step 1: Start Nexus and Jenkins

In this lab, we use basic Docker to make setup simple. We do not set up a volume to persist the data since the emphasis is Groovy setup. (We will start Sonar at the end after stopping Nexus and Jenkins to limit the laptop resources needed by this lab)

### 1.1 - Create network bridge

Create network for services to communicate across:

**docker network create hol-network**

### 1.2 - Install Nexus

At the command line, run:

**docker run -d -p 8081:8081 --name nexus --network hol-network sonatype/nexus3:3.13.0**

*Note: If you’ve run it in the past, type* **docker start nexus** *instead*

Validation

In a browser, go to <http://localhost:8081>. If you do not see Nexus, wait 15 seconds and try again. (It could take up to a minute)

### 1.3 - Install Jenkins

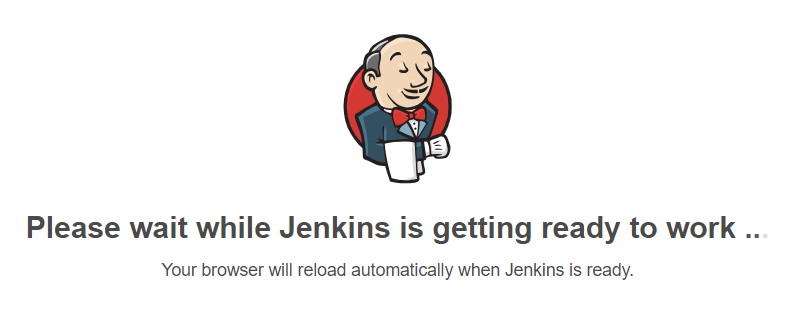
At the command line, run

**docker run -d -p 8080:8080 --name jenkins --network hol-network jenkins/jenkins:2.146**

*Note: If you’ve run it in the past, type* ***docker start jenkins*** *instead*

### 1.4 – Verify Jenkins is Running

1. In a browser, go to <http://localhost:8080>
2. You should see the following screen:



1. Following this page, you will see a page asking for the administrator password. Once you see this, you can continue to the next step.

If you don’t see this screen, you either do not have Jenkins running or may a different service running on port 8080.

### 1.5 - Unlock Jenkins

1. At the command line, run:

**docker exec -it jenkins bash**

1. Print the password:

**cat /var/jenkins\_home/secrets/initialAdminPassword**

1. Back in your browser visit <http://localhost:8080> again.



1. Paste in the password and click continue
2. Allow Jenkins to install the suggested plugins
   1. Failure to install the suggested plugins will cause problems later in the lab.
3. In the command line window, type exit to get out of bash.
4. Pick a username/password for your admin test user. Enter all the fields and click “Save and Continue”
5. Click to Finish
6. Click “Start using Jenkins”



### 1.6 – Add additional plugins

We need two additional plugins to create jobs for this lab.

1. In the left navigation, click “Manage Jenkins”
2. Click “Manage Plugins”
3. Click the “Available” tab
4. Select **Groovy**, as well as the **Role-based Authorization Strategy** plugin. We’ll use that one later.



1. Click the button “Download now and install after restart”
2. Check to restart



1. Refresh the page after a few seconds (or click “Enable Auto Refresh” on top)
2. Login as admin
3. Click “Manage Jenkins” again
4. Click “Global Tool Configuration”
5. Click “Add Groovy”



1. Set the name to “Groovy 2.X”. Leave the version as the default. (This gives us a slightly different of Groovy, but this is fine as long as we stay on the 2.X series.)



1. Click “Save” (scroll down/right if you don’t see the save button)

## Step 2: Basic Jenkins Scripting

### 2.1 - Run your first Groovy script in Jenkins

Let’s confirm what version of Groovy is being used in Jenkins.

1. On the left navigation, click “Manage Jenkins”

*Note: Jenkins will tell you that you aren’t the latest version. Just ignore this. (We wanted everyone to be on the same version so we picked a version available from a month or so ago)*

1. Click “Script Console”
2. Write:

**println 'Hello Oracle Code One!** **'**

**println GroovySystem.version**

1. The result is right below the text area:



### 2.2 - Run your first job containing Groovy scripting

1. In the left navigation, click “New item”
2. Enter “my-first-script” as the job name and choose “Freestyle Project”



1. Scroll down and click “Ok”
2. Add a Groovy build step



1. Choose “Groovy 2.X” to run
2. In the textbox, enter the code

**println 'Hello Oracle Code One!** **'**

**println GroovySystem.version**

****

1. Click “Save”
2. Click “Build Now”
3. Click your job number and view the Console Output.

*Tip:* You can click the circle to go directly to the console.



1. Note that Jenkins installed Groovy the first time it was needed.



### 2.3 - Writing your own script in Jenkins

This time we are going to write a script where you fill in the blank to print out all the strings that end with “day”.

*Tip*: If you’ve never used Groovy before, see the solution guide for how to do this. (also note that Groovy uses grep where Java uses filter)

def list = ['monday', 'wednesday', 'chocolate', 'friday']

println \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Use the Jenkins admin script console to test your script until you are happy with it. Then create a job named “days” that runs the same Groovy code.

## Step 3: Basic Nexus Scripting

### 3.1 - Run your first Groovy script in Nexus

Let’s confirm what version of Groovy is being used.

1. Login to Nexus (localhost:8081) using admin/admin123.
2. Click the gear icon to get the administration options



1. In the left navigation, scroll down and choose the last line “Tasks”
2. Click “Create Task”
3. Choose “Admin - Execute Script”
4. Enter a task name.
5. For the script source, enter:

**log.info 'Hello Oracle Code One!** **'**

**log.info GroovySystem.version**

1. For task frequency, choose “Manual”
2. Click “Create Task”
3. Click the task name
4. Click Run



1. Click “Yes” to confirm
2. Click Summary tab. Depending on how fast you are, it will either say Running or Waiting. Refresh if it is still running to confirm it completes.



1. In the left navigation go to Support > Logging > Log Viewer
2. Notice your logging is there:



1. Note that this is not the same version as Jenkins used; but it is close enough to not cause us difficulties.

### 3.2 - Looking in the task log on the command line

1. In a new command line tab/window, run:

**docker exec -it nexus bash**

1. Print the log file:

**cd /nexus-data/log/tasks**

**ls**

**cat \*.log**

1. Confirm you see 8 lines.
2. Now can you find the main nexus.log file. If so, run

**tail –f nexus.log**

1. In your browser, re-run your Groovy task. How many lines do you see added to the tail output? It’s not 8 lines. Can you figure out the difference between the nexus log and task log?

### 3.3 - Writing your own script in Nexus

Now try to write your own Groovy script that prints out a countdown. The output includes the arrows and should be:

--> 10

--> 9

--> 8

--> 7

--> 6

--> 5

--> 4

--> 3

--> 2

--> 1

Blast off!

Tip for Groovy developers: the log.info method takes a Java String and not a GString.

Tip for Java developers: you can use groovy on your machine or the Jenkins scripting console to interactively nail down the syntax. Or look at the solution guide.

Check the output in both a browser (nexus log) and command line (task log).

**Challenge**: can you write the Groovy code in two lines of no more than 40 characters each? You can use <https://www.lettercount.com> to check the number of characters.

### 3.4 - log vs println

1. In your prior example, change **log.info** to **println**
2. Run the task
3. Check the output in both the browser and command line task log. Where do you see it?

## Step 4: Jenkins System Scripting

We are going to setup Jenkins to have different teams and permissions for each.

* The Open Ospreys allow all Jenkins users to see their projects. Olivia and Owen are on this team.
* The Secret Sea Lions only allow their team members to see their projects. Sam and Sophia are on this team.

It’s easiest to start in the scripting console and create our script interactively. Once we know the syntax and APIs, we’ll delete that configuration. Then we will run the Groovy code through a job to be repeatable.

Note: If you are using LDAP/AD and/or Jenkins Enterprise, you’ll have more powerful access control options available to you.

### 4.1 - Tools for finding methods

Note that Jenkins was an offshoot of Hudson. The source code betrays this fact and still has some Hudson class/package names.

#### Tool 1 – JavaDoc

1. In the Jenkins scripting console, write the following code

**def instance = Jenkins.getInstance()**

**println instance.class**

1. This prints out

class hudson.model.Hudson

1. Knowing the class name allows you to look at the JavaDoc for Jenkins core along with popular plugins:

<https://javadoc.jenkins.io>

<https://javadoc.jenkins.io/plugin>

#### Tool 2 – Groovy

1. Now write the following code

**def instance = Jenkins.getInstance()**

**println instance.metaClass.methods\*.name.sort().unique()**

1. The metaClass methods approach is a quick way to find out what methods are available on an object you currently have.
2. You can even see the method signatures:

**def instance = Jenkins.getInstance()**

**println instance.metaClass.methods**

#### Tool 3 – Google

Seriously. People have posted many Groovy scripts online that you can either use directly or make minor edits to.

### 4.2 - Creating a user

To help us keep track of who is who, we are going to give our users the same username and password. Obviously, don’t do this on your real Jenkins!

1. Users are created in security realms. Run this code in the “Script Console” to create a user. Remember, the “Script Console” is available under “Manage Jenkins”.

**def instance = Jenkins.getInstance()**

**def realm = Jenkins.getInstance().securityRealm**

**realm.createAccount('olivia', 'olivia')**

**instance.save()**

**println 'Done'**

1. In the left navigation, click “People” and note Olivia is there now.
2. Click her id and then click “Delete” from the left navigation.
3. Create a new freestyle job
4. This time add a System Groovy build step



1. Add three more lines of code so Owen, Sam and Sophia get accounts.

Note: Since we are now running in a job, we need to explicitly include the package for Jenkins. The console assumed this for you. (**import jenkins.model.Jenkins**)

1. Run the job.
2. Go to “People” in the left navigation and confirm the accounts were added.

### 4.3 - Setting up the authorization strategy

Jenkins has a number of authorization strategies. Since the Ospreys and Sea Lions have different requirements, we are using the project level authorization strategy. We set up the admin and general user settings. We will also set up roles so the right users can see each project.

1. Create another Jenkins job called create-auth-strategy
2. In the Groovy console section, paste the code from

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/blob/master/jenkinsScripts/auth.groovy>

* 1. If your administrator username is \*not\* admin, then you need to change the second 'admin' script on line 14, such as was done below:

auth.doAssignRole('globalRoles', 'admin', 'melissa')

**Failure to do so could result in your having reset your Jenkins permissions (see Appendix II) and/or start over!**

1. Run the job
2. Look at <http://localhost:8080/role-strategy/manage-roles>
3. Note that the ospreys now have team permissions.
4. Update the groovy code to set up the sea lions.

Their team project prefix is sea-lion.\*

1. Update the groovy code from Step 6 to add Sophia and Sam to this new team. (remember that saving must be the last statement).
   1. Do not remove the existing statements for ospreys/Olivia/Owen from the script, as running the script replaces the previous authorization entirely.
2. Re-run the job and confirm:
   1. The assigned roles table has a column for the sea-lions. The rows for Sam and Sophia should have one checkbox selected on each.
   2. The items role table has rows for Sam and Sophia. Their rows should have two checkboxes selected on each.

*Note:* Another option is to have Jenkins pull the project from GitHub and run the Groovy code as a script. However, this triggers the script security plugin and requires an extra step. Since this is a conference and not a system we are maintaining, we optimized. The effort to setup script security properly is more than the effort to copy/paste this config.

Jeanne’s rant about the script security plugin is here:

<https://www.selikoff.net/2018/09/02/a-rant-about-jenkins-script-security/>

## Step 5: Nexus System Scripting

### 5.1 - Learn what objects are available

Nexus exposes some variables to Groovy for ease in scripting:

* core
* repository
* blobStore
* security
* container

For this to be useful, you need to know the class name of each. This allows you to use JavaDoc (or autocomplete) to determine what methods are available.

Write your own Groovy task to output the classes in use here. (See the solution guide if you get stuck)

Note: Looking at the source code for these classes in the IDE, it is possible to find the interfaces as well. The technique of using a Groovy task to learn more about a class remains useful.

### 5.2 - Create global access and Jenkins access

Jenkins needs access to Nexus. While it can download open source jars without credentials, it does need to provide credentials to upload the artifacts from Osprey and Sea Lion projects. We don’t want to use the admin id for this! We also need to create an upload role and the repositories.

We used a combination of IDE autocomplete and examples online to create the Groovy script.

1. Copy the code from

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/blob/master/nexus-scripts/src/main/groovy/nexusBasicSetup.groovy>

1. Run it in a Groovy task in Nexus.
2. In the left navigation, click on Roles and see that there is now a jenkins-role.

### 5.3 - Setup Nexus Access

Now we are going to create content selectors, privileges and roles to configure access. The Sea Lion team wants their jars only available to their team. The Osprey team wants their jars available to all logged in users, but not anonymous users.

1. Copy the code from

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/blob/master/nexus-scripts/src/main/groovy/teamSetup.groovy>

1. Run it in a Groovy task in Nexus.
2. Now your turn. Try writing the Groovy code to set up the Sea Lion’s access. Remember that they get access to the Osprey code in addition to their own.

Note: You probably noticed it is a bit tedious to run the Nexus tasks. Luckily, Nexus provides REST APIs. However, much of this REST API is the Scripting API we have been using. So you both upload and run the script directly from your machine (or a build server).

## Step 6 – Create a Jenkins pipeline

### 6.1 - Setup Nexus Credentials in Jenkins

1. In the left navigation bar, click “Credentials”
2. Click “Jenkins”



1. Click “Global credentials (unrestricted)”
2. Click “Add Credentials”
3. Enter the username/password for Nexus (the one we set in the Groovy script). For id, make sure to name it “nexus”.

### 6.2 - Create a job to setup jobs with proper configuration

Teams at our imaginary company always start out with the same types of build – pull from github and run a gradle clean/install/publish. To save them some time, let’s create a meta-job that can generate Jenkins jobs with the build pipeline pre-configured.

1. Create a new job named “job-generator”
2. Select “freestyle project” as the type.
3. Select “this project is parameterized”
4. Add a string parameter with the name gitUrl and the description “URL in GitHub”
5. Add another string parameter with the name gitFolder and the description “Subfolder name within GitHub project”
6. Add a build step to execute a system groovy script.
7. Paste in the script from

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/blob/master/jenkinsScripts/jobGenerator.groovy>

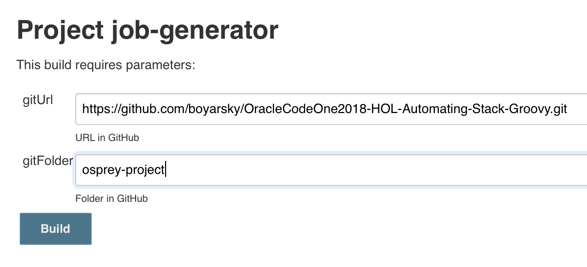
1. Save
2. Click “Build with parameters” to run this job twice.

Set the girUrl as follows:

**https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy.git**

Set the gitFolder as follows:

**osprey-project**



1. Run the job again, but enter **sea-lion-project** for the gitFolder.

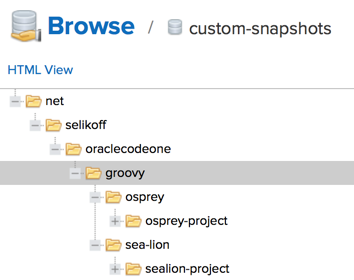
### 6.3 - Testing Access and Running Jenkins Jobs

Now that we have jobs and security, we can try everything out.

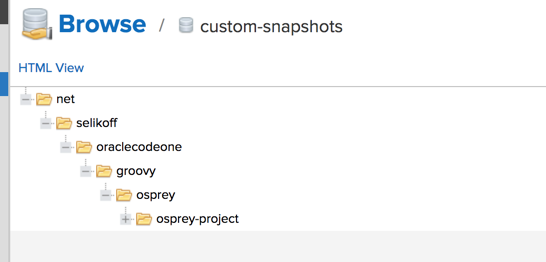
1. Logon to Jenkins as Sophia.
2. Confirm this user can see both the Osprey and Sea Lion job.
3. Run the Sea Lions job and ensure it passes.
4. Log out.
5. Logon as Olivia.
6. Confirm this user can see the Osprey job, but not the Sea Lion job.
7. Run the Osprey job and ensure it passes.

### 6.4 - Testing access and Viewing Nexus artifacts

1. Logon to Nexus as an admin.
2. Click Browse > Custom Snapshots
3. Then drill down and see both artifacts were deployed.



1. Now login as Olivia. Drill down and confirm she can’t see the sea lion project.



1. Next logout. Refresh the page and try to go to browse again. Note that this time you can’t see anything, not even the repository.
2. Finally, login as Sophia and confirm you can see both the osprey and sea lion projects.

### 6.6 - Editing a pipeline job

The Sea Lions have decided they want to deploy to Nexus on every other build. For even numbered builds they want to just print a message to the console that they are skipping deploy. For odd numbered builds, they want the pipeline to behave normally.

*Tip*: This is the code to get the build number.

def buildNum = env['BUILD\_NUMBER'] as Integer

To validate:

* Run the sea lion job twice
* For the odd numbered job number, confirm “skip publish” is in the log.
* For the even numbered job number, confirm :publishMavenPublicationToSnapshotsRepository is in the log.

## Step 7 – Switch services (Optional)

### /clone - Download and Build sea-lion Project

Before we install and start SonarQube, we need to utilize our local Nexus repository to build the sea-lion project.

1. Start Nexus if it is not already running using the command:

docker start nexus

1. You’ll need a local copy of the sea-lion-project folder located at:

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/tree/master/sea-lion-project>

For this step, it’s probably easier to just download/clone the entire project repository if you haven’t already:

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy>

1. Navigate (cd) into the sea-lion-project folder
2. Start a gradle build by executing the following command (the ./ prefix is required for Linux/Mac, but not Windows)

./gradlew build

1. The build should finish with the message BUILD SUCCESSFUL.

### 7.2 - Stop Nexus and Jenkins to free up some resources

SonarQube tends to use a lot of CPU and memory. To improve performance for the next section of this lab, we can a good deal of memory usage by turning off Jenkins and Nexus used in the previous labs by running the following two commands:

* docker stop jenkins
* docker stop nexus

Note: If you want to use Nexus and/or Jenkins again later, just run the command with start instead of stop

### 7.3 - Install SonarQube

At the command line, run:

**docker run -d -p 9000:9000 -p 9092:9092 --name sonarqube --network hol-network sonarqube:7.1**

Note: this uses the in memory database. For a real install, you’ll want to use an external database.

*Validation:*

In a browser, go to http://localhost:9000. It might take about a minute before the URL returns a webpage.

## Step 8 – Creating a custom SonarQube rule

The company is concerned about the Sea Lions committing trade secrets. In true Dilbert fashion, they decided the solution was to ban the word “secret” from method and variable names.

Conveniently, we had a developer (Jeanne) handy to write the rule. You can browse the source code at

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/tree/master/sonar-custom-rule>

(SecretNotAllowedRule.java is the most interesting class)

### 8.1 - Deploying a custom rule

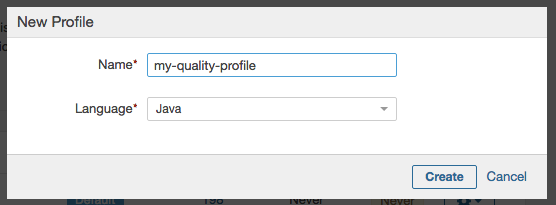
1. Copy the snapshot jar of this rule to a directory on your machine. You can use Maven to build sonar-custom-rule or use the pre-built version from

<https://github.com/boyarsky/OracleCodeOne2018-HOL-Automating-Stack-Groovy/blob/master/sonar-custom-rule-0.0.1-SNAPSHOT.jar>

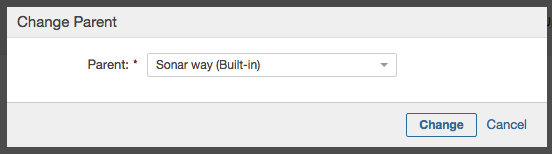
1. cd to the directory where you downloaded (or built) the jar.
2. docker cp sonar-custom-rule-0.0.1-SNAPSHOT.jar sonarqube:/opt/sonarqube/extensions/plugins/sonar-custom-rule-0.0.1-SNAPSHOT.jar
3. docker restart sonarqube

### 8.2 - Add this rule to the default quality profile

1. Go to <http://localhost:9000> (remember it could take a minute so refresh if you don’t see the screen)
2. Login (admin/admin)
3. Close the tutorial popup by clicking the Skip button
4. Click “Quality Profiles” in the top navigation
5. Click “Create” on the upper right
6. Enter a name of your choosing and select “Java” from the pulldown



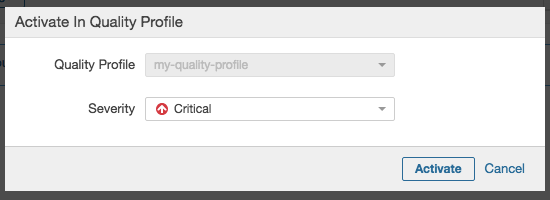
1. Click “Create”
2. Note your quality profile has zero rules
3. Click “Change parent” and choose the “Sonar way (Built-in)”



1. Note how many rules are in the quality profile now. (It was 299 active rules when we tested)
2. Click “Activate More”
3. Search for “secret”



1. Click “Activate”
2. Leave the default of “Critical” and choose “Activate” again.



1. Click “Quality Profiles” in the top navigation and observe one more rule is active.

### 8.3 - Run a scan with this custom rule

For this step you will need to have completed Section 7.1 - “Download and Build sea-lion Project”, in which the sea-lion project was build using the local Nexus repository.

The sea-lion-project directory referred to in Steps 5 and 6 assume you are running it in the directory where the sea-lions project was previously built.

1. Download the CLI for your operating system from

<https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Scanner>

1. Extract the files to a new directory and make sure to write down where placed it, since you will need the full path later, such as:

~/Downloads/sonar-scanner-1.2.3

1. Navigate to the /conf directory of the extracted files, open the sonar-scanner.properties file with your favorite text editor, and uncomment the # in the following line:

sonar.host.url=http://localhost:9000

1. Save the scanner.properties file.
2. Navigate (cd) into the sea-lion-project folder
3. Run the /bin/sonar-scanner executable from the extracted folder in the sea-lion-project directory. You’ll need the full path you created in Step 2. The following example demonstrates this, although your paths may vary locally:

$ cd OracleCodeOne2018-HOL-Automating-Stack-

Groovy/sea-lion-project

$ ~/Downloads/sonar-scanner-1.2.3*/bin/sonar-scanner*

1. The process should finish with the message EXECUTION SUCCESS.
2. Go back into Sonar in the browser and search for “sea lion” in the top-right search box. Select “Sea Lion Project”.
3. Go to the project and note that now there is one vulnerability.



1. Click it to see the details. It’s our ‘secret’ rule!

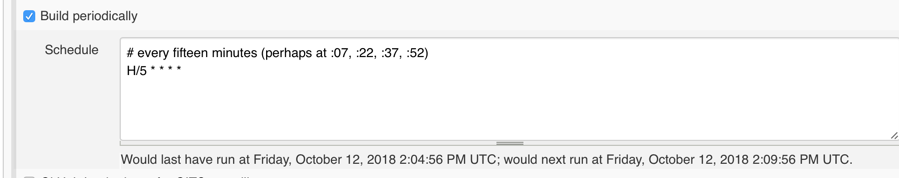


## Step 9 – Extra credit in Jenkins (Optional)

We have a security hole in the design here. Anyone can create any job they want. While solving this problem is out of scope for the lab, let’s deal with one piece of it. The task is to write Groovy code to ensure that only jobs with the prefix “osprey” build the osprey-project and only jobs with the prefix “sea-lion” build the sea-lion-project.

This one is extra credit so it comes with less instructions.

1. Stop the Sonar container
2. Restart the Jenkins container
3. In the Jenkins Groovy console, write a script to check this. (The Groovy is in the solution guide. While we hinted at the knowledge to write this in the lab, it takes more than 2 hours to be able to build it quickly. We left this as optional to write in case students came in with experience writing Jenkins scripts or managed to get through all the above really fast!)
4. Create a Jenkins FreeStyle job that includes this a Groovy System build step with this code.
5. Add a build trigger to this job runs every 5 minutes. Note that Jenkins tells you when the build will next run so you can see if you did it right:



1. Try creating a new project called “osprey-invalid-permissions”. Instead of choosing “FreeStyle job”, scroll down and make a copy of sea-lion-project. Click save for that new project.
2. See that your new validator project fails. (Feel free to disable the validator project after it fails so it doesn’t keep running every 5 minutes.)

While this doesn’t solve the actual security problem, it at least tells someone about it. (or it would, if we had build notifications set up). So you’ve made a toy example on your machine a bit safer ☺.

## Appendix I: Cleanup

### I.1 Stop containers:

Remember you can enter the first couple characters of the hash rather than the whole thing.

**docker ps**

**docker stop nexus**

**docker stop jenkins**

**docker stop sonarqube**

### II.2 Reclaiming Disk Space

#### Remove containers

**docker ps –a**

**docker rm sonarqube**

**docker rm jenkins**

**docker rm nexus**

#### Remove images:

**docker images**

**docker rmi <hash1>**

**docker rmi <hash2>**

**docker rmi <hash3>**

#### Delete configuration

**docker network rm hol-network**

## Appendix II: Corrupted Jenkins Roles

“Uh oh. I managed to make it so the admin user doesn’t have read access to Jenkins”

If you manage to change permissions so admin no longer has admin rights, you have two choices on how to fix it

### II.1 Faster way – install your favorite text editor

1. Launch bash as root

**docker exec -it --user root jenkins bash**

1. Install your favorite text editor. We choose vim

**apt-get update**

**apt-get install –y vim**

1. Open the config.xml

**vim /var/jenkins\_home/config.xml**

1. Update the authorization strategy and security realm to the following:

<authorizationStrategy class="hudson.security.FullControlOnceLoggedInAuthorizationStrategy">

<denyAnonymousReadAccess>true</denyAnonymousReadAccess>

</authorizationStrategy>

<securityRealm class="hudson.security.HudsonPrivateSecurityRealm">

<disableSignup>true</disableSignup>

<enableCaptcha>false</enableCaptcha>

</securityRealm>

1. Exit your text editor
2. Exit bash
3. Restart Jenkins

**docker restart jenkins**

### II.2 lower way – delete your docker container/image and start over

1. docker rm jenkins
2. Follow the setup again (the run command and all future steps)

## Appendix III: Useful References

<https://hub.docker.com/r/jenkins/jenkins>

<https://github.com/jenkinsci/docker/blob/master/README.md>

<https://hub.docker.com/r/sonatype/nexus3>

<https://hub.docker.com/r/library/sonarqube/>

<https://support.sonatype.com/hc/en-us/articles/115015812727-Nexus-3-Groovy-Script-development-environment-setup>

<https://help.sonatype.com/repomanager3/rest-and-integration-api/script-api/writing-scripts#app>

<https://help.sonatype.com/repomanager3/rest-and-integration-api>

<https://github.com/SonarSource/sonar-custom-rules-examples/tree/master/java-custom-rules>

<https://docs.sonarqube.org/display/PLUG/Writing+Custom+Java+Rules+101>

<http://groovy-lang.org/style-guide.html>