CI / CD automation with

Jenkins

For DevOps engineers

by Gábor Szabó

Jenkins book

Gábor Szabó

This book is for sale at http://leanpub.com/jenkins-book

This version was published on 2019-04-21

Contents

About the book

Leanpub provides the opportunity to update an already sold book and for the reader to get the new edition without any extra payment.

As we all of my other books[1] sold on Leanpub, this too is a work in progress. I'll add more pages. Update old ones etc. Hopefully make it a better book.

Once you buy the book you can come back to Leanpub at any time and download the new edition. However you will only get notified about the new edition if you opt-in to that.

You can do that by visiting your library[2] on Leanpub, clicking on the book image, and making sure the "New version available" checkbox is checked.
It does not need an extra step of saving but it takes a number of seconds to be actually saved. So wait till a "Successfully updated!" message appears at the top of the page.

You will have to do it one-by-one with each book for which you'd like to get notifications.

Enjoy the book!

[1]https://leanpub.com/u/szabgab
[2]https://leanpub.com/user_dashboard/library

Preface

This book about Jenkins contains the User handbook and some of my own writings.

License and Copyright information of the "User handbook" can be found at the end of the book.

The formatting is still far from being nice. I am working on it.

There is some code[3] that generates Markua files Leanpu uses to create the actual eBook.

[3]https://github.com/szabgab/books

Changes

v0.04 2019-04-06

Regenerate the book with all the updates from the Jenkins site.

v0.03 2018-08-23

- Improved display of special section with CAUTION and NOTE.

v0.02 2018-08-21

- Properly formatting many of the code snippets.
- Fix some unicode issues.

v0.01 2018-08-20

- Initial release

Articles

Jenkins

Jenkins

Jenkins[4] is an automation server. It allows for all kinds of automations. It is primarily used for Build automation, Continuous Integration, and Continuous Deployment.

- Install Jenkins on Ubuntu (using Vagrant) * Vagrant for Jenkins on Ubuntu[5] * Jenkins Pipeline - Hello World * Jenkins Pipeline: running external programs with sh or bat, returnStdout, trim * Jenkins Pipeline: Send e-mail notifications * Jenkins Pipeline: Add some text to the job using shortText * Jenkins CLI: create node * Jenkins Pipeline BuildUser plugin[6] * Jenkins Pipeline - set and use environment variables[7] * Jenkins Pipeline: git checkout using reference to speed up cloning large repositories[8]
- Triggers from Version Control Systems * Report failures. * Send alerts * Collect test coverage data. * Jenkins slides[9]

Add badges

```
manager.addBadge("error.gif", "Failed build")
```

Run external code, capture output

```
script {
    v = sh(script: 'echo " 42"; echo', returnStdout: true).trim()
    echo v
    echo "a${v}b"
}
```

`bat` for windows.

catch and print error in jenkins

[4] https://jenkins.io/
[5] https://code-maven.com/vagrant-for-jenkins-on-ubuntu
[6] https://code-maven.com/jenkins-pipeline-builduser
[7] https://code-maven.com/jenkins-pipeline-environment-variables
[8] https://code-maven.com/jenkins-git-check-out-using-reference
[9] https://code-maven.com/slides/jenkins/

```
pipeline {
   agent none
   stages {
       stage ('Catch crash') {
           agent { label 'master'}
           steps {
               echo "before crash"
               script {
                   try {
                       sh 'exit 1'
                   } catch (err) {
                       echo "exception caught, going on"
                       println err // java.lang.ClassCastException:
org.jenkinsci.plugins.workflow.steps.EchoStep.message expects class java.lang.String\
 but received
class hudson.AbortException
                   }
               }
               echo "after crash"
           }
       }
       stage ('Continue after crash') {
           agent { label 'master'}
           steps {
               echo "stage after crash"
           }
       }
   }
}
```

dir and tmp are problematic

```
  stages {
       stage ('Run external exe') {
           agent { label 'master'}
           steps {
               sh 'pwd'
               dir('/tmp/gabor') {
                   echo "inside"
                   sh 'pwd'
                   //sh 'sudo ./do-something.py'
               }
               sh 'pwd'
```

```
            //sh "sudo sh -c 'cd /tmp; ./do-something.py; cd -'"
        }
    }
```

```
java.io.IOException: Failed to mkdirs: /tmp@tmp/durable-e569697c
        at hudson.FilePath.mkdirs(FilePath.java:1170)
        at org.jenkinsci.plugins.durabletask.FileMonitoringTask$FileMonitoringContro\
ller.<init>(FileMonitori
ngTask.java:156)
        at org.jenkinsci.plugins.durabletask.BourneShellScript$ShellController.<init\
>(BourneShellScript.java
:198)
        at org.jenkinsci.plugins.durabletask.BourneShellScript$ShellController.<init\
>(BourneShellScript.java
:190)
        at org.jenkinsci.plugins.durabletask.BourneShellScript.launchWithCookie(Bour\
neShellScript.java:111)
        at org.jenkinsci.plugins.durabletask.FileMonitoringTask.launch(FileMonitorin\
gTask.java:86)
        at org.jenkinsci.plugins.workflow.steps.durable_task.DurableTaskStep$Executi\
on.start(DurableTaskStep
.java:182)
        at org.jenkinsci.plugins.workflow.cps.DSL.invokeStep(DSL.java:229)
        at org.jenkinsci.plugins.workflow.cps.DSL.invokeMethod(DSL.java:153)
        at org.jenkinsci.plugins.workflow.cps.CpsScript.invokeMethod(CpsScript.java:\
122)
        at sun.reflect.GeneratedMethodAccessor1989.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorI\
mpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:498)
        at org.codehaus.groovy.reflection.CachedMethod.invoke(CachedMethod.java:93)
        at groovy.lang.MetaMethod.doMethodInvoke(MetaMethod.java:325)
        at groovy.lang.MetaClassImpl.invokeMethod(MetaClassImpl.java:1213)
        at groovy.lang.MetaClassImpl.invokeMethod(MetaClassImpl.java:1022)
        at org.codehaus.groovy.runtime.callsite.PogoMetaClassSite.call(PogoMetaClass\
Site.java:42)
        at org.codehaus.groovy.runtime.callsite.CallSiteArray.defaultCall(CallSiteAr\
ray.java:48)
        at org.codehaus.groovy.runtime.callsite.AbstractCallSite.call(AbstractCallSi\
te.java:113)
        at org.kohsuke.groovy.sandbox.impl.Checker$1.call(Checker.java:157)
        at org.kohsuke.groovy.sandbox.GroovyInterceptor.onMethodCall(GroovyIntercept\
or.java:23)
        at org.jenkinsci.plugins.scriptsecurity.sandbox.groovy.SandboxInterceptor.on\
MethodCall(SandboxInterc
eptor.java:133)
        at org.kohsuke.groovy.sandbox.impl.Checker$1.call(Checker.java:155)
        at org.kohsuke.groovy.sandbox.impl.Checker.checkedCall(Checker.java:159)
        at org.kohsuke.groovy.sandbox.impl.Checker.checkedCall(Checker.java:129)
        at org.kohsuke.groovy.sandbox.impl.Checker.checkedCall(Checker.java:129)
        at com.cloudbees.groovy.cps.sandbox.SandboxInvoker.methodCall(SandboxInvoker\
.java:17)
        at WorkflowScript.run(WorkflowScript:16)
```

Jenkins / Groovy - define functions and call them with parameters

```
def report(status) {
   println "status=${status}"
}
```

and call them

```
report("text")
```

Environment variables on Linux

```
sh 'printenv'
sh 'env'
```

Input during the process

```
pipeline {
   agent { label 'master' }
   stages {
       stage('build') {
           steps {
               echo "Hello World!"
               //input("Continue?")
               echo "OK"
               //input(
               //    message: 'Was this successful?', parameters: [
               //   [$class: 'BooleanParameterDefinition', defaultValue: true, descr\
iption: '',
name: 'Please confirm you agree with this']
               //])

       /*
               script {
                   res = input(
                       message: 'Was this successful?', parameters: [
                       [$class: 'BooleanParameterDefinition', defaultValue: false, d\
escription:
'', name: 'Apple'],
                       [$class: 'BooleanParameterDefinition', defaultValue: false, d\
escription:
'', name: 'Banana']
                   ])
                                     print(res)
               }
*/
               script {
                   values = ['Apple', 'Banana', 'Peach']
                   parameters = []
                   values.each {
                       echo it
                       parameters.add( [$class: 'BooleanParameterDefinition', defaul\
tValue:
false, description: '', name: it ] )
                   }

                   res = input(
                       message: 'Was this successful?', parameters: parameters
                   )
                                                        print(res)
               }


               //                input(
//                    message: 'What now?', parameters: [
//                        [$class: 'AppDetectorParamaterDefinition')
//                ])
                                  //echo result
                              // python scripts/aws_instances.py --what selftest --c\
ommand start
           }
       }
```

```
    }
}
```

git Backup

gist[10]

List agents by name and by label

```
def jenkins = Jenkins.instance
def computers = jenkins.computers
computers.each {
   //  println "${it.displayName} ${it.hostName}"
}

def labels = jenkins.getLabels()
labels.each {
   println "${it.displayName}"
}
```

Other

```
echo bat(returnStdout: true, script: 'set')

build(job: 'RevertServerAutomationCloud', parameters: [
     string(name: 'VM_SNAPSHOT', value: 'CleanDb')
])
```

how to include one jenkinsfile in another one?

how to avoid repetititon?

[10]https://gist.github.com/cenkalti/5089392

```
stage('Revert agent 100')
         {
             steps
                     {
                     }
         }

 stage('Revert agent 102')
         {
             steps
                     {

                     }
         }
```

how do try - catch and repeat interact?

```
vSphere buildStep: [$class: 'RevertToSnapshot', snapshotName: "${params.VM_SNAPSHOT}\
", vm: "${params.VM_NAME}"], serverName: '192.168.1.1'

httpRequest authentication: 'df8-b86d-3272', consoleLogResponseBody: true, httpMode:\
 'POST', ignoreSslErrors: true, responseHandle: 'NONE', url:
"http://192.168.1.1:8080/computer/${params.AGENT_NAME}/doDisconnect?offlineMessage=b\
ye", validResponseCodes: '100:404'
```

Active Choices Parameter

```
try {
   List<String> subnets = new ArrayList<String>()
   def subnetsRaw = "gcloud compute networks subnets list --project=${GCE_PROJECT} -\
-network=corp-development --format=(NAME)".execute().text
   for (subnet in  subnetsRaw.split()) {
       subnets.add(subnet)
   }
   return subnets
} catch (Exception e) {
   print e
   print "There was a problem fetching the artifacts"
}
```

Options

```
   options {
       ansiColor('xterm')
       timestamps()
   }
```

Scripts

Scripts not permitted to use method groovy.lang.GroovyObject invokeMethod java.lang.String java.lang.Object (org.jenkinsci.plugins.workflow.cps.EnvActionImpl keys). Administrators can decide whether to approve or reject this signature.

archiveArtifacts can be called multiple times

```
archiveArtifacts artifacts: 'mydata.json', onlyIfSuccessful: true
writeJSON(file: 'otherfile.log', json: data, pretty: 4)
archiveArtifacts artifacts: '*.log', onlyIfSuccessful: true
```

Environment variable values must either be single quoted, double quoted, or function calls.

They cannot be earlier defined environment variables or parameter values. We can however overcome this limitation by calling a function and passing the values to it.

```
pipeline {
   agent none
   options {
       ansiColor('xterm')
       timestamps()
   }
   parameters {
       string(name: 'machine', defaultValue: 'asos', description: 'Some text input')
       string(name: 'size',   defaultValue: '23', description: 'Some number input')
   }
   environment {
       answer = 42
       // machine_name = params.machine  // -> Environment variable values must eith\
er be single quoted, double quoted, or function calls.
       machine_name = set_machine_name(params.machine)
   }
   stages {
       stage('try') {
           agent { label 'master' }
           steps {
               script {
                   sh "hostname"
                   print("params.machine=${params.machine}")
                   print("params.size=${params.size}")
                   print("env.answer=${env.answer}")
                   print("env.machine_name=${env.machine_name}")

               }
           }
       }
       stage('try-agent') {
           agent { label 'jenkins-simple-slave' }
           steps {
               script {
                   sh "hostname"
               }
           }
       }
   }
}

def set_machine_name(value) {
   return value
}
```

Jenkins environment

Even if there is an exception in the environment section Jenkins will still run the “success” part of the post section. Same problem if there is an exception on one of the functions.

To overcome this we create an environment variable as the last step in the environment section and then we check that variable using

if (! binding.hasVariable(‘environment_is_set’))

That does not help in case there is an exception in the functions.

http_request

```
response = httpRequest discovery_url
println response
config_str = response.getContent()
for (item in config.sources) {
  item.value
  item.key
```

Sending e-mail problem fixed

https://stackoverflow.com/questions/20188456/how-to-change-the-security-type-from-ssl-to-tls-in-jenkins

- Sending e-mail In Manage Jenkins - Configure System in the Extended mail section set the SMTP: smtp.office365.com Domain name: @company.com Advanced: Use SMTP Authentication: + User Name: cicdserver@company.com Password: SMTP port: 587 E-mail notification section: SMTP server: smtp.office365.com Default user e-mail suffix: @company.com Advanced User Name: cicdserver@company.com Password: SMTP port: 587

Shut down Jenkins (via the Windows services) Open the file: C:Program Files (x86)Jenkins\jenkins.xml and change the arguments line to be:

```
<arguments>-Xrs -Xmx256m -Dhudson.lifecycle=hudson.lifecycle.WindowsServiceLifecycle\
  -Dmail.smtp.starttls.enable=true -jar
"%BASE%\jenkins.war" --httpPort=8080 --webroot="%BASE%\war"</arguments>
```

(specifically add: -Dmail.smtp.starttls.enable=true) Then start Jenkins again.

Client was not authenticated to send anonymous mail Error sending to the following VALID addresses

```
pipeline {
   agent none
   stages {
       stage('try') {
           agent { label 'master' }
           steps {
               script {
                   //some_strange_name = null
                   //print(some_strange_name)
                   if (true) {
                       print("creating variable")
                       some_strange_name = 1
                   }
```

```
                    print(some_strange_name)

                    if (binding.hasVariable('some_strange_name')) {
                        print("has some_strange_name")
                        print(some_strange_name)
                    } else {
                        print("DOES NOT have some_strange_name")
                    }
                }
            }
        }
        stage('try again') {
            agent { label 'master' }
            steps {
                script {
                    if (binding.hasVariable('some_strange_name')) {
                        print("has some_strange_name")
                        print(some_strange_name)
                    } else {
                        print("DOES NOT have some_strange_name")
                    }
                }
            }
        }
    }
}
```

Parallel stages

```
pipeline {
   agent { label 'master' }
   stages {
       stage('before') {
           steps {
               println("before")
           }
       }
       stage('para') {
           parallel {
               stage('apple') {
                   steps {
                       println("apple 1")
                       sleep(20 * Math.random())
```

```
                        println("apple 2")
                    }
                }
                stage('banana') {
                    steps {
                        println("banana 1")
                        sleep(20 * Math.random())
                        println("banana 2")
                    }
                }
                stage('peach') {
                    steps {
                        println("peach 1")
                        sleep(20 * Math.random())
                        println("peach 2")
                    }
                }
            }
        }
        stage('after') {
            steps {
                println("after")
            }
        }
    }
}
```

Skip steps

Jenkins pipeline stop early with success How to indicate that a job is successful pipeline conditional step stage[11]

```
pipeline {
   agent none
   options {
       ansiColor('xterm')
       timestamps()
   }
   parameters {
       booleanParam(defaultValue: false, description: 'Checkbox', name: 'yesno')
   }
```

[11]https://stackoverflow.com/questions/37690920/jenkins-pipeline-conditional-step-stage

```
   stages {
       stage('first') {
           agent { label 'master' }
           steps {
               script {
                   println("first before")
                   println(params.yesno)
                   done = true
                   return
                   println("first after")
               }
           }
       }
       stage('second') {
           agent { label 'master' }
           when {
               expression {
                  return ! done;
               }
           }
           steps {
               script {
                   println("second")
               }
           }
       }
   }
}
```

```
import java.text.SimpleDateFormat
pipeline {
   agent none
   options {
       ansiColor('xterm')
       timestamps()
   }
   parameters {
       string(name: 'machine', defaultValue: '', description: 'Name of the machine')
       string(name: 'size',   defaultValue: '23', description: 'The size')
       choice(choices: ['Mercury', 'Venus', 'Earth', 'Mars'], description:  'Pick a \
planet', name: 'planet')
   //}
```

```
    stages {
        stage('try') {
            agent { label 'master' }
            steps {
                script {
                    sh "hostname"

                    def data = readJSON text: '{}'
                    data.name = "test-529" as String
                    data.date = new java.text.SimpleDateFormat('yyyyMMddHHmmss').form\
at(new Date())
                    writeJSON(file: 'mydata.json', json: data, pretty: 4)
                    archiveArtifacts artifacts: 'mydata.json', onlyIfSuccessful: true

                    //error("Fail after first artifact")

                    writeJSON(file: 'otherfile.log', json: data, pretty: 4)
                    archiveArtifacts artifacts: '*.log', onlyIfSuccessful: true
                }
            }
        }
    }
}
```

jenkins sh commnad fails - jenkins stops

```
pipeline {
    agent { label 'master' }
    stages {
        stage('only') {
            steps {
                println("one")
                sh "ls -l"
                println("two")
                sh "ls -l no_such"
                println("three")
            }
        }
    }
}
```

Repository branch filter for Git

It will start multiple jobs if more than one branch was pushed out. It is triggered even if there were no new commits in the branch that was pushed out

By default it will run every branch matching the filter, even if that branch was last changed 2 years ago. This can be a problem if for some reason your have hundreds or thousands of historical branches.

```
:^origin/(work|dev)-.*
```

You can limit this by selecting another option and setting the ancestry date to limit how many days you are ready to go back in time.

- Strategy for choosing what to build * Choosing strategy: Ancestry * Maximum Age of Commit: 1

In a pipeline

```
checkout([
    $class: 'GitSCM',
    branches: [[name: '*/master']],
    doGenerateSubmoduleConfigurations: false,
    extensions: [[
        $class: 'BuildChooserSetting',
        buildChooser: [$class: 'AncestryBuildChooser', ancestorCommitSha1: '', maxim\
umAgeInDays: 1]
    ]],
    submoduleCfg: [],
    userRemoteConfigs: [[]]
])
```

Jenkins Pipeline code reuse

https://cleverbuilder.com/articles/jenkins-shared-library/ https://jenkins.io/doc/book/pipeline/shared-libraries/

Exceptions

When you encounter one of those 40-lines long Java stack-traces, look for **WorkflowScript** to locate the source of the problem.

```
pipeline {
    agent { label 'master' }
    stages {
        stage('only') {
            steps {
                script {
                    println("one")
                    sh "ls -l"
                    println("two")

                    try {
                        //sh "ls -l no_such"
                        a = 10
                        b = 0
                        c = a/b

                    }
                    catch(Exception ex) {
                         //currentBuild.result = 'FAILURE'
                        println("exception")
                        println(ex) // hudson.AbortException: script returned exit c\
ode 2
                        println(ex.toString())
                        println(ex.getMessage())
                        println(ex.getStackTrace())
                    }

                    //} catch(ArrayIndexOutOfBoundsException ex) {
                    //println("Catching the Array out of Bounds exception");
                    //}catch(Exception ex) {

                    println("three")
                    is_it_the_answer(42)
                    echo "try again"
                    is_it_the_answer(23)
                }
            }
        }
        stage('second') {
            steps {
                script {
//                    if (manager.logContains("three")) {
//                        manager.addWarningBadge("tres")
//                    } else {
//                        manager.addWarningBadge("nem harom")
//                    }

                }
            }
        }
    }
}

def is_it_the_answer(n) {
    if (n == 42) {
        return 'yes'
    }
    throw new Exception('Nope')
}


                    try {
                        is_it_the_answer(23)
                    } catch (err) {
                        print(err)
                        print(err.getMessage())
                    }
```

Jenkins parse console output

The **logContains** can parse the log created be the previous stages (but not the current stage) It can also be used in a post-action.

"manager" is org.jvnet.hudson.plugins.groovypostbuild.GroovyPostbuildRecorder$BadgeManager@41fe3861

Postbuild plugin[12]

[12]https://wiki.jenkins.io/display/JENKINS/Groovy+Postbuild+Plugin

```
        stage('second') {
            steps {
                script {
                    if (manager.logContains("three")) {
                        manager.addWarningBadge("drei")
                    } else {
                        manager.addWarningBadge("kein drei")
                    }
                }
            }
        }


         print("A disk image was created: zorg-1552278641")

         def matcher = manager.getLogMatcher(/.* (zorg-\d+).*/)
         print(matcher)
         if (matcher?.matches()) {
             def image_name = matcher.group(1)
             print(image_name)
             manager.addShortText(image_name)
         }
```

readJSON

no such dsl method[13]

Install Jenkins on Ubuntu

In order to experiment with Jenkins, I am going to use Vagrant[14] and VirtialBox[15] to set up a box running Ubuntu 17.10[16].

Install Vagrant and VirtualBox

Nothing special, you just need to install the two applications with using the standard installation process of your operating system. Download Vagrant[17] and VirtialBox[18] and intsall them both.

[13]https://stackoverflow.com/questions/46841877/java-lang-nosuchmethoderror-no-such-dsl-method-readjson
[14]https://www.vagrantup.com/
[15]https://www.virtualbox.org/
[16]https://www.ubuntu.com/
[17]https://www.vagrantup.com/
[18]https://www.virtualbox.org/

Set up the Ubuntu 17.10 box using Vagrant

Create an empty directory and in that directory create a file called `Vagrantfile` (no extension) with the following content:

```
Vagrant.configure(2) do |config|
  config.vm.box = "generic/ubuntu1710"
  config.vm.network "forwarded_port", guest: 8080, host:8080
  #config.vm.synced_folder "/Users/gabor/work", "/vagrant"
  config.vm.provider "virtualbox" do |vb|
    vb.memory = "512"
  end
end
```

Open a terminal window or in MS Windows a Command window. Change to the directory you created for our work. Then type in

```
vagrant up
```

This will take some time as it first downloads an Ubuntu image and then it will create a VirtualBox and set up the Ubuntu image as a new Virtual Box. (It took me about 5-10 minutes.)

Once it completed the createtion successfully you can log in to the machine by typing:

```
vagrant ssh
```

Install Jenkins

Execute the following commands inside the VirtualBox image (after you ran `vagrant ssh` and were logged in to the Virtual Box).

```
sudo apt-get update
sudo apt-get -y upgrade
wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
echo "deb https://pkg.jenkins.io/debian-stable binary/" | sudo tee -a  /etc/apt/sour\
ces.list > /dev/null
sudo apt-get update
sudo apt-get install -y jenkins
```

Check if Vagrant is running

From inside the Virtual Box images you can run the following command:

```
curl http://localhost:8080/
```

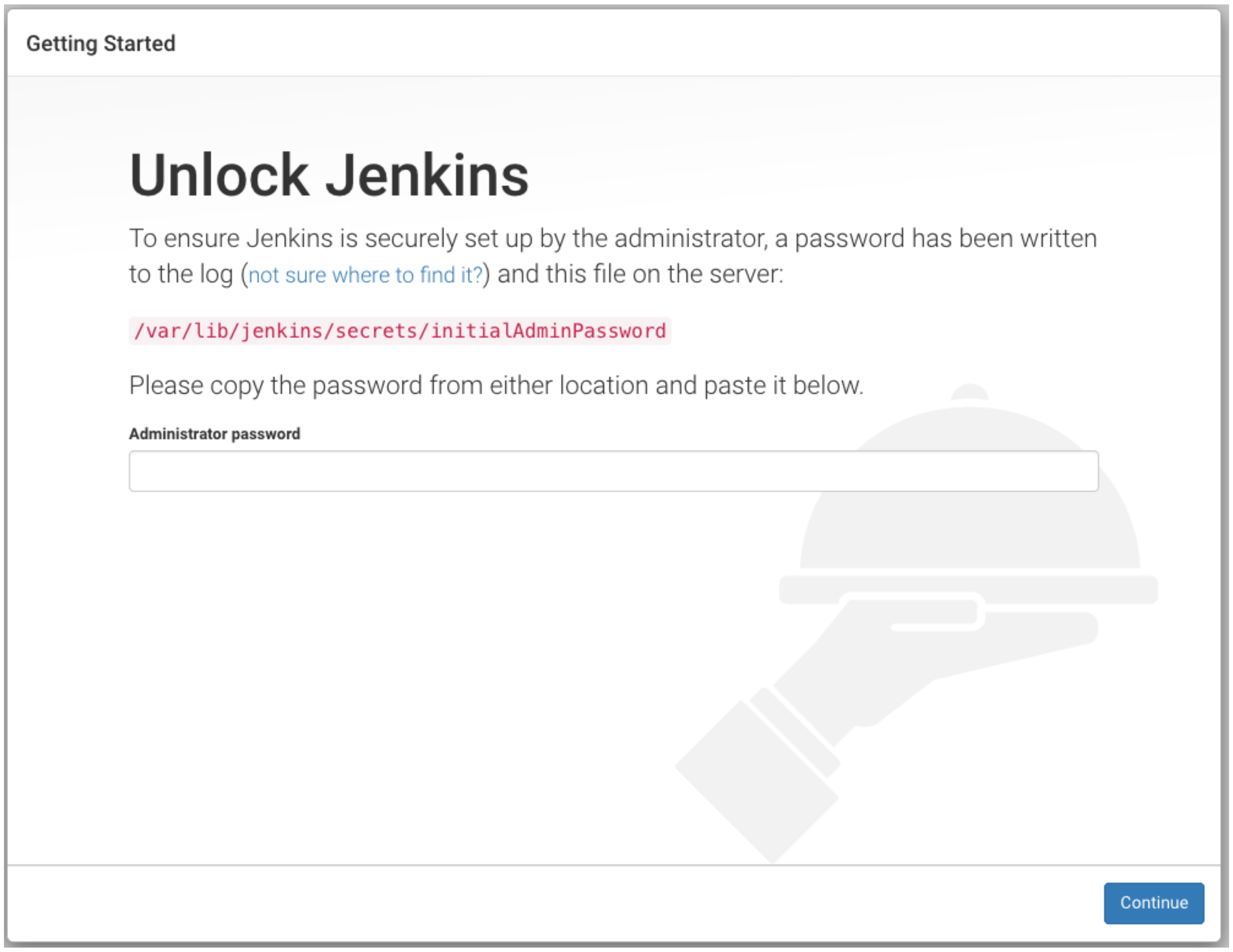
You will most likely get some message about being forbidden. That’s actually a good sign.

Set up Vagrant

Visit the newly installed Jenkins using your regular browser on your computer by following this URL:

http://localhost:8080/login?from=%2F

You should see something like this:



Getting Started

Unlock Jenkins

To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:

```
/var/lib/jenkins/secrets/initialAdminPassword
```

Please copy the password from either location and paste it below.

Administrator password

Basically the following text:

```
Unlock Jenkins

To ensure Jenkins is securely set up by the administrator, a password has been writt\
en to the log (not sure where to find it?) and this file on the server:

/var/lib/jenkins/secrets/initialAdminPassword

Please copy the password from either location and paste it below.
Administrator password
```

On the command line type in the following:

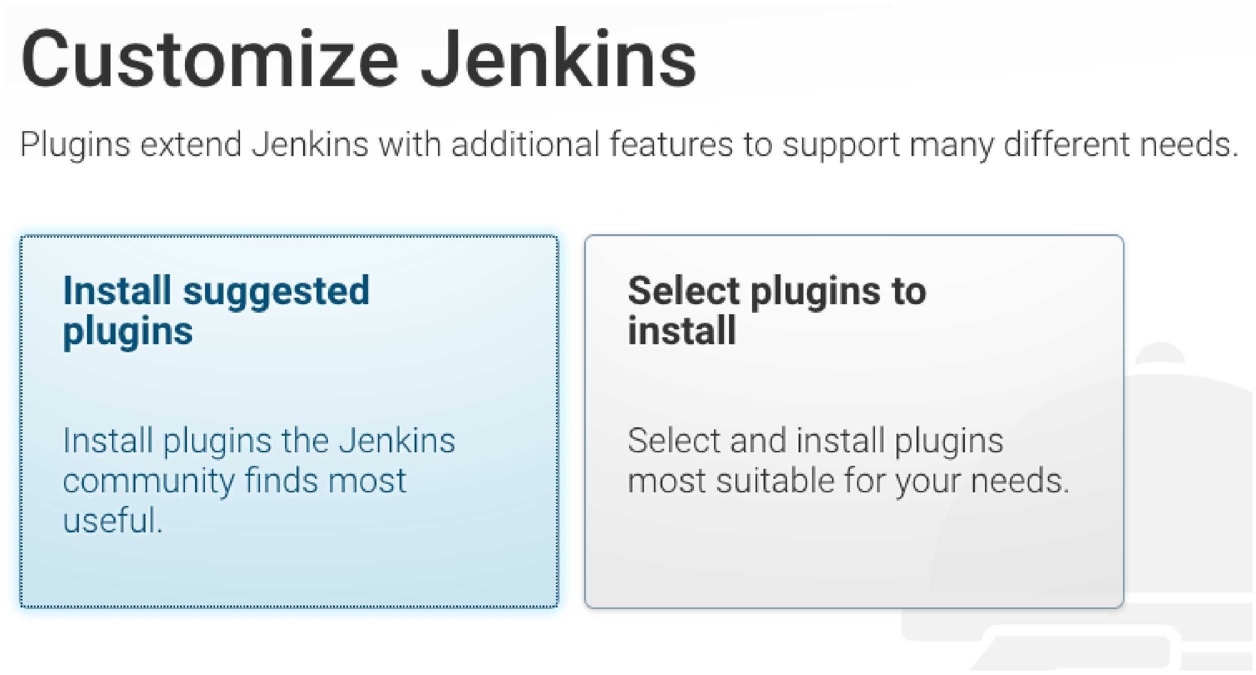
```
sudo cat /var/lib/jenkins/secrets/initialAdminPassword
```

This will print the password. Something like this:

```
da3160af7d0f4c8db649d4b8000380a6
```

Copy that string and paste in the above window.

The next page will offer you to Customize Jenkins:



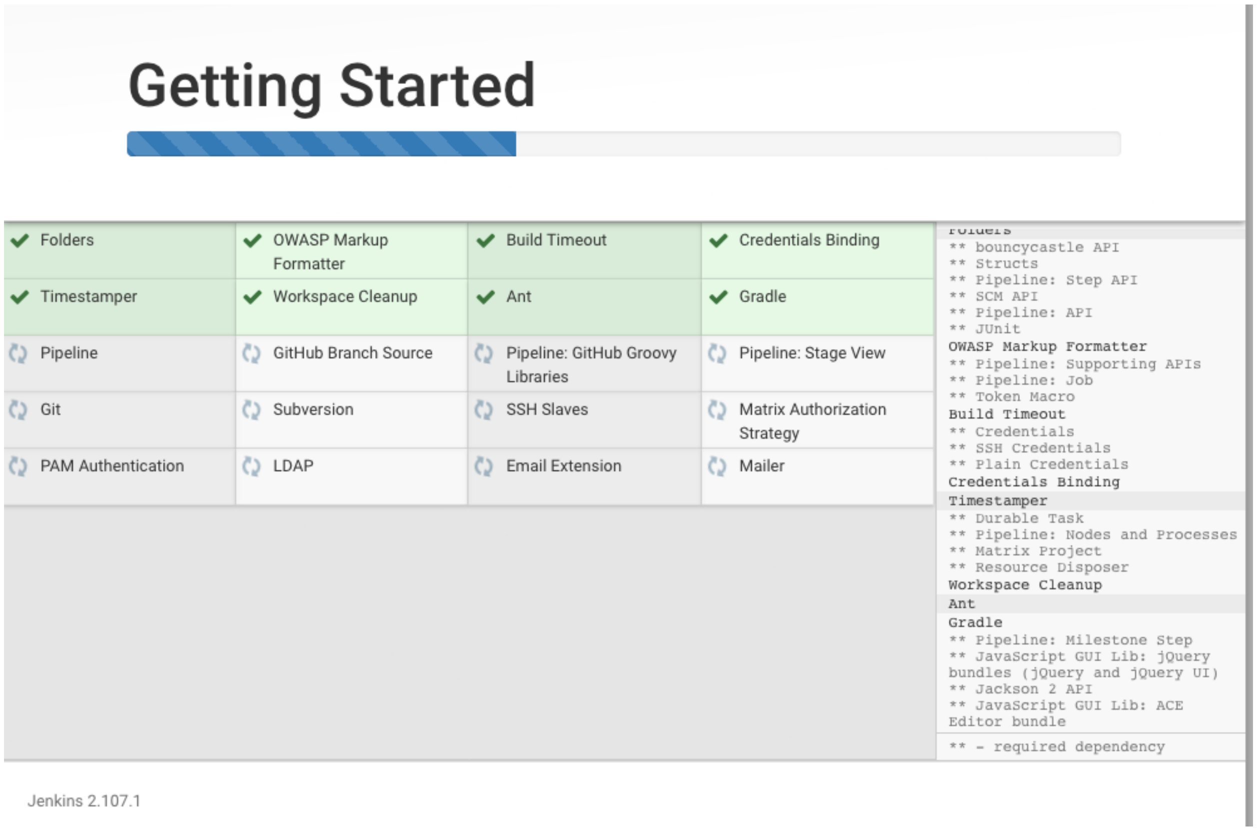
Customize Jenkins

Plugins extend Jenkins with additional features to support many different needs.

Install suggested plugins
Install plugins the Jenkins community finds most useful.
Select plugins to install
Select and install plugins most suitable for your needs.

Select `Install suggested plugins`

You will see a progress window saying `Getting Started:`

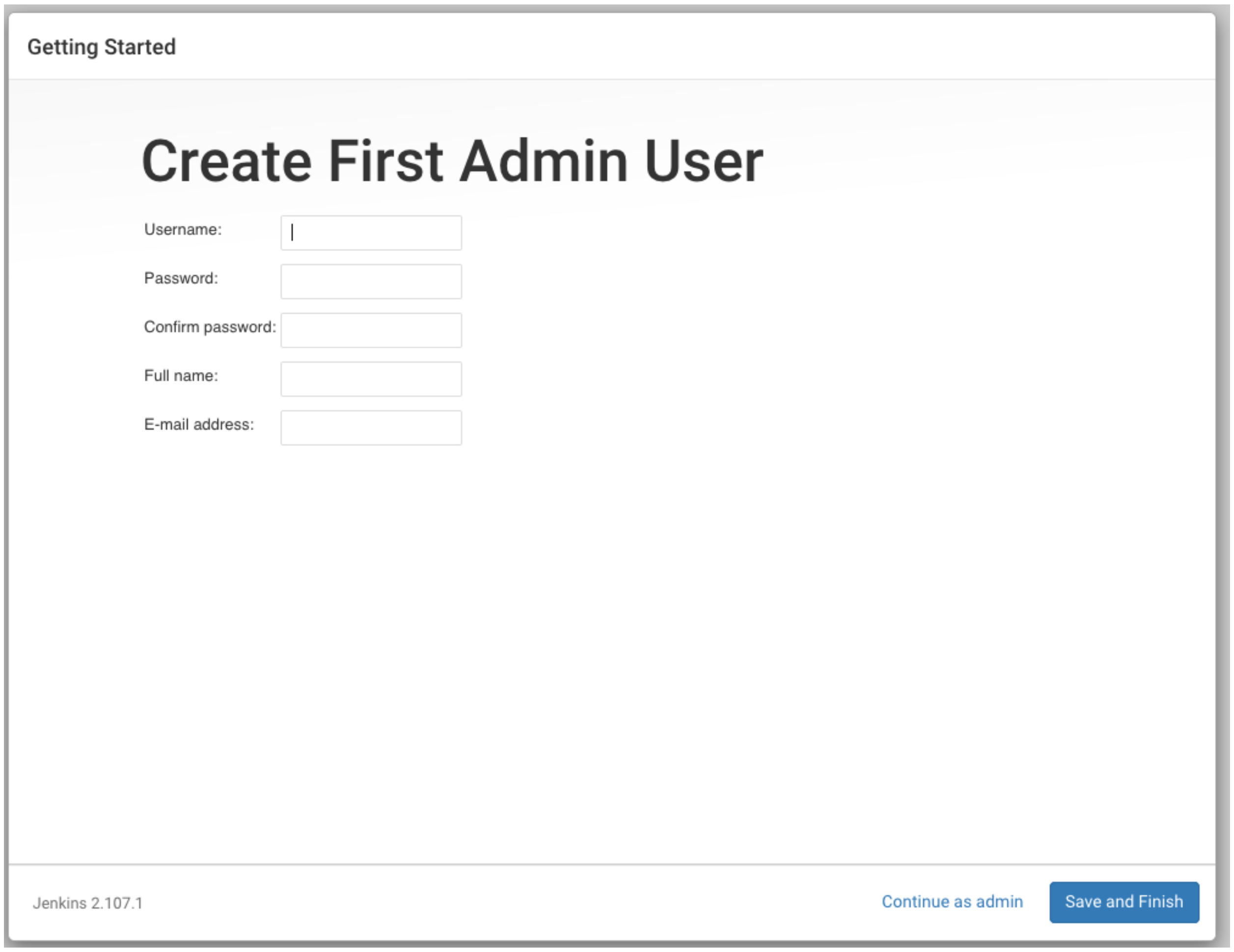

Getting Started

✓ Folders	✓ OWASP Markup Formatter	✓ Build Timeout	✓ Credentials Binding
✓ Timestamper	✓ Workspace Cleanup	✓ Ant	✓ Gradle
Pipeline	GitHub Branch Source	Pipeline: GitHub Groovy Libraries	Pipeline: Stage View
Git	Subversion	SSH Slaves	Matrix Authorization Strategy
PAM Authentication	LDAP	Email Extension	Mailer

```
Folders
** bouncycastle API
** Structs
** Pipeline: Step API
** SCM API
** Pipeline: API
** JUnit
OWASP Markup Formatter
** Pipeline: Supporting APIs
** Pipeline: Job
** Token Macro
Build Timeout
** Credentials
** SSH Credentials
** Plain Credentials
Credentials Binding
Timestamper
** Durable Task
** Pipeline: Nodes and Processes
** Matrix Project
** Resource Disposer
Workspace Cleanup
Ant
Gradle
** Pipeline: Milestone Step
** JavaScript GUI Lib: jQuery
bundles (jQuery and jQuery UI)
** Jackson 2 API
** JavaScript GUI Lib: ACE
Editor bundle
** - required dependency
```

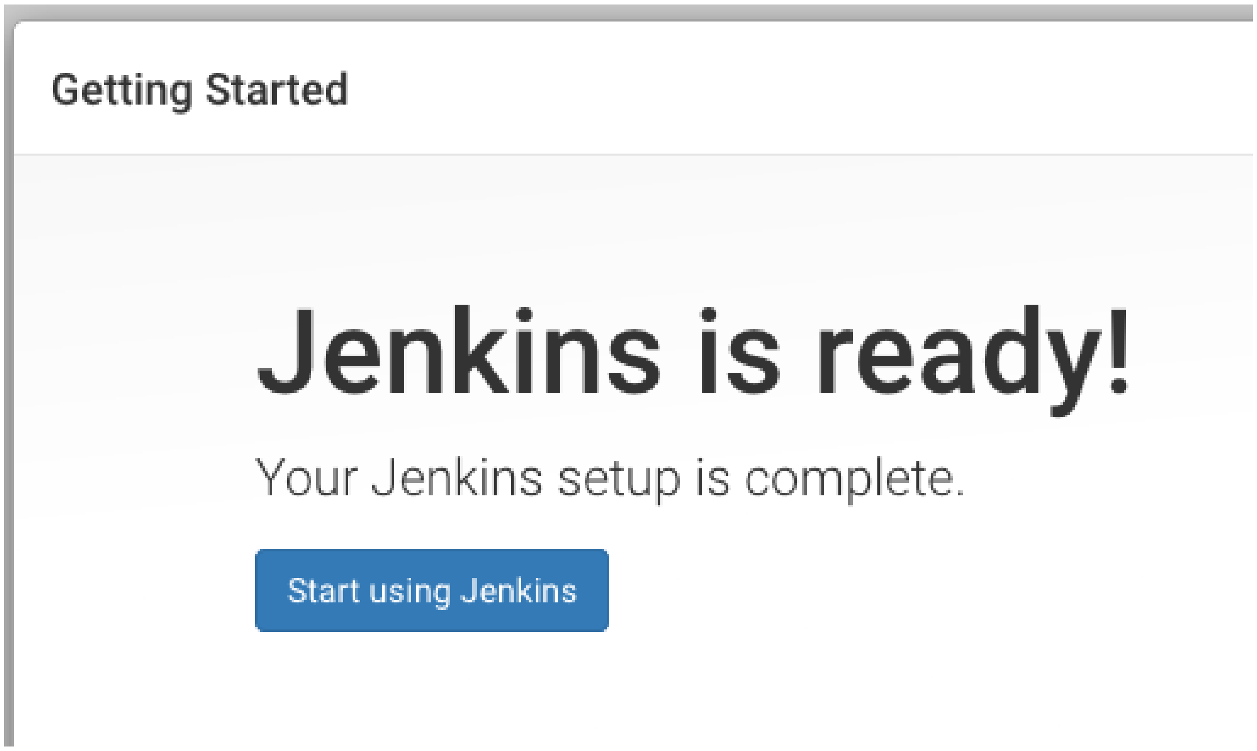
Jenkins 2.107.1

After a while it finished and shows a new page asking you to `Create Firs Admin User`:



I typed in "foobar" as the username, "Foo Bar" as the Full name and my real e-mail address.

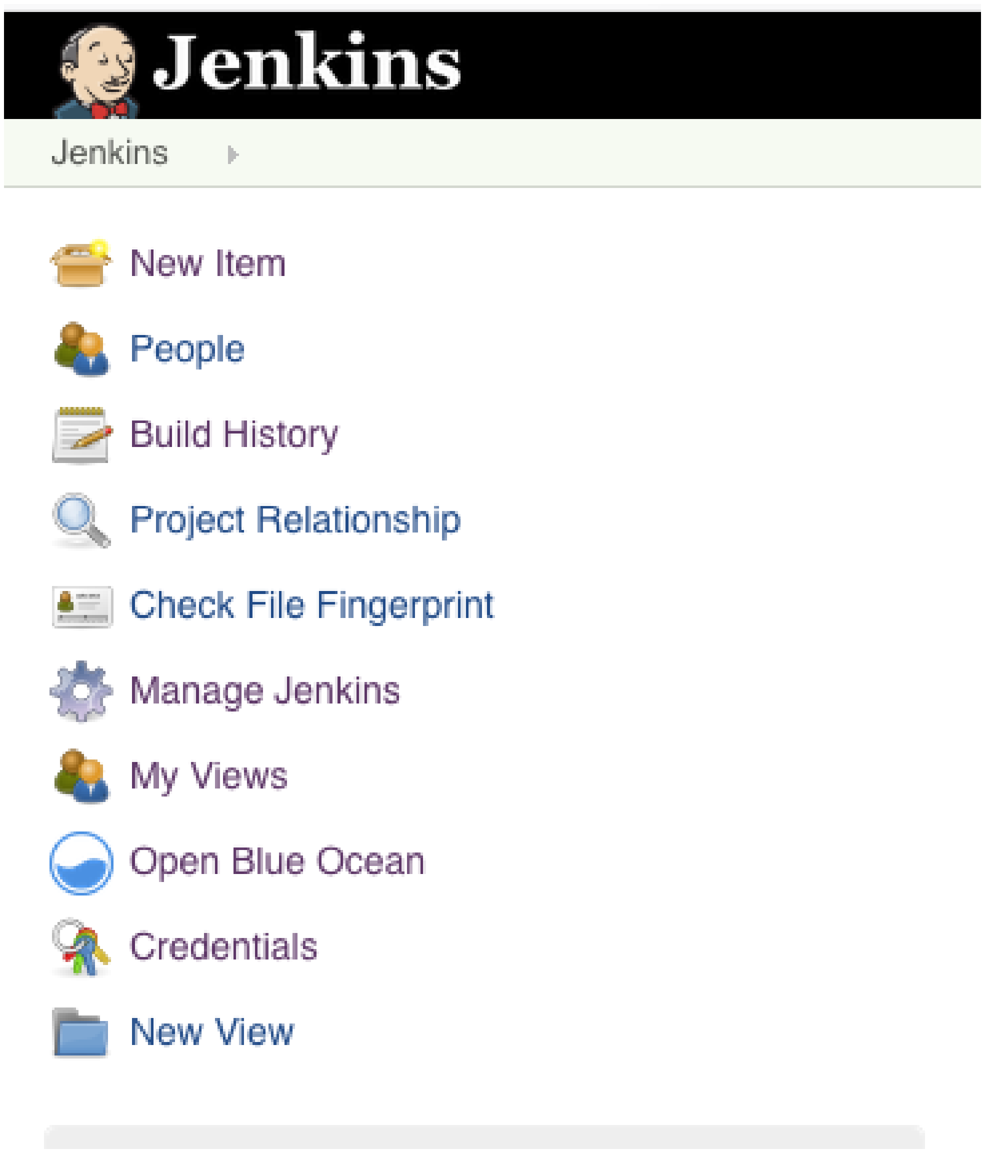
Then that's done you will see a page confirming our success:



Jenkins Pipeline - Hello World

Let’s create our first Jenkins Pipeline. Without any actual software, just printing “Hello World”.

Aftr logging in to Jenkins click on the “New Item” menu option:

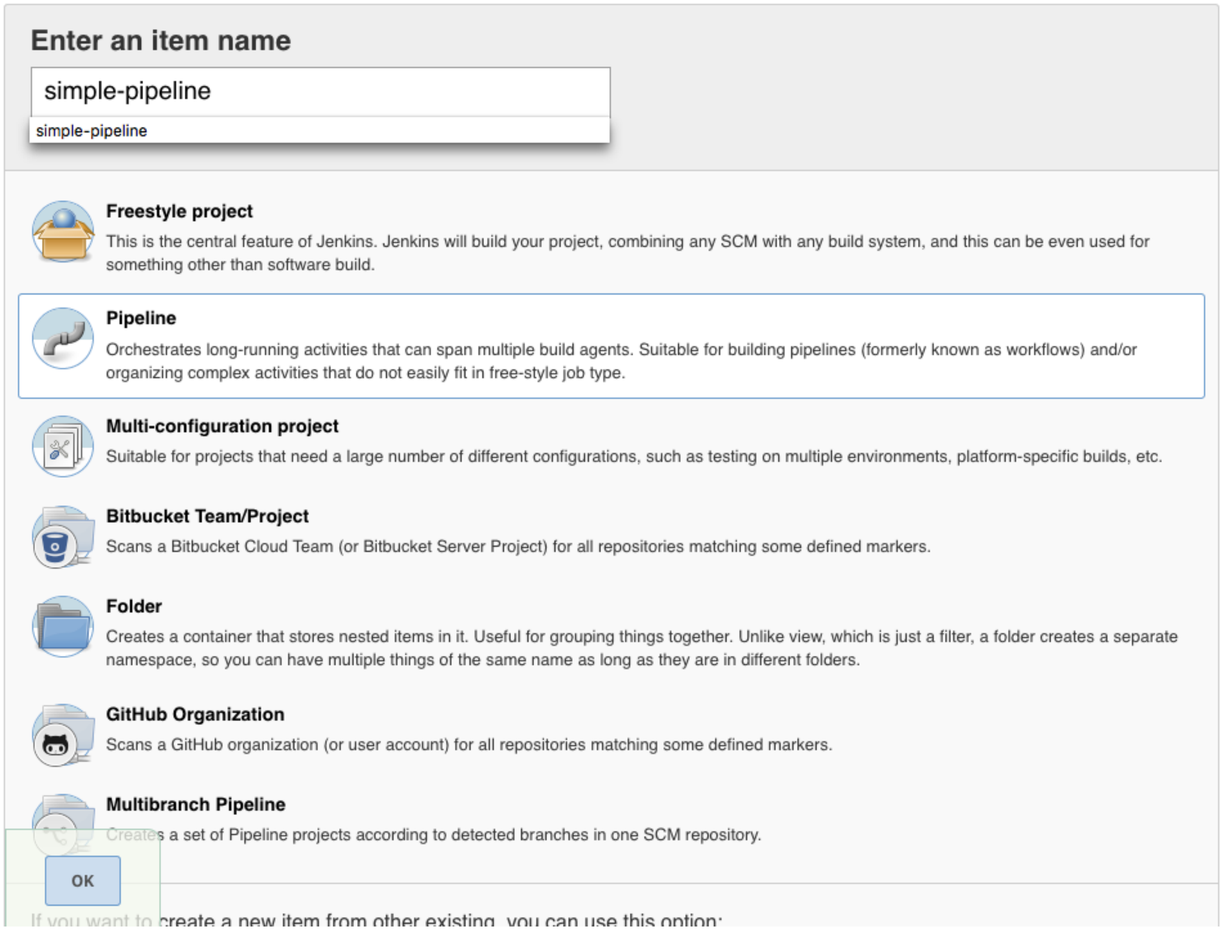


Jenkins Menu

Type in the name of the Jenkins Pipeline (simple-pipeline in our case).

Click on the “Pipeline”.

Then press the “OK” button. (It will be disabled until you select a project-type)



Enter an item name

simple-pipeline

simple-pipeline

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

Bitbucket Team/Project
Scans a Bitbucket Cloud Team (or Bitbucket Server Project) for all repositories matching some defined markers.

Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

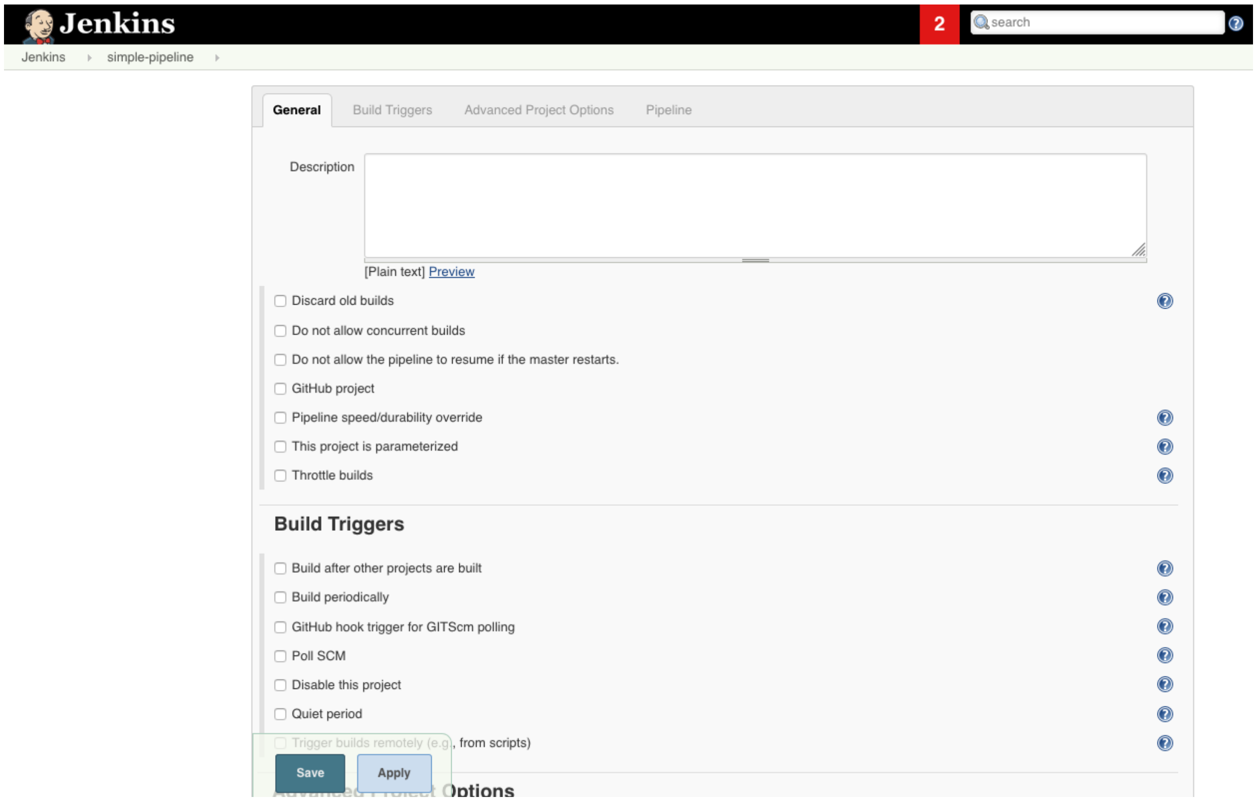
GitHub Organization
Scans a GitHub organization (or user account) for all repositories matching some defined markers.

Multibranch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

If you want to create a new item from other existing, you can use this option:

Jenkins New Item

It will take you directly to the “Configuration” page of the project that looks like this:



Description

[Plain text] Preview

- [ ] Discard old builds
- [ ] Do not allow concurrent builds
- [ ] Do not allow the pipeline to resume if the master restarts.
- [ ] GitHub project
- [ ] Pipeline speed/durability override
- [ ] This project is parameterized
- [ ] Throttle builds

Build Triggers

- [ ] Build after other projects are built
- [ ] Build periodically
- [ ] GitHub hook trigger for GITScm polling
- [ ] Poll SCM
- [ ] Disable this project
- [ ] Quiet period
- [ ] Trigger builds remotely (e.g., from scripts)

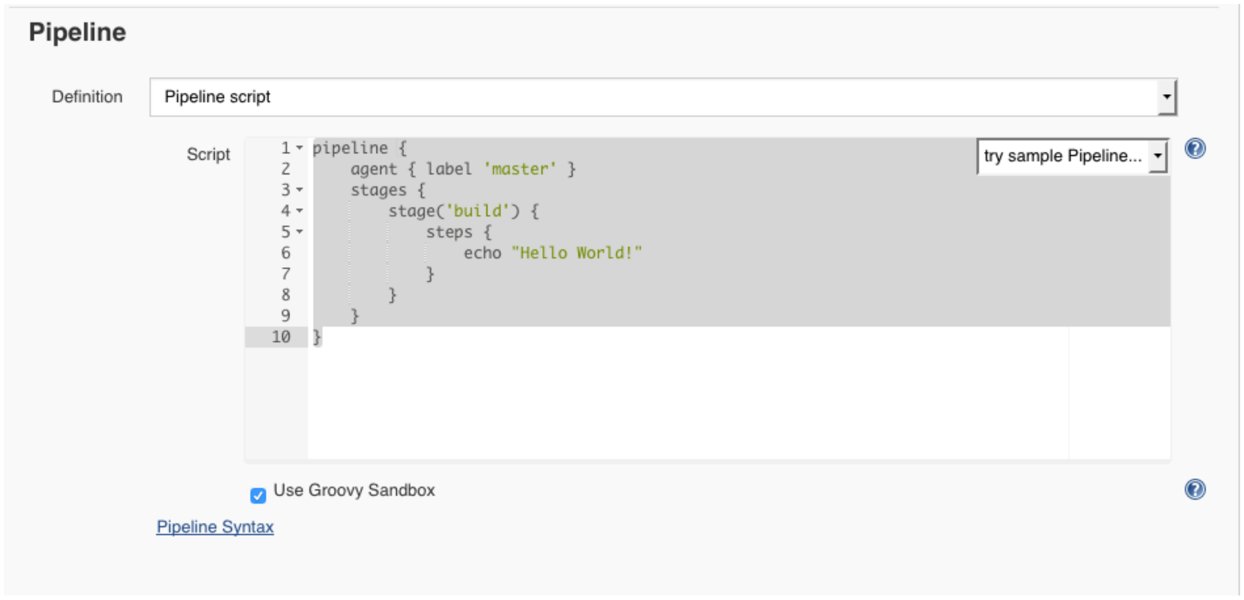
Advanced Project Options

Jenkins Pipeline config

Scroll down to the section called "Pipeline", paste the following code:

```
pipeline {
    agent { label 'master' }
    stages {
        stage('build') {
            steps {
                echo "Hello World!"
            }
        }
    }
}
```

It will look like this:

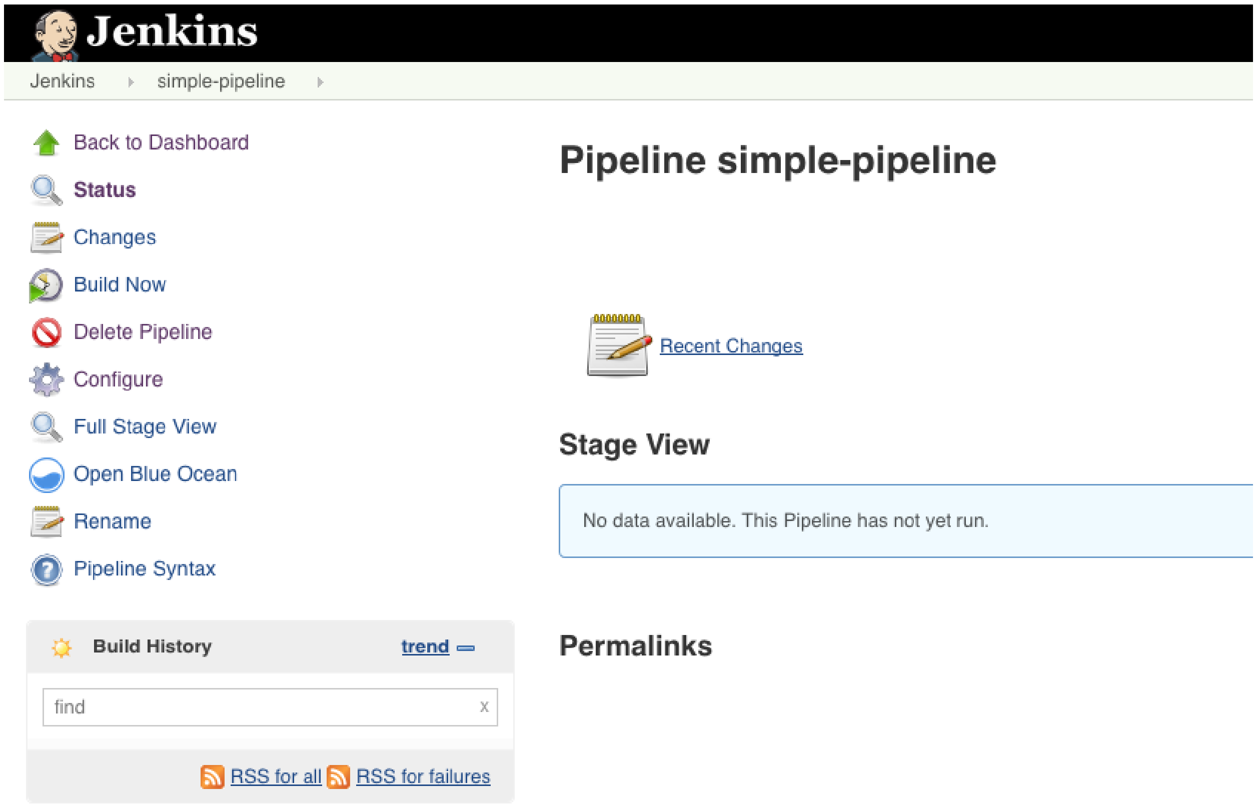


```
pipeline {
    agent { label 'master' }
    stages {
        stage('build') {
            steps {
                echo "Hello World!"
            }
        }
    }
}
```

Jenkins Pipeline

Click on "Save".

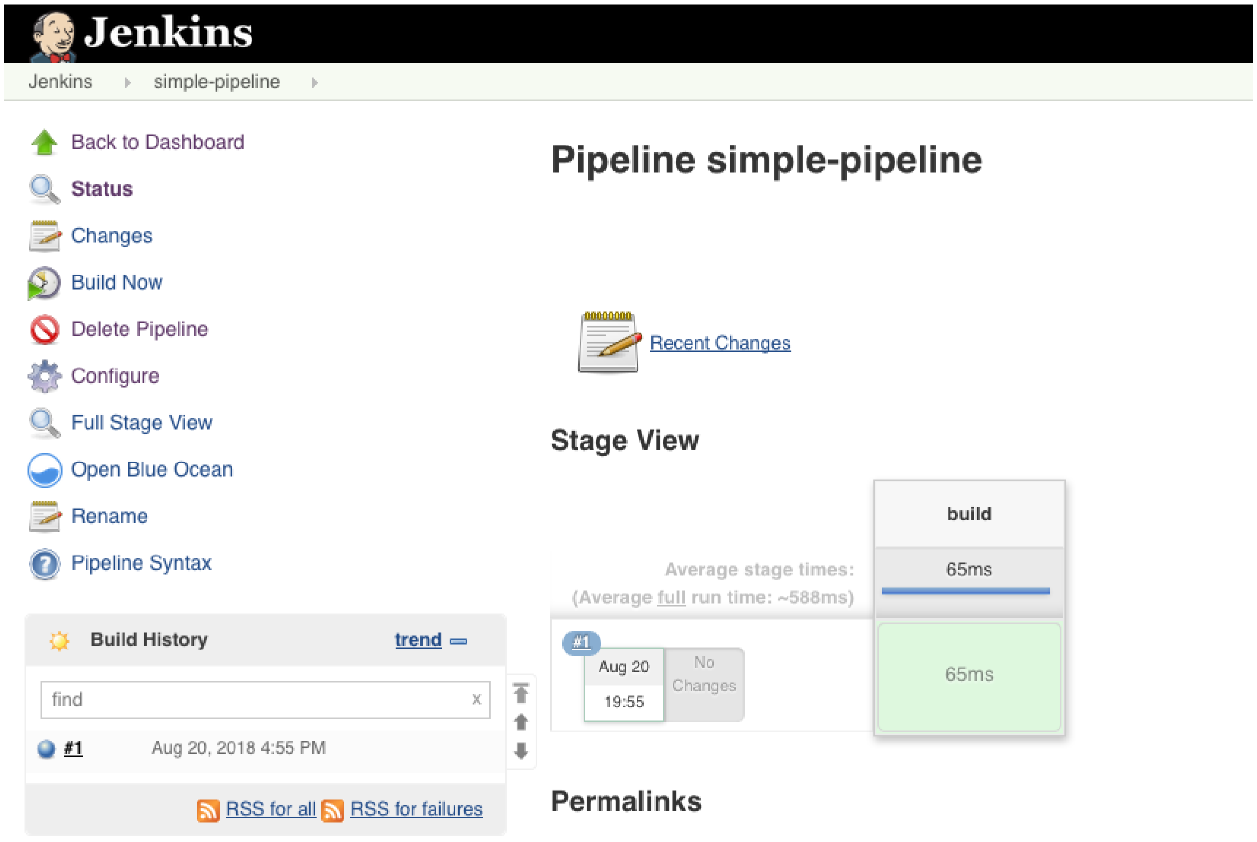
It will take to the menu of the specific project:



Jenkins Pipeline menu

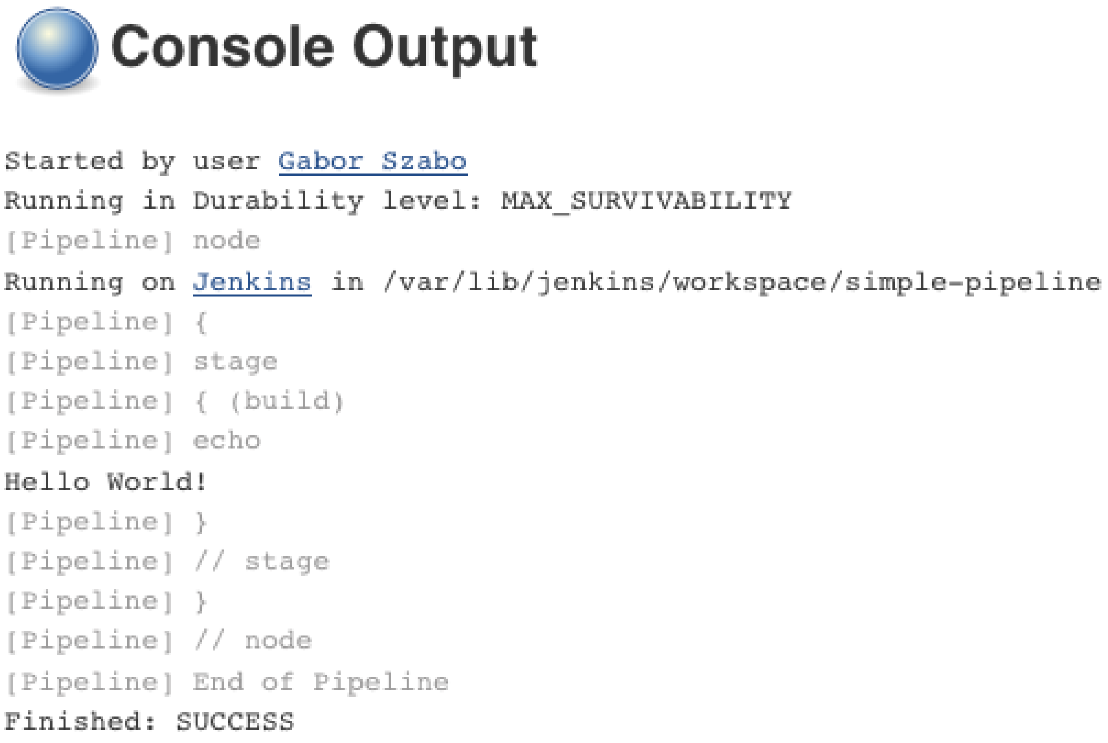
Click on the "Build Now" button.

It will start running the pipeline and within a few seconds you'll see an indicator of your first job being successful (blue dot on the left hand side).



Jenkins First job

If you click on that blue dot on the left hand side it will take you to the "Console Output" that looks like this:



```
Started by user Gabor Szabo
Running in Durability level: MAX_SURVIVABILITY
[Pipeline] node
Running on Jenkins in /var/lib/jenkins/workspace/simple-pipeline
[Pipeline] {
[Pipeline] stage
[Pipeline] { (build)
[Pipeline] echo
Hello World!
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Jenkins Console output

What is in the first pipeline?

You can see the basic structure of the pipelines.

Everything is wrapped in a block called “pipeline”. Inside we need to declare on which agents can the pipeline run. In this example we requested it to run on the Jenkins “master”. Usually only very small setups rely on the “master”. Once your project starts to grow you’ll start setting up agents Later we’ll see how to set up agents and how to tell the different parts of the pipeline to run on different agents. (Originally these were called “slaves”. While they are being renamed to “agents” you’ll still find a lot of examples using the word “slave”. In some places thet are also called “nodes”. In the end they refer to the same things. Maybe the right way to think about them is that nodes = master + agents, but then in the pipeline we also call “master” to be an agent. Go figure.

Inside the `pipeline` there can be `stages` (We have one). Inside the `stages` The can be several `stage` element. Inside each `stage` there must be `steps`. The steps themselves are Jenkins commands.

`echo` will just print something on the console. It can be useful for displaying values as the pipeline makes progress.

Jenkins Pipeline: running external programs with sh or bat

From within a Jenkins pipeline you can any external program. If your pipeline will run on Unix/Linux you need to use the `sh` command. If your pipeline will run on MS Windows you'll need to use the `bat` command.

Naturally the commands you pass to these will also need to make sense on the specific operating system.

In this example first we use the internal `echo` command of Jenkins.

Then we call `sh` and run the `echo` of our Unix shell.

Then we execute the `hostname` command and finally the `uptime` command.

```
pipeline {
    agent { label 'master' }
    stages {
        stage('build') {
            steps {
                echo "Hello World!"
                sh "echo Hello from the shell"
                sh "hostname"
                sh "uptime"
            }
        }
    }
}
```

The result looks like this:

```
Started by user Gabor Szabo
Running in Durability level: MAX_SURVIVABILITY
[Pipeline] node
Running on Jenkins in /var/lib/jenkins/workspace/simple-pipeline
[Pipeline] {
[Pipeline] stage
[Pipeline] { (build)
[Pipeline] echo
Hello World!
[Pipeline] sh
[simple-pipeline] Running shell script
+ echo Hello from the shell
Hello from the shell
[Pipeline] sh
[simple-pipeline] Running shell script
+ hostname
s17
[Pipeline] sh
[simple-pipeline] Running shell script
+ uptime
 17:15:35 up 3 days,  1:59,  0 users,  load average: 0.00, 0.00, 0.00
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

MS Windows

A few examples in Windows:

Show the name of the computer (a bit like hostname on Unix):

```
bat 'wmic computersystem get name'
```

Print out the content of the PATH environment variable as seen by Windows.

```
bat 'echo %PATH%'
```

Of course we could have printed the PATH environment variable without invoking an external call:

```
echo env.PATH
```

Print out all the environment variables seen by Windows.

```
echo bat(returnStdout: true, script: 'set')
```

Get the disk size of a local disk

```
script {
    def disk_size = sh(script: "df / --output=avail | tail -1", returnStdout: true).\
trim() as Integer
    println("disk_size = ${disk_size}")
}
```

Full examples:

```
pipeline {
    agent { label 'master' }
    stages {
        stage('build') {
            steps {
                script {
                    def disk_size = sh(script: "df / --output=avail | tail -1", retu\
rnStdout: true).trim() as Integer
                    println("disk_size = ${disk_size}")
                }
            }
        }
    }
}
```

Get the disk size of a remote disk

```
script {
    def disk_size = sh(script: "ssh remote-server df / --output=avail | tail -1", re\
turnStdout: true).trim() as Integer
    println("disk_size = ${disk_size}")
}
```

Jenkins Pipeline: Send e-mail notifications

Configuring Jenkins to send e-mail will be covered later. For now let's see a few snippets of pipeline code that will send the e-mail.

```
emailext (
    subject: "Job '${env.JOB_NAME} ${env.BUILD_NUMBER}'",
    body: """<p>Check console output at <a href="${env.BUILD_URL}">${env.JOB_NAME}</\
a></p>""",
    to: "report@code-maven.com",
    from: "jenkins@code-maven.com"
)
```

BuildUser plugin and e-mail

```
def notify(status) {
   wrap([$class: 'BuildUser']) {
       emailext (
       subject: "${status}: Job ${env.JOB_NAME} ([${env.BUILD_NUMBER})",
       body: """
       Check console output at <a href="${env.BUILD_URL}">${env.JOB_NAME} (${env.BUI\
LD_NUMBER})</a>""",
       to: "${BUILD_USER_EMAIL}",
       from: 'jenkins@company.com')
   }
}
```

Jenkins Pipeline: Add some text to the job using shortText

This will add text to the specific job on the summary page of the classic UI. The text does not show up on the BlueOcean UI.

```
script {
   manager.addShortText("Some text")
   manager.addShortText("\ntext")
   manager.addShortText("same line", "black", "lightgreen", "0px", "white")
}
```

Jenkins CLI: create node

In some situation you might need to add nodes (aka. agents) programmatically to a Jenkins setup. This is a shell script to register the new node based on the gist of Christopher Davenport[19].

[19]https://gist.github.com/ChristopherDavenport/bc5ba7a33d5dd5fc975da81c4a270a90

```
#!/bin/bash

JENKINS_URL=$1
NODE_NAME=$2
NODE_HOME='/home/build/jenkins-node'
EXECUTORS=1
SSH_PORT=22
CRED_ID=$3
LABELS=build
USERID=${USER}

cat <<EOF | java -jar ~/bin/jenkins-cli.jar -s $1 create-node $2
<slave>
  <name>${NODE_NAME}</name>
  <description></description>
  <remoteFS>${NODE_HOME}</remoteFS>
  <numExecutors>${EXECUTORS}</numExecutors>
  <mode>NORMAL</mode>
  <retentionStrategy class="hudson.slaves.RetentionStrategy$Always"/>
  <launcher class="hudson.plugins.sshslaves.SSHLauncher" plugin="ssh-slaves@1.5">
    <host>${NODE_NAME}</host>
    <port>${SSH_PORT}</port>
    <credentialsId>${CRED_ID}</credentialsId>
  </launcher>
  <label>${LABELS}</label>
  <nodeProperties/>
  <userId>${USERID}</userId>
</slave>
EOF
```

Notes:

- "Agent" and "node" is often used interchangably and in the old days they were called "slaves" so you will still see that word used in some documentation and in the code. * The origrinal name of the Jenkins project was Hudson and that too still appears in a lot of the code. * remove the -remoting flag

Index

User Handbook

User Handbook overview

This page provides an overview of the documentation in the Jenkins User Handbook.

If you want to get up and running with Jenkins, see Installing Jenkins for procedures on how to install Jenkins on your supported platform of choice.

If you are a typical Jenkins user (of any skill level) who wants to know more about Jenkins usage, see Using Jenkins. Also refer to the separate Pipeline and Blue Ocean chapters for more information about these core Jenkins features.

If you are a Jenkins administrator and want to know more about managing Jenkins nodes and instances, see Managing Jenkins.

If you are a system administrator and want to learn how to back-up, restore, maintain as Jenkins servers and nodes, see Jenkins System Administration.

Installing Jenkins

The procedures on this page are for new installations of Jenkins on a single/local machine.

Jenkins is typically run as a standalone application in its own process with the built-in Java servlet[20] container/application server (Jetty[21]).

Jenkins can also be run as a servlet in different Java servlet containers such as Apache Tomcat[22] or GlassFish[23]. However, instructions for setting up these types of installations are beyond the scope of this page.

Note: Although this page focuses on local installations of Jenkins, this content can also be used to help set up Jenkins in production environments.

Prerequisites

Minimum hardware requirements:

- 256 MB of RAM
- 1 GB of drive space (although 10 GB is a recommended minimum if running Jenkins as a Docker container)

Recommended hardware configuration for a small team:

- 1 GB+ of RAM
- 50 GB+ of drive space

Software requirements:

- Java: see the

Java Requirements page

- Web browser: see the

Web Browser Compatibility page

[20]https://stackoverflow.com/questions/7213541/what-is-java-servlet
[21]https://www.eclipse.org/jetty/
[22]https://tomcat.apache.org/
[23]https://javaee.github.io/glassfish/

Installation platforms

This section describes how to install/run Jenkins on different platforms and operating systems.

Docker

Docker[24] is a platform for running applications in an isolated environment called a "container" (or Docker container). Applications like Jenkins can be downloaded as read-only "images" (or Docker images), each of which is run in Docker as a container. A Docker container is in effect a "running instance" of a Docker image. From this perspective, an image is stored permanently more or less (i.e. insofar as image updates are published), whereas containers are stored temporarily. Read more about these concepts in the Docker documentation's Getting Started, Part 1: Orientation and setup[25] page.

Docker's fundamental platform and container design means that a single Docker image (for any given application like Jenkins) can be run on any supported operating system (macOS, Linux and Windows) or cloud service (AWS and Azure) which is also running Docker.

Installing Docker

To install Docker on your operating system, visit the Docker store[26] website and click the *Docker Community Edition* box which is suitable for your operating system or cloud service. Follow the installation instructions on their website.

Jenkins can also run on Docker Enterprise Edition, which you can access through *Docker EE* on the Docker store website.

```
If you are installing Docker on a Linux-based operating system, ensure
you configure Docker so it can be managed as a non-root user. Read more about
this in Docker's
link:https://docs.docker.com/engine/installation/linux/linux-postinstall/[Post-insta\
llation
steps for Linux] page of their documentation. This page also contains
information about how to configure Docker to start on boot.
```

Downloading and running Jenkins in Docker

There are several Docker images of Jenkins available.

The recommended Docker image to use is the `jenkinsci/blueocean` image[27] (from the Docker Hub repository[28]). This image contains the current Long-Term Support (LTS) release of Jenkins (which

[24]https://docs.docker.com/engine/docker-overview/
[25]https://docs.docker.com/get-started/
[26]https://store.docker.com/search?type=edition&offering=community
[27]https://hub.docker.com/r/jenkinsci/blueocean/
[28]https://hub.docker.com/

is production-ready) bundled with all Blue Ocean plugins and features. This means that you do not need to install the Blue Ocean plugins separately.

```
A new `jenkinsci/blueocean` image is published each time a new release of Blue
Ocean is published. You can see a list of previously published versions of the
`jenkinsci/blueocean` image on the
link:https://hub.docker.com/r/jenkinsci/blueocean/tags/[tags] page.

There are also other Jenkins Docker images you can use (accessible through
link:https://hub.docker.com/r/jenkins/jenkins/[`jenkins/jenkins`] on Docker
Hub). However, these do not come with Blue Ocean, which would need to be
installed via the link:../managing[*Manage Jenkins*] >
link:../managing/plugins[*Manage Plugins*] page in Jenkins. Read more
about this in link:../blueocean/getting-started[Getting started with Blue Ocean].
```

include::doc/book/installing/_docker.adoc[]

WAR file

The Web application ARchive (WAR) file version of Jenkins can be installed on any operating system or platform that supports Java.

To download and run the WAR file version of Jenkins:

. Download the latest stable Jenkins WAR file[29] to an appropriate directory on your machine. . Open up a terminal/command prompt window to the download directory. . Run the command `java -jar jenkins.war`. . Browse to `\http://localhost:8080` and wait until the *Unlock Jenkins* page appears. . Continue on with the Post-installation setup wizard below.

Notes:

- Unlike downloading and running Jenkins with Blue Ocean in Docker
- You can change the port by specifying the `--httpPort` option when you run the (above), this process does not automatically install the Blue Ocean features, which would need to installed separately via the **Manage Jenkins** > **Manage Plugins** page in Jenkins. Read more about the specifics for installing Blue Ocean on the Getting started with Blue Ocean page. `java -jar jenkins.war` command. For example, to make Jenkins accessible through port 9090, then run Jenkins using the command: + `java -jar jenkins.war --httpPort=9090`

macOS

To install from the website, using a package:

[29]http://mirrors.jenkins.io/war-stable/latest/jenkins.war

*
Download the latest package[30]

- Open the package and follow the instructions

Jenkins can also be installed using `brew`:

- Install the latest release version

```
brew install jenkins
```

- Install the LTS version

```
brew install jenkins-lts
```

Linux

Debian/Ubuntu

On Debian-based distributions, such as Ubuntu, you can install Jenkins through `apt`.

Recent versions are available in an apt repository[31]. Older but stable LTS versions are in this apt repository[32].

```
wget -q -O - https://pkg.jenkins.io/debian/jenkins.io.key | sudo apt-key add -
sudo sh -c 'echo deb https://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources\
.list.d/jenkins.list'
sudo apt-get update
sudo apt-get install jenkins
```

This package installation will:

- Setup Jenkins as a daemon launched on start. See `/etc/init.d/jenkins` for more details.
- Create a ‘`jenkins`’ user to run this service.
- Direct console log output to the file `/var/log/jenkins/jenkins.log`. Check this file if you are troubleshooting Jenkins.
- Populate `/etc/default/jenkins` with configuration parameters for the launch, e.g `JENKINS_-HOME`
- Set Jenkins to listen on port 8080. Access this port with your browser to start configuration.

[30]http://mirrors.jenkins.io/osx/latest
[31]https://pkg.jenkins.io/debian/
[32]https://pkg.jenkins.io/debian-stable/

```
If your `/etc/init.d/jenkins` file fails to start Jenkins, edit the `/etc/default/je\
nkins` to replace the line
`----HTTP_PORT=8080----` with `----HTTP_PORT=8081----`
Here, "8081" was chosen but you can put another port available.
```

Fedora

You can install Jenkins through `dnf`. You need to add the Jenkins repository from the Jenkins website to the package manager first.

```
sudo wget -O /etc/yum.repos.d/jenkins.repo http://pkg.jenkins-ci.org/redhat/jenkins.\
repo
sudo rpm --import https://jenkins-ci.org/redhat/jenkins-ci.org.key
```

Then, you can install Jenkins. The following command also ensures you have java installed.

```
sudo dnf upgrade && sudo dnf install jenkins java
```

Next, start the Jenkins service.

```
sudo service jenkins start
sudo chkconfig jenkins on
```

You can check the status of the Jenkins service using this systemctl command:

```
systemctl status jenkins
```

If everything has been set up correctly, you should see an output like this:

```
Loaded: loaded (/etc/rc.d/init.d/jenkins; generated)
Active: active (running) since Tue 2018-11-13 16:19:01 +03; 4min 57s ago
...
```

```
firewall-cmd --permanent --new-service=jenkins
firewall-cmd --permanent --service=jenkins --set-short="Jenkins Service Ports"
firewall-cmd --permanent --service=jenkins --set-description="Jenkins service firewa\
lld port exceptions"
firewall-cmd --permanent --service=jenkins --add-port=YOURPORT/tcp
firewall-cmd --permanent --add-service=jenkins
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --reload
```

```
If you have a firewall installed, you must add Jenkins as an exception.
You must change `YOURPORT` in the script below to the port you want to use. Port `80\
80` is the most common.
```

Windows

To install from the website, using the installer:

*

Download the latest package[33]

- Open the package and follow the instructions

Other operating systems

OpenIndiana Hipster

On a system running OpenIndiana Hipster[34] Jenkins can be installed in either the local or global zone using the link:https://en.wikipedia.org/wiki/Image*Packaging*System[Image Packaging System] (IPS).

[IMPORTANT] ==== Disclaimer: This platform is NOT officially supported by the Jenkins team, use it at your own risk. Packaging and integration described in this section is maintained by the OpenIndiana Hipster team, bundling the generic `jenkins.war` to work in that operating environment. ====

For the common case of running the newest packaged weekly build as a standalone (Jetty) server, simply execute:

[33]http://mirrors.jenkins.io/windows/latest
[34]https://www.openindiana.org/

```
pkg install jenkins
svcadm enable jenkins
```

The common packaging integration for a standalone service will:

- Create a `jenkins` user to run the service and to own the directory structures under `/var/lib/jenkins`.
- Pull the OpenJDK8 and other packages required to execute Jenkins, including
- Set up Jenkins as an SMF service instance (`svc:/network/http:jenkins`) which
- Set up Jenkins to listen on port 8080.
- Configure the log output to be managed by SMF at `/var/svc/log/network-http:jenkins.log`. the `jenkins-core-weekly` package with the latest `jenkins.war`. + CAUTION: Long-Term Support (LTS) Jenkins releases currently do not support OpenZFS-based systems, so no packaging is provided at this time. can then be enabled with the `svcadm` command demonstrated above.

Once Jenkins is running, consult the log (`/var/svc/log/network-http:jenkins.log`) to retrieve the generated administrator password for the initial set up of Jenkins, usually it will be found at `/var/lib/jenkins/home/secrets/initialAdminPassword`. Then navigate to localhost:8080[35] to complete configuration of the Jenkins instance.

To change attributes of the service, such as environment variables like `JENKINS_HOME` or the port number used for the Jetty web server, use the `svccfg` utility:

```
svccfg -s svc:/network/http:jenkins editprop
svcadm refresh svc:/network/http:jenkins
```

You can also refer to `/lib/svc/manifest/network/jenkins-standalone.xml` for more details and comments about currently supported tunables of the SMF service. Note that the `jenkins` user account created by the packaging is specially privileged to allow binding to port numbers under 1024.

The current status of Jenkins-related packages available for the given release of OpenIndiana can be queried with:

```
pkg info -r '*jenkins*'
```

Upgrades to the package can be performed by updating the entire operating environment with `pkg update`, or specifically for Jenkins core software with:

```
pkg update jenkins-core-weekly
```

[35]http://localhost:8080

```
Procedure for updating the package will restart the currently running Jenkins
process. Make sure to prepare it for shutdown and finish all running jobs
before updating, if needed.
```

Solaris, OmniOS, SmartOS, and other siblings

Generally it should suffice to install Java 8 and download the `jenkins.war` and run it as a standalone process or under an application server such as Apache Tomcat[36].

Some caveats apply:

- Headless JVM and fonts: For OpenJDK builds on minimalized-footprint systems,
- ZFS-related JVM crashes: When Jenkins runs on a system detected as a `SunOS`,
  there may be issues running the headless JVM[37], because Jenkins needs some fonts to render certain pages. it tries to load integration for advanced ZFS features using the bundled `libzfs.jar` which maps calls from Java to native `libzfs.so` routines provided by the host OS. Unfortunately, that library was made for binary utilities built and bundled by the OS along with it at the same time, and was never intended as a stable interface exposed to consumers. As the forks of Solaris legacy, including ZFS and later the OpenZFS initiative evolved, many different binary function signatures were provided by different host operating systems - and when Jenkins `libzfs.jar` invoked the wrong signature, the whole JVM process crashed. A solution was proposed and integrated in `jenkins.war` since weekly release 2.55 (and not yet in any LTS to date) which enables the administrator to configure which function signatures should be used for each function known to have different variants, apply it to their application server initialization options and then run and update the generic `jenkins.war` without further workarounds. See the libzfs4j Git repository[38] for more details, including a script to try and "lock-pick" the configuration needed for your particular distribution (in particular if your kernel updates bring a new incompatible `libzfs.so`).

Also note that forks of the OpenZFS initiative may provide ZFS on various BSD, Linux, and macOS distributions. Once Jenkins supports detecting ZFS capabilities, rather than relying on the `SunOS` check, the above caveats for ZFS integration with Jenkins should be considered.

include::doc/book/installing/_setup-wizard.adoc[]

[36]https://tomcat.apache.org
[37]https://wiki.jenkins.io/display/JENKINS/Jenkins+got+java.awt.headless+problem
[38]https://github.com/kohsuke/libzfs4j

Using Jenkins

This chapter contains topics for typical Jenkins users (of all skill levels) about Jenkins usage which is outside the scope of the core Jenkins features: Pipeline and Blue Ocean.

If you want to create and configure a Pipeline project through a `Jenkinsfile` or through Blue Ocean, or you wish to find out more about these core Jenkins features, refer to the relevant topics within the respective Pipeline and Blue Ocean chapters.

If you are a Jenkins administrator and want to know more about managing Jenkins nodes and instances, see Managing Jenkins.

If you are a system administrator and want learn how to back-up, restore, maintain as Jenkins servers and nodes, see Jenkins System Administration.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

Using credentials

There are numerous 3rd-party sites and applications that can interact with Jenkins, for example, artifact repositories, cloud-based storage systems and services, and so on.

A systems administrator of such an application can configure credentials in the application for dedicated use by Jenkins. This would typically be done to “lock down” areas of the application’s functionality available to Jenkins, usually by applying access controls to these credentials. Once a Jenkins manager (i.e. a Jenkins user who administers a Jenkins site) adds/configures these credentials in Jenkins, the credentials can be used by Pipeline projects to interact with these 3rd party applications.

Note: The Jenkins credentials functionality described on this and related pages is provided by the plugin:credentials-binding[Credentials Binding plugin].

Credentials stored in Jenkins can be used:

- anywhere applicable throughout Jenkins (i.e. global credentials),
- by a specific Pipeline project/item (read more about this in the
- by a specific Jenkins user (as is the case for
  [[types-of-credentials]] Handling credentials section of Using a Jenkinsfile), Pipeline projects created in Blue Ocean).

Jenkins can store the following types of credentials:

- *Secret text* - a token such as an API token (e.g. a GitHub personal access
- *Username and password* - which could be handled as separate components or as
- *Secret file* - which is essentially secret content in a file,
- *SSH Username with private key* - an
- *Certificate* - a link:https://tools.ietf.org/html/rfc7292[PKCS#12 certificate
- *Docker Host Certificate Authentication* credentials.
  token), a colon separated string in the format `username:password` (read more about this in Handling credentials), SSH public/private key pair[39], file] and optional password, or

Credential security

To maximize security, credentials configured in Jenkins are stored in an encrypted form on the master Jenkins instance (encrypted by the Jenkins instance ID) and are only handled in Pipeline projects via their credential IDs.

This minimizes the chances of exposing the actual credentials themselves to Jenkins users and hinders the ability to copy functional credentials from one Jenkins instance to another.

[39]http://www.snailbook.com/protocols.html

Configuring credentials

This section describes procedures for configuring credentials in Jenkins.

Credentials can be added to Jenkins by any Jenkins user who has the *Credentials > Create* permission (set through *Matrix-based security*). These permissions can be configured by a Jenkins user with the *Administer* permission. Read more about this in the Authorization section of Managing Security.

Otherwise, any Jenkins user can add and configure credentials if the *Authorization* settings of your Jenkins instance's *Configure Global Security* settings page is set to the default *Logged-in users can do anything* setting or *Anyone can do anything* setting.

Adding new global credentials

To add new global credentials to your Jenkins instance:

. If required, ensure you are logged in to Jenkins (as a user with the *Credentials > Create* permission). . From the Jenkins home page (i.e. the Dashboard of the Jenkins classic UI), click *Credentials > System* on the left. . Under *System*, click the *Global credentials (unrestricted)* link to access this default domain. . Click *Add Credentials* on the left. + *Note:* If there are no credentials in this default domain, you could also click the *add some credentials* link (which is the same as clicking the *Add Credentials* link). . From the *Kind* field, choose the type of credentials to add. . From the *Scope* field, choose either: * *Global* - if the credential/s to be added is/are for a Pipeline project/item. Choosing this option applies the scope of the credential/s to the Pipeline project/item "object" and all its descendent objects. * *System* - if the credential/s to be added is/are for the Jenkins instance itself to interact with system administration functions, such as email authentication, agent connection, etc. Choosing this option applies the scope of the credential/s to a single object only. . Add the credentials themselves into the appropriate fields for your chosen credential type: * *Secret text* - copy the secret text and paste it into the *Secret* field. * *Username and password* - specify the credential's *Username* and *Password* in their respective fields. * *Secret file* - click the *Choose file* button next to the *File* field to select the secret file to upload to Jenkins. * *SSH Username with private key* - specify the credentials *Username*, *Private Key* and optional *Passphrase* into their respective fields. + *Note:* Choosing *Enter directly* allows you to copy the private key's text and paste it into the resulting *Key* text box. * *Certificate* - specify the *Certificate* and optional *Password*. Choosing *Upload PKCS#12 certificate* allows you to upload the certificate as a file via the resulting *Upload certificate* button. * *Docker Host Certificate Authentication* - copy and paste the appropriate details into the *Client Key*, *Client Certificate* and *Server CA Certificate* fields. . In the *ID* field, specify a meaningful credential ID value - for example, `jenkins-user-for-xyz-artifact-repository`. You can use upper- or lower-case letters for the credential ID, as well as any valid separator character. However, for the benefit of all users on your Jenkins instance, it is best to use a single and consistent convention for specifying credential IDs. + *Note:* This field is optional. If you do not specify its value, Jenkins assigns a globally unique ID (GUID) value for the credential ID. Bear in mind that once a credential ID is set, it can no longer be changed. . Specify an optional *Description* for the credential/s. . Click *OK* to save the credentials.

Pipeline

This chapter covers all recommended aspects of Jenkins Pipeline functionality, including how to:
*
get started with Pipeline - covers how to
*
create and use a `Jenkinsfile` - covers use-case scenarios

- work with

branches and pull requests,
*
use Docker with Pipeline - covers how Jenkins can invoke Docker
*
extend Pipeline with shared libraries,

- use different

development tools to facilitate the creation

- work with

Pipeline syntax - this page is a comprehensive
 define a Jenkins Pipeline (i.e. your `Pipeline`) through Blue Ocean, through the classic UI or in SCM, on how to craft and construct your `Jenkinsfile`, containers on agents/nodes (from a `Jenkinsfile`) to build your Pipeline projects, of your Pipeline, and reference of all Declarative Pipeline syntax.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

What is Jenkins Pipeline?

[[overview]]

Jenkins Pipeline (or simply "Pipeline" with a capital "P") is a suite of plugins which supports implementing and integrating *continuous delivery pipelines* into Jenkins.

A *continuous delivery (CD) pipeline* is an automated expression of your process for getting software from version control right through to your users and customers. Every change to your software (committed in source control) goes through a complex process on its way to being released. This process involves building the software in a reliable and repeatable manner, as well as progressing the built software (called a "build") through multiple stages of testing and deployment.

Pipeline provides an extensible set of tools for modeling simple-to-complex delivery pipelines "as code" via the Pipeline domain-specific language (DSL) syntax. footnoteref:[dsl,Domain-specific language[40]]

The definition of a Jenkins Pipeline is written into a text file (called a `Jenkinsfile`) which in turn can be committed to a project's source control repository. footnoteref:[scm,Source control management[41]] This is the foundation of "Pipeline-as-code"; treating the CD pipeline a part of the application to be versioned and reviewed like any other code.

Creating a `Jenkinsfile` and committing it to source control provides a number of immediate benefits:

- Automatically creates a Pipeline build process for all branches and pull
- Code review/iteration on the Pipeline (along with the remaining source code).
- Audit trail for the Pipeline.
- Single source of truth
  requests. footnote:[link:https://en.wikipedia.org/wiki/Single_source*of*truth[Single source of truth]] for the Pipeline, which can be viewed and edited by multiple members of the project.

While the syntax for defining a Pipeline, either in the web UI or with a `Jenkinsfile` is the same, it is generally considered best practice to define the Pipeline in a `Jenkinsfile` and check that in to source control.

Declarative versus Scripted Pipeline syntax

A `Jenkinsfile` can be written using two types of syntax - Declarative and Scripted.

Declarative and Scripted Pipelines are constructed fundamentally differently. Declarative Pipeline is a more recent feature of Jenkins Pipeline which:

- provides richer syntactical features over Scripted Pipeline syntax, and
- is designed to make writing and reading Pipeline code easier.

Many of the individual syntactical components (or "steps") written into a `Jenkinsfile`, however, are common to both Declarative and Scripted Pipeline. Read more about how these two types of syntax differ in <<pipeline-concepts>> and <<pipeline-syntax-overview>> below.

[40]https://en.wikipedia.org/wiki/Domain-specific_language
[41]https://en.wikipedia.org/wiki/Version_control

Why Pipeline?

[[why]]

Jenkins is, fundamentally, an automation engine which supports a number of automation patterns. Pipeline adds a powerful set of automation tools onto Jenkins, supporting use cases that span from simple continuous integration to comprehensive CD pipelines. By modeling a series of related tasks, users can take advantage of the many features of Pipeline:

- *Code*: Pipelines are implemented in code and typically checked into source
- *Durable*: Pipelines can survive both planned and unplanned restarts of the
- *Pausable*: Pipelines can optionally stop and wait for human input or approval
- *Versatile*: Pipelines support complex real-world CD requirements, including
- *Extensible*: The Pipeline plugin supports custom extensions to its DSL
  control, giving teams the ability to edit, review, and iterate upon their delivery pipeline. Jenkins master. before continuing the Pipeline run. the ability to fork/join, loop, and perform work in parallel. footnoteref:[dsl] and multiple options for integration with other plugins.

While Jenkins has always allowed rudimentary forms of chaining Freestyle Jobs together to perform sequential tasks, footnote:[Additional plugins have been used to implement complex behaviors utilizing Freestyle Jobs such as the Copy Artifact, Parameterized Trigger, and Promoted Builds plugins] Pipeline makes this concept a first-class citizen in Jenkins.

Building on the core Jenkins value of extensibility, Pipeline is also extensible both by users with Pipeline Shared Libraries and by plugin developers. footnoteref:[ghof,plugin:github-organization-folder[GitHub Organization Folder plugin]]

The flowchart below is an example of one CD scenario easily modeled in Jenkins Pipeline:

image:pipeline/realworld-pipeline-flow.png[alt="Pipeline Flow",width=100%]

Pipeline concepts

The following concepts are key aspects of Jenkins Pipeline, which tie in closely to Pipeline syntax (see the overview below).

Pipeline

A Pipeline is a user-defined model of a CD pipeline. A Pipeline's code defines your entire build process, which typically includes stages for building an application, testing it and then delivering it.

Also, a `pipeline` block is a key part of Declarative Pipeline syntax.

Node

A node is a machine which is part of the Jenkins environment and is capable of executing a Pipeline.

Also, a `node` block is a key part of Scripted Pipeline syntax.

Stage

A `stage` block defines a conceptually distinct subset of tasks performed through the entire Pipeline (e.g. "Build", "Test" and "Deploy" stages), which is used by many plugins to visualize or present Jenkins Pipeline status/progress. footnoteref:[blueocean,Blue Ocean, plugin:pipeline-stage-view[Pipeline: Stage View plugin]]

Step

A single task. Fundamentally, a step tells Jenkins *what* to do at a particular point in time (or "step" in the process). For example, to execute the shell command `make` use the `sh` step: `sh 'make'`. When a plugin extends the Pipeline DSL, footnoteref:[dsl] that typically means the plugin has implemented a new *step*.

Pipeline syntax overview

The following Pipeline code skeletons illustrate the fundamental differences between Declarative Pipeline syntax and Scripted Pipeline syntax.

Be aware that both stages and steps (above) are common elements of both Declarative and Scripted Pipeline syntax.

Declarative Pipeline fundamentals

In Declarative Pipeline syntax, the `pipeline` block defines all the work done throughout your entire Pipeline.

[pipeline] —- // Declarative // pipeline // Script // —- <1> Execute this Pipeline or any of its stages, on any available agent. <2> Defines the "Build" stage. <3> Perform some steps related to the "Build" stage. <4> Defines the "Test" stage. <5> Perform some steps related to the "Test" stage. <6> Defines the "Deploy" stage. <7> Perform some steps related to the "Deploy" stage.

Scripted Pipeline fundamentals

In Scripted Pipeline syntax, one or more `node` blocks do the core work throughout the entire Pipeline. Although this is not a mandatory requirement of Scripted Pipeline syntax, confining your Pipeline's work inside of a `node` block does two things:

. Schedules the steps contained within the block to run by adding an item to the Jenkins queue. As soon as an executor is free on a node, the steps will run. . Creates a workspace (a directory specific to that particular Pipeline) where work can be done on files checked out from source control. + *Caution:* Depending on your Jenkins configuration, some workspaces may not get automatically cleaned up after a period of inactivity. See tickets and discussion linked from https://issues.jenkins-ci.org/browse/JENKINS-2111[JENKINS-2111] for more information.

[pipeline] —- // Declarative // // Script // node —- <1> Execute this Pipeline or any of its stages, on any available agent. <2> Defines the "Build" stage. `stage` blocks are optional in Scripted Pipeline syntax. However, implementing `stage` blocks in a Scripted Pipeline provides clearer visualization of each `stage`'s subset of tasks/steps in the Jenkins UI. <3> Perform some steps related to the "Build" stage. <4> Defines the "Test" stage. <5> Perform some steps related to the "Test" stage. <6> Defines the "Deploy" stage. <7> Perform some steps related to the "Deploy" stage.

Pipeline example

Here is an example of a `Jenkinsfile` using Declarative Pipeline syntax - its Scripted syntax equivalent can be accessed by clicking the *Toggle Scripted Pipeline* link below:

[pipeline] —- // Declarative // pipeline —- <1> `pipeline` is Declarative Pipeline-specific syntax that defines a "block" containing all content and instructions for executing the entire Pipeline. <2> `agent` is Declarative Pipeline-specific syntax that instructs Jenkins to allocate an executor (on a node) and workspace for the entire Pipeline. <3> `stage` is a syntax block that describes a stage of this Pipeline. Read more about `stage` blocks in Declarative Pipeline syntax on the Pipeline syntax page. As mentioned above, `stage` blocks are optional in Scripted Pipeline syntax. <4> `steps` is Declarative Pipeline-specific syntax that describes the steps to be run in this `stage`. <5> `sh` is a Pipeline step (provided by the plugin:workflow-durable-task-step[Pipeline: Nodes and Processes plugin]) that executes the given shell command. <6> `junit` is another a Pipeline step (provided by the plugin:junit[JUnit plugin]) for aggregating test reports. <7> `node` is Scripted Pipeline-specific syntax that instructs Jenkins to execute this Pipeline (and any stages contained within it), on any available agent/node. This is effectively equivalent to `agent` in Declarative Pipeline-specific syntax.

Read more about Pipeline syntax on the Pipeline Syntax page.

Getting started with Pipeline

As mentioned previously, Jenkins Pipeline is a suite of plugins that supports implementing and integrating continuous delivery pipelines into Jenkins. Pipeline provides an extensible set of tools for modeling simple-to-complex delivery pipelines "as code" via the Pipeline DSL. footnoteref:[dsl,Domain-specific language[42]]

This section describes how to get started with creating your Pipeline project in Jenkins and introduces you to the various ways that a `Jenkinsfile` can be created and stored.

Prerequisites

To use Jenkins Pipeline, you will need:

- Jenkins 2.x or later (older versions back to 1.642.3 may work but are not
- Pipeline plugin,
  recommended) footnoteref:[pipeline,Pipeline plugin[43]] which is installed as part of the "suggested plugins" (specified when running through the Post-installation setup wizard after installing Jenkins).

Read more about how to install and manage plugins in Managing Plugins.

Defining a Pipeline

Both Declarative and Scripted Pipeline are DSLs footnoteref:[dsl] to describe portions of your software delivery pipeline. Scripted Pipeline is written in a limited form of Groovy syntax[44].

Relevant components of Groovy syntax will be introduced as required throughout this documentation, so while an understanding of Groovy is helpful, it is not required to work with Pipeline.

A Pipeline can be created in one of the following ways:

- <<through-blue-ocean>> - after setting up a Pipeline project in Blue Ocean,
- <<through-the-classic-ui>> - you can enter a basic Pipeline directly in

[42]https://en.wikipedia.org/wiki/Domain-specific_language
[43]https://plugins.jenkins.io/workflow-aggregator
[44]http://groovy-lang.org/semantics.html

*

In SCM - you can write a `Jenkinsfile`
 the Blue Ocean UI helps you write your Pipeline's `Jenkinsfile` and commit it to source control. Jenkins through the classic UI. manually, which you can commit to your project's source control repository. footnoteref:[scm,Source control management[45]]

The syntax for defining a Pipeline with either approach is the same, but while Jenkins supports entering Pipeline directly into the classic UI, it is generally considered best practice to define the Pipeline in a `Jenkinsfile` which Jenkins will then load directly from source control.

Through Blue Ocean

If you are new to Jenkins Pipeline, the Blue Ocean UI helps you set up your Pipeline project, and automatically creates and writes your Pipeline (i.e. the `Jenkinsfile`) for you through the graphical Pipeline editor.

As part of setting up your Pipeline project in Blue Ocean, Jenkins configures a secure and appropriately authenticated connection to your project's source control repository. Therefore, any changes you make to the `Jenkinsfile` via Blue Ocean's Pipeline editor are automatically saved and committed to source control.

Read more about Blue Ocean in the Blue Ocean chapter and Getting started with Blue Ocean page.

Through the classic UI

A `Jenkinsfile` created using the classic UI is stored by Jenkins itself (within the Jenkins home directory).

To create a basic Pipeline through the Jenkins classic UI:

. If required, ensure you are logged in to Jenkins. . From the Jenkins home page (i.e. the Dashboard of the Jenkins classic UI), click *New Item* at the top left. + [.boxshadow] image:pipeline/classic-ui-left-column.png[alt="Classic UI left column",width=30%] . In the *Enter an item name* field, specify the name for your new Pipeline project. + *Caution:* Jenkins uses this item name to create directories on disk. It is recommended to avoid using spaces in item names, since doing so may uncover bugs in scripts that do not properly handle spaces in directory paths. . Scroll down and click *Pipeline*, then click *OK* at the end of the page to open the Pipeline configuration page (whose *General* tab is selected). + [.boxshadow] image:pipeline/new-item-creation.png[alt="Enter a name, click *Pipeline* and then click *OK*",width=100%] . Click the *Pipeline* tab at the top of the page to scroll down to the *Pipeline* section. + *Note:* If instead you are defining your `Jenkinsfile` in source control, follow the instructions in In SCM below. . In the *Pipeline* section, ensure that the *Definition* field indicates the *Pipeline script* option. . Enter your Pipeline code into the *Script* text area. + For instance, copy the following Declarative example Pipeline code (below the *Jenkinsfile (…)* heading) or its Scripted version equivalent and paste this into the *Script* text area. (The Declarative example below is used

[45]https://en.wikipedia.org/wiki/Version_control

throughout the remainder of this procedure.) + [pipeline] —- // Declarative // pipeline —- <1> `agent` instructs Jenkins to allocate an executor (on any available agent/node in the Jenkins environment) and workspace for the entire Pipeline. <2> `echo` writes simple string in the console output. <3> `node` effectively does the same as `agent` (above). + [.boxshadow] image:pipeline/example-pipeline-in-classic-ui.png[alt="Example Pipeline in the classic UI",width=100%] + *Note:* You can also select from canned *Scripted* Pipeline examples from the *try sample Pipeline* option at the top right of the *Script* text area. Be aware that there are no canned Declarative Pipeline examples available from this field. . Click *Save* to open the Pipeline project/item view page. . On this page, click *Build Now* on the left to run the Pipeline. + [.boxshadow] image:pipeline/classic-ui-left-column-on-item.png[alt="Classic UI left column on an item",width=35%] . Under *Build History* on the left, click *#1* to access the details for this particular Pipeline run. . Click *Console Output* to see the full output from the Pipeline run. The following output shows a successful run of your Pipeline. + [.boxshadow] image:pipeline/hello-world-console-output.png[alt="*Console Output* for the Pipeline",width=70%] + *Notes:*

- You can also access the console output directly from the Dashboard by clicking
- Defining a Pipeline through the classic UI is convenient for testing Pipeline
  the colored globe to the left of the build number (e.g. *#1*). code snippets, or for handling simple Pipelines or Pipelines that do not require source code to be checked out/cloned from a repository. As mentioned above, unlike `Jenkinsfiles` you define through Blue Ocean (above) or in source control (below), `Jenkinsfiles` entered into the *Script* text area area of Pipeline projects are stored by Jenkins itself, within the Jenkins home directory. Therefore, for greater control and flexibility over your Pipeline, particularly for projects in source control that are likely to gain complexity, it is recommended that you use Blue Ocean or source control to define your `Jenkinsfile`.

In SCM

// Despite :sectanchors:, explicitly defining an anchor because it will be // referenced from other documents [[defining-a-pipeline-in-scm]]

Complex Pipelines are difficult to write and maintain within the classic UI's *Script* text area of the Pipeline configuration page.

To make this easier, your Pipeline's `Jenkinsfile` can be written in a text editor or integrated development environment (IDE) and committed to source control footnoteref:[scm] (optionally with the application code that Jenkins will build). Jenkins can then check out your `Jenkinsfile` from source control as part of your Pipeline project's build process and then proceed to execute your Pipeline.

To configure your Pipeline project to use a `Jenkinsfile` from source control:

. Follow the procedure above for defining your Pipeline through the classic UI until you reach step 5 (accessing the *Pipeline* section on the Pipeline configuration page). . From the *Definition* field, choose the *Pipeline script from SCM* option. . From the *SCM* field, choose the type of source control system of the repository containing your `Jenkinsfile`. . Complete the fields specific to your repository's source control system. + *Tip:* If you are uncertain of what value to specify for a given field, click its *?* icon to the right for more information. . In the *Script Path* field, specify the location (and name) of your `Jenkinsfile`. This location is the one that Jenkins checks out/clones the repository containing your `Jenkinsfile`, which should match that of the repository's file structure. The default value of this field assumes that your `Jenkinsfile` is named "Jenkinsfile" and is located at the root of the repository.

When you update the designated repository, a new build is triggered, as long as the Pipeline is configured with an SCM polling trigger.

[TIP] ==== Since Pipeline code (i.e. Scripted Pipeline in particular) is written in Groovy-like syntax, if your IDE is not correctly syntax highlighting your `Jenkinsfile`, try inserting the line `#!/usr/bin/env groovy` at the top of the `Jenkinsfile`, footnoteref:[shebang,Shebang (general definition)[46]] footnoteref:[groovy_shebang,link:http://groovy-lang.org/syntax.html#*shebang*line[Shebang line (Groovy syntax)]] which may rectify the issue. ====

Built-in Documentation

Pipeline ships with built-in documentation features to make it easier to create Pipelines of varying complexities. This built-in documentation is automatically generated and updated based on the plugins installed in the Jenkins instance.

The built-in documentation can be found globally at: localhost:8080/pipeline-syntax/[47], assuming you have a Jenkins instance running on localhost port 8080. The same documentation is also linked as *Pipeline Syntax* in the side-bar for any configured Pipeline project.

[.boxshadow] image:pipeline/classic-ui-left-column-on-item.png[alt="Classic UI left column on an item",width=35%]

Snippet Generator

[[snippet-generator]]

The built-in "Snippet Generator" utility is helpful for creating bits of code for individual steps, discovering new steps provided by plugins, or experimenting with different parameters for a particular step.

The Snippet Generator is dynamically populated with a list of the steps available to the Jenkins instance. The number of steps available is dependent on the plugins installed which explicitly expose steps for use in Pipeline.

To generate a step snippet with the Snippet Generator:

[46] https://en.wikipedia.org/wiki/Shebang_(Unix)
[47] http://localhost:8080/pipeline-syntax/

. Navigate to the *Pipeline Syntax* link (referenced above) from a configured Pipeline, or at localhost:8080/pipeline-syntax[48]. . Select the desired step in the *Sample Step* dropdown menu . Use the dynamically populated area below the *Sample Step* dropdown to configure the selected step. . Click *Generate Pipeline Script* to create a snippet of Pipeline which can be copied and pasted into a Pipeline.

[.boxshadow] image:pipeline/snippet-generator.png[alt="Snippet Generator",width=100%]

To access additional information and/or documentation about the step selected, click on the help icon (indicated by the red arrow in the image above).

Global Variable Reference

In addition to the Snippet Generator, which only surfaces steps, Pipeline also provides a built-in "*Global Variable Reference*." Like the Snippet Generator, it is also dynamically populated by plugins. Unlike the Snippet Generator however, the Global Variable Reference only contains documentation for *variables* provided by Pipeline or plugins, which are available for Pipelines.

The variables provided by default in Pipeline are:

env::

Environment variables accessible from Scripted Pipeline, for example: `env.PATH` or `env.BUILD_ID`. Consult the built-in Global Variable Reference[49] for a complete, and up to date, list of environment variables available in Pipeline.

params::

Exposes all parameters defined for the Pipeline as a read-only Map[50], for example: `params.MY*PARAM*NAME`.

currentBuild::

May be used to discover information about the currently executing Pipeline, with properties such as `currentBuild.result`, `currentBuild.displayName`, etc. Consult the built-in Global Variable Reference[51] for a complete, and up to date, list of properties available on `currentBuild`.

Declarative Directive Generator

[[directive-generator]]

While the Snippet Generator helps with generating steps for a Scripted Pipeline or for the `steps` block in a `stage` in a Declarative Pipeline, it does not cover the sections and directives used to define a Declarative Pipeline. The "Declarative Directive Generator" utility helps with that. Similar to the <<snippet-generator>>, the Directive Generator allows you to choose a Declarative directive,

[48] http://localhost:8080/pipeline-syntax
[49] http://localhost:8080/pipeline-syntax/globals#env
[50] http://groovy-lang.org/syntax.html#_maps
[51] http://localhost:8080/pipeline-syntax/globals#currentBuild

configure it in a form, and generate the configuration for that directive, which you can then use in your Declarative Pipeline.

To generate a Declarative directive using the Declarative Directive Generator:

. Navigate to the *Pipeline Syntax* link (referenced above) from a configured Pipeline, and then click on the *Declarative Directive Generator* link in the sidepanel, or go directly to localhost:8080/directive-generator[52]. . Select the desired directive in the dropdown menu . Use the dynamically populated area below the dropdown to configure the selected directive. . Click *Generate Directive* to create the directive's configuration to copy into your Pipeline.

The Directive Generator can generate configuration for nested directives, such as conditions inside a `when` directive, but it cannot generate Pipeline steps. For the contents of directives which contain steps, such as `steps` inside a `stage` or conditions like `always` or `failure` inside `post`, the Directive Generator adds a placeholder comment instead. You will still need to add steps to your Pipeline by hand.

[pipeline] —- // Declarative // stage('Stage 1') // Script // —-

Further Reading

This section merely scratches the surface of what can be done with Jenkins Pipeline, but should provide enough of a foundation for you to start experimenting with a test Jenkins instance.

In the next section, The Jenkinsfile, more Pipeline steps will be discussed along with patterns for implementing successful, real-world, Jenkins Pipelines.

Additional Resources

*

Pipeline Steps Reference,
*

Pipeline Examples, a
 encompassing all steps provided by plugins distributed in the Jenkins Update Center. community-curated collection of copyable Pipeline examples.

[52]http://localhost:8080/directive-generator

Using Docker with Pipeline

Many organizations use Docker[53] to unify their build and test environments across machines, and to provide an efficient mechanism for deploying applications. Starting with Pipeline versions 2.5 and higher, Pipeline has built-in support for interacting with Docker from within a `Jenkinsfile`.

While this section will cover the basics of utilizing Docker from with a `Jenkinsfile`, it will not cover the fundamentals of Docker, which can be read about in the Docker Getting Started Guide[54].

Customizing the execution environment

[[execution-environment]]

Pipeline is designed to easily use Docker[55] images as the execution environment for a single Stage or the entire Pipeline. Meaning that a user can define the tools required for their Pipeline, without having to manually configure agents. Practically any tool which can be packaged in a Docker container[56]. can be used with ease by making only minor edits to a `Jenkinsfile`.

[pipeline] —- // Declarative // pipeline —-

When the Pipeline executes, Jenkins will automatically start the specified container and execute the defined steps within it:

```
[Pipeline] stage
[Pipeline] { (Test)
[Pipeline] sh
[guided-tour] Running shell script
+ node --version
v7.4.0
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
```

Caching data for containers

Many build tools will download external dependencies and cache them locally for future re-use. Since containers are initially created with “clean” file systems, this can result in slower Pipelines, as they may not take advantage of on-disk caches between subsequent Pipeline runs.

[53]https://www.docker.com
[54]https://docs.docker.com/get-started/
[55]https://docs.docker.com/
[56]https://hub.docker.com

Pipeline supports adding custom arguments which are passed to Docker, allowing users to specify custom Docker Volumes[57] to mount, which can be used for caching data on the agent between Pipeline runs. The following example will cache `~/.m2` between Pipeline runs utilizing the `maven` container[58], thereby avoiding the need to re-download dependencies for subsequent runs of the Pipeline.

[pipeline] —- // Declarative // pipeline —-

Using multiple containers

It has become increasingly common for code bases to rely on multiple, different, technologies. For example, a repository might have both a Java-based back-end API implementation *and* a JavaScript-based front-end implementation. Combining Docker and Pipeline allows a `Jenkinsfile` to use *multiple* types of technologies by combining the `agent {}` directive, with different stages.

[pipeline] —- // Declarative // pipeline // Script // node { /* Requires the Docker Pipeline plugin to be installed */

stage('Back-end')

stage('Front-end') —-

Using a Dockerfile

[[dockerfile]]

For projects which require a more customized execution environment, Pipeline also supports building and running a container from a `Dockerfile` in the source repository. In contrast to the previous approach of using an "off-the-shelf" container, using the `agent { dockerfile true }` syntax will build a new image from a `Dockerfile` rather than pulling one from Docker Hub[59].

Re-using an example from above, with a more custom `Dockerfile`:

```
FROM node:7-alpine

RUN apk add -U subversion
```

.Dockerfile

By committing this to the root of the source repository, the `Jenkinsfile` can be changed to build a container based on this `Dockerfile` and then run the defined steps using that container:

[57]https://docs.docker.com/engine/tutorials/dockervolumes/
[58]https://hub.docker.com/_/maven/
[59]https://hub.docker.com

[pipeline] —- // Declarative // pipeline // Script // —-

The `agent { dockerfile true }` syntax supports a number of other options which are described in more detail in the Pipeline Syntax section.

.Using a Dockerfile with Jenkins Pipeline video::Pi2kJ2RJS50[youtube, width=852, height=480]

Specifying a Docker Label

By default, Pipeline assumes that *any* configured agent is capable of running Docker-based Pipelines. For Jenkins environments which have macOS, Windows, or other agents, which are unable to run the Docker daemon, this default setting may be problematic. Pipeline provides a global option in the **Manage Jenkins** page, and on the Folder level, for specifying which agents (by Label) to use for running Docker-based Pipelines.

image::pipeline/configure-docker-label.png[Configuring the Pipeline Docker Label]

Advanced Usage with Scripted Pipeline

Running "sidecar" containers

Using Docker in Pipeline can be an effective way to run a service on which the build, or a set of tests, may rely. Similar to the sidecar pattern[60], Docker Pipeline can run one container "in the background", while performing work in another. Utilizing this sidecar approach, a Pipeline can have a "clean" container provisioned for each Pipeline run.

Consider a hypothetical integration test suite which relies on a local MySQL database to be running. Using the `withRun` method, implemented in the plugin:docker-workflow[Docker Pipeline] plugin's support for Scripted Pipeline, a `Jenkinsfile` can run MySQL as a sidecar:

```
node {
    checkout scm
    /*
     * In order to communicate with the MySQL server, this Pipeline explicitly
     * maps the port (`3306`) to a known port on the host machine.
     */
    docker.image('mysql:5').withRun('-e "MYSQL_ROOT_PASSWORD=my-secret-pw" -p 3306:3\
306') { c ->
        /* Wait until mysql service is up */
        sh 'while ! mysqladmin ping -h0.0.0.0 --silent; do sleep 1; done'
        /* Run some tests which require MySQL */
        sh 'make check'
```

[60]https://docs.microsoft.com/en-us/azure/architecture/patterns/sidecar

```
    }
}
```

This example can be taken further, utilizing two containers simultaneously. One "sidecar" running MySQL, and another providing the execution environment, by using the Docker container links[61].

```
node {
    checkout scm
    docker.image('mysql:5').withRun('-e "MYSQL_ROOT_PASSWORD=my-secret-pw"') { c ->
        docker.image('mysql:5').inside("--link ${c.id}:db") {
            /* Wait until mysql service is up */
            sh 'while ! mysqladmin ping -hdb --silent; do sleep 1; done'
        }
        docker.image('centos:7').inside("--link ${c.id}:db") {
            /*
             * Run some tests which require MySQL, and assume that it is
             * available on the host name `db`
             */
            sh 'make check'
        }
    }
}
```

The above example uses the object exposed by `withRun`, which has the running container's ID available via the `id` property. Using the container's ID, the Pipeline can create a link by passing custom Docker arguments to the `inside()` method.

The `id` property can also be useful for inspecting logs from a running Docker container before the Pipeline exits:

```
sh "docker logs ${c.id}"
```

Building containers

In order to create a Docker image, the plugin:docker-workflow[Docker Pipeline] plugin also provides a `build()` method for creating a new image, from a `Dockerfile` in the repository, during a Pipeline run.

One major benefit of using the syntax `docker.build("my-image-name")` is that a Scripted Pipeline can use the return value for subsequent Docker Pipeline calls, for example:

[61]https://docs.docker.com/engine/userguide/networking/default_network/dockerlinks/

```
node {
    checkout scm

    def customImage = docker.build("my-image:${env.BUILD_ID}")

    customImage.inside {
        sh 'make test'
    }
}
```

The return value can also be used to publish the Docker image to Docker Hub[62], or a custom Registry, via the `push()` method, for example:

```
node {
    checkout scm
    def customImage = docker.build("my-image:${env.BUILD_ID}")
    customImage.push()
}
```

One common usage of image "tags" is to specify a `latest` tag for the most recently, validated, version of a Docker image. The `push()` method accepts an optional `tag` parameter, allowing the Pipeline to push the `customImage` with different tags, for example:

```
node {
    checkout scm
    def customImage = docker.build("my-image:${env.BUILD_ID}")
    customImage.push()

    customImage.push('latest')
}
```

The `build()` method builds the `Dockerfile` in the current directory by default. This can be overridden by providing a directory path containing a `Dockerfile` as the second argument of the `build()` method, for example:

[62]https://hub.docker.com

```
node {
    checkout scm
    def testImage = docker.build("test-image", "./dockerfiles/test") // <1>

    testImage.inside {
        sh 'make test'
    }
}
```

<1> Builds `test-image` from the Dockerfile found at `./dockerfiles/test/Dockerfile`.

It is possible to pass other arguments to docker build[63] by adding them to the second argument of the `build()` method. When passing arguments this way, the last value in the that string must be the path to the docker file.

This example overrides the default `Dockerfile` by passing the `-f` flag:

```
node {
    checkout scm
    def dockerfile = 'Dockerfile.test'
    def customImage = docker.build("my-image:${env.BUILD_ID}", "-f ${dockerfile} ./d\
ockerfiles") // <1>
}
```

<1> Builds `my-image:${env.BUILD_ID}` from the Dockerfile found at `./dockerfiles/Dockerfile.test`.

Using a remote Docker server

By default, the plugin:docker-workflow[Docker Pipeline] plugin will communicate with a local Docker daemon, typically accessed through `/var/run/docker.sock`.

To select a non-default Docker server, such as with Docker Swarm[64], the `withServer()` method should be used.

By passing a URI, and optionally the Credentials ID of a **Docker Server Certificate Authentication** pre-configured in Jenkins, to the method with:

[63] https://docs.docker.com/engine/reference/commandline/build/
[64] https://docs.docker.com/swarm/

```
node {
    checkout scm

    docker.withServer('tcp://swarm.example.com:2376', 'swarm-certs') {
        docker.image('mysql:5').withRun('-p 3306:3306') {
            /* do things */
        }
    }
}
```

```
cannot create /…@tmp/durable-…/pid: Directory nonexistent
```

```
`inside()` and `build()` will not work properly with a Docker Swarm server out
of the box

For `inside()` to work, the Docker server and the Jenkins agent must use the
same filesystem, so that the workspace can be mounted.

Currently neither the Jenkins plugin nor the Docker CLI will automatically
detect the case that the server is running remotely; a typical symptom would be
errors from nested `sh` commands such as


When Jenkins detects that the agent is itself running inside a Docker
container, it will automatically pass the `--volumes-from` argument to the
`inside` container, ensuring that it can share a workspace with the agent.

Additionally some versions of Docker Swarm do not support custom Registries.
```

Using a custom registry

[[custom-registry]]

By default the plugin:docker-workflow[Docker Pipeline] integrates assumes the default Docker Registry of Docker Hub[65].

In order to use a custom Docker Registry, users of Scripted Pipeline can wrap steps with the `withRegistry()` method, passing in the custom Registry URL, for example:

[65] https://hub.docker.com

```
node {
    checkout scm

    docker.withRegistry('https://registry.example.com') {

        docker.image('my-custom-image').inside {
            sh 'make test'
        }
    }
}
```

For a Docker Registry which requires authentication, add a “Username/Password” Credentials item from the Jenkins home page and use the Credentials ID as a second argument to `withRegistry()`:

```
node {
    checkout scm

    docker.withRegistry('https://registry.example.com', 'credentials-id') {

        def customImage = docker.build("my-image:${env.BUILD_ID}")

        /* Push the container to the custom Registry */
        customImage.push()
    }
}
```

Using a Jenkinsfile

This section builds on the information covered in Getting started with Pipeline and introduces more useful steps, common patterns, and demonstrates some non-trivial `Jenkinsfile` examples.

Creating a `Jenkinsfile`, which is checked into source control footnoteref:[scm, https://en.wikipedia.org/wiki/Source
provides a number of immediate benefits:

- Code review/iteration on the Pipeline
- Audit trail for the Pipeline
- Single source of truth footnote:[https://en.wikipedia.org/wiki/Single_Source*of*Truth] for the Pipeline, which can be viewed and edited by multiple members of the project.

Pipeline supports two syntaxes, Declarative (introduced in Pipeline 2.5) and Scripted Pipeline. Both of which support building continuous delivery pipelines. Both may be used to define a Pipeline in either the web UI or with a `Jenkinsfile`, though it's generally considered a best practice to create a `Jenkinsfile` and check the file into the source control repository.

Creating a Jenkinsfile

As discussed in the Defining a Pipeline in SCM, a `Jenkinsfile` is a text file that contains the definition of a Jenkins Pipeline and is checked into source control. Consider the following Pipeline which implements a basic three-stage continuous delivery pipeline.

[pipeline] —- // Declarative // pipeline { agent any

stages —-

Not all Pipelines will have these same three stages, but it is a good starting point to define them for most projects. The sections below will demonstrate the creation and execution of a simple Pipeline in a test installation of Jenkins.

```
It is assumed that there is already a source control repository set up for
the project and a Pipeline has been defined in Jenkins following
<<getting-started#defining-a-pipeline-in-scm, these instructions>>.
```

Using a text editor, ideally one which supports Groovy[66] syntax highlighting, create a new `Jenkinsfile` in the root directory of the project.

[role=declarative-pipeline] The Declarative Pipeline example above contains the minimum necessary structure to implement a continuous delivery pipeline. The agent directive, which is required, instructs Jenkins to allocate an executor and workspace for the Pipeline. Without an `agent` directive, not only is the Declarative Pipeline not valid, it would not be capable of doing any work! By default the `agent` directive ensures that the source repository is checked out and made available for steps in the subsequent stages‘

The stages directive, and steps directives are also required for a valid Declarative Pipeline as they instruct Jenkins what to execute and in which stage it should be executed.

[role=scripted-pipeline] ==== For more advanced usage with Scripted Pipeline, the example above `node` is a crucial first step as it allocates an executor and workspace for the Pipeline. In essence, without `node`, a Pipeline cannot do any work! From within `node`, the first order of business will be to checkout the source code for this project. Since the `Jenkinsfile` is being pulled directly from source control, Pipeline provides a quick and easy way to access the right revision of the source code

[pipeline] —- // Script // node // Declarative not yet implemented // —- <1> The `checkout` step will checkout code from source control; `scm` is a special variable which instructs the `checkout` step to clone the specific revision which triggered this Pipeline run. ====

Build

For many projects the beginning of "work" in the Pipeline would be the "build" stage. Typically this stage of the Pipeline will be where source code is assembled, compiled, or packaged. The `Jenkinsfile` is *not* a replacement for an existing build tool such as GNU/Make, Maven, Gradle, etc, but rather can be viewed as a glue layer to bind the multiple phases of a project's development lifecycle (build, test, deploy, etc) together.

Jenkins has a number of plugins for invoking practically any build tool in general use, but this example will simply invoke `make` from a shell step (`sh`). The `sh` step assumes the system is Unix/Linux-based, for Windows-based systems the `bat` could be used instead.

[pipeline] —- // Declarative // pipeline { agent any

stages —- <1> The `sh` step invokes the `make` command and will only continue if a zero exit code is returned by the command. Any non-zero exit code will fail the Pipeline. <2> `archiveArtifacts` captures the files built matching the include pattern (`+**/target/*.jar+`) and saves them to the Jenkins master for later retrieval.

[TIP] ==== Archiving artifacts is not a substitute for using external artifact repositories such as Artifactory or Nexus and should be considered only for basic reporting and file archival. ====

[66] http://groovy-lang.org

Test

Running automated tests is a crucial component of any successful continuous delivery process. As such, Jenkins has a number of test recording, reporting, and visualization facilities provided by a number of plugins[67]. At a fundamental level, when there are test failures, it is useful to have Jenkins record the failures for reporting and visualization in the web UI. The example below uses the `junit` step, provided by the plugin:junit[JUnit plugin].

In the example below, if tests fail, the Pipeline is marked "unstable", as denoted by a yellow ball in the web UI. Based on the recorded test reports, Jenkins can also provide historical trend analysis and visualization.

[pipeline] —- // Declarative // pipeline { agent any

stages —- <1> Using an inline shell conditional (`sh 'make check || true'`) ensures that the `sh` step always sees a zero exit code, giving the `junit` step the opportunity to capture and process the test reports. Alternative approaches to this are covered in more detail in the <<handling-failure>> section below. <2> `junit` captures and associates the JUnit XML files matching the inclusion pattern (`+**/target/*.xml+`).

Deploy

Deployment can imply a variety of steps, depending on the project or organization requirements, and may be anything from publishing built artifacts to an Artifactory server, to pushing code to a production system.

At this stage of the example Pipeline, both the "Build" and "Test" stages have successfully executed. In essence, the "Deploy" stage will only execute assuming previous stages completed successfully, otherwise the Pipeline would have exited early.

[pipeline] —- // Declarative // pipeline { agent any

stages —- <1> Accessing the `currentBuild.result` variable allows the Pipeline to determine if there were any test failures. In which case, the value would be `UNSTABLE`.

Assuming everything has executed successfully in the example Jenkins Pipeline, each successful Pipeline run will have associated build artifacts archived, test results reported upon and the full console output all in Jenkins.

[role=scripted-pipeline] A Scripted Pipeline can include conditional tests (shown above), loops, try/catch/finally blocks and even functions. The next section will cover this advanced Scripted Pipeline syntax in more detail.

[67]https://plugins.jenkins.io/?labels=report

Working with your Jenkinsfile

The following sections provide details about handling:

- specific Pipeline syntax in your `Jenkinsfile` and
- features and functionality of Pipeline syntax which are essential in building your application or Pipeline project.

String interpolation

Jenkins Pipeline uses rules identical to Groovy[68] for string interpolation. Groovy's String interpolation support can be confusing to many newcomers to the language. While Groovy supports declaring a string with either single quotes, or double quotes, for example:

```
def singlyQuoted = 'Hello'
def doublyQuoted = "World"
```

Only the latter string will support the dollar-sign ($) based string interpolation, for example:

```
def username = 'Jenkins'
echo 'Hello Mr. ${username}'
echo "I said, Hello Mr. ${username}"
```

Would result in:

```
Hello Mr. ${username}
I said, Hello Mr. Jenkins
```

Understanding how to use string interpolation is vital for using some of Pipeline's more advanced features.

Using environment variables

Jenkins Pipeline exposes environment variables via the global variable `env`, which is available from anywhere within a `Jenkinsfile`. The full list of environment variables accessible from within Jenkins Pipeline is documented at localhost:8080/pipeline-syntax/globals#env[69], assuming a Jenkins master is running on `localhost:8080`, and includes:

[68] http://groovy-lang.org
[69] http://localhost:8080/pipeline-syntax/globals#env

BUILD_ID:: The current build ID, identical to BUILD_NUMBER for builds created in Jenkins versions 1.597+ JOB_NAME:: Name of the project of this build, such as “foo” or “foo/bar”. JENKINS_URL:: Full URL of Jenkins, such as https://example.com:port/jenkins/ (NOTE: only available if Jenkins URL set in “System Configuration”)

Referencing or using these environment variables can be accomplished like accessing any key in a Groovy Map[70], for example:

[pipeline] —- // Declarative // pipeline —-

Setting environment variables

Setting an environment variable within a Jenkins Pipeline is accomplished differently depending on whether Declarative or Scripted Pipeline is used.

Declarative Pipeline supports an environment directive, whereas users of Scripted Pipeline must use the `withEnv` step.

[pipeline] —- // Declarative // pipeline —- <1> An `environment` directive used in the top-level `pipeline` block will apply to all steps within the Pipeline. <2> An `environment` directive defined within a `stage` will only apply the given environment variables to steps within the `stage`.

Setting environment variables dynamically

In the case where environment variable need to be set dynamically at run time this can be done with the use of a shell scripts (`sh`), Windows Batch Script (`bat`) or PowerShell Script (`powershell`). Each script can either `returnStatus` or `returnStdout`. More information on scripts[71].

Below is an example in a declarative pipeline using `sh` (shell) with both `returnStatus` and `returnStdout`.

[pipeline] —- // Declarative // pipeline // Script // —- <1> An `agent` must be set at the top level of the pipeline. This will fail if agent is set as `agent none`. <2> When using `returnStdout` a trailing whitespace will be append to the returned string. Use `.trim()` to remove this.

Handling credentials

Credentials configured in Jenkins can be handled in Pipelines for immediate use. Read more about using credentials in Jenkins on the Using credentials page.

For secret text, usernames and passwords, and secret files

Jenkins’ declarative Pipeline syntax has the `credentials()` helper method (used within the `environment` directive) which supports secret text, username and password, as well as secret file credentials. If you want to handle other types of credentials, refer to the For other credential types section (below).

[70]http://groovy-lang.org/syntax.html#_maps
[71]https://jenkins.io/doc/pipeline/steps/workflow-durable-task-step

Secret text

The following Pipeline code shows an example of how to create a Pipeline using environment variables for secret text credentials.

In this example, two secret text credentials are assigned to separate environment variables to access Amazon Web Services (AWS). These credentials would have been configured in Jenkins with their respective credential IDs + `jenkins-aws-secret-key-id` and `jenkins-aws-secret-access-key`.

[pipeline] —- // Declarative // pipeline // Script // —- <1> You can reference the two credential environment variables (defined in this Pipeline's `environment` directive), within this stage's steps using the syntax `$AWS_ACCESS*KEY*ID` and `$AWS_SECRET*ACCESS*KEY`. For example, here you can authenticate to AWS using the secret text credentials assigned to these credential variables. + To maintain the security and anonymity of these credentials, if you attempt to retrieve the value of these credential variables from within the Pipeline (e.g. `echo $AWS_SECRET*ACCESS*KEY`), Jenkins only returns the value "+*****+" to prevent secret information from being written to the console output and any logs. Any sensitive information in credential IDs themselves (such as usernames) are also returned as "+*****+" in the Pipeline run's output. <2> In this Pipeline example, the credentials assigned to the two `AWS_...` environment variables are scoped globally for the entire Pipeline, so these credential variables could also be used in this stage's steps. If, however, the `environment` directive in this Pipeline were moved to a specific stage (as is the case in the Usernames and passwords Pipeline example below), then these `AWS_...` environment variables would only be scoped to the steps in that stage.

Usernames and passwords

The following Pipeline code snippets show an example of how to create a Pipeline using environment variables for username and password credentials.

In this example, username and password credentials are assigned to environment variables to access a Bitbucket repository in a common account or team for your organization; these credentials would have been configured in Jenkins with the credential ID `jenkins-bitbucket-common-creds`.

When setting the credential environment variable in the `environment` directive:

```
environment {
    BITBUCKET_COMMON_CREDS = credentials('jenkins-bitbucket-common-creds')
}
```

this actually sets the following three environment variables:

- 'BITBUCKET

*COMMON*CREDS' - contains a username and a password separated by a

- ‘BITBUCKET_COMMON

*CREDS*USR‘ - an additional variable containing the username

- ‘BITBUCKET_COMMON

*CREDS*PSW `- an additional variable containing the password colon in the format` username:password‘. component only. component only.

```
By convention, variable names for environment variables are typically specified
in capital case, with individual words separated by underscores. You can,
however, specify any legitimate variable name using lower case characters. Bear
in mind that the additional environment variables created by the `credentials()`
method (above) will always be appended with `_USR` and `_PSW` (i.e. in the
format of an underscore followed by three capital letters).
```

The following code snippet shows the example Pipeline in its entirety:

- ‘$BITBUCKET

*COMMON*CREDS‘

- ‘$BITBUCKET_COMMON

*CREDS*USR‘

- ‘$BITBUCKET_COMMON

*CREDS*PSW `[pipeline] ---- // Declarative // pipeline { agent { // Define agent details here } stages { stage('Example stage 1') { environment { BITBUCKET*COMMON*CREDS = credentials('jenkins-bitbucket-common-creds') } steps { // // <1> } } stage('Example stage 2') { steps { // // <2> } } } } // Script // ---- <1> The following credential environment variables (defined in this Pipeline's` [environment‘](#syntax#environment) directive) are available within this stage’s steps and can be referenced using the syntax:

+ For example, here you can authenticate to Bitbucket with the username and password assigned to these credential variables. + To maintain the security and anonymity of these credentials, if you attempt to retrieve the value of these credential variables from within the Pipeline, the same behavior described in the Secret text example above applies to these username and password credential variable types too. <2> In this Pipeline example, the credentials assigned to the three `COMMON*BITBUCKET*CREDS...` environment variables are scoped only to `Example stage 1`, so these credential variables are not available for use in this `Example stage 2` stage’s steps. If, however, the `environment` directive in this Pipeline were moved immediately within the `pipeline` block (as is the case in the Secret text Pipeline example above), then these `COMMON*BITBUCKET*CREDS...` environment variables would be scoped globally and could be used in any stage’s steps.

Secret files

As far as Pipelines are concerned, secret files are handled in exactly the same manner as secret text (above).

Essentially, the only difference between secret text and secret file credentials are that for secret text, the credential itself is entered directly into Jenkins whereas for a secret file, the credential is originally stored in a file which is then uploaded to Jenkins.

Unlike secret text, secret files cater for credentials that are:

- too unwieldy to enter directly into Jenkins, and/or
- in binary format, such as a GPG file.

For other credential types

If you need to set credentials in a Pipeline for anything other than secret text, usernames and passwords, or secret files (above) - i.e SSH keys or certificates, then use Jenkins' *Snippet Generator* feature, which you can access through Jenkins' classic UI.

To access the *Snippet Generator* for your Pipeline project/item:

. From the Jenkins home page (i.e. the Dashboard of Jenkins' classic UI), click the name of your Pipeline project/item. . On the left, click *Pipeline Syntax* and ensure that the *Snippet Generator* link is in bold at the top-left. (If not, click its link.) . From the *Sample Step* field, choose *withCredentials: Bind credentials to variables*. . Under *Bindings*, click *Add* and choose from the dropdown: * *SSH User Private Key* - to handle SSH public/private key pair credentials[72], from which you can specify: ** *Key File Variable* - the name of the environment variable that will be bound to these credentials. Jenkins actually assigns this temporary variable to the secure location of the private key file required in the SSH public/private key pair authentication process. ** *Passphrase Variable* (*Optional*) - the name of the environment variable that will be bound to the passphrase[73] associated with the SSH public/private key pair. ** *Username Variable* (*Optional*) - the name of the environment variable that will be bound to username associated with the SSH public/private key pair. ** *Credentials* - choose the SSH public/private key credentials stored in Jenkins. The value of this field is the credential ID, which Jenkins writes out to the generated snippet. * *Certificate* - to handle PKCS#12 certificates[74], from which you can specify: ** *Keystore Variable* - the name of the environment variable that will be bound to these credentials. Jenkins actually assigns this temporary variable to the secure location of the certificate's keystore required in the certificate authentication process. ** *Password Variable* (*Optional*) - the name of the environment variable that will be bound to the password associated with the certificate. ** *Alias Variable* (*Optional*) - the name of the environment variable that will be bound to the unique alias associated with the certificate. ** *Credentials* - choose the certificate credentials stored in Jenkins. The value of this field is the credential ID, which Jenkins writes out to the generated snippet. * *Docker client certificate* - to handle Docker Host Certificate

[72]http://www.snailbook.com/protocols.html
[73]https://tools.ietf.org/html/rfc4251#section-9.4.4
[74]https://tools.ietf.org/html/rfc7292

Authentication. . Click *Generate Pipeline Script* and Jenkins generates a `withCredentials( ... ) { ... }` Pipeline step snippet for the credentials you specified, which you can then copy and paste into your Declarative or Scripted Pipeline code. + *Notes:* * The *Credentials* fields (above) show the names of credentials configured in Jenkins. However, these values are converted to credential IDs after clicking *Generate Pipeline Script.* [[withcredentials-script-examples]] * To combine more than one credential in a single `withCredentials( ... ) { ... }` Pipeline step, see Combining credentials in one step (below) for details.

SSH User Private Key example

```
withCredentials(bindings: [sshUserPrivateKey(credentialsId: 'jenkins-ssh-key-for-abc\
', \
                                             keyFileVariable: 'SSH_KEY_FOR_ABC', \
                                             passphraseVariable: '', \
                                             usernameVariable: '')]) {
  // some block
}
```

The optional `passphraseVariable` and `usernameVariable` definitions can be deleted in your final Pipeline code.

Certificate example

```
withCredentials(bindings: [certificate(aliasVariable: '', \
                                       credentialsId: 'jenkins-certificate-for-xyz',\
 \
                                       keystoreVariable: 'CERTIFICATE_FOR_XYZ', \
                                       passwordVariable: 'XYZ-CERTIFICATE-PASSWORD')\
]) {
  // some block
}
```

The optional `aliasVariable` and `passwordVariable` variable definitions can be deleted in your final Pipeline code.

The following code snippet shows an example Pipeline in its entirety, which implements the *SSH User Private Key* and *Certificate* snippets above:

[pipeline] —- // Declarative // pipeline `steps, so these credential variables are not available for use in this` Example stage 2‘ stage's steps.

To maintain the security and anonymity of these credentials, if you attempt to retrieve the value of these credential variables from within these `withCredentials( ... ) { ... }` steps, the same behavior described in the Secret text example (above) applies to these SSH public/private key pair credential and certificate variable types too.

```
* When using the *Sample Step* field's *withCredentials: Bind credentials to
variables* option in the *Snippet Generator*, only credentials which your
current Pipeline project/item has access to can be selected from any
*Credentials* field's list. While you can manually write a
`withCredentials( ... ) { ... }` step for your Pipeline (like the examples
<<#withcredentials-script-examples,above>>), using the *Snippet Generator* is
recommended to avoid specifying credentials that are out of scope for this
Pipeline project/item, which when run, will make the step fail.
* You can also use the *Snippet Generator* to generate `withCredentials( ... )
{ ... }` steps to handle secret text, usernames and passwords and secret files.
However, if you only need to handle these types of credentials, it is
recommended you use the relevant procedure described in the section
<<#for-secret-text-usernames-and-passwords-and-secret-files,above>> for improved
Pipeline code readability.
* The use of **single-quotes** instead of  **double-quotes** to define the `script`
(the implicit parameter to `sh`) in Groovy above.
The single-quotes will cause the secret to be expanded by the shell as an environmen\
t variable.
The double-quotes are potentially less secure as the secret is interpolated by Groov\
y,
and so typical operating system process listings (as well as Blue Ocean,
and the pipeline steps tree in the classic UI) will accidentally disclose it :
```

node {
  withCredentials([string(credentialsId: 'mytoken', variable: 'TOKEN')]) {

sh /* WRONG! / """ *set +x*
    curl -H 'Token: $TOKEN' https://some.api/
  """ *sh* / CORRECT */ ''' set +x
    curl -H 'Token: $TOKEN' https://some.api/
  ''' }
}

```

```

Combining credentials in one step

Using the *Snippet Generator*, you can make multiple credentials available within a single `withCredentials( ... ) { ... }` step by doing the following:

. From the Jenkins home page (i.e. the Dashboard of Jenkins' classic UI), click the name of your Pipeline project/item. . On the left, click *Pipeline Syntax* and ensure that the *Snippet Generator* link is in bold at the top-left. (If not, click its link.) . From the *Sample Step* field, choose *withCredentials: Bind credentials to variables.* . Click *Add* under *Bindings.* . Choose the credential type to add to the `withCredentials( ... ) { ... }` step from the dropdown list. . Specify the credential *Bindings* details. Read more above these in the procedure under For other credential types (above). . Repeat from "Click *Add* …" (above) for each (set of) credential/s to add to the `withCredentials( ... ) { ... }` step. . Click *Generate Pipeline Script* to generate the final `withCredentials( ... ) { ... }` step snippet.

Handling parameters

Declarative Pipeline supports parameters out-of-the-box, allowing the Pipeline to accept user-specified parameters at runtime via the parameters directive. Configuring parameters with Scripted Pipeline is done with the `properties` step, which can be found in the Snippet Generator.

If you configured your pipeline to accept parameters using the *Build with Parameters* option, those parameters are accessible as members of the `params` variable.

Assuming that a String parameter named "Greeting" has been configuring in the `Jenkinsfile`, it can access that parameter via `${params.Greeting}`:

[pipeline] —- // Declarative // pipeline // Script // properties([parameters([string(defaultValue: 'Hello', description: 'How should I greet the world?', name: 'Greeting')])])

node —-

Handling failure

Declarative Pipeline supports robust failure handling by default via its post section which allows declaring a number of different "post conditions" such as: `always`, `unstable`, `success`, `failure`, and `changed`. The Pipeline Syntax section provides more detail on how to use the various post conditions.

[pipeline] —- // Declarative // pipeline —-

[role=scripted-pipeline] ==== Scripted Pipeline however relies on Groovy's built-in `try`/`catch`/`finally` semantics for handling failures during execution of the Pipeline.

In the <<test>> example above, the `sh` step was modified to never return a non-zero exit code (`sh 'make check || true'`). This approach, while valid, means the following stages need to check `currentBuild.result` to know if there has been a test failure or not.

An alternative way of handling this, which preserves the early-exit behavior of failures in Pipeline, while still giving `junit` the chance to capture test reports, is to use a series of `try`/`finally` blocks: ====

Using multiple agents

In all the previous examples, only a single agent has been used. This means Jenkins will allocate an executor wherever one is available, regardless of how it is labeled or configured. Not only can this behavior be overridden, but Pipeline allows utilizing multiple agents in the Jenkins environment from within the *same* `Jenkinsfile`, which can helpful for more advanced use-cases such as executing builds/tests across multiple platforms.

In the example below, the “Build” stage will be performed on one agent and the built results will be reused on two subsequent agents, labelled “linux” and “windows” respectively, during the “Test” stage.

[pipeline] —- // Declarative // pipeline

stage(‘Test’) —- <1> The `stash` step allows capturing files matching an inclusion pattern (`+**/target/*.jar+`) for reuse within the *same* Pipeline. Once the Pipeline has completed its execution, stashed files are deleted from the Jenkins master. <2> The parameter in `agent/node` allows for any valid Jenkins label expression. Consult the Pipeline Syntax section for more details. <3> `unstash` will retrieve the named “stash” from the Jenkins master into the Pipeline’s current workspace. <4> The `bat` script allows for executing batch scripts on Windows-based platforms.

Optional step arguments

Pipeline follows the Groovy language convention of allowing parentheses to be omitted around method arguments.

Many Pipeline steps also use the named-parameter syntax as a shorthand for creating a Map in Groovy, which uses the syntax `[key1: value1, key2: value2]`. Making statements like the following functionally equivalent:

```
git url: 'git://example.com/amazing-project.git', branch: 'master'
git([url: 'git://example.com/amazing-project.git', branch: 'master'])
```

For convenience, when calling steps taking only one parameter (or only one mandatory parameter), the parameter name may be omitted, for example:

```
sh 'echo hello' /* short form  */
sh([script: 'echo hello'])  /* long form */
```

Advanced Scripted Pipeline

Scripted Pipeline is a domain-specific language footnoteref:[dsl, https://en.wikipedia.org/wiki/Domain-specific_language] based on Groovy, most Groovy syntax[75] can be used in Scripted Pipeline without modification.

[75]http://groovy-lang.org/semantics.html

Parallel execution

The example in the section above runs tests across two different platforms in a linear series. In practice, if the `make check` execution takes 30 minutes to complete, the "Test" stage would now take 60 minutes to complete!

Fortunately, Pipeline has built-in functionality for executing portions of Scripted Pipeline in parallel, implemented in the aptly named `parallel` step.

Refactoring the example above to use the `parallel` step:

[pipeline] —- // Script // stage('Build')

stage('Test') // Declarative not yet implemented // —-

Instead of executing the tests on the "linux" and "windows" labelled nodes in series, they will now execute in parallel assuming the requisite capacity exists in the Jenkins environment.

Branches and Pull Requests

In the previous section a `Jenkinsfile` which could be checked into source control was implemented. This section covers the concept of *Multibranch* Pipelines which build on the `Jenkinsfile` foundation to provide more dynamic and automatic functionality in Jenkins.

Creating a Multibranch Pipeline

The *Multibranch Pipeline* project type enables you to implement different Jenkinsfiles for different branches of the same project. In a Multibranch Pipeline project, Jenkins automatically discovers, manages and executes Pipelines for branches which contain a `Jenkinsfile` in source control.

This eliminates the need for manual Pipeline creation and management.

To create a Multibranch Pipeline:

- Click *New Item* on Jenkins home page.

image::pipeline/classic-ui-left-column.png[alt="Classic UI left column",width=30%]

- Enter a name for your Pipeline, select *Multibranch Pipeline* and click *OK*.

```
Jenkins uses the name of the Pipeline to create directories on disk. Pipeline
names which include spaces may uncover bugs in scripts which do not expect
paths to contain spaces.
```

image::pipeline/new-item-multibranch-creation.png["Enter a name, select *Multibranch Pipeline*, and click *OK*", role=center]

- Add a *Branch Source* (for example, Git) and enter the location of the repository.

image::pipeline/multibranch-branch-source.png["Add a Branch Source", role=center] image::pipeline/multibranch-branch-source-configuration.png["Add the URL to the project repository", role=center]

- *Save* the Multibranch Pipeline project.

Upon *Save*, Jenkins automatically scans the designated repository and creates appropriate items for each branch in the repository which contains a `Jenkinsfile`.

By default, Jenkins will not automatically re-index the repository for branch additions or deletions (unless using an Organization Folder), so it is often useful to configure a Multibranch Pipeline to periodically re-index in the configuration:

image::pipeline/multibranch-branch-indexing.png[“Setting up branch re-indexing”, role=center]

Additional Environment Variables

Multibranch Pipelines expose additional information about the branch being built through the `env` global variable, such as:

BRANCH_NAME:: Name of the branch for which this Pipeline is executing, for example `master`.

CHANGE_ID:: An identifier corresponding to some kind of change request, such as a pull request number

Additional environment variables are listed in the Global Variable Reference.

Supporting Pull Requests

With the “GitHub” or “Bitbucket” Branch Sources, Multibranch Pipelines can be used for validating pull/change requests. This functionality is provided, respectively, by the plugin:github-branch-source[GitHub Branch Source] and plugin:cloudbees-bitbucket-branch-source[Bitbucket Branch Source] plugins. Please consult their documentation for further information on how to use those plugins.

Using Organization Folders

[[organization-folders]]

Organization Folders enable Jenkins to monitor an entire GitHub Organization, or Bitbucket Team/Project and automatically create new Multibranch Pipelines for repositories which contain branches and pull requests containing a `Jenkinsfile`.

Currently, this functionality exists only for GitHub and Bitbucket, with functionality provided by the plugin:github-organization-folder[GitHub Organization Folder] and plugin:cloudbees-bitbucket-branch-source[Bitbucket Branch Source] plugins.

Running a Pipeline

// TODO: WEBSITE-495 - flesh out placeholder sections.

Multibranch

See the Multibranch documentation for more information.

Parameters

See the Jenkinsfile documentation for more information

Restarting or Rerunning a Pipeline

There are a number of ways to rerun or restart a completed Pipeline.

Replay

See the Replay documentation for more information.

Restart from a Stage

You can restart any completed Declarative Pipeline from any top-level stage which ran in that Pipeline. This allows you to rerun a Pipeline from a stage which failed due to transient or environmental considerations, for example. All inputs to the Pipeline will be the same. This includes SCM information, build parameters, and the contents of any `stash` step calls in the original Pipeline, if specified.

How to Use

No additional configuration is needed in the Jenkinsfile to allow you to restart stages in your Declarative Pipelines. This is an inherent part of Declarative Pipelines and is available automatically.

Restarting from the Classic UI

Once your Pipeline has completed, whether it succeeds or fails, you can go to the side panel for the run in the classic UI and click on “Restart from Stage”.

image::pipeline/restart-stages-sidebar.png[Restart from Stage link]

You will be prompted to choose from a list of top-level stages that were executed in the original run, in the order they were executed. Stages which were skipped due to an earlier failure will not be available to be restarted, but stages which were skipped due to a `when` condition not being satisfied will be available. The parent stage for a group of `parallel` stages, or a group of nested `stages` to be run sequentially will also not be available - only top-level stages are allowed.

image::pipeline/restart-stages-dropdown.png[Choose the stage to restart]

Once you choose a stage to restart from and click submit, a new build, with a new build number, will be started. All stages before the selected stage will be skipped, and the Pipeline will start executing at the selected stage. From that point on, the Pipeline will run as normal.

Restarting from the Blue Ocean UI

Restarting stages can also be done in the Blue Ocean UI. Once your Pipeline has completed, whether it succeeds or fails, you can click on the node which represents the stage. You can then click on the `Restart` link for that stage.

image::pipeline/pipeline-restart-stages-blue-ocean.png[Click on Restart link for stage]

Preserving `stash`es for Use with Restarted Stages

Normally, when you run the `stash` step in your Pipeline, the resulting stash of artifacts is cleared when the Pipeline completes, regardless of the result of the Pipeline. Since `stash` artifacts aren't accessible outside of the Pipeline run that created them, this has not created any limitations on usage. But with Declarative stage restarting, you may want to be able to `unstash` artifacts from a stage which ran before the stage you're restarting from.

To enable this, there is a job property that allows you to configure a maximum number of completed runs whose `stash` artifacts should be preserved for reuse in a restarted run. You can specify anywhere from `1` to `50` as the number of runs to preserve.

This job property can be configured in your Declarative Pipeline's `options` section, as below:

```
options {
    preserveStashes() // <1>
    // or
    preserveStashes(buildCount: 5) // <2>
}
```

<1> The default number of runs to preserve is `1`, just the most recent completed build. <2> If a number for `buildCount` outside of the range of `1` to `50` is specified, the Pipeline will fail with a validation error.

When a Pipeline completes, it will check to see if any previously completed runs should have their `stash` artifacts cleared.

Using Speed/Durability Settings To Reduce Disk I/O Needs

One of the main bottlenecks in Pipeline is that it writes transient data to disk *FREQUENTLY* so that running pipelines can handle an unexpected Jenkins restart or system crash. This durability is useful for many users but its performance cost can be a problem.

Pipeline now includes features to let users improve performance by reducing how much data is written to disk and how often it is written – at a small cost to durability. In some special cases, users may not be able to resume or visualize running Pipelines if Jenkins shuts down suddenly without getting a chance to write data.

Because these settings include a trade-off of speed vs. durability, they are initially opt-in. To enable performance-optimized modes, users need to explicity set a *Speed/Durability Setting* for Pipelines. If no explicit choice is made, pipelines currently default to the "maximum durability" setting and write to disk as they have in the past. There are some I/O optimizations to this mode included in the same plugin releases, but the benefits are much smaller.

How Do I Set Speed/Durability Settings?

There are 3 ways to configure the durability setting:

. *Globally*, you can choose a global default durability setting under "Manage Jenkins" > "Configure System", labelled "Pipeline Speed/Durability Settings". You can override these with the more specific settings below.

. *Per pipeline job:* at the top of the job configuration, labelled "Custom Pipeline Speed/Durability Level" - this overrides the global setting. Or, use a "properties" step - the setting will apply to the NEXT run after the step is executed (same result).

. *Per-branch for a multibranch project:* configure a custom Branch Property Strategy (under the SCM) and add a property for Custom Pipeline Speed/Durability Level. This overrides the global setting. You can also use a "properties" step to override the setting, but remember that you may have to run the step again to undo this.

Durability settings will take effect with the next applicable Pipeline run, not immediately. The setting will be displayed in the log.

Will Higher-Performance Durability Settings Help Me?

- Yes, if your Jenkins instance uses NFS, magnetic storage, runs many Pipelines at once, or shows high iowait.
- Yes, if you are running Pipelines with many steps (more than several hundred).
- Yes, if your Pipeline stores large files or complex data to variables in the script, keeps that variable in scope for future use, and then runs steps. This sounds oddly specific but happens more than you'd expect.
- No, if your Pipelines spend almost all their time waiting for a few shell/batch scripts to finish. This ISN'T a magic "go fast" button for everything!
- No, if Pipelines are writing massive amounts of data to logs (logging is unchanged).
- No, if you are not using Pipelines, or your system is loaded down by other factors.
- No, if you don't enable higher-performance modes for pipelines.

** For example: `readFile` step with a large XML/JSON file, or using configuration information from parsing such a file with One of the Utility Steps[76]. ** Another common pattern is a "summary" object containing data from many branches (logs, results, or statistics). Often this is visible because you'll be adding to it often via an add/append or `Map.put()` operations. ** Large arrays of data or `Maps` of configuration information are another common example of this situation.

What Am I Giving Up With This Durability Setting "Trade-Off?"

Stability of Jenkins ITSELF is not changed regardless of this setting - it only applies to Pipelines. The worst-case behavior for Pipelines reverts to something like Freestyle builds – running Pipelines that cannot persist transient data may not be able to resume or be displayed in Blue Ocean/Stage View/etc, but will show logs. This impacts *only* running Pipelines and only when Jenkins is shut down abruptly and not gracefully before they get to complete.

A *"graceful" shutdown* is where Jenkins goes through a full shutdown process, such as visiting http://[jenkins-server]/exit, or using normal service shutdown scripts (if Jenkins is healthy). Sending a SIGTERM/SIGINT to Jenkins will trigger a graceful shutdown. Note that running Pipelines do not need to complete (you do not need to use /safeExit to shut down).

A *"dirty" shutdown* is when Jenkins does not get to do normal shutdown processes. This can occur if the process is forcibly terminated. The most common causes are using SIGKILL to terminate the Jenkins process or killing the container/VM running Jenkins. Simply stopping or pausing the container/VM will not cause this, as long as the Jenkins process is able to resume. A dirty shutdown can also happen due to catastrophic operating system failures, including the Linux OOMKiller attacking the Jenkins java process to free memory.

[76]https://jenkins.io/doc/pipeline/steps/pipeline-utility-steps/#code-readjson-code-read-json-from-files-in-the-workspace

Atomic writes: All settings *except* "maximum durability" currently avoid atomic writes – what this means is that if the operating system running Jenkins fails, data that is buffered for writing to disk will not be flushed, it will be lost. This is quite rare, but can happen as a result of container or virtualization operations that halt the operating system or disconnect storage. Usually this data is flushed pretty quickly to disk, so the window for data loss is brief. On Linux this flush-to-disk can be forced by running 'sync'. In some rare cases this can also result in a build that cannot be loaded.

Requirements To Use Durability Settings

- Jenkins LTS 2.73+ or higher (or a weekly 2.62+)
- For *all* the Pipeline plugins below, at least the specified minimum version must be installed
- Restart the master to use the updated plugins - note: you need all of them to take advantage. - Pipeline: API (workflow-api) v2.25 - Pipeline: Groovy (workflow-cps) v2.43 - Pipeline: Job (workflow-job) v2.17 - Pipeline: Supporting APIs (workflow-support) v2.17 - Pipeline: Multibranch (workflow-multibranch) v2.17 - optional, only needed to enable this setting for multibranch pipelines.

What Are The Durability Settings?

- Performance-optimized mode ("PERFORMANCE_OPTIMIZED") - *Greatly* reduces disk I/O. If Pipelines do not finish AND Jenkins is not shut down gracefully, they may lose data and behave like Freestyle projects – see details above.
- Maximum durability ("MAX_SURVIVABILITY") - behaves just like Pipeline did before, slowest option. Use this for running your most critical Pipelines.
- Less durable, a bit faster ("SURVIVABLE_NONATOMIC") - Writes data with every step but avoids atomic writes. This is faster than maximum durability mode, especially on networked filesystems. It carries a small extra risk (details above under "What Am I Giving Up: Atomic Writes").

Suggested Best Practices And Tips for Durability Settings

- Use the "performance-optimized" mode for most pipelines and especially basic build-test Pipelines or anything that can simply be run again if needed.
- Use either the "maximum durability" or "less durable" mode for pipelines when you need a guaranteed record of their execution (auditing). These two modes record every step run. For example, use one of these two modes when:
- Set a global default (see above) of "performance-optimized" for the Durability Setting, and then where needed set "maximum durability" on specific Pipeline jobs or Multibranch Pipeline branches ("master" or release branches).

- You can force a Pipeline to persist data by pausing it.

** you have a pipeline that modifies the state of critical infrastructure ** you do a production deployment

Other Scaling Suggestions

- Use @NonCPS-annotated functions for more complex work. This means more involved processing, logic, and transformations. This lets you leverage additional Groovy & functional features for more powerful, concise, and performant code.
- *Whenever possible, run Jenkins with fast SSD-backed storage and not hard drives. This can make a

huge difference.*

- In general try to fit the tool to the job. Consider writing short Shell/Batch/Groovy/Python scripts when running a complex process using a build agent. Good examples include processing data, communicating interactively with REST APIs, and parsing/templating larger XML or JSON files. The `sh` and `bat` steps are helpful to invoke these, especially with `returnStdout: true` to return the output from this script and save it as a variable (Scripted Pipeline).
- Use the latest versions of the Pipeline plugins and Script Security, if applicable. These include regular performance improvements.
- Try to simplify Pipeline code by reducing the number of steps run and using simpler Groovy code for Scripted Pipelines.
- Consolidate sequential steps of the same type if you can, for example by using one Shell step to invoke a helper script rather than running many steps.
- Try to limit the amount of data written to logs by Pipelines. If you are writing several MB of log data, such as from a build tool, consider instead writing this to an external file, compressing it, and archiving it as a build artifact.
- When using Jenkins with more than 6 GB of heap use the

suggested garbage collection tuning options[77] to minimize garbage collection pause times and overhead.
** This still runs on masters so be aware of complexity of the work, but is much faster than native Pipeline code because it doesn't provide durability and uses a faster execution model. Still, be mindful of the CPU cost and offload to executors when the cost becomes too high. ** @NonCPS functions can use a much broader subset of the Groovy language, such as iterators and functional features, which makes them more terse and fast to write. ** @NonCPS functions *should not use* Pipeline steps internally, however you can store the result of a Pipeline step to a variable and use it that as the input to a @NonCPS function. ** *Gotcha*: It's not guaranteed that use of a step will

[77] https://jenkins.io/blog/2016/11/21/gc-tuning/

generate an error (there is an open RFE to implement that), but you should not rely on that behavior. You may see improper handling of exceptions. ** While normal Pipeline is restricted to serializable local variables, @NonCPS functions can use more complex, nonserializable types internally (for example regex matchers, etc). Parameters and return types should still be Serializable, however. ** **Gotcha*: improper usages are not guaranteed to raise an error with normal Pipeline (optimizations may mask the issue), but it is unsafe to rely on this behavior. ** *General Gotcha*: when using running @NonCPS functions, the actual error can sometimes be swallowed by pipeline creating a confusing error message. Combat this by using a `try/catch` block and potentially using an `echo` to plain text print the error message in the `catch` ** The Pipeline DSL is not designed for arbitrary networking and computation tasks - it is intended for CI/CD scripting.

Extending with Shared Libraries

As Pipeline is adopted for more and more projects in an organization, common patterns are likely to emerge. Oftentimes it is useful to share parts of Pipelines between various projects to reduce redundancies and keep code “DRY” footnoteref:[dry, https://en.wikipedia.org/wiki/Don’t*repeat*yourself].

Pipeline has support for creating “Shared Libraries” which can be defined in external source control repositories and loaded into existing Pipelines.

Defining Shared Libraries

A Shared Library is defined with a name, a source code retrieval method such as by SCM, and optionally a default version. The name should be a short identifier as it will be used in scripts.

The version could be anything understood by that SCM; for example, branches, tags, and commit hashes all work for Git. You may also declare whether scripts need to explicitly request that library (detailed below), or if it is present by default. Furthermore, if you specify a version in Jenkins configuration, you can block scripts from selecting a *different* version.

The best way to specify the SCM is using an SCM plugin which has been specifically updated to support a new API for checking out an arbitrary named version (*Modern SCM* option). As of this writing, the latest versions of the Git and Subversion plugins support this mode; others should follow.

If your SCM plugin has not been integrated, you may select *Legacy SCM* and pick anything offered. In this case, you need to include `${library.yourLibName.version}` somewhere in the configuration of the SCM, so that during checkout the plugin will expand this variable to select the desired version. For example, for Subversion, you can set the *Repository URL* to `https://svnserver/project/${library.yourLibNam` and then use versions such as `trunk` or `branches/dev` or `tags/1.0`.

Directory structure

The directory structure of a Shared Library repository is as follows:

```
(root)
+- src                     # Groovy source files
|   +- org
|       +- foo
|           +- Bar.groovy  # for org.foo.Bar class
+- vars
|   +- foo.groovy          # for global 'foo' variable
|   +- foo.txt             # help for 'foo' variable
+- resources               # resource files (external libraries only)
|   +- org
|       +- foo
|           +- bar.json    # static helper data for org.foo.Bar
```

The `src` directory should look like standard Java source directory structure. This directory is added to the classpath when executing Pipelines.

The `vars` directory hosts script files that are exposed as a variable in Pipelines. The name of the file is the name of the variable in the Pipeline. So if you had a file called `vars/log.groovy` with a function like `def info(message)...` in it, you can access this function like `log.info "hello world"` in the Pipeline. You can put as many functions as you like inside this file. Read on below for more examples and options.

The basename of each `.groovy` file should be a Groovy (~ Java) identifier, conventionally `camelCased`. The matching `.txt`, if present, can contain documentation, processed through the system's configured https://wiki.jenkins.io/display/JENKINS/Markup+formatting[markup formatter] (so may really be HTML, Markdown, etc., though the `.txt` extension is required). This documentation will only be visible on the https://jenkins.io/doc/book/pipeline/getting-started/#global-variable-reference[Global Variable Reference] pages that are accessed from the navigation sidebar of Pipeline jobs that import the shared library. In addition, those jobs must run successfully once before the shared library documentation will be generated.

The Groovy source files in these directories get the same "CPS transformation" as in Scripted Pipeline.

A `resources` directory allows the `libraryResource` step to be used from an external library to load associated non-Groovy files. Currently this feature is not supported for internal libraries.

Other directories under the root are reserved for future enhancements.

Global Shared Libraries

There are several places where Shared Libraries can be defined, depending on the use-case. *Manage Jenkins » Configure System » Global Pipeline Libraries* as many libraries as necessary can be configured.

image::pipeline/add-global-pipeline-libraries.png["Add a Global Pipeline Library", role=center]

Since these libraries will be globally usable, any Pipeline in the system can utilize functionality implemented in these libraries.

These libraries are considered "trusted:" they can run any methods in Java, Groovy, Jenkins internal APIs, Jenkins plugins, or third-party libraries. This allows you to define libraries which encapsulate individually unsafe APIs in a higher-level wrapper safe for use from any Pipeline. Beware that **anyone able to push commits to this SCM repository could obtain unlimited access to Jenkins**. You need the *Overall/RunScripts* permission to configure these libraries (normally this will be granted to Jenkins administrators).

Folder-level Shared Libraries

Any Folder created can have Shared Libraries associated with it. This mechanism allows scoping of specific libraries to all the Pipelines inside of the folder or subfolder.

Folder-based libraries are not considered "trusted:" they run in the Groovy sandbox just like typical Pipelines.

Automatic Shared Libraries

Other plugins may add ways of defining libraries on the fly. For example, the plugin:github-branch-source[GitHub Branch Source] plugin provides a "GitHub Organization Folder" item which allows a script to use an untrusted library such as `github.com/someorg/somerepo` without any additional configuration. In this case, the specified GitHub repository would be loaded, from the `master` branch, using an anonymous checkout.

Using libraries

Shared Libraries marked *Load implicitly* allows Pipelines to immediately use classes or global variables defined by any such libraries. To access other shared libraries, the `Jenkinsfile` needs to use the `@Library` annotation, specifying the library's name:

image::pipeline/configure-global-pipeline-library.png["Configuring a Global Pipeline Library", role=center]

```
@Library('my-shared-library') _
/* Using a version specifier, such as branch, tag, etc */
@Library('my-shared-library@1.0') _
/* Accessing multiple libraries with one statement */
@Library(['my-shared-library', 'otherlib@abc1234']) _
```

The annotation can be anywhere in the script where an annotation is permitted by Groovy. When referring to class libraries (with `src/` directories), conventionally the annotation goes on an `import` statement:

```
@Library('somelib')
import com.mycorp.pipeline.somelib.UsefulClass
```

[TIP] ==== For Shared Libraries which only define Global Variables (`vars/`), or a `Jenkinsfile` which only needs a Global Variable, the annotation[78] pattern `@Library('my-shared-library') _` may be useful for keeping code concise. In essence, instead of annotating an unnecessary `import` statement, the symbol _ is annotated.

It is not recommended to `import` a global variable/function, since this will force the compiler to interpret fields and methods as `static` even if they were intended to be instance. The Groovy compiler in this case can produce confusing error messages. ====

Libraries are resolved and loaded during *compilation* of the script, before it starts executing. This allows the Groovy compiler to understand the meaning of symbols used in static type checking, and permits them to be used in type declarations in the script, for example:

```
@Library('somelib')
import com.mycorp.pipeline.somelib.Helper

int useSomeLib(Helper helper) {
    helper.prepare()
    return helper.count()
}

echo useSomeLib(new Helper('some text'))
```

Global Variables however, are resolved at runtime.

Loading libraries dynamically

As of version 2.7 of the *Pipeline: Shared Groovy Libraries* plugin, there is a new option for loading (non-implicit) libraries in a script: a `library` step that loads a library *dynamically*, at any time during the build.

If you are only interested in using global variables/functions (from the `vars/` directory), the syntax is quite simple:

```
library 'my-shared-library'
```

Thereafter, any global variables from that library will be accessible to the script.

Using classes from the `src/` directory is also possible, but trickier. Whereas the `@Library` annotation prepares the "classpath" of the script prior to compilation, by the time a `library` step is encountered

[78]http://groovy-lang.org/objectorientation.html#_annotation

the script has already been compiled. Therefore you cannot `import` or otherwise "statically" refer to types from the library.

However you may use library classes dynamically (without type checking), accessing them by fully-qualified name from the return value of the `library` step. `static` methods can be invoked using a Java-like syntax:

```
library('my-shared-library').com.mycorp.pipeline.Utils.someStaticMethod()
```

You can also access `static` fields, and call constructors as if they were `static` methods named `new`:

```
def useSomeLib(helper) { // dynamic: cannot declare as Helper
    helper.prepare()
    return helper.count()
}

def lib = library('my-shared-library').com.mycorp.pipeline // preselect the package

echo useSomeLib(lib.Helper.new(lib.Constants.SOME_TEXT))
```

Library versions

The "Default version" for a configured Shared Library is used when "Load implicitly" is checked, or if a Pipeline references the library only by name, for example `@Library('my-shared-library') _`. If a "Default version" is *not* defined, the Pipeline must specify a version, for example `@Library('my-shared-library@mas`
_.

If "Allow default version to be overridden" is enabled in the Shared Library's configuration, a `@Library` annotation may also override a default version defined for the library. This also allows a library with "Load implicitly" to be loaded from a different version if necessary.

When using the `library` step you may also specify a version:

```
library 'my-shared-library@master'
```

Since this is a regular step, that version could be *computed* rather than a constant as with the annotation; for example:

```
library "my-shared-library@$BRANCH_NAME"
```

would load a library using the same SCM branch as the multibranch `Jenkinsfile`. As another example, you could pick a library by parameter:

```
properties([parameters([string(name: 'LIB_VERSION', defaultValue: 'master')])])
library "my-shared-library@${params.LIB_VERSION}"
```

Note that the `library` step may not be used to override the version of an implicitly loaded library. It is already loaded by the time the script starts, and a library of a given name may not be loaded twice.

Retrieval Method

The best way to specify the SCM is using an SCM plugin which has been specifically updated to support a new API for checking out an arbitrary named version (**Modern SCM** option). As of this writing, the latest versions of the Git and Subversion plugins support this mode.

image::pipeline/global-pipeline-library-modern-scm.png[“Configuring a ‘Modern SCM’ for a Pipeline Library”, role=center]

Legacy SCM

SCM plugins which have not yet been updated to support the newer features required by Shared Libraries, may still be used via the **Legacy SCM** option. In this case, include `${library.yourlibrarynamehere.version` wherever a branch/tag/ref may be configured for that particular SCM plugin. This ensures that during checkout of the library’s source code, the SCM plugin will expand this variable to checkout the appropriate version of the library.

image::pipeline/global-pipeline-library-legacy-scm.png[“Configuring a ‘Legacy SCM’ for a Pipeline Library”, role=center]

Dynamic retrieval

If you only specify a library name (optionally with version after `@`) in the `library` step, Jenkins will look for a preconfigured library of that name. (Or in the case of a `github.com/owner/repo` automatic library it will load that.)

But you may also specify the retrieval method dynamically, in which case there is no need for the library to have been predefined in Jenkins. Here is an example:

```
library identifier: 'custom-lib@master', retriever: modernSCM(
  [$class: 'GitSCMSource',
   remote: 'git@git.mycorp.com:my-jenkins-utils.git',
   credentialsId: 'my-private-key'])
```

It is best to refer to *Pipeline Syntax* for the precise syntax for your SCM.

Note that the library version *must* be specified in these cases.

Writing libraries

At the base level, any valid Groovy code[79] is okay for use. Different data structures, utility methods, etc, such as:

```
// src/org/foo/Point.groovy
package org.foo

// point in 3D space
class Point {
  float x,y,z
}
```

Accessing steps

Library classes cannot directly call steps such as `sh` or `git`. They can however implement methods, outside of the scope of an enclosing class, which in turn invoke Pipeline steps, for example:

```
// src/org/foo/Zot.groovy
package org.foo

def checkOutFrom(repo) {
  git url: "git@github.com:jenkinsci/${repo}"
}

return this
```

Which can then be called from a Scripted Pipeline:

```
def z = new org.foo.Zot()
z.checkOutFrom(repo)
```

This approach has limitations; for example, it prevents the declaration of a superclass.

Alternately, a set of `steps` can be passed explicitly using `this` to a library class, in a constructor, or just one method:

[79]http://groovy-lang.org/syntax.html

```
package org.foo
class Utilities implements Serializable {
  def steps
  Utilities(steps) {this.steps = steps}
  def mvn(args) {
    steps.sh "${steps.tool 'Maven'}/bin/mvn -o ${args}"
  }
}
```

When saving state on classes, such as above, the class *must* implement the `Serializable` interface. This ensures that a Pipeline using the class, as seen in the example below, can properly suspend and resume in Jenkins.

```
@Library('utils') import org.foo.Utilities
def utils = new Utilities(this)
node {
  utils.mvn 'clean package'
}
```

If the library needs to access global variables, such as `env`, those should be explicitly passed into the library classes, or methods, in a similar manner.

Instead of passing numerous variables from the Scripted Pipeline into a library,

```
package org.foo
class Utilities {
  static def mvn(script, args) {
    script.sh "${script.tool 'Maven'}/bin/mvn -s ${script.env.HOME}/jenkins.xml -o $\
{args}"
  }
}
```

The above example shows the script being passed in to one `static` method, invoked from a Scripted Pipeline as follows:

```
@Library('utils') import static org.foo.Utilities.*
node {
  mvn this, 'clean package'
}
```

Defining global variables

Internally, scripts in the `vars` directory are instantiated on-demand as singletons. This allows multiple methods to be defined in a single `.groovy` file for convenience. For example:

```
def info(message) {
    echo "INFO: ${message}"
}

def warning(message) {
    echo "WARNING: ${message}"
}
```

.vars/log.groovy

```
@Library('utils') _

log.info 'Starting'
log.warning 'Nothing to do!'
```

.Jenkinsfile

```
@groovy.transform.Field
def yourField = [:]

def yourFunction....
```

Note that if you wish to use a field in your global for some state, annotate it as such:

Declarative Pipeline does not allow method calls on objects outside "script" blocks. (JENKINS-42360[80]). The method calls above would need to be put inside a `script` directive:

```
@Library('utils') _

pipeline {
    agent none
    stage ('Example') {
        steps {
            // log.info 'Starting' // <1>
            script { // <2>
                log.info 'Starting'
                log.warning 'Nothing to do!'
            }
        }
    }
}
```

.Jenkinsfile <1> This method call would fail because it is outside a `script` directive. <2> `script` directive required to access global variables in Declarative Pipeline.

[80]https://issues.jenkins-ci.org/browse/JENKINS-42360

```
A variable defined in a shared library will only show up in _Global Variables
Reference_ (under _Pipeline Syntax_) after Jenkins loads and uses that library
as part of a successful Pipeline run.
```

.Avoid preserving state in global variables [WARNING] ==== Avoid defining global variables with methods that interact or preserve state. Use a static class or instantiate a local variable of a class instead. ====

Defining custom steps

Shared Libraries can also define global variables which behave similarly to built-in steps, such as `sh` or `git`. Global variables defined in Shared Libraries *must* be named with all lower-case or “camel-Cased” in order to be loaded properly by Pipeline. footnote:[https://gist.github.com/rtyler/e5e57f075af381fce4ed3ae5

For example, to define `sayHello`, the file `vars/sayHello.groovy` should be created and should implement a `call` method. The `call` method allows the global variable to be invoked in a manner similar to a step:

```
// vars/sayHello.groovy
def call(String name = 'human') {
    // Any valid steps can be called from this code, just like in other
    // Scripted Pipeline
    echo "Hello, ${name}."
}
```

The Pipeline would then be able to reference and invoke this variable:

```
sayHello 'Joe'
sayHello() /* invoke with default arguments */
```

If called with a block, the `call` method will receive a `Closure`[81]. The type should be defined explicitly to clarify the intent of the step, for example:

```
// vars/windows.groovy
def call(Closure body) {
    node('windows') {
        body()
    }
}
```

The Pipeline can then use this variable like any built-in step which accepts a block:

[81]http://groovy-lang.org/closures.html

```
windows {
    bat "cmd /?"
}
```

Defining a more structured DSL

If you have a lot of Pipelines that are mostly similar, the global variable mechanism provides a handy tool to build a higher-level DSL that captures the similarity. For example, all Jenkins plugins are built and tested in the same way, so we might write a step named `buildPlugin`:

```
// vars/buildPlugin.groovy
def call(Map config) {
    node {
        git url: "https://github.com/jenkinsci/${config.name}-plugin.git"
        sh 'mvn install'
        mail to: '...', subject: "${config.name} plugin build", body: '...'
    }
}
```

Assuming the script has either been loaded as a Global Shared Library or as a Folder-level Shared Library the resulting `Jenkinsfile` will be dramatically simpler:

[pipeline] —- // Script // buildPlugin name: 'git' // Declarative not yet implemented // —-

There is also a "builder pattern" trick using Groovy's `Closure.DELEGATE_FIRST`, which permits `Jenkinsfile` to look slightly more like a configuration file than a program, but this is more complex and error-prone and is not recommended.

Using third-party libraries

It is possible to use third-party Java libraries, typically found in Maven Central[82], from *trusted* library code using the `@Grab` annotation. Refer to the link:https://docs.groovy-lang.org/latest/html/documentation/grape.ht
documentation] for details, but simply put:

[82]https://search.maven.org/

```
@Grab('org.apache.commons:commons-math3:3.4.1')
import org.apache.commons.math3.primes.Primes
void parallelize(int count) {
  if (!Primes.isPrime(count)) {
    error "${count} was not prime"
  }
  // …
}
```

Third-party libraries are cached by default in ~/.groovy/grapes/ on the Jenkins master.

Loading resources

External libraries may load adjunct files from a `resources/` directory using the `libraryResource` step. The argument is a relative pathname, akin to Java resource loading:

```
def request = libraryResource 'com/mycorp/pipeline/somelib/request.json'
```

The file is loaded as a string, suitable for passing to certain APIs or saving to a workspace using `writeFile`.

It is advisable to use an unique package structure so you do not accidentally conflict with another library.

Pretesting library changes

If you notice a mistake in a build using an untrusted library, simply click the *Replay* link to try editing one or more of its source files, and see if the resulting build behaves as expected. Once you are satisfied with the result, follow the diff link from the build's status page, and apply the diff to the library repository and commit.

(Even if the version requested for the library was a branch, rather than a fixed version like a tag, replayed builds will use the exact same revision as the original build: library sources will not be checked out again.)

Replay is not currently supported for trusted libraries. Modifying resource files is also not currently supported during *Replay*.

Defining Declarative Pipelines

Starting with Declarative 1.2, released in late September, 2017, you can define Declarative Pipelines in your shared libraries as well. Here's an example, which will execute a different Declarative Pipeline depending on whether the build number is odd or even:

```groovy
// vars/evenOrOdd.groovy
def call(int buildNumber) {
  if (buildNumber % 2 == 0) {
    pipeline {
      agent any
      stages {
        stage('Even Stage') {
          steps {
            echo "The build number is even"
          }
        }
      }
    }
  } else {
    pipeline {
      agent any
      stages {
        stage('Odd Stage') {
          steps {
            echo "The build number is odd"
          }
        }
      }
    }
  }
}
```

```groovy
// Jenkinsfile
@Library('my-shared-library') _

evenOrOdd(currentBuild.getNumber())
```

Only entire `pipelines` can be defined in shared libraries as of this time. This can only be done in `vars/*.groovy`, and only in a `call` method. Only one Declarative Pipeline can be executed in a single build, and if you attempt to execute a second one, your build will fail as a result.

Pipeline Syntax

This section builds on the information introduced in Getting started with Pipeline and should be treated solely as a reference. For more information on how to use Pipeline syntax in practical examples, refer to the Using a Jenkinsfile section of this chapter. As of version 2.5 of the Pipeline plugin, Pipeline supports two discrete syntaxes which are detailed below. For the pros and cons of each, see the <<compare>>.

As discussed at the start of this chapter, the most fundamental part of a Pipeline is the "step". Basically, steps tell Jenkins *what* to do and serve as the basic building block for both Declarative and Scripted Pipeline syntax.

For an overview of available steps, please refer to the Pipeline Steps reference which contains a comprehensive list of steps built into Pipeline as well as steps provided by plugins.

Declarative Pipeline

[role=syntax]

Declarative Pipeline is a relatively recent addition to Jenkins Pipeline footnoteref:[declarative-version, Version 2.5 of the "Pipeline plugin" introduces support for Declarative Pipeline syntax] which presents a more simplified and opinionated syntax on top of the Pipeline sub-systems.

All valid Declarative Pipelines must be enclosed within a `pipeline` block, for example:

```
pipeline {
    /* insert Declarative Pipeline here */
}
```

The basic statements and expressions which are valid in Declarative Pipeline follow the same rules as Groovy's syntax[83] with the following exceptions:

- The top-level of the Pipeline must be a

block, specifically: `pipeline { }`

- No semicolons as statement separators. Each statement has to be on its own
- Blocks must only consist of <<declarative-sections>>,

[83]http://groovy-lang.org/syntax.html

- A property reference statement is treated as no-argument method invocation. So for line <<declarative-directives>>, <<declarative-steps>>, or assignment statements. example, input is treated as input()

You can use the Declarative Directive Generator to help you get started with configuring the directives and sections in your Declarative Pipeline.

Sections

[[declarative-sections]]

Sections in Declarative Pipeline typically contain one or more <<declarative-directives>> or <<declarative-steps>>.

agent

The `agent` section specifies where the entire Pipeline, or a specific stage, will execute in the Jenkins environment depending on where the `agent` section is placed. The section must be defined at the top-level inside the `pipeline` block, but stage-level usage is optional.

[cols="^10h,>90a",role=syntax] |=== | Required | Yes

| Parameters | Described below

| Allowed | In the top-level `pipeline` block and each `stage` block. |===

Parameters

[[agent-parameters]]

In order to support the wide variety of use-cases Pipeline authors may have, the `agent` section supports a few different types of parameters. These parameters can be applied at the top-level of the `pipeline` block, or within each `stage` directive.

any:: Execute the Pipeline, or stage, on any available agent. For example: `agent any`

none:: When applied at the top-level of the `pipeline` block no global agent will be allocated for the entire Pipeline run and each `stage` section will need to contain its own `agent` section. For example: `agent none`

label:: Execute the Pipeline, or stage, on an agent available in the Jenkins environment with the provided label. For example: `agent { label 'my-defined-label' }`

node:: `agent { node { label 'labelName' } }` behaves the same as `agent { label 'labelName' }`, but `node` allows for additional options (such as `customWorkspace`).

```
agent {
    docker {
        image 'maven:3-alpine'
        label 'my-defined-label'
        args  '-v /tmp:/tmp'
    }
}
```

```
agent {
    docker {
        image 'myregistry.com/node'
        label 'my-defined-label'
        registryUrl 'https://myregistry.com/'
        registryCredentialsId 'myPredefinedCredentialsInJenkins'
    }
}
```

docker:: Execute the Pipeline, or stage, with the given container which will be dynamically provisioned on a node pre-configured to accept Docker-based Pipelines, or on a node matching the optionally defined `label` parameter. `docker` also optionally accepts an `args` parameter which may contain arguments to pass directly to a `docker run` invocation, and an `alwaysPull` option, which will force a `docker pull` even if the image name is already present. For example: `agent { docker 'maven:3-alpine' }` or + + `docker` also optionally accepts a `registryUrl` and `registryCredentialsId` parameters which will help to specify the Docker Registry to use and its credentials. For example: +

```
agent {
    // Equivalent to "docker build -f Dockerfile.build --build-arg version=1.0.2 ./b\
uild/
    dockerfile {
        filename 'Dockerfile.build'
        dir 'build'
        label 'my-defined-label'
        additionalBuildArgs  '--build-arg version=1.0.2'
        args '-v /tmp:/tmp'
    }
}
```

```
agent {
    dockerfile {
        filename 'Dockerfile.build'
        dir 'build'
        label 'my-defined-label'
        registryUrl 'https://myregistry.com/'
        registryCredentialsId 'myPredefinedCredentialsInJenkins'
    }
}
```

dockerfile:: Execute the Pipeline, or stage, with a container built from a `Dockerfile` contained in the source repository. In order to use this option, the `Jenkinsfile` must be loaded from either a Multibranch Pipeline, or a "Pipeline from SCM." Conventionally this is the `Dockerfile` in the root of the source repository: `agent { dockerfile true }`. If building a `Dockerfile` in another directory, use the `dir` option: `agent { dockerfile { dir 'someSubDir' } }`. If your `Dockerfile` has another name, you can specify the file name with the `filename` option. You can pass additional arguments to the `docker build ...` command with the `additionalBuildArgs` option, like `agent { dockerfile { additionalBuildArgs '--build-arg foo=bar' } }`. For example, a repository with the file `build/Dockerfile.build`, expecting a build argument `version`: + + `dockerfile` also optionally accepts a `registryUrl` and `registryCredentialsId` parameters which will help to specify the Docker Registry to use and its credentials. For example: +

Common Options

These are a few options that can be applied two or more `agent` implementations. They are not required unless explicitly stated.

label:: A string. The label on which to run the Pipeline or individual `stage`. + This option is valid for `node`, `docker` and `dockerfile`, and is required for `node`.

```
agent {
    node {
        label 'my-defined-label'
        customWorkspace '/some/other/path'
    }
}
```

customWorkspace:: A string. Run the Pipeline or individual `stage` this `agent` is applied to within this custom workspace, rather than the default. It can be either a relative path, in which case the custom workspace will be under the workspace root on the node, or an absolute path. For example: + + This option is valid for `node`, `docker` and `dockerfile`.

reuseNode:: A boolean, false by default. If true, run the container on the node specified at the top-level of the Pipeline, in the same workspace, rather than on a new node entirely. + This option is valid for `docker` and `dockerfile`, and only has an effect when used on an `agent` for an individual `stage`.

args:: A string. Runtime arguments to pass to `docker run`. + This option is valid for `docker` and `dockerfile`.

Example

[[agent-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> Execute all the steps defined in this Pipeline within a newly created container of the given name and tag (`maven:3-alpine`).

Stage-level `agent` section

[pipeline] —- // Declarative // pipeline // Script // —- <1> Defining `agent none` at the top-level of the Pipeline ensures that an Executor will not be assigned unnecessarily. Using `agent none` also forces each `stage` section to contain its own `agent` section. <2> Execute the steps in this stage in a newly created container using this image. <3> Execute the steps in this stage in a newly created container using a different image from the previous stage.

post

The `post` section defines one or more additional steps that are run upon the completion of a Pipeline's or stage's run (depending on the location of the `post` section within the Pipeline). `post` can support any of of the following post-condition blocks: `always`, `changed`, `fixed`, `regression`, `aborted`, `failure`, `success`, `unstable`, `unsuccessful`, and `cleanup`. These condition blocks allow the execution of steps inside each condition depending on the completion status of the Pipeline or stage. The condition blocks are executed in the order shown below.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | In the top-level `pipeline` block and each `stage` block. |===

Conditions

[[post-conditions]]

`always`:: Run the steps in the `post` section regardless of the completion status of the Pipeline's or stage's run. `changed`:: Only run the steps in `post` if the current Pipeline's or stage's run has a different completion status from its previous run. `fixed`:: Only run the steps in `post` if the current Pipeline's or stage's run is successful and the previous run failed or was unstable. `regression`:: Only run the steps in `post` if the current Pipeline's or stage's run's status is failure, unstable, or aborted and the previous run was successful. `aborted`:: Only run the steps in `post` if the current Pipeline's or stage's run has an "aborted" status, usually due to the Pipeline being manually aborted. This is typically denoted by gray in the web UI. `failure`:: Only run the steps in `post` if the current Pipeline's or stage's run has a "failed" status, typically denoted by red in the web UI. `success`:: Only run the steps in `post` if the current Pipeline's or stage's run has a "success" status, typically denoted by blue or green in the web UI. `unstable`:: Only run the steps in `post` if the current Pipeline's or stage's run has an "unstable" status, usually caused by test failures, code violations, etc. This is typically denoted by yellow in the web UI. `unsuccessful`:: Only run the steps in `post` if the current Pipeline's or stage's run has not a "success" status. This is typically denoted in the web UI depending on the status previously mentioned `cleanup`:: Run the steps in this `post` condition after every other `post` condition has been evaluated, regardless of the Pipeline or stage's status.

Example

[[post-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> Conventionally, the `post` section should be placed at the end of the Pipeline. <2> Post-condition blocks contain steps the same as the <<steps>> section.

stages

Containing a sequence of one or more <<stage>> directives, the `stages` section is where the bulk of the "work" described by a Pipeline will be located. At a minimum it is recommended that `stages` contain at least one <<stage>> directive for each discrete part of the continuous delivery process, such as Build, Test, and Deploy.

[cols="^10h,>90a",role=syntax] |=== | Required | Yes

| Parameters | *None*

| Allowed | Only once, inside the `pipeline` block. |===

Example

[[stages-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> The `stages` section will typically follow the directives such as `agent`, `options`, etc.

steps

The `steps` section defines a series of one or more steps to be executed in a given `stage` directive.

[cols="^10h,>90a",role=syntax] |=== | Required | Yes

| Parameters | *None*

| Allowed | Inside each `stage` block. |===

Example

[[steps-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> The `steps` section must contain one or more steps.

Directives

[[declarative-directives]]

environment

The `environment` directive specifies a sequence of key-value pairs which will be defined as environment variables for the all steps, or stage-specific steps, depending on where the `environment` directive is located within the Pipeline.

This directive supports a special helper method `credentials()` which can be used to access pre-defined Credentials by their identifier in the Jenkins environment. For Credentials which are of type "Secret Text", the `credentials()` method will ensure that the environment variable specified contains the Secret Text contents. For Credentials which are of type "Standard username and password", the environment variable specified will be set to `username:password` and two additional environment variables will be automatically be defined: `MYVARNAME_USR` and `MYVARNAME_PSW` respectively.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Inside the `pipeline` block, or within `stage` directives. |===

Example

[[environment-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> An `environment` directive used in the top-level `pipeline` block will apply to all steps within the Pipeline. <2> An `environment` directive defined within a `stage` will only apply the given environment variables to steps within the `stage`. <3> The `environment` block has a helper method `credentials()` defined which can be used to access pre-defined Credentials by their identifier in the Jenkins environment.

options

The `options` directive allows configuring Pipeline-specific options from within the Pipeline itself. Pipeline provides a number of these options, such as `buildDiscarder`, but they may also be provided by plugins, such as `timestamps`.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Only once, inside the `pipeline` block. |===

Available Options

buildDiscarder:: Persist artifacts and console output for the specific number of recent Pipeline runs. For example: `options { buildDiscarder(logRotator(numToKeepStr: '1')) }`

checkoutToSubdirectory:: Perform the automatic source control checkout in a subdirectory of the workspace. For example: `options { checkoutToSubdirectory('foo') }`

disableConcurrentBuilds:: Disallow concurrent executions of the Pipeline. Can be useful for preventing simultaneous accesses to shared resources, etc. For example: `options { disableConcurrentBuilds() }`

newContainerPerStage:: Used with `docker` or `dockerfile` top-level agent. When specified, each stage will run in a new container instance on the same node, rather than all stages running in the same container instance.

overrideIndexTriggers:: Allows overriding default treatment of branch indexing triggers. If branch indexing triggers are disabled at the multibranch or organization label, `options { overrideIndexTriggers(true) }` will enable them for this job only. Otherwise, `options { overrideIndexTriggers(false) }` will disable branch indexing triggers for this job only.

preserveStashes:: Preserve stashes from completed builds, for use with stage restarting. For example: `options { preserveStashes() }` to preserve the stashes from the most recent completed build, or `options { preserveStashes(buildCount: 5) }` to preserve the stashes from the five most recent completed builds.

quietPeriod:: Set the quiet period, in seconds, for the Pipeline, overriding the global default. For example: `options { quietPeriod(30) }`

retry:: On failure, retry the entire Pipeline the specified number of times. For example: `options { retry(3) }`

skipDefaultCheckout:: Skip checking out code from source control by default in the `agent` directive. For example: `options { skipDefaultCheckout() }`

skipStagesAfterUnstable:: Skip stages once the build status has gone to UNSTABLE. For example: `options { skipStagesAfterUnstable() }`

timeout:: Set a timeout period for the Pipeline run, after which Jenkins should abort the Pipeline. For example: `options { timeout(time: 1, unit: 'HOURS') }`

timestamps:: Prepend all console output generated by the Pipeline run with the time at which the line was emitted. For example: `options { timestamps() }`

parallelsAlwaysFailFast:: Set failfast true for all subsequent parallel stages in the pipeline. For example: `options { parallelsAlwaysFailFast() }`

Example

[[options-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> Specifying a global execution timeout of one hour, after which Jenkins will abort the Pipeline run.

```
A comprehensive list of available options is pending the completion of
link:https://issues.jenkins-ci.org/browse/INFRA-1053[INFRA-1503].
```

stage options

The `options` directive for a `stage` is similar to the `options` directive at the root of the Pipeline. However, the `stage`-level `options` can only contain steps like `retry`, `timeout`, or `timestamps`, or Declarative options that are relevant to a `stage`, like `skipDefaultCheckout`.

Inside a `stage`, the steps in the `options` directive are invoked before entering the `agent` or checking any `when` conditions.

Available Stage Options

skipDefaultCheckout:: Skip checking out code from source control by default in the `agent` directive. For example: `options { skipDefaultCheckout() }`

timeout:: Set a timeout period for this stage, after which Jenkins should abort the stage. For example: `options { timeout(time: 1, unit: 'HOURS') }`

retry:: On failure, retry this stage the specified number of times. For example: `options { retry(3) }`

timestamps:: Prepend all console output generated during this stage with the time at which the line was emitted. For example: `options { timestamps() }`

Example

[[stage-options-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> Specifying a execution timeout of one hour for the `Example` stage, after which Jenkins will abort the Pipeline run.

parameters

The `parameters` directive provides a list of parameters which a user should provide when triggering the Pipeline. The values for these user-specified parameters are made available to Pipeline steps via the `params` object, see the <<parameters-example>> for its specific usage.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Only once, inside the `pipeline` block. |===

Available Parameters

string:: A parameter of a string type, for example: `parameters { string(name: 'DEPLOY_ENV', defaultValue: 'staging', description: '') }`

text:: A text parameter, which can contain multiple lines, for example: `parameters { text(name: 'DEPLOY_TEXT', defaultValue: 'One\nTwo\nThree\n', description: '') }`

booleanParam:: A boolean parameter, for example: `parameters { booleanParam(name: 'DEBUG_-BUILD', defaultValue: true, description: '') }`

choice:: A choice parameter, for example: `parameters { choice(name: 'CHOICES', choices: ['one', 'two', 'three'], description: '') }`

file:: A file parameter, which specifies a file to be submitted by the user when scheduling a build, for example: `parameters { file(name: 'FILE', description: 'Some file to upload') }`

password:: A password parameter, for example: `parameters { password(name: 'PASSWORD', defaultValue: 'SECRET', description: 'A secret password') }`

Example

[[parameters-example]]

[pipeline] —- // Declarative // pipeline { agent any parameters { string(name: 'PERSON', default-Value: 'Mr Jenkins', description: 'Who should I say hello to?')

text(name: 'BIOGRAPHY', defaultValue: '', description: 'Enter some information about the person')

booleanParam(name: 'TOGGLE', defaultValue: true, description: 'Toggle this value')

choice(name: 'CHOICE', choices: ['One', 'Two', 'Three'], description: 'Pick something')

password(name: 'PASSWORD', defaultValue: 'SECRET', description: 'Enter a password')

file(name: "FILE", description: "Choose a file to upload") } stages"

echo "Biography: $"

echo "Toggle: $"

echo "Choice: $"

echo "Password: $ // Script // —-

```
A comprehensive list of available parameters is pending the completion of
link:https://issues.jenkins-ci.org/browse/INFRA-1053[INFRA-1503].
```

triggers

The `triggers` directive defines the automated ways in which the Pipeline should be re-triggered. For Pipelines which are integrated with a source such as GitHub or BitBucket, `triggers` may not be necessary as webhooks-based integration will likely already be present. The triggers currently available are `cron`, `pollSCM` and `upstream`.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Only once, inside the `pipeline` block. |===

cron:: Accepts a cron-style string to define a regular interval at which the Pipeline should be re-triggered, for example: `triggers { cron('H */4 * * 1-5') }` pollSCM:: Accepts a cron-style string to define a regular interval at which Jenkins should check for new source changes. If new changes exist, the Pipeline will be re-triggered. For example: `triggers { pollSCM('H */4 * * 1-5') }` upstream:: Accepts a comma separated string of jobs and a threshold. When any job in the string finishes with the minimum threshold, the Pipeline will be re-triggered. For example: `triggers { upstream(upstreamProjects: 'job1,job2', threshold: hudson.model.Result.SUCCESS) }`

```
The `pollSCM` trigger is only available in Jenkins 2.22 or later.
```

Example

[[triggers-example]]

[pipeline] —- // Declarative // pipeline // Script // —-

Jenkins cron syntax

[[cron-syntax]] The Jenkins cron syntax follows the syntax of the cron utility[84] (with minor differences). Specifically, each line consists of 5 fields separated by TAB or whitespace:

[%header,cols=5*] |=== |MINUTE |HOUR |DOM |MONTH |DOW

|Minutes within the hour (0–59) |The hour of the day (0–23) |The day of the month (1–31) |The month (1–12) |The day of the week (0–7) where 0 and 7 are Sunday. |===

To specify multiple values for one field, the following operators are available. In the order of precedence,

- * specifies all valid values

[84] https://en.wikipedia.org/wiki/Cron

- `M-N` specifies a range of values
- `M-N/X` or `*/X` steps by intervals of `X` through the specified range or whole valid range
- `A,B,...,Z` enumerates multiple values

To allow periodically scheduled tasks to produce even load on the system, the symbol `H` (for "hash") should be used wherever possible. For example, using `0 0 * * *` for a dozen daily jobs will cause a large spike at midnight. In contrast, using `H H * * *` would still execute each job once a day, but not all at the same time, better using limited resources.

The `H` symbol can be used with a range. For example, `H H(0-7) * * *` means some time between 12:00 AM (midnight) to 7:59 AM. You can also use step intervals with `H`, with or without ranges.

The `H` symbol can be thought of as a random value over a range, but it actually is a hash of the job name, not a random function, so that the value remains stable for any given project.

Beware that for the day of month field, short cycles such as `*/3` or `H/3` will not work consistently near the end of most months, due to variable month lengths. For example, `*/3`j will run on the 1st, 4th, …31st days of a long month, then again the next day of the next month. Hashes are always chosen in the 1-28 range, so `H/3` will produce a gap between runs of between 3 and 6 days at the end of a month. (Longer cycles will also have inconsistent lengths but the effect may be relatively less noticeable.)

Empty lines and lines that start with `#` will be ignored as comments.

In addition, `@yearly`, `@annually`, `@monthly`, `@weekly`, `@daily`, `@midnight`, and `@hourly` are supported as convenient aliases. These use the hash system for automatic balancing. For example, `@hourly` is the same as `H * * * *` and could mean at any time during the hour. `@midnight` actually means some time between 12:00 AM and 2:59 AM.

[[cron-syntax-examples]] .Jenkins cron syntax examples [cols=1] |=== |every fifteen minutes (perhaps at :07, :22, :37, :52) |`triggers{ cron('H/15 * * * *') }` |every ten minutes in the first half of every hour (three times, perhaps at :04, :14, :24) |`triggers{ cron('H(0-29)/10 * * * *') }` |once every two hours at 45 minutes past the hour starting at 9:45 AM and finishing at 3:45 PM every weekday. |`triggers{ cron('45 9-16/2 * * 1-5') }` |once in every two hours slot between 9 AM and 5 PM every weekday (perhaps at 10:38 AM, 12:38 PM, 2:38 PM, 4:38 PM) |`triggers{ cron('H H(9-16)/2 * * 1-5') }` |once a day on the 1st and 15th of every month except December |`triggers{ cron('H H 1,15 1-11 *') }` |===

stage

The `stage` directive goes in the `stages` section and should contain a <<steps>> section, an optional `agent` section, or other stage-specific directives. Practically speaking, all of the real work done by a Pipeline will be wrapped in one or more `stage` directives.

[cols="^10h,>90a",role=syntax] |=== | Required | At least one

| Parameters | One mandatory parameter, a string for the name of the stage.

| Allowed | Inside the `stages` section. |===

Example

[[stage-example]]

[pipeline] —- // Declarative // pipeline // Script // —-

tools

A section defining tools to auto-install and put on the `PATH`. This is ignored if `agent none` is specified.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Inside the `pipeline` block or a `stage` block. |===

Supported Tools

maven:: jdk:: gradle::

Example

[[tools-example]]

[pipeline] —- // Declarative // pipeline // Script // —- <1> The tool name must be pre-configured in Jenkins under *Manage Jenkins* -> *Global Tool Configuration*.

input

The `input` directive on a `stage` allows you to prompt for input, using the `input` step[85]. The `stage` will pause after any `options` have been applied, and before entering the `stage`s `agent` or evaluating its `when` condition. If the `input` is approved, the `stage` will then continue. Any parameters provided as part of the `input` submission will be available in the environment for the rest of the `stage`.

Configuration options

message:: Required. This will be presented to the user when they go to submit the `input`.

id:: An optional identifier for this `input`. Defaults to the `stage` name.

ok:: Optional text for the "ok" button on the `input` form.

submitter:: An optional comma-separated list of users or external group names who are allowed to submit this `input`. Defaults to allowing any user.

submitterParameter:: An optional name of an environment variable to set with the `submitter` name, if present.

parameters:: An optional list of parameters to prompt the submitter to provide. See <<parameters>> for more information.

[85]https://jenkins.io/doc/pipeline/steps/pipeline-input-step/#input-wait-for-interactive-input

Example

[[input-example]]

[pipeline] —- // Declarative // pipeline // Script // —-

when

The `when` directive allows the Pipeline to determine whether the stage should be executed depending on the given condition. The `when` directive must contain at least one condition. If the `when` directive contains more than one condition, all the child conditions must return true for the stage to execute. This is the same as if the child conditions were nested in an `allOf` condition (see the examples below). If an `anyOf` condition is used, note that the condition skips remaining tests as soon as the first "true" condition is found.

More complex conditional structures can be built using the nesting conditions: `not`, `allOf`, or `anyOf`. Nesting conditions may be nested to any arbitrary depth.

[cols="^10h,>90a",role=syntax] |=== | Required | No

| Parameters | *None*

| Allowed | Inside a `stage` directive |===

Built-in Conditions

branch:: Execute the stage when the branch being built matches the branch pattern given, for example: `when { branch 'master' }`. Note that this only works on a multibranch Pipeline.

buildingTag:: Execute the stage when the build is building a tag. Example: `when { buildingTag() }`

changelog:: Execute the stage if the build's SCM changelog contains a given regular expression pattern, for example: `when { changelog '.*^\\[DEPENDENCY\\] .+$' }`

changeset:: Execute the stage if the build's SCM changeset contains one or more files matching the given string or glob. Example: `+when { changeset "**/*.js" }+` + By default the path matching will be case insensitive, this can be turned off with the `caseSensitive` parameter, for example: `when { changeset glob: "ReadMe.*", caseSensitive: true }`

changeRequest:: Executes the stage if the current build is for a "change request" (a.k.a. Pull Request on GitHub and Bitbucket, Merge Request on GitLab or Change in Gerrit etc.). When no parameters are passed the stage runs on every change request, for example: `when { changeRequest() }`. + By adding a filter attribute with parameter to the change request, the stage can be made to run only on matching change requests. Possible attributes are `id`, `target`, `branch`, `fork`, `url`, `title`, `author`, `authorDisplayName`, and `authorEmail`. Each of these corresponds to a `CHANGE_*` environment variable, for example: `when { changeRequest target: 'master' }`. + The optional parameter `comparator` may be added after an attribute to specify how any patterns are evaluated for a match: `EQUALS` for a simple string comparison (the default), `GLOB` for an ANT style path glob (same as for example `changeset`), or `REGEXP` for regular expression matching. Example: `when { changeRequest authorEmail: "[\\w_-.]+@example.com", comparator: 'REGEXP' }`

environment:: Execute the stage when the specified environment variable is set to the given value, for example: `when { environment name: 'DEPLOY_TO', value: 'production' }`

equals:: Execute the stage when the expected value is equal to the actual value, for example: `when { equals expected: 2, actual: currentBuild.number }`

expression:: Execute the stage when the specified Groovy expression evaluates to true, for example: `when { expression { return params.DEBUG_BUILD } }` Note that when returning strings from your expressions they must be converted to booleans or return `null` to evaluate to false. Simply returning "`0`" or "false" will still evaluate to "true".

tag:: Execute the stage if the `TAG_NAME` variable matches the given pattern. Example: `when { tag "release-*" }`. If an empty pattern is provided the stage will execute if the `TAG_NAME` variable exists (same as `buildingTag()`). + The optional parameter `comparator` may be added after an attribute to specify how any patterns are evaluated for a match: `EQUALS` for a simple string comparison, `GLOB` (the default) for an ANT style path glob (same as for example `changeset`), or `REGEXP` for regular expression matching. For example: `when { tag pattern: "release-\\d+", comparator: "REGEXP"}`

not:: Execute the stage when the nested condition is false. Must contain one condition. For example: `when { not { branch 'master' } }`

allOf:: Execute the stage when all of the nested conditions are true. Must contain at least one condition. For example: `when { allOf { branch 'master'; environment name: 'DEPLOY_TO', value: 'production' } }`

anyOf:: Execute the stage when at least one of the nested conditions is true. Must contain at least one condition. For example: `when { anyOf { branch 'master'; branch 'staging' } }`

triggeredBy:: Execute the stage when the current build has been triggered by the param given. For example:

- `when { triggeredBy 'SCMTrigger' }`
- `when { triggeredBy 'TimerTrigger' }`
- `when { triggeredBy 'UpstreamCause' }`
- `when { triggeredBy cause: "UserIdCause", detail: "vlinde" }`

Evaluating `when` before entering `agent` in a `stage`

By default, the `when` condition for a `stage` will be evaluated after entering the `agent` for that `stage`, if one is defined. However, this can be changed by specifying the `beforeAgent` option within the `when` block. If `beforeAgent` is set to `true`, the `when` condition will be evaluated first, and the `agent` will only be entered if the `when` condition evaluates to true.

Evaluating `when` before the `input` directive

By default, the when condition for a stage will be evaluated before the input, if one is defined. However, this can be changed by specifying the `beforeInput` option within the when block. If `beforeInput` is set to true, the when condition will be evaluated first, and the input will only be entered if the when condition evaluates to true.

Examples

[[when-example]]

.Single condition [pipeline] —- // Declarative // pipeline // Script // —-

.Multiple condition [pipeline] —- // Declarative // pipeline // Script // —-

.Nested condition (same behavior as previous example) [pipeline] —- // Declarative // pipeline // Script // —-

.Multiple condition and nested condition [pipeline] —- // Declarative // pipeline // Script // —-

.Expression condition and nested condition [pipeline] —- // Declarative // pipeline // Script // —-

`.beforeAgent` [pipeline] —- // Declarative // pipeline // Script // —-

`.beforeInput` [pipeline] —- // Declarative // pipeline // Script // —-

`.triggeredBy` [pipeline] —- // Declarative // pipeline // Script // —-

Sequential Stages

Stages in Declarative Pipeline may declare a list of nested stages to be run within them in sequential order. Note that a stage must have one and only one of `steps`, `parallel`, or `stages`, the last for sequential stages. It is not possible to nest a `parallel` block within a `stage` directive if that `stage` directive is nested within a `parallel` block itself. However, a `stage` directive within a `parallel` block can use all other functionality of a `stage`, including `agent`, `tools`, `when`, etc.

Example

[[sequential-stages-example]]

[pipeline] —- // Declarative // pipeline // Script // —-

Parallel

Stages in Declarative Pipeline may declare a number of nested stages within a `parallel` block, which will be executed in parallel. Note that a stage must have one and only one of `steps`, `stages`, or `parallel`. The nested stages cannot contain further `parallel` stages themselves, but otherwise behave the same as any other `stage`, including a list of sequential stages within `stages`. Any stage containing `parallel` cannot contain `agent` or `tools`, since those are not relevant without `steps`.

In addition, you can force your `parallel` stages to all be aborted when one of them fails, by adding `failFast true` to the `stage` containing the `parallel`. Another option for adding `failfast` is adding an option to the pipeline definition: `parallelsAlwaysFailFast()`

Example

[[parallel-stages-example]]

[pipeline] —- // Declarative // pipeline

// Script // —- .`parallelsAlwaysFailFast` [pipeline] —- // Declarative // pipeline// Script // —-

Steps

[[declarative-steps]]

Declarative Pipelines may use all the available steps documented in the Pipeline Steps reference, which contains a comprehensive list of steps, with the addition of the steps listed below which are *only supported* in Declarative Pipeline.

script

The `script` step takes a block of <<scripted-pipeline>> and executes that in the Declarative Pipeline. For most use-cases, the `script` step should be unnecessary in Declarative Pipelines, but it can provide a useful "escape hatch." `script` blocks of non-trivial size and/or complexity should be moved into Shared Libraries instead.

Example

[[script-example]]

[pipeline] —- // Declarative // pipeline { agent any stages { stage('Example') { steps { echo 'Hello World'

script // Script // —-

Scripted Pipeline

[role=syntax]

Scripted Pipeline, like <<declarative-pipeline>>, is built on top of the underlying Pipeline sub-system. Unlike Declarative, Scripted Pipeline is effectively a general purpose DSL footnoteref:[dsl,Domain-specific language[86]] built with Groovy[87]. Most functionality provided by the Groovy language is made available to users of Scripted Pipeline, which means it can be a very expressive and flexible tool with which one can author continuous delivery pipelines.

Flow Control

Scripted Pipeline is serially executed from the top of a `Jenkinsfile` downwards, like most traditional scripts in Groovy or other languages. Providing flow control therefore rests on Groovy expressions, such as the `if/else` conditionals, for example:

[pipeline] —- // Scripted // node // Declarative // —-

Another way Scripted Pipeline flow control can be managed is with Groovy's exception handling support. When <<scripted-steps>> fail for whatever reason they throw an exception. Handling behaviors on-error must make use of the `try/catch/finally` blocks in Groovy, for example:

[pipeline] —- // Scripted // node // Declarative // —-

Steps

[[scripted-steps]]

As discussed at the start of this chapter, the most fundamental part of a Pipeline is the "step". Fundamentally, steps tell Jenkins *what* to do and serve as the basic building block for both Declarative and Scripted Pipeline syntax.

Scripted Pipeline does *not* introduce any steps which are specific to its syntax; Pipeline Steps reference contains a comprehensive list of steps provided by Pipeline and plugins.

Differences from plain Groovy

In order to provide *durability*, which means that running Pipelines can survive a restart of the Jenkins master, Scripted Pipeline must serialize data back to the master. Due to this design requirement, some Groovy idioms such as `collection.each { item -> /* perform operation */ }` are not fully supported. See https://issues.jenkins-ci.org/browse/JENKINS-27421[JENKINS-27421] and https://issues.jenkins-ci.org/browse/JENKINS-26481[JENKINS-26481] for more information.

[86] https://en.wikipedia.org/wiki/Domain-specific_language
[87] http://groovy-lang.org/syntax.html

Syntax Comparison

[[compare]]

When Jenkins Pipeline was first created, Groovy was selected as the foundation. Jenkins has long shipped with an embedded Groovy engine to provide advanced scripting capabilities for admins and users alike. Additionally, the implementors of Jenkins Pipeline found Groovy to be a solid foundation upon which to build what is now referred to as the "Scripted Pipeline" DSL. footnoteref:[dsl].

As it is a fully featured programming environment, Scripted Pipeline offers a tremendous amount of flexibility and extensibility to Jenkins users. The Groovy learning-curve isn't typically desirable for all members of a given team, so Declarative Pipeline was created to offer a simpler and more opinionated syntax for authoring Jenkins Pipeline.

Both are fundamentally the same Pipeline sub-system underneath. They are both durable implementations of "Pipeline as code." They are both able to use steps built into Pipeline or provided by plugins. Both are able to utilize Shared Libraries

Where they differ however is in syntax and flexibility. Declarative limits what is available to the user with a more strict and pre-defined structure, making it an ideal choice for simpler continuous delivery pipelines. Scripted provides very few limits, insofar that the only limits on structure and syntax tend to be defined by Groovy itself, rather than any Pipeline-specific systems, making it an ideal choice for power-users and those with more complex requirements. As the name implies, Declarative Pipeline encourages a declarative programming model. footnoteref:[declarative, Declarative Programming[88]] Whereas Scripted Pipelines follow a more imperative programming model. footnoteref:[imperative, Imperative Programming[89]]

[88]https://en.wikipedia.org/wiki/Declarative_programming
[89]https://en.wikipedia.org/wiki/Imperative_programming

Blue Ocean

[[blue-ocean]]

This chapter covers all aspects of Blue Ocean’s functionality, including how to:

*
get started with Blue Ocean - covers how to set up Blue
*
create a new Pipeline project,

- use Blue Ocean’s

Dashboard,

- use the

Activity view - where you can access

- use the

Pipeline run details view - where you can

- use the

Pipeline Editor to modify Pipelines as code,
Ocean in Jenkins and access the Blue Ocean interface, lists of your current and previously completed Pipeline/item runs, as well as your Pipeline project’s branches and any opened Pull Requests, access details (i.e. the console output) for a particular Pipeline/item run, and which are committed to source control.

This chapter is intended for Jenkins users of all skill levels, but beginners may need to refer to some sections of the Pipeline chapter to understand some topics covered in this Blue Ocean chapter.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

What is Blue Ocean?

[[blue-ocean-overview]]

Blue Ocean rethinks the user experience of Jenkins. Designed from the ground up for Jenkins Pipeline, but still compatible with freestyle jobs, Blue Ocean reduces clutter and increases clarity for every member of the team. Blue Ocean's main features include:

- *Sophisticated visualizations* of continuous delivery (CD) Pipelines,
- *Pipeline editor* - makes creation of Pipelines approachable by guiding the
- *Personalization* to suit the role-based needs of each member of the team.
- *Pinpoint precision* when intervention is needed and/or issues arise. Blue
- *Native integration for branch and pull requests*, enables maximum developer allowing for fast and intuitive comprehension of your Pipeline's status. user through an intuitive and visual process to create a Pipeline. Ocean shows where in the pipeline attention is needed, facilitating exception handling and increasing productivity. productivity when collaborating on code with others in GitHub and Bitbucket.

To start using Blue Ocean, see Getting started with Blue Ocean.

Frequently asked questions

Why does Blue Ocean exist?

The world has moved on from developer tools that are purely functional to developer tools being part of a "developer experience". That is to say, it is no longer about a single tool but the many tools developers use throughout the day and how they work together to achieve a workflow that is beneficial for the developer - this is "developer experience".

Developer tools companies like Heroku, Atlassian and Github have raised the bar for what is considered good developer experience, and developers are increasingly expecting exceptional design. In recent years, developers have become more rapidly attracted to tools that are not only functional but are designed to fit into their workflow seamlessly and are a joy to use. This shift represents a higher standard of design and user experience. Jenkins needs to rise to meet this higher standard.

Creating and visualising CD pipelines is something valuable for many Jenkins users and this is demonstrated in the 5+ plugins that the Jenkins community has created to meet their needs. This indicates a need to revisit how Jenkins currently expresses these concepts and consider delivery pipelines as a central theme to the Jenkins user experience.

It is not just CD concepts but the tools that developers use every day – Github, Bitbucket, Slack, HipChat, Puppet or Docker. It is about more than Jenkins – it is the developer workflow which surrounds Jenkins that spans multiple tools.

New teams have little time to learn how to assemble their own Jenkins experience – they want to improve their time to market by shipping better software faster. Assembling that ideal Jenkins experience is something we can work together as a community of Jenkins users and contributors to define. As time progresses, developers' expectations of good user experience changes and the mission of Blue Ocean enables the Jenkins project to respond.

The Jenkins community has poured its sweat and tears into building the most technically capable and extensible software automation tool in existence. Not doing anything to revolutionize the Jenkins developer experience today is just inviting someone else – in closed source – to do it.

Where is the name from?

The name Blue Ocean comes from the book link:https://en.wikipedia.org/wiki/Blue*Ocean*Strategy[Blue Ocean Strategy] where instead of looking at strategic problems within a contested space, you look at problems in the larger uncontested space. To put this more simply, consider this quote from ice hockey legend Wayne Gretzky: "skate to where the puck is going to be, not where it has been".

Does Blue Ocean support freestyle jobs?

Blue Ocean aims to deliver a great experience around Pipeline and be compatible with any freestyle jobs you already have configured on your Jenkins instance. However, you will not benefit from any of the features built for Pipelines – for example, Pipeline visualization.

As Blue Ocean is designed to be extensible, it is possible for the Jenkins community to extend Blue Ocean to support other job types in the future.

What does this mean for the Jenkins classic UI?

The intention is that as Blue Ocean matures, there will be fewer reasons for users to go back to the existing "classic UI". Read more about the classic UI in Getting started with Pipeline.

For example, early versions of Blue Ocean are mainly targeted at Pipeline jobs. You might be able to see your existing non-pipeline jobs in Blue Ocean but it might not be possible to configure them from the Blue Ocean UI for some time. This means users will have to jump back to the classic UI to configure items/projects/jobs other than Pipeline ones.

There are likely going to be more examples of this, which is why the classic UI will remain important in the long term.

What does this mean for my plugins?

Extensibility is a core feature of Jenkins. Therefore, being able to extend the Blue Ocean UI is important. The + `<ExtensionPoint name=..>` can be used in the markup of Blue Ocean, leaving places for plugins to contribute to the Blue Ocean UI - i.e. plugins can have their own Blue Ocean extension points, just like they can in the Jenkins classic UI. So far, Blue Ocean itself is implemented using these extension points.

Extensions are delivered by plugins as usual. However, plugin developers will need to include some additional JavaScript to hook into Blue Ocean's extension points and contribute to the Blue Ocean user experience.

What technologies are currently in use?

Blue Ocean is built as a collection of Jenkins plugins itself. There is one key difference - Blue Ocean provides both its own endpoint for HTTP requests and delivers up HTML/JavaScript via a different path, without the existing Jenkins UI markup/scripts. React.js and ES6 are used to deliver the JavaScript components of Blue Ocean. Inspired by this excellent open source project (read more about this in the Building Plugins for React Apps[90] blog post), an `<ExtensionPoint>` pattern was established that allows extensions to come from any Jenkins plugin (only with JavaScript) and should they fail to load, have their failures isolated.

Where can I find the source code?

The source code can be found on Github:

*

Blue Ocean[91]

*

Jenkins Design Language[92]

Join the community

There a few ways you can join the community:

. Chat with the community and development team on Gitter image:https://badges.gitter.im/jenkinsci/blueocean-plugin.svg[link="https://gitter.im/jenkinsci/blueocean-plugin?utm_source=badge&utm_medium=badge&utm_-campaign=pr-badge"] . Request features or report bugs against the `blueocean-plugin` component in JIRA[93]. . Subscribe and ask questions on the Jenkins Users mailing list[94]. . Developer? We've labeled a few issues[95] that are great for anyone wanting to get started developing Blue Ocean. Don't forget to drop by the Gitter chat and introduce yourself!

[90]https://nylas.com/blog/react-plugins
[91]https://github.com/jenkinsci/blueocean-plugin
[92]https://github.com/jenkinsci/jenkins-design-language
[93]https://issues.jenkins-ci.org/
[94]https://groups.google.com/forum/#!forum/jenkinsci-users
[95]https://issues.jenkins-ci.org/issues/?filter=16142

Activity View

The Blue Ocean Activity View shows the all activity related to one Pipeline.

image:blueocean/activity/overview.png[Overview of the Activity View, role=center]

Navigation Bar

The Activity View includes the standard navigation bar at the top, with a local navigation bar below that. The local navigation bar includes:

- *Pipeline Name* - Clicking on this displays the
- *Favorites Toggle* - Clicking the "Favorite" symbol (a star outline "") adds a branch to the favorites list shown on the
- *Tabs*

default activity tab Dashboard's "Favorites" list for this user. (Activity, Branches, Pull Requests) - Clicking one of these will display that tab of the Activity View.

Activity

The default tab of the Activity View, the "Activity" tab, shows a list of the latest completed or in-progress Runs. Each line in the list shows the status of the Run, id number, commit information, duration, and when the run completed. Clicking on a Run will bring up the Pipeline Run Details for that Run. "In Progress" Runs can be aborted from this list by clicking on the "Stop" symbol (a square "" inside a circle). Runs that have completed can be re-run by clicking the "Re-run" symbol (a counter-clockwise arrow ""). The list can be filtered by branch or pull request by clicking on the "branch" drop-down in the list header.

This list does not allow runs to be edited or marked as favorites. Those actions can be done from the "branches" tab.

Branches

The "Branches" tab shows a list of all branches that have a completed or in-progress Run in the current Pipeline. Each line in the list corresponds to a branch in source control, footnoteref:[scm, https://en.wikipedia.org/wiki/Source*control*management] showing overall health of the branch based on recent runs, status of the most recent run, id number, commit information, duration, and when the run completed.

image:blueocean/activity/branches.png[Branches Tab of Activity View, role=center]

Clicking on a branch in this list will bring up the Pipeline Run Details for the latest completed or in-progress Run of that branch. “In Progress” runs can be aborted from this list by clicking on the “Stop” symbol (a square “” inside a circle). Pull requests whose latest run has completed can be run again by clicking the “Play” symbol (a triangle “” inside a circle). Clicking the “Edit” symbol (similar to a pencil “”) opens the pipeline editor on the Pipeline for that brach. Clicking the “Favorite” symbol (a star outline “”) adds a branch to the favorites list shown on the Dashboard’s “Favorites” list for this user. A favorite branch will show a solid star “” and clicking it removes this branch from the favorites.

Pull Requests

The “Pull Requests” tab shows a list of all Pull Requests for the current Pipeline that have a completed or in-progress Run. (Some source control systems call these “Merge Requests”, others do not support them at all.) Each line in the list corresponds to a pull request in source control, showing the status of the most recent run, id number, commit information, duration, and when the run completed.

image:blueocean/activity/pull-requests.png[Activity Pull Requests view, role=center]

Blue Ocean displays pull requests separately from branches, but otherwise the Pull Requests list behaves similar to the Branches list. Clicking on a pull request in this list will bring up the Pipeline Run Details for the latest completed or in-progress Run of that pull request. “In Progress” runs can be aborted from this list by clicking on the “Stop” symbol (a square “” inside a circle). Pull requests whose latest run has completed can be run again by clicking the “Play” symbol (a triangle “” inside a circle). Pull request do not display “Heath Icons” and cannot be edited or marked as favorites.

NOTE: By default, when a Pull Request is closed, Jenkins will remove the Pipeline from Jenkins (to be cleaned up at a later date), and runs for that Pull Request will not longer be accessible from Jenkins. That can be changed by changing the configuration of the underlying Multi-branch Pipeline job.

Creating a Pipeline

Blue Ocean makes it easy to create a Pipeline project in Jenkins.

A Pipeline can be generated from an existing `Jenkinsfile` in source control, or you can use the Blue Ocean Pipeline editor to create a new Pipeline for you (as a `Jenkinsfile` that will be committed to source control).

Setting up your Pipeline project

To start setting up your Pipeline project in Blue Ocean, at the top-right of the Blue Ocean Dashboard, click the *New Pipeline* button.

[.boxshadow] image:blueocean/creating-pipelines/new-pipeline-button.png['New Pipeline Button',width=50%]

If your Jenkins instance is new or has no Pipeline projects or other items configured (and the Dashboard is empty), Blue Ocean displays a *Welcome to Jenkins* message box on which you can click the *Create a new Pipeline* button to start setting up your Pipeline project.

[.boxshadow] image:blueocean/creating-pipelines/create-a-new-pipeline-box.png['Welcome to Jenkins - Create a New Pipeline message box',width=50%]

You now have a choice of creating your new Pipeline project from a:

*
standard Git repository
*
repository on GitHub or GitHub Enterprise
*
repository on Bitbucket Cloud or
 Bitbucket Server

For a Git repository

To create your Pipeline project for a Git repository, click the *Git* button under *Where do you store your code?*

[.boxshadow] image:blueocean/creating-pipelines/where-do-you-store-your-code.png['Where do you store your code',width=70%]

In the *Connect to a Git repository* section, enter the URL for your Git repository in the *Repository URL* field.

[.boxshadow] image:blueocean/creating-pipelines/connect-to-a-git-repository.png[‘Connect to a Git repository’,width=70%]

You now need to specify a local or a remote repository from which to build your Pipeline project.

Local repository

If your URL is a local directory path (e.g. beginning with a forward slash `/` such as `/home/cloned-git-repos/my-git-` you can proceed to click the *Create Pipeline* button.

Blue Ocean will then scan your local repository’s branches for a `Jenkinsfile` and will commence a Pipeline run for each branch containing a `Jenkinsfile`. If Blue Ocean cannot find any `Jenkinsfile`, you will be prompted to begin creating one through the Pipeline editor.

Remote repository

Since the Pipeline editor saves edited Pipelines to Git repositories as `Jenkinsfiles`, Blue Ocean only supports connections to remote Git repositories over the SSH protocol.

If your URL is for a remote Git repository, then as soon as you begin typing the URL, starting with either:

- `ssh://` - e.g.
- `user@host:path/to/git/repo.git` - e.g. `ssh://gituser@git-server-url/git-server-repos-group/my-git-repo.git` + or `gituser@git-server-url:g`

Blue Ocean automatically generates an SSH public/private key pair (or presents you with an existing one) for your current/logged in Jenkins user. This credential is automatically registered in Jenkins with the following details for this Jenkins user:

- *Domain*: `blueocean-private-key-domain`
- *ID*: `jenkins-generated-ssh-key`
- *Name*: `<jenkins-username> (jenkins-generated-ssh-key)`

You need to ensure that this SSH public/private key pair has been registered with your Git server before continuing. If you have not already done this, follow these 2 steps. Otherwise, continue on.

. Configure the SSH public key component of this key pair (which you can copy and paste from the Blue Ocean interface) for the remote Git server’s user account (e.g. within the `authorized_keys` file of the machine’s `gituser/.ssh` directory). + [[continuing-on]] *Note:* This process allows your Jenkins user to access the repositories that your Git server’s user account (e.g. `gituser`) has access to. Read more about this in Setting Up the Server[96] of the Pro Git documentation[97]. . When done, return to the Blue Ocean interface.

[96]https://git-scm.com/book/en/v2/Git-on-the-Server-Setting-Up-the-Server
[97]https://git-scm.com/book/en/v2/

Click the *Create Pipeline* button.

Blue Ocean will then scan your local repository's branches for a `Jenkinsfile` and will commence a Pipeline run for each branch containing a `Jenkinsfile`. If Blue Ocean cannot find any `Jenkinsfile`, you will be prompted to begin creating one through the Pipeline editor.

For a repository on GitHub

To create your Pipeline project directly for a repository on GitHub, click the *GitHub* button under *Where do you store your code?*

[.boxshadow] image:blueocean/creating-pipelines/where-do-you-store-your-code.png['Where do you store your code',width=70%]

In the *Connect to GitHub* section, enter your GitHub access token into the *Your GitHub access token* field. + If you previously configured Blue Ocean to connect to GitHub using a personal access token, Blue Ocean takes you directly to the choosing your GitHub account/organization and repository steps below.

[.boxshadow] image:blueocean/creating-pipelines/connect-to-github.png['Connect to GitHub',width=70%]

If you do not have a GitHub access token, click the *Create an access key here* link to open GitHub to the *New personal access token* page.

Create your access token

- *Domain*: `blueocean-github-domain`
- *ID*: `github`
- *Name*: `+<jenkins-username>/****** (GitHub Access Token)+`

. In the new tab, sign in to your GitHub account (if necessary) and on the GitHub *New Personal Access Token* page, specify a brief *Token description* for your GitHub access token (e.g. `Blue Ocean`). + *Note:* An access token is usually an alphanumeric string that respresents your GitHub account along with permissions to access various GitHub features and areas through your GitHub account. The new access token process (triggered through the *Create an access key here* link above) has the appropriate permissions pre-selected, which Blue Ocean requires to access and interact with your GitHub account. . Scroll down to the end of the page and click *Generate token*. . On the resulting *Personal access tokens* page, copy your newly generated access token. . Back in Blue Ocean, paste the access token into the *Your GitHub access token* field and click *Connect*. + Your current/logged in Jenkins user now has access to your GitHub account (provided by your access token), so you can now choose your GitHub account/organization and repository. + Jenkins registers this credential with the following details for this Jenkins user:

Choose your GitHub account/organization and repository

At this point, Blue Ocean prompts you to choose your GitHub account or an organization you are a member of, as well as the repository it contains from which to build your Pipeline project.

- Your GitHub account to create a Pipeline project for one of your own GitHub
- An organization you are a member of to create a Pipeline project for a GitHub

. In the *Which organization does the repository belong to?* section, click either: repositories or one which you have forked from elsewhere on GitHub. repository located within this organization. . In the *Choose a repository* section, click the repository (within your GitHub account or organization) from which to build your Pipeline project. + *Tip:* If your list of repositories is long, you can filter this list using the *Search* option. [.boxshadow] image:blueocean/creating-pipelines/choose-a-repository.png['Choose a repository',width=70%] . Click *Create Pipeline.* + Blue Ocean will then scan your local repository's branches for a `Jenkinsfile` and will commence a Pipeline run for each branch containing a `Jenkinsfile`. If Blue Ocean cannot find any `Jenkinsfile`, you will be prompted to begin creating one through the Pipeline editor (by clicking *Create Pipeline* again). + *Note:* Under the hood, a Pipeline project created through Blue Ocean is actually "multibranch Pipeline". Therefore, Jenkins looks for the presence of at least one Jenkinsfile in any branch of your repository.

For a repository on Bitbucket Cloud

To create your Pipeline project directly for a Git or Mercurial repository on Bitbucket Cloud, click the *Bitbucket Cloud* button under *Where do you store your code?*

[.boxshadow] image:blueocean/creating-pipelines/where-do-you-store-your-code.png['Where do you store your code',width=70%]

In the *Connect to Bitbucket* section, enter your Bitbucket email address and password into the *Username* and *Password* fields, respectively. Note that:

- If you previously configured Blue Ocean to connect to Bitbucket with your
- If you entered these credentials, Jenkins registers them with the following
  email address and password, Blue Ocean takes you directly to the choosing your Bitbucket account/team and repository steps below. details for this Jenkins user: ** *Domain*: `blueocean-bitbucket-cloud-domain` ** *ID*: `bitbucket-cloud` ** *Name*: `+<bitbucket-user@email.address>/** (Bitbucket server credentials)+`

[.boxshadow] image:blueocean/creating-pipelines/connect-to-bitbucket.png['Connect to Bitbucket',width=70%]

Click *Connect* and your current/logged in Jenkins user will now have access to your Bitbucket account. You can now choose your Bitbucket account/team and repository.

Choose your Bitbucket account/team and repository

At this point, Blue Ocean prompts you to choose your Bitbucket account or a team you are a member of, as well as the repository it contains from which to build your Pipeline project.

- Your Bitbucket account to create a Pipeline project for one of your own
- A team you are a member of to create a Pipeline project for a Bitbucket

. In the *Which team does the repository belong to?* section, click either: Bitbucket repositories or one which you have forked from elsewhere on Bitbucket. repository located within this team. . In the *Choose a repository* section, click the repository (within your Bitbucket account or team) from which to build your Pipeline project. + *Tip:* If your list of repositories is long, you can filter this list using the *Search* option. [.boxshadow] image:blueocean/creating-pipelines/choose-a-repository.png['Choose a repository',width=70%] . Click *Create Pipeline.* + Blue Ocean will then scan your local repository's branches for a `Jenkinsfile` and will commence a Pipeline run for each branch containing a `Jenkinsfile`. If Blue Ocean cannot find any `Jenkinsfile`, you will be prompted to begin creating one through the Pipeline editor (by clicking *Create Pipeline* again). + *Note:* Under the hood, a Pipeline project created through Blue Ocean is actually "multibranch Pipeline". Therefore, Jenkins looks for the presence of at least one Jenkinsfile in any branch of your repository.

Dashboard

Blue Ocean's "Dashboard" is the default view shown when you open Blue Ocean and shows an overview of all Pipeline projects configured on a Jenkins instance.

The Dashboard consists of a blue navigation bar at the top, the Pipelines list, as well as the Favorites list.

[.boxshadow] image:blueocean/dashboard/overview.png[Overview of the Dashboard,role=center,width=100%]

Navigation bar

The Dashboard includes the blue-colored navigation bar along the top of the interface.

This bar is divided into two sections - a common section along the top and a contextual section below. The contextual section changes depending on the current Blue Ocean page you are viewing.

When viewing the Dashboard, the navigation bar's contextual section includes the:

- *Search pipelines* field, to filter the

Pipelines list

- *New Pipeline* button, which begins the
  to show items containing the text you enter into this field. create a Pipeline process.

Pipelines list

The "Pipelines" list is the Dashboard's default list and upon accessing Blue Ocean for the first time, this is the only list shown on the Dashboard.

This list shows the overall state of each Pipeline configured on the Jenkins instance (which can also include other Jenkins items). For a given item in this list, the following information is indicated:

- The item's *NAME*,
- The item's

HEALTH,

- The numbers of **BRANCH**es and pull requests (**PR**s) of the
- A star indicating whether or not the default/main branch of the item has been
  Pipeline's source control repository which are passing or failing, and manually added to your current Jenkins user's <<favorites-list>>.

Clicking on an item's star will toggle between:

- Adding the default branch of the item's repository to your current user's
- Removing the item's default branch from this list (indicated by an outlined
  Favorites list (indicated by a solid ""), and "").

Clicking on an item in the Pipelines list will display that item's Activity View.

Favorites list

The *Favorites* list appears above the Dashboard's default <<pipelines-list>> when at least one Pipeline/item is present in your user's Favorites list.

This list provides key information and actions for a core subset of your user's accessible items in the <<pipelines-list>>. This key information includes the current run status for an item and its repository's branch, as well as other details about the item's run, including the name of the branch, the initial part of the commit hash and the time of the last run. Items in this list also include clickable icons to run or re-run the item on the repository branch indicated.

You should only add an item (or one of the repository's specific branches) to your Favorites list if you need to examine that item's branch on a regular basis. Adding an item's specific branch to your Favorites list can be done through the item's Activity View.

Blue Ocean automatically adds branches or PRs to this list when a they contain a run that has changes authored by the current user.

You can also manually remove items from your Favorites list by clicking on the solid "" in this list. When the last item is removed from this list, the list is removed from the interface.

Clicking on an item in the Favorites list will open the Pipeline run details for latest run on the repository branch or PR indicated.

Health icons

[[pipeline-health]]

Blue Ocean represents the overall health of a Pipeline/item or one of its repository's branches using weather icons, which change depending on the number of recent builds that have passed.

Health icons on the Dashboard represent overall Pipeline health, whereas the health icons in the Branches tab of the Activity View represent the overall health for each branch.

.Health icons (best to worst) |=== |Icon |Health

|image:blueocean/icons/weather/sunny.svg[Sunny,role=center] |*Sunny*, more than 80% of Runs passing

|image:blueocean/icons/weather/partially-sunny.svg[Partially Sunny,role=center] |*Partially Sunny*, 61% to 80% of Runs passing

|image:blueocean/icons/weather/cloudy.svg[Cloudy,role=center,width=100] |*Cloudy*, 41% to 60% of Runs passing

|image:blueocean/icons/weather/raining.svg[Raining,role=center] |*Raining*, 21% to 40% of Runs passing

|image:blueocean/icons/weather/storm.svg[Storm,role=center] |*Storm*, less than 21% of Runs passing |===

Run status

Blue Ocean represents the run status of a Pipeline/item or one of its repository's branches using a consistent set of icons throughout.

.Run status icons |=== |Icon |Status

|image:blueocean/dashboard/status-in-progress.png["In Progress" Status Icon,role=center] |*In Progress*

|image:blueocean/dashboard/status-passed.png["Passed" Status Icon,role=center] |*Passed*

|image:blueocean/dashboard/status-unstable.png["Unstable" Status Icon,role=center] |*Unstable*

|image:blueocean/dashboard/status-failed.png["Failed" Status Icon,role=center] |*Failed*

|image:blueocean/dashboard/status-aborted.png["Aborted" Status Icon,role=center] |*Aborted* |===

Getting started with Blue Ocean

This section describes how to get started with Blue Ocean in Jenkins. It includes instructions for setting up Blue Ocean on your Jenkins instance as well as how to access the Blue Ocean UI and return to the Jenkins classic UI.

Installing Blue Ocean

Blue Ocean can be installed using the following methods:

- As a suite of plugins on an
- As part of

Jenkins in Docker.
existing Jenkins instance, or

On an existing Jenkins instance

When Jenkins is installed on most platforms, the plugin:blueocean[Blue Ocean plugin] and all its other dependent plugins (which form the Blue Ocean “suite of plugins”) are not installed by default.

To install the Blue Ocean suite of plugins on an existing Jenkins instance, your Jenkins instance must be running Jenkins 2.7.x or later.

Plugins can be installed on a Jenkins instance by any Jenkins user who has the *Administer* permission (set through *Matrix-based security*). Jenkins users with this permission can also configure the permissions of other users on their system. Read more about this in the Authorization section of Managing Security.

To install the Blue Ocean suite of plugins to your Jenkins instance:

- There is no need to select the check boxes of the other plugins in this
- If you chose the *Install without restart* button, you may need to restart

. If required, ensure you are logged in to Jenkins (as a user with the *Administer* permission). . From the Jenkins home page (i.e. the Dashboard of the Jenkins classic UI), click *Manage Jenkins* on the left and then *Manage Plugins* in the center. . Click the *Available* tab and type `blue ocean` into the *Filter* text box, which filters the list of plugins to those whose name and/or description contains the words "blue" and "ocean". + [.boxshadow] image:blueocean/intro/blueocean-plugins-filtered.png[alt="Blue Ocean plugins filtered",width=100%] . Select the *Blue Ocean* plugin's check box near the top of the the *Install* column and then click either the *Download now and install after restart* button (recommended) or the *Install without restart* button at the the end of the page. + *Notes:* filtered list because the main *Blue Ocean* plugin has other plugin dependencies (constituting the Blue Ocean suite of plugins) which will automatically be selected and installed when you click one of these "Install" buttons. Jenkins in order to gain full Blue Ocean functionality.

Read more about how to install and manage plugins in the Managing Plugins page.

Blue Ocean requires no additional configuration after installation, and existing Pipelines projects and other items such as freestyle projects will continue to work as usual.

Be aware, however, that the first time a Pipeline is created in Blue Ocean for a specific Git server (i.e. GitHub, Bitbucket or an ordinary Git server), Blue Ocean prompts you for credentials to access your repositories on the Git server in order to create Pipelines based on those repositories. This is required since Blue Ocean can write `Jenkinsfiles` to your repositories.

As part of Jenkins in Docker

The Blue Ocean suite of plugins are also bundled with Jenkins as part of a Jenkins Docker image (`jenkinsci/blueocean`[98]), which is available from the Docker Hub repository[99].

Read more about running Jenkins and Blue Ocean this way in the Docker section of the Installing Jenkins page.

Accessing Blue Ocean

Once a Jenkins environment has Blue Ocean installed, after logging in to the Jenkins classic UI, you can access the Blue Ocean UI by clicking *Open Blue Ocean* on the left.

[.boxshadow] image:blueocean/intro/open-blue-ocean-link.png[alt="Open Blue Ocean link",width=20%]

Alternatively, you can access Blue Ocean directly by appending `/blue` to the end of your Jenkins server's URL - e.g. `\https://jenkins-server-url/blue`.

If your Jenkins instance:

- already has existing Pipeline projects or other items present, then the
- is new or has no Pipeline projects or other items configured, then Blue Ocean Blue Ocean Dashboard is displayed. displays a *Welcome to Jenkins* box with a *Create a new Pipeline* button you can use to begin creating a new Pipeline project. Read more about this in Creating a Pipeline. + [.boxshadow] image:blueocean/creating-pipelines/create-a-new-pipeline-box.png['Welcome to Jenkins - Create a New Pipeline message box',width=50%]

[98] https://hub.docker.com/r/jenkinsci/blueocean/
[99] https://hub.docker.com/

Navigation bar

The Blue Ocean UI has a navigation bar along the top of its interface, which allows you to access the different views and other features of Blue Ocean.

Th navigation bar is divided into two sections - a common section along the top of most Blue Ocean views and a contextual section below. The contextual section is specific to the current Blue Ocean page you are viewing.

The navigation bar's common section includes the following buttons:

- *Jenkins* logo - takes you to the

Dashboard, or reloads

- *Pipelines* - also takes you to the Dashboard, or does nothing if you are
- *Administration* - takes you to the *

Manage Jenkins* page

- *Go to classic* icon - takes you back to the Jenkins classic UI. Read more
- *Logout* - Logs out your current Jenkins user and returns to the Jenkins login
  this page if you are already viewing it. already viewing the Dashboard. This button serves a different purpose when you are viewing a Pipeline run details page. of the Jenkins classic UI. + *Note:* This button is not available if your Jenkins user does not have the *Administer* permission (set through *Matrix-based security*). Read more about this in the Authorization section of Managing Security. about this in <<switching-to-the-classic-ui>>. page.

Views that use the standard navigation bar will add another bar below it with options specific to that view. Some views replace the common navigation bar with one specifically suited to that view.

Switching to the classic UI

Blue Ocean does not support some legacy or administrative features of Jenkins that are necessary to some users.

If you need to leave the Blue Ocean user experience to access these features, click the *Go to classic* icon at the top of common section of Blue Ocean's navigation bar.

[.boxshadow] image:blueocean/intro/go-to-classic-icon.png[alt="Go to classic icon",width=5%]

Clicking this button takes you to the equivalent page in the Jenkins classic UI, or the most relevant classic UI page that parallels the current page in Blue Ocean.

Pipeline Editor

The Blue Ocean Pipeline Editor is the simplest way for anyone to get started with creating Pipelines in Jenkins. It's also a great way for existing Jenkins users to start adopting Pipeline.

The editor allows users to create and edit Declarative Pipelines, add stages and parallelized tasks that can run at the same time, depending on their needs. When finished, the editor saves the Pipeline to a source code repository as a `Jenkinsfile`. If the Pipeline needs to be changed again, Blue Ocean makes it easy to jump back in into the visual editor to modify the Pipeline at any time.

image:blueocean/editor/overview.png[Pipeline Editor, role=center]

Starting the editor

To use the editor a user must first have created a pipeline in Blue Ocean or have one or more existing Pipelines already created in Jenkins. If editing an existing pipeline, the credentials for that pipeline must allow pushing of changes to the target repository.

The editor can be launched via:

- Dashboard "New Pipeline" button
- Activity View for Single Run
- Pipeline Run Details

Limitations

- SCM-based Declarative Pipelines only
- Credentials must have write permission
- Does not have full parity with Declarative Pipeline
- Pipeline re-ordered and comments removed

Navigation bar

The Pipeline Editor includes the standard navigation bar at the top, with a local navigation bar below that. The local navigation bar includes:

- *Pipeline Name* - This will include the branch depending or how
- *Cancel* - Discard changes made to the pipeline.
- *Save* - Open the

Save Pipeline Dialog.

Pipeline settings

By default, the right side of editor shows the “Pipeline Settings”. This sheet can be accessed by clicking anywhere in the Stage editor that is not a Stage or one of the “Add Stage” buttons.

Agent

The “Agent” section controls what agent the Pipeline will use. This is the same as the “agent” directive.

Environment

The “Environment” sections lets us set environment variables for the Pipeline. This is the same as the “environment” directive.

Stage editor

The left side editor screen contains the Stage editor, used for creating the stages of a Pipeline.

image:blueocean/editor/stage-editor-basic.png[Stage editor simple, role=center]

Stages can be added to the Pipeline by clicking the “+” button to the right of an existing stage. Parallel stages can be added by clicking the “+” button below an existing Stage. Stages can be deleted using the context menu in the stage configuration sheet.

The Stage editor will display the name of each Stage once it has been set. Stages that contain incomplete or invalid information will display a warning symbol. Pipelines can have validation errors while they are being edited, but cannot be saved until the errors are fixed.

image:blueocean/editor/stage-editor-error.png[Stage editor with error, role=center]

Stage configuration

Selecting a stage in the Stage editor will open the “Stage Configuration” sheet on the right side. Here we can can change the name of the Stage, delete the Stage, and add steps to the Stage.

image:blueocean/editor/stage-configuration.png[Stage Configuration, role=center]

The name of the Stage can be set at the top of the Stage Configuration sheet. The context menu (three dots on the upper right), can be used to delete the current stage. Clicking “Add step” will display the list of available Steps types with a search bar at the top. Steps can be deleted using the context context menu in the step configuration sheet. Adding a step or selecting an existing step will open the step configuration sheet.

image:blueocean/editor/step-list.png[Step list filtered by ‘file’, role=center]

Step configuration

Selecting a step from the Stage configuration sheet will open the Step Configuration sheet.

image:blueocean/editor/step-configuration.png[Step configuration for JUnit step, role=center]

This sheet will differ depending on the step type, containing whatever fields or controls are needed. The name of the Step cannot be changed. The context menu (three dots on the upper right), can be used to delete the current step. Fields that contain incomplete or invalid information will display a warning symbol. Pipelines can have validation errors while they are being edited, but cannot be saved until the errors are fixed.

image:blueocean/editor/step-error.png[Step configuration with error, role=center]

Save Pipeline dialog

In order to be run, changes to a Pipeline must be saved in source control The “Save Pipeline” dialog controls saving of changes to source control.

image:blueocean/editor/save-pipeline.png[Save Pipeline Dialog, role=center]

A helpful description of the changes can be added or left blank. The dialog also supports saving changes the same branch or entering a new branch to save to. Clicking on “Save & run” will save any changes to the Pipeline as a new commit, will start a new Pipeline Run based on those changes, and will navigate to the Activity View for this pipeline.

Pipeline Run Details View

The Blue Ocean Pipeline Run Details view shows the information related to a single Pipeline Run and allows users to edit or replay that run. Below is a detailed overview of the parts of the Run Details view.

image:blueocean/pipeline-run-details/overview.png[Overview of the Pipeline Run Details, role=center]

. *Run Status* - This icon, along with the background color of the top menu bar, indicates the status of this Pipeline run. . *Pipeline Name* - The name of this run's Pipeline. . *Run Number* - The id number for this Pipeline run. Id numbers unique for each Branch (and Pull Request) of a Pipeline. . *Tab Selector* - View one of the detail tabs for this run. The default is "Pipeline". . *Re-run Pipeline* - Execute this run's Pipeline again. . *Edit Pipeline* - Open this run's Pipeline in the Pipeline Editor. . *Go to Classic* - Switch to the "Classic" UI view of the details for this run. . *Close Details* - This closes the Details view and returns the user to the <<activity, Activity view> for this Pipeline. . *Branch* or *Pull Request* - the branch or pull request for this run. . *Commit Id* - Commit id for this run. . *Duration* - The duration of this run. . *Completed Time* - How long ago the this run completed. . *Change Author* - Names of the authors with changes in this run. . *Tab View* - Shows the information for the selected tab.

Pipeline Run Status

Blue Ocean makes it easy to see the status of the current Pipeline Run by changing the color of the top menu bar to match the status: blue for "In progress", green for "Passed", yellow for "Unstable", red for "Failed", and gray for "Aborted".

Special cases

Blue Ocean is optimized for working with Pipelines in Source Control, but it can display details for other kinds of projects as well. Blue Ocean offers the same tabs for all supported projects types, but those tabs may display different information.

Pipelines outside of Souce Control

For Pipelines that are not based on Source Control, Blue Ocean still shows the "Commit Id", "Branch", and "Changes", but those fields are left blank. In this case, the top menu bar does not include the "Edit" option.

Freestyle Projects

For Freestyle projects, Blue Ocean still offers the same tabs, but the Pipeline tab only shows the console log output. The “Rerun” or “Edit” options are also not shown in the top menu bar.

Matrix projects

Matrix projects are not supported in Blue Ocean. Viewing a Matrix project will redirect to the “Classic UI” view for that project.

Tabs

Each of the tabs of the Run Detail view provides information on a specific aspect of a run.

Pipeline

This is the default tab and gives an overall view of the flow of this Pipeline Run. It shows each stage and parallel branch, the steps in those stages, and the console output from those steps. The overview image above shows a successful Pipeline run. If a particular step during the run fails, this tab will automatically default to showing the console log from the failed step. The image below shows a failed Run.

image:blueocean/pipeline-run-details/pipeline-failed.png[Failed Run, role=center]

Changes

image:blueocean/pipeline-run-details/changes-one-change.png[List of Changes for a Run, role=center]

Tests

The “Tests” tab shows information about test results for this run. This tab will only contain information if a test result publishing step, such as the “Publish JUnit test results” (`junit`) step. If no results are recorded this table will say that, If all tests pass, this tab will report the total number of passing tests. In the case of failures, the tab will display logs details from the failures as shown below.

image:blueocean/pipeline-run-details/tests-unstable.png[Test Results for Unstable Run, role=center]

When the previous Run had failures and the current run fixes those failures, this tab will note the fixed texts and display their logs as well.

image:blueocean/pipeline-run-details/tests-fixed.png[Test Results for Fixed Run, role=center]

Artifacts

The “Artifacts” tabs show a list of any artifacts saved using the “Archive Artifacts” (`archive`) step. Clicking on a item in the list will download it. The full output log from the Run can be downloaded from this list.

image:blueocean/pipeline-run-details/artifacts-list.png[List of Artifacts from a Run, role=center]

Managing Jenkins

This chapter cover how to manage and configure Jenkins masters and nodes.

This chapter is intended for Jenkins administrators. More experienced users may find this information useful, but only to the extent that they will understand what is and is not possible for administrators to do. Individual sections may assume knowledge of information from previous sections, but such assumptions will be explicitly called out and cross-referenced.

If you are a system administrator and want learn how to back-up, restore, maintain as Jenkins servers and nodes, see Jenkins System Administration.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

Jenkins CLI

Jenkins has a built-in command line interface that allows users and administrators to access Jenkins from a script or shell environment. This can be convenient for scripting of routine tasks, bulk updates, troubleshooting, and more.

The command line interface can be accessed over SSH or with the Jenkins CLI client, a `.jar` file distributed with Jenkins.

[WARNING] ==== Use of the CLI client distributed with Jenkins 2.53 and older and Jenkins LTS 2.46.1 and older is **not recommended** for security reasons.

The client distributed with Jenkins 2.54 and newer and Jenkins LTS 2.46.2 and newer is considered secure in its default (`-http`) or `-ssh` modes, as is using the standard `ssh` command.

Jenkins 2.165 and newer no longer supports the old (`-remoting`) mode in either the client or server. ====

Using the CLI over SSH

[[ssh]]

In a new Jenkins installation, the SSH service is disabled by default. Administrators may choose to set a specific port or ask Jenkins to pick a random port in the Configure Global Security page. In order to determine the randomly assigned SSH port, inspect the headers returned on a Jenkins URL, for example:

```
% curl -Lv https://JENKINS_URL/login 2>&1 | grep -i 'x-ssh-endpoint'
< X-SSH-Endpoint: localhost:53801
%
```

With the random SSH port (`53801` in this example), and <<Authentication>> configured, any modern SSH client may securely execute CLI commands.

Authentication

Whichever user used for authentication with the Jenkins master must have the `Overall/Read` permission in order to *access* the CLI. The user may require additional permissions depending on the commands executed.

Authentication relies on SSH-based public/private key authentication. In order to add an SSH public key for the appropriate user, navigate to `https://JENKINS_URL/user/USERNAME/configure` and paste an SSH public key into the appropriate text area.

image::managing/cli-adding-ssh-public-keys.png["Adding public SSH keys for a user", role=center]

Common Commands

Jenkins has a number of built-in CLI commands which can be found in every Jenkins environment, such as `build` or `list-jobs`. Plugins may also provide CLI commands; in order to determine the full list of commands available in a given Jenkins environment, execute the CLI `help` command:

```
% ssh -l kohsuke -p 53801 localhost help
```

The following list of commands is not comprehensive, but it is a useful starting point for Jenkins CLI usage.

build

One of the most common and useful CLI commands is `build`, which allows the user to trigger any job or Pipeline for which they have permission.

The most basic invocation will simply trigger the job or Pipeline and exit, but with the additional options a user may also pass parameters, poll SCM, or even follow the console output of the triggered build or Pipeline run.

```
% ssh -l kohsuke -p 53801 localhost help build

java -jar jenkins-cli.jar build JOB [-c] [-f] [-p] [-r N] [-s] [-v] [-w]
Starts a build, and optionally waits for a completion.  Aside from general
scripting use, this command can be used to invoke another job from within a
build of one job.  With the -s option, this command changes the exit code based
on the outcome of the build (exit code 0 indicates a success) and interrupting
the command will interrupt the job.  With the -f option, this command changes
the exit code based on the outcome of the build (exit code 0 indicates a
success) however, unlike -s, interrupting the command will not interrupt the
job (exit code 125 indicates the command was interrupted).  With the -c option,
a build will only run if there has been an SCM change.
 JOB : Name of the job to build
 -c  : Check for SCM changes before starting the build, and if there's no
       change, exit without doing a build
 -f  : Follow the build progress. Like -s only interrupts are not passed
       through to the build.
 -p  : Specify the build parameters in the key=value format.
 -s  : Wait until the completion/abortion of the command. Interrupts are passed
       through to the build.
 -v  : Prints out the console output of the build. Use with -s
 -w  : Wait until the start of the command
% ssh -l kohsuke -p 53801 localhost build build-all-software -f -v
Started build-all-software #1
Started from command line by admin
Building in workspace /tmp/jenkins/workspace/build-all-software
[build-all-software] $ /bin/sh -xe /tmp/hudson1100603797526301795.sh
+ echo hello world
hello world
Finished: SUCCESS
Completed build-all-software #1 : SUCCESS
%
```

console

Similarly useful is the `console` command, which retrieves the console output for the specified build or Pipeline run. When no build number is provided, the `console` command will output the last completed build's console output.

```
% ssh -l kohsuke -p 53801 localhost help console

java -jar jenkins-cli.jar console JOB [BUILD] [-f] [-n N]
Produces the console output of a specific build to stdout, as if you are doing 'cat \
build.log'
 JOB   : Name of the job
 BUILD : Build number or permalink to point to the build. Defaults to the last
         build
 -f    : If the build is in progress, stay around and append console output as
         it comes, like 'tail -f'
 -n N  : Display the last N lines
% ssh -l kohsuke -p 53801 localhost console build-all-software
Started from command line by kohsuke
Building in workspace /tmp/jenkins/workspace/build-all-software
[build-all-software] $ /bin/sh -xe /tmp/hudson1100603797526301795.sh
+ echo hello world
yes
Finished: SUCCESS
%
```

who-am-i

The `who-am-i` command is helpful for listing the current user's credentials and permissions available to the user. This can be useful when debugging the absence of CLI commands due to the lack of certain permissions.

```
% ssh -l kohsuke -p 53801 localhost help who-am-i

java -jar jenkins-cli.jar who-am-i
Reports your credential and permissions.
% ssh -l kohsuke -p 53801 localhost who-am-i
Authenticated as: kohsuke
Authorities:
  authenticated
%
```

Using the CLI client

While the SSH-based CLI is fast and covers most needs, there may be situations where the CLI client distributed with Jenkins is a better fit. For example, the default transport for the CLI client is HTTP which means no additional ports need to be opened in a firewall for its use.

Downloading the client

The CLI client can be downloaded directly from a Jenkins master at the URL `/jnlpJars/jenkins-cli.jar`, in effect `https://JENKINS_URL/jnlpJars/jenkins-cli.jar`

While a CLI `.jar` can be used against different versions of Jenkins, should any compatibility issues arise during use, please re-download the latest `.jar` file from the Jenkins master.

Using the client

The general syntax for invoking the client is as follows:

```
java -jar jenkins-cli.jar [-s JENKINS_URL] [global options...] command [command opti\
ons...] [arguments...]
```

The `JENKINS_URL` can be specified via the environment variable `$JENKINS_URL`. Summaries of other general options can be displayed by running the client with no arguments at all.

Client connection modes

There are two basic modes in which the client may be used, selectable by global option: `-http` and `-ssh`.

HTTP connection mode

This is the default mode, though you may pass the `-http` option explicitly for clarity.

Authentication is preferably with an `-auth` option, which takes a `username:apitoken` argument. Get your API token from `/me/configure`:

```
java -jar jenkins-cli.jar [-s JENKINS_URL] -auth kohsuke:abc1234ffe4a command ...
```

(Actual passwords are also accepted, but this is discouraged.)

You can also precede the argument with `@` to load the same content from a file:

```
java -jar jenkins-cli.jar [-s JENKINS_URL] -auth @/home/kohsuke/.jenkins-cli command\
 ...
```

[WARNING] ==== For security reasons the use of a file to load the authentication credentials is the recommended authentication way. ====

An alternative authentication method is to configure environment variables in a similar way as the `$JENKINS_URL` is used. The `username` can be specified via the environment variable `$JENKINS*USER*ID` while the `apitoken` can be specified via the variable `$JENKINS*API*TOKEN`. Both variables have to be set all at once.

```
export JENKINS_USER_ID=kohsuke
export JENKINS_API_TOKEN=abc1234ffe4a
java -jar jenkins-cli.jar [-s JENKINS_URL] command ...
```

In case these environment variables are configured you could still override the authentication method using different credentials with the `-auth` option, which takes preference over them.

Generally no special system configuration need be done to enable HTTP-based CLI connections. If you are running Jenkins behind an HTTP(S) reverse proxy, ensure it does not buffer request or response bodies.

[WARNING] ==== The HTTP(S) connection mode of the CLI does not work correctly behind an Apache HTTP reverse proxy server using mod_proxy. Workarounds include using a different reverse proxy such as Nginx or HAProxy, or using the SSH connection mode where possible. See JENKINS-47279[100]. ====

SSH connection mode

Authentication is via SSH keypair. You must select the Jenkins user ID as well:

[100]https://issues.jenkins-ci.org/browse/JENKINS-47279

```
java -jar jenkins-cli.jar [-s JENKINS_URL] -ssh -user kohsuke command ...
```

In this mode, the client acts essentially like a native `ssh` command.

By default the client will try to connect to an SSH port on the same host as is used in the `JENKINS_-URL`. If Jenkins is behind an HTTP reverse proxy, this will not generally work, so run Jenkins with the system property `-Dorg.jenkinsci.main.modules.sshd.SSHD.hostName=ACTUALHOST` to define a hostname or IP address for the SSH endpoint.

Common Problems with the CLI client

There are a number of common problems that may be experienced when running the CLI client.

Server key did not validate

You may get the error below and find a log entry just below that concerning `mismatched keys`:

```
org.apache.sshd.common.SshException: Server key did not validate
    at org.apache.sshd.client.session.AbstractClientSession.checkKeys(AbstractClient\
Session.java:523)
    at org.apache.sshd.common.session.helpers.AbstractSession.handleKexMessage(Abstr\
actSession.java:616)
    ...
```

This means your SSH configuration does not recognize the public key presented by the server. It's often the case when you run Jenkins in dev mode and multiple instances of the application are run under the same SSH port over time.

In a development context, access your `~/.ssh/known_hosts` (or in `C:/Users/<your_name>/.ssh/known_-hosts` for Windows) and remove the line corresponding to your current SSH port (e.g. `[localhost]:3485`). In a production context, check with the Jenkins administrator if the public key of the server changed recently. If so, ask the administrator to do the the steps described above.

UsernameNotFoundException

If your client displays a stacktrace that looks like:

```
org.acegisecurity.userdetails.UsernameNotFoundException: <name_you_used>
    ...
```

This means your SSH keys were recognized and validated against the stored users but the username is not valid for the security realm your application is using at the moment. This could occur when you were using the Jenkins database initially, configured your users, and then switched to another security realm (like LDAP, etc.) where the defined users do not exist yet.

To solve the problem, ensure your users exist in your configured security realm.

Troubleshooting logs

To get more information about the authentication process:

. Go into *Manage Jenkins* > *System Log* > *Add new log recorder*. . Enter any name you want and click on *Ok*. . Click on *Add* . Type `org.jenkinsci.main.modules.sshd.PublicKeyAuthenticatorImpl` (or type `PublicKeyAuth` and then select the full name) . Set the level to *ALL*. . Repeat the previous three steps for `hudson.model.User` . Click on *Save*

When you try to authenticate, you can then refresh the page and see what happen internally.

Managing Nodes

Managing Plugins

Plugins are the primary means of enhancing the functionality of a Jenkins environment to suit organization- or user-specific needs. There are over a thousand different plugins[101] which can be installed on a Jenkins master and to integrate various build tools, cloud providers, analysis tools, and much more.

Plugins can be automatically downloaded, with their dependencies, from the Update Center. The Update Center is a service operated by the Jenkins project which provides an inventory of open source plugins which have been developed and maintained by various members of the Jenkins community.

This section will cover everything from the basics of managing plugins within the Jenkins web UI, to making changes on the master's file system.

Installing a plugin

Jenkins provides a couple of different methods for installing plugins on the master:

. Using the "Plugin Manager" in the web UI. . Using the Jenkins CLI `install-plugin` command.

Each approach will result in the plugin being loaded by Jenkins but may require different levels of access and trade-offs in order to use.

The two approaches require that the Jenkins master be able to download meta-data from an Update Center, whether the primary Update Center operated by the Jenkins project footnoteref:[uc, https://updates.jenkins.io], or a custom Update Center.

The plugins are packaged as self-contained `.hpi` files, which have all the necessary code, images, and other resources which the plugin needs to operate successfully.

From the web UI

The simplest and most common way of installing plugins is through the *Manage Jenkins* > *Manage Plugins* view, available to administrators of a Jenkins environment.

Under the *Available* tab, plugins available for download from the configured Update Center can be searched and considered:

image::managing/plugin-manager-available.png["Available tab in the Plugin Manager", role=center]

Most plugins can be installed and used immediately by checking the box adjacent to the plugin and clicking *Install without restart.*

[101]https://plugins.jenkins.io

```
If the list of available plugins is empty, the master might be incorrectly
configured or has not yet downloaded plugin meta-data from the Update Center.
Clicking the *Check now* button will force Jenkins to attempt to contact its
configured Update Center.
```

Using the Jenkins CLI

[[install-with-cli]]

Administrators may also use the Jenkins CLI which provides a command to install plugins. Scripts to manage Jenkins environments, or configuration management code, may need to install plugins without direct user interaction in the web UI. The Jenkins CLI allows a command line user or automation tool to download a plugin and its dependencies.

```
java -jar jenkins-cli.jar -s http://localhost:8080/ install-plugin SOURCE ... [-depl\
oy] [-name VAL] [-restart]

Installs a plugin either from a file, an URL, or from update center.

 SOURCE    : If this points to a local file, that file will be installed. If
             this is an URL, Jenkins downloads the URL and installs that as a
             plugin.Otherwise the name is assumed to be the short name of the
             plugin in the existing update center (like "findbugs"),and the
             plugin will be installed from the update center.
 -deploy   : Deploy plugins right away without postponing them until the reboot.
 -name VAL : If specified, the plugin will be installed as this short name
             (whereas normally the name is inferred from the source name
             automatically).
 -restart  : Restart Jenkins upon successful installation.
```

Advanced installation

The Update Center only allows the installation of the most recently released version of a plugin. In cases where an older release of the plugin is desired, a Jenkins administrator can download an older `.hpi` archive and manually install that on the Jenkins master.

From the web UI

Assuming a `.hpi` file has been downloaded, a logged-in Jenkins administrator may upload the file from within the web UI:

. Navigate to the *Manage Jenkins* > *Manage Plugins* page in the web UI. . Click on the *Advanced* tab. . Choose the `.hpi` file under the *Upload Plugin* section. . *Upload* the plugin file.

image::managing/plugin-manager-upload.png["Advanced tab in the Plugin Manager", role=center]

Once a plugin file has been uploaded, the Jenkins master must be manually restarted in order for the changes to take effect.

On the master

Assuming a `.hpi` file has been explicitly downloaded by a systems administrator, the administrator can manually place the `.hpi` file in a specific location on the file system.

Copy the downloaded `.hpi file into the` JENKINS_HOME/plugins `directory on the Jenkins master (for example, on Debian systems` JENKINS_HOME `is generally` /var/lib/jenkins‘).

The master will need to be restarted before the plugin is loaded and made available in the Jenkins environment.

```
The names of the plugin directories in the Update Site footnoteref:[uc] are
not always the same as the plugin's display name. Searching
link:https://plugins.jenkins.io/[plugins.jenkins.io]
for the desired plugin will provide the appropriate link to the `.hpi` files.
```

Updating a plugin

Updates are listed in the *Updates* tab of the *Manage Plugins* page and can be installed by checking the checkboxes of the desired plugin updates and clicking the *Download now and install after restart* button.

image::managing/plugin-manager-update.png["Updates tab in the Plugin Manager", role=center] By default, the Jenkins master will check for updates from the Update Center once every 24 hours. To manually trigger a check for updates, simply click on the *Check now* button in the *Updates* tab.

Removing a plugin

When a plugin is no longer used in a Jenkins environment, it is prudent to remove the plugin from the Jenkins master. This provides a number of benefits such as reducing memory overhead at boot or runtime, reducing configuration options in the web UI, and removing the potential for future conflicts with new plugin updates.

Uninstalling a plugin

The simplest way to uninstall a plugin is to navigate to the *Installed* tab on the *Manage Plugins* page. From there, Jenkins will automatically determine which plugins are safe to uninstall, those which are not dependencies of other plugins, and present a button for doing so.

image::managing/plugin-manager-uninstall.png[“Installed tab in the Plugin Manager”, role=center]

A plugin may also be uninstalled by removing the corresponding `.hpi` file from the `JENKINS_-HOME/plugins` directory on the master. The plugin will continue to function until the master has been restarted.

```
If a plugin `.hpi` file is removed but required by other plugins, the Jenkins
master may fail to boot correctly.
```

Uninstalling a plugin does *not* remove the configuration that the plugin may have created. If there are existing jobs/nodes/views/builds/etc configurations that reference data created by the plugin, during boot Jenkins will warn that some configurations could not be fully loaded and ignore the unrecognized data.

Since the configuration(s) will be preserved until they are overwritten, re-installing the plugin will result in those configuration values reappearing.

Removing old data

Jenkins provides a facility for purging configuration left behind by uninstalled plugins. Navigate to *Manage Jenkins* and then click on *Manage Old Data* to review and remove old data.

Disabling a plugin

Disabling a plugin is a softer way to retire a plugin. Jenkins will continue to recognize that the plugin is installed, but it will not start the plugin, and no extensions contributed from this plugin will be visible.

A Jenkins administrator may disable a plugin by unchecking the box on the *Installed* tab of the *Manage Plugins* page (see below).

image::managing/plugin-manager-disable.png[“Installed tab in the Plugin Manager”, role=center]

A systems administrator may also disable a plugin by creating a file on the Jenkins master, such as: `JENKINS_HOME/plugins/PLUGIN_NAME.hpi.disabled`.

The configuration(s) created by the disabled plugin behave as if the plugin were uninstalled, insofar that they result in warnings on boot but are otherwise ignored.

Using the Jenkins CLI

It is also possible to enable or disable plugins via the Jenkins CLI using the `enable-plugin` or `disable-plugin` commands.

```
The `enable-plugin` command was added to Jenkins in https://jenkins.io/changelog/#v2\
.136[v2.136].
The `disable-plugin` command was added to Jenkins in https://jenkins.io/changelog/#v\
2.151[v2.151].
```

The `enable-plugin` command receives a list of plugins to be enabled. Any plugins which a selected plugin depends on will also be enabled by this command.

```
java -jar jenkins-cli.jar -s http://localhost:8080/ enable-plugin PLUGIN ... [-resta\
rt]

Enables one or more installed plugins transitively.

 PLUGIN   : Enables the plugins with the given short names and their
            dependencies.
 -restart : Restart Jenkins after enabling plugins.
```

The `disable-plugin` command receives a list of plugins to be disabled. The output will display messages for both successful and failed operations. If you only want to see error messages, the `-quiet` option can be specified. The `-strategy` option controls what action will be taken when one of the specified plugins is listed as an optional or mandatory dependency of another enabled plugin.

```
java -jar jenkins-cli.jar -s http://localhost:8080/ disable-plugin PLUGIN ... [-quie\
t (-q)]
[-restart (-r)] [-strategy (-s) strategy]

Disable one or more installed plugins.
Disable the plugins with the given short names. You can define how to proceed with t\
he
dependant plugins and if a restart after should be done. You can also set the quiet \
mode
to avoid extra info in the console.

 PLUGIN                  : Plugins to be disabled.
 -quiet (-q)             : Be quiet, print only the error messages
 -restart (-r)           : Restart Jenkins after disabling plugins.
 -strategy (-s) strategy : How to process the dependant plugins.
                           - none: if a mandatory dependant plugin exists and
                           it is enabled, the plugin cannot be disabled
                           (default value).
                           - mandatory: all mandatory dependant plugins are
                           also disabled, optional dependant plugins remain
```

```
                            enabled.
                            - all: all dependant plugins are also disabled, no
                            matter if its dependency is optional or mandatory.
```

```
In the same way than enabling and disabling plugins from the UI requires a restart
to complete the process, the changes made with the CLI commands will take effect
once Jenkins is restarted. The `-restart` option forces a safe restart of the
instance once the command has successfully finished, so the changes will be
immediately applied.
```

Pinned plugins

```
Pinned plugins feature was removed in Jenkins 2.0. Versions later than Jenkins
2.0 do not bundle plugins, instead providing a wizard to install the most
useful plugins.
```

The notion of *pinned plugins* applies to plugins that are bundled with Jenkins 1.x, such as the plugin:matrix-auth[*Matrix Authorization plugin*].

By default, whenever Jenkins is upgraded, its bundled plugins overwrite the versions of the plugins that are currently installed in `JENKINS_HOME`.

However, when a bundled plugin has been manually updated, Jenkins will mark that plugin as pinned to the particular version. On the file system, Jenkins creates an empty file called `JENKINS_HOME/plugins/PLUGIN_NAME.hpi.pinned` to indicate the pinning.

Pinned plugins will never be overwritten by bundled plugins during Jenkins startup. (Newer versions of Jenkins do warn you if a pinned plugin is *older* than what is currently bundled.)

It is safe to update a bundled plugin to a version offered by the Update Center. This is often necessary to pick up the newest features and fixes. The bundled version is occasionally updated, but not consistently.

The Plugin Manager allows plugins to be explicitly unpinned. The `JENKINS_HOME/plugins/PLUGIN_NAME.hpi.pinned` file can also be manually created/deleted to control the pinning behavior. If the `pinned` file is present, Jenkins will use whatever plugin version the user has specified. If the file is absent, Jenkins will restore the plugin to the default version on startup.

In-process Script Approval

Jenkins, and a number of plugins, allow users to execute Groovy scripts *in* Jenkins. These scripting capabilities are provided by:

*

Script Console.

*

Jenkins Pipeline.

- The plugin:email-ext[Extended Email plugin].
- The plugin:groovy[Groovy plugin] - when using the "Execute system Groovy
- The plugin:job-dsl[JobDSL plugin] as of version 1.60 and later.
  script" step.

To protect Jenkins from execution of malicious scripts, these plugins execute user-provided scripts in a <<groovy-sandbox>> that limits what internal APIs are accessible. Administrators can then use the "In-process Script Approval" page, provided by the plugin:script-security[Script Security plugin], to manage which unsafe methods, if any, should be allowed in the Jenkins environment.

image::managing/manage-inprocess-script-approval.png["Entering the In-process Script Approval configuration", role=center]

Getting Started

The plugin:script-security[Script Security plugin] is installed automatically by the Post-install Setup Wizard, although initially no additional scripts or operations are approved for use.

[IMPORTANT] ==== Older versions of this plugin may not be safe to use. Please review the security warnings listed on plugin:script-security[the Script Security plugin page] in order to ensure that the plugin:script-security[Script Security plugin] is up to date. ====

Security for in-process scripting is provided by two different mechanisms: the <<groovy-sandbox>> and <<script-approval>>. The first, the Groovy Sandbox, is enabled by default for Jenkins Pipeline allowing user-supplied Scripted and Declarative Pipeline to execute without prior Administrator intervention. The second, Script Approval, allows Administrators to approve or deny unsandboxed scripts, or allow sandboxed scripts to execute additional methods.

For most instances, the combination of the Groovy Sandbox and the Script Security's built-in list[102] of approved method signatures, will be sufficient. It is strongly recommended that Administrators only deviate from these defaults if absolutely necessary.

[102]https://github.com/jenkinsci/script-security-plugin/tree/master/src/main/resources/org/jenkinsci/plugins/scriptsecurity/sandbox/whitelists

Groovy Sandbox

[[groovy-sandbox]]

To reduce manual interventions by Administrators, most scripts will run in a Groovy Sandbox by default, including all Jenkins Pipelines. The sandbox only allows a subset of Groovy's methods deemed sufficiently safe for "untrusted" access to be executed without prior approval. Scripts using the Groovy Sandbox are *all* subject to the same restrictions, therefore a Pipeline authored by an Administrator is subject to the restrictions as one authorized by a non-administrative user.

When a script attempts to use features or methods unauthorized by the sandbox, a script is halted immediately, as shown below with Jenkins Pipeline

.Unauthorized method signature rejected at runtime via Blue Ocean image::managing/script-sandbox-rejection.png["Sandbox method rejection", role=center]

The Pipeline above will not execute until an Administrator approves the method signature via the *In-process Script Approval* page.

In addition to adding approved method signatures, users may also disable the Groovy Sandbox entirely as shown below. Disabling the Groovy Sandbox requires that the **entire** script must be reviewed and manually approved by an administrator.

.Disabling the Groovy Sandbox for a Pipeline image::managing/unchecked-groovy-sandbox-on-pipeline.png["Creating a Scripted Pipeline and unchecking 'Use Groovy Sandbox'", role=center]

Script Approval

[[script-approval]]

Manual approval of entire scripts, or method signatures, by an administrator provides Administrators with additional flexibility to support more advanced usages of in-process scripting. When the <<groovy-sandbox>> is disabled, or a method outside of the built-in list is invoked, the Script Security plugin will check the Administrator-managed list of approved scripts and methods.

For scripts which wish to execute outside of the <<groovy-sandbox>>, the Administrator must approve the *entire* script in the *In-process Script Approval* page:

[[approving-unsandboxed-pipeline]] .Approving an unsandboxed Scripted Pipeline image::managing/inprocess-script-approval-pipeline.png["Approving an unsandboxed Scripted Pipeline", role=center]

For scripts which use the <<groovy-sandbox>>, but wish to execute an currently unapproved method signature will also be halted by Jenkins, and require an Administrator to approve the specific method signature before the script is allowed to execute:

[[approving-method-signature]] .Approving a new method signature image::managing/inprocess-script-approval-method.png["Approving a new method signature", role=center]

Approve assuming permissions check

Script approval provides three options: Approve, Deny, and “Approve assuming permissions check.” While the purpose of the first two are self-evident, the third requires some additional understanding of what internal data scripts are able to access and how permissions checks inside of Jenkins function.

Consider a script which accesses the method `hudson.model.AbstractItem.getParent()`, which by itself is harmless and will return an object containing either the folder or root item which contains the currently executing Pipeline or Job. Following that method invocation, executing `hudson.model.ItemGroup.getItems()`, which will list items in the folder or root item, requires the `Job/Read` permission.

This could mean that approving the `hudson.model.ItemGroup.getItems()` method signature would allow a script to bypass built-in permissions checks.

Instead, it is usually more desirable to click *Approve assuming permissions check* which will cause the Script Approval engine to allow the method signature assuming the user running the script has the permissions to execute the method, such as the `Job/Read` permission in this example.

Script Console

Plugins can provide additional security realms which may be useful for incorporating Jenkins into existing identity systems, such as:

- plugin:active-directory[Active Directory]
- plugin:github-oauth[GitHub Authentication]
- plugin:crowd2[Atlassian Crowd 2]

Authorization

The Security Realm, or authentication, indicates *who* can access the Jenkins environment. The other piece of the puzzle is *Authorization*, which indicates *what* they can access in the Jenkins environment. By default Jenkins supports a few different Authorization options:

Anyone can do anything:: Everyone gets full control of Jenkins, including anonymous users who haven't logged in. *Do not use this setting* for anything other than local test Jenkins masters. Legacy mode:: Behaves exactly the same as Jenkins <1.164. Namely, if a user has the "admin" role, they will be granted full control over the system, and otherwise (including anonymous users) will only have the read access. *Do not use this setting* for anything other than local test Jenkins masters. Logged in users can do anything:: In this mode, every logged-in user gets full control of Jenkins. Depending on an advanced option, anonymous users get read access to Jenkins, or no access at all. This mode is useful to force users to log in before taking actions, so that there is an audit trail of users' actions. Matrix-based security:: This authorization scheme allows for granular control over which users and groups are able to perform which actions in the Jenkins environment (see the screenshot below). Project-based Matrix Authorization Strategy:: This authorization scheme is an extension to Matrix-based security which allows additional access control lists (ACLs) to be defined for *each project* separately in the Project configuration screen. This allows granting specific users or groups access only to specified projects, instead of all projects in the Jenkins environment. The ACLs defined with Project-based Matrix Authorization are additive such that access grants defined in the Configure Global Security screen will be combined with project-specific ACLs.

```
Matrix-based security and Project-based Matrix Authorization Strategy are provided
by the plugin:matrix-auth[Matrix Authorization Strategy Plugin]
and may not be installed on your Jenkins.
```

For most Jenkins environments, Matrix-based security provides the most security and flexibility so it is recommended as a starting point for "production" environments.

.Matrix-based security image::managing/configure-global-security-matrix-authorization.png["Configure Global Security - Enable Security - Matrix authorization", role=center]

The table shown above can get quite wide as each column represents a permission provided by Jenkins core or a plugin. Hovering the mouse over a permission will display more information about the permission.

Each row in the table represents a user or group (also known as a "role"). This includes special entries named "anonymous" and "authenticated." The "anonymous" entry represents permissions granted to all unauthenticated users accessing the Jenkins environment. Whereas "authenticated' can be used to grant permissions to all authenticated users accessing the environment.

The permissions granted in the matrix are additive. For example, if a user "kohsuke" is in the groups "developers" and "administrators", then the permissions granted to "kohsuke" will be a union of all those permissions granted to "kohsuke", "developers", "administrators", "authenticated", and "anonymous."

Markup Formatter

Jenkins allows user-input in a number of different configuration fields and text areas which can lead to users inadvertently, or maliciously, inserting unsafe HTML and/or JavaScript.

By default the *Markup Formatter* configuration is set to *Plain Text* which will escape unsafe characters such as `<` and `&` to their respective character entities.

Using the *Safe HTML* Markup Formatter allows for users and administrators to inject useful and information HTML snippets into Project Descriptions and elsewhere.

Cross Site Request Forgery

A cross site request forgery (or CSRF/XSRF) footnoteref:[csrf, https://www.owasp.org/index.php/Cross-Site*Request*Forgery] is an exploit that enables an unauthorized third party to perform requests against a web application by impersonating another, authenticated, user. In the context of a Jenkins environment, a CSRF attack could allow an malicious actor to delete projects, alter builds, or modify Jenkins' system configuration. To guard against this class of vulnerabilities, CSRF protection has been enabled by default with all Jenkins versions since `2.0`.

image::managing/configure-global-security-prevent-csrf.png["Configure Global Security - Prevent Cross Site Request Forgery exploits", role=center]

When the option is enabled, Jenkins will check for a CSRF token, or "crumb", on any request that may change data in the Jenkins environment. This includes any form submission and calls to the remote API, including those using "Basic" authentication.

It is *strongly recommended* that this option be left *enabled*, including on instances operating on private, fully trusted networks.

Caveats

CSRF protection *may* result in challenges for more advanced usages of Jenkins, such as:

- Some Jenkins features, like the remote API, are more difficult to use when
- Accessing Jenkins through a poorly-configured reverse proxy may result in the
- Out-dated plugins, not tested with CSRF protection enabled, may not properly
  this option is enabled. Consult the Remote API documentation for more information. CSRF HTTP header being stripped from requests, resulting in protected actions failing. function.

More information about CSRF exploits can be found link:https://www.owasp.org/index.php/Cross-Site*Request*Forgery[on the OWASP website].

Agent/Master Access Control

Conceptually, the Jenkins master and agents can be thought of as a cohesive system which happens to execute across multiple discrete processes and machines. This allows an agent to ask the master process for information available to it, for example, the contents of files, etc.

For larger or mature Jenkins environments where a Jenkins administrator might enable agents provided by other teams or organizations, a flat agent/master trust model is insufficient.

The Agent/Master Access Control system was introduced footnote:[Starting with 1.587, and 1.580.1, releases] to allow Jenkins administrators to add more granular access control definitions between the Jenkins master and the connected agents.

image::managing/configure-global-security-enable-agent-master.png["Configure Global Security - Enable Agent ⇒ Master Access Control", role=center]

As of Jenkins 2.0, this subsystem has been turned on by default.

Customizing Access

For advanced users who may wish to allow certain access patterns from the agents to the Jenkins master, Jenkins allows administrators to create specific exemptions from the built-in access control rules.

image::managing/configure-global-security-access-control-rules.png["Configure Global Security - Enable Agent ⇒ Master Access Control - Editing Rules", role=center]

By following the link highlighted above, an administrator may edit *Commands* and *File Access* Agent/Master access control rules.

Commands

“Commands” in Jenkins and its plugins are identified by their fully-qualified class names. The majority of these commands are intended to be executed on agents by a request of a master, but some of them are intended to be executed on a master by a request of an agent.

Plugins not yet updated for this subsystem may not classify which category each command falls into, such that when an agent requests that the master execute a command which is not explicitly allowed, Jenkins will err on the side of caution and refuse to execute the command.

In such cases, Jenkins administrators may “whitelist” footnote:[https://en.wikipedia.org/wiki/Whitelist] certain commands as acceptable for execution on the master.

image::managing/configure-global-security-whitelist-commands.png[“Configure Global Security - Enable Agent ⇒ Master Access Control - Editing Rules - Command Whitelisting”, role=center]

Advanced

Administrators may also whitelist classes by creating files with the `.conf` extension in the directory `JENKINS_HOME/secrets/whitelisted-callables.d/`. The contents of these `.conf` files should list command names on separate lines.

The contents of all the `.conf` files in the directory will be read by Jenkins and combined to create a `default.conf` file in the directory which lists all known safe command. The `default.conf` file will be re-written each time Jenkins boots.

Jenkins also manages a file named `gui.conf`, in the `whitelisted-callables.d` directory, where commands added via the web UI are written. In order to disable the ability of administrators to change whitelisted commands from the web UI, place an empty `gui.conf` file in the directory and change its permissions such that is not writeable by the operating system user Jenkins run as.

File Access Rules

The File Access Rules are used to validate file access requests made from agents to the master. Each File Access Rule is a triplet which must contain each of the following elements:

. `allow` / `deny`: if the following two parameters match the current request being considered, an `allow` entry would allow the request to be carried out and a `deny` entry would deny the request to be rejected, regardless of what later rules might say. . *operation*: Type of the operation requested. The following 6 values exist. The operations can also be combined by comma-separating the values. The value of `all` indicates all the listed operations are allowed or denied. ** `read`: read file content or list directory entries ** `write`: write file content ** `mkdirs`: create a new directory ** `create`: create a file in an existing directory ** `delete`: delete a file or directory ** `stat`: read metadata of a file/directory, such as timestamp, length, file access modes. . *file path*: regular expression that specifies file paths that matches this rule. In addition to the base regexp syntax, it supports the following tokens: ** `<JENKINS_HOME>` can be used as a prefix to match the master’s `JENKINS_HOME` directory. ** `<BUILDDIR>` can be used as a prefix to match the build record directory, such as

`/var/lib/jenkins/job/foo/builds/2014-10-17_12-34-56`. ** `<BUILDID>` matches the timestamp-formatted build IDs, like `2014-10-17_12-34-56`.

The rules are ordered, and applied in that order. The earliest match wins. For example, the following rules allow access to all files in `JENKINS_HOME` except the `secrets` folders:

```
# To avoid hassle of escaping every '\' on Windows, you can use / even on Windows.
deny all <JENKINS_HOME>/secrets/.*
allow all <JENKINS_HOME>/.*
```

Ordering is very important! The following rules are incorrectly written because the 2nd rule will never match, and allow all agents to access all files and folders under `JENKINS_HOME`:

```
allow all <JENKINS_HOME>/.*
deny all <JENKINS_HOME>/secrets/.*
```

Advanced

Administrators may also add File Access Rules by creating files with the `.conf.` extension in the directory `JENKINS_HOME/secrets/filepath-filters.d/`. Jenkins itself generates the `30-default.conf` file on boot in this directory which contains defaults considered the best balance between compatibility and security by the Jenkins project. In order to disable these built-in defaults, replace `30-default.conf` with an empty file which is not writable by the operating system user Jenkins run as.

On each boot, Jenkins will read all `.conf` files in the `filepath-filters.d` directory in alphabetical order, therefore it is good practice to name files in a manner which indicates their load order.

Jenkins also manages `50-gui.conf`, in the `filepath-filters/` directory, where File Access Rules added via the web UI are written. In order to disable the ability of administrators to change the File Access Rules from the web UI, place an empty `50-gui.conf` file in the directory and change its permissions such that is not writeable by the operating system user Jenkins run as.

Disabling

While it is not recommended, if all agents in a Jenkins environment can be considered “trusted” to the same degree that the master is trusted, the Agent/Master Access Control feature may be disabled.

Additionally, all the users in the Jenkins environment should have the same level of access to all configured projects.

An administrator can disable Agent/Master Access Control in the web UI by un-checking the box on the *Configure Global Security* page. Alternatively an administrator may create a file in `JENKINS_HOME/secrets` named `slave-to-master-security-kill-switch` with the contents of `true` and restart Jenkins.

```
Most Jenkins environments grow over time requiring their trust models to evolve
as the environment grows. Please consider scheduling regular "check-ups" to
review whether any disabled security settings should be re-enabled.
```

Configuring the System

Managing Tools

Built-in tool providers

Ant

Ant build step

Git

JDK

Maven

Managing Users

System Administration

This chapter for system administrators of Jenkins servers and nodes. It will cover system maintenance topics including security, monitoring, and backup/restore.

Users not involved with system-level tasks will find this chapter of limited use. Individual sections may assume knowledge of information from previous sections, but such assumptions will be explicitly called out and cross-referenced.

If you are a Jenkins administrator and want to know more about managing Jenkins nodes and instances, see Managing Jenkins.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

Backing-up/Restoring Jenkins

references:

Monitoring Jenkins

Securing Jenkins

In the default configuration of Jenkins 1.x, Jenkins does not perform any security checks. This means the ability of Jenkins to launch processes and access local files are available to anyone who can access Jenkins web UI and some more.

Securing Jenkins has two aspects to it.

- Access control, which ensures users are authenticated when accessing Jenkins
- Protecting Jenkins against external threats
  and their activities are authorized.

Access Control

You should lock down the access to Jenkins UI so that users are authenticated and appropriate set of permissions are given to them. This setting is controlled mainly by two axes:

- *Security Realm*, which determines users and their passwords, as well as what
- *Authorization Strategy*, which determines who has access to what.
  groups the users belong to.

These two axes are orthogonal, and need to be individually configured. For example, you might choose to use external LDAP or Active Directory as the security realm, and you might choose "everyone full access once logged in" mode for authorization strategy. Or you might choose to let Jenkins run its own user database, and perform access control based on the permission/user matrix.

- https://wiki.jenkins-ci.org/display/JENKINS/Quick+and+Simple+Security[Quick and Simple Security] — if you are running Jenkins like `java -jar jenkins.war` and only need a very simple setup
- https://wiki.jenkins-ci.org/display/JENKINS/Standard+Security+Setup[Standard Security Setup] — discusses the most common setup of letting Jenkins run its own user database and do finer-grained access control
- https://wiki.jenkins-ci.org/display/JENKINS/Apache+frontend+for+security[Apache frontend for security] — run Jenkins behind Apache and perform access control in Apache instead of Jenkins
- https://wiki.jenkins-ci.org/display/JENKINS/Authenticating+scripted+clients[Authenticating scripted clients] — if you need to programmatically access security-enabled Jenkins web UI, use BASIC auth

- https://wiki.jenkins-ci.org/display/JENKINS/Matrix-based+security[Matrix-based security|Matrix-based security] — Granting and denying finer-grained permissions

In addition to access control of users, access control for builds limits what builds can do, once started.

Protect users of Jenkins from other threats

There are additional security subsystems in Jenkins that protect Jenkins and users of Jenkins from indirect attacks.

The following topics discuss features that are *off by default*. We recommend you read them first and act on them immediately.

- https://wiki.jenkins-ci.org/display/JENKINS/CSRF+Protection[CSRF Protection] — prevent a remote attack against Jenkins running inside your firewall. This feature is *off by default* in Jenkins 1.x and when upgrading to 2.x.
- https://wiki.jenkins-ci.org/display/JENKINS/Security+implication+of+building+on+master[Security implication of building on master] — protect Jenkins master from malicious builds
- https://wiki.jenkins-ci.org/display/JENKINS/Slave+To+Master+Access+Control[Slave To Master Access Control] — protect Jenkins master from malicious build agents
- https://wiki.jenkins.io/display/JENKINS/Securing+JENKINS_HOME[Securing JENKINS_HOME] — protect Jenkins from users with local access

The following topics discuss other security features that are on by default. You'll only need to look at them when they are causing problems.

- https://wiki.jenkins-ci.org/display/JENKINS/Configuring+Content+Security+Policy[Configuring Content Security Policy] — protect users of Jenkins from malicious builds
- https://wiki.jenkins-ci.org/display/JENKINS/Markup+formatting[Markup formatting] — protect users of Jenkins from malicious users of Jenkins

Disabling Security

One may accidentally set up a security realm / authorization in such a way that you may no longer be able to reconfigure Jenkins.

When this happens, you can fix this by the following steps:

. Stop Jenkins (the easiest way to do this is to stop the servlet container.) . Go to `$JENKINS_HOME` in the file system and find `config.xml` file. . Open this file in the editor. . Look for the `<useSecurity>true</useSecurity>` element in this file. . Replace `true` with `false` . Remove the elements `authorizationStrategy` and `securityRealm` . Start Jenkins . When Jenkins comes back, it will be in an unsecured mode where everyone gets full access to the system.

If this is still not working, trying renaming or deleting `config.xml`.

Managing Jenkins with Chef

Managing Jenkins with Puppet

Scaling Jenkins

This chapter will cover topics related to using and managing large scale Jenkins configurations: large numbers of users, nodes, agents, folders, projects, concurrent jobs, job results and logs, and even large numbers of masters.

The audience for this chapter is expert Jenkins users, administrators, and those planning large-scale installations.

If you are a Jenkins administrator and want to know more about managing Jenkins nodes and instances, see Managing Jenkins.

For an overview of content in the Jenkins User Handbook, see User Handbook overview.

Appendix

[appendix]

These sections are generally intended for Jenkins administrators and system administrators. Each section covers a different topic independent of the other sections. They are advanced topics, reference material, and topics that do not fit into other chapters.

[WARNING] ==== *To Contributors*: Please consider adding material elsewhere before adding it here. In fact, topics that do not fit elsewhere may even be out of scope for this handbook. See Contributing to Jenkins for details of how to contact project contributors and discuss what you want to add. ====

Glossary

[[glossary]]

General Terms

[glossary] Agent:: [[agent]] An agent is typically a machine, or container, which connects to a Jenkins master and executes tasks when directed by the master. Artifact:: [[artifact]] An immutable file generated during a Build or Pipeline run which is *archived* onto the Jenkins Master for later retrieval by users. Build:: [[build]] Result of a single execution of a Project Cloud:: [[cloud]] A System Configuration which provides dynamic Agent provisioning and allocation, such as that provided by the plugin:azure-vm-agents[Azure VM Agents] or plugin:ec2[Amazon EC2] plugins. Core:: [[core]] The primary Jenkins application (`jenkins.war`) which provides the basic web UI, configuration, and foundation upon which Plugins can be built. Downstream:: [[downstream]] A configured Pipeline or Project which is triggered as part of the execution of a separate Pipeline or Project. Executor:: [[executor]] A slot for execution of work defined by a Pipeline or Project on a Node. A Node may have zero or more Executors configured which corresponds to how many concurrent Projects or Pipelines are able to execute on that Node. Fingerprint:: [[fingerprint]] A hash considered globally unique to track the usage of an Artifact or other entity across multiple Pipelines or Projects. Folder:: [[folder]] An organizational container for Pipelines and/or Projects, similar to folders on a file system. Item:: [[item]] An entity in the web UI corresponding to either a: Folder, Pipeline, or Project. Job:: [[job]] A deprecated term, synonymous with Project. Label:: [[label]] User-defined text for grouping Agents, typically by similar functionality or capability. For example `linux` for Linux-based agents or `docker` for Docker-capable agents. Master:: [[master]] The central, coordinating process which stores configuration, loads plugins, and renders the various user interfaces for Jenkins. Node:: [[node]] A machine which is part of the Jenkins environment and capable of executing Pipelines or Projects. Both the Master and Agents are considered to be Nodes. Project:: [[project]] A user-configured description of work which Jenkins should perform, such as building a piece of software, etc. Pipeline:: [[pipeline]] A user-defined model of a continuous delivery pipeline, for more read the Pipeline chapter in this handbook. Plugin:: [[plugin]] An extension to Jenkins functionality provided separately from Jenkins Core. Publisher:: [[publisher]] Part of a Build after the completion of all configured Steps which publishes reports, sends notifications, etc. Stage:: [[stage]] `stage` is part of Pipeline, and used for defining a conceptually distinct subset of the entire Pipeline, for example: “Build”, “Test”, and “Deploy”, which is used by many plugins to visualize or present Jenkins Pipeline status/progress. Step:: [[step]] A single task; fundamentally steps tell Jenkins *what* to do inside of a Pipeline or Project. Trigger:: [[trigger]] A criteria for triggering a new Pipeline run or Build. Update Center:: [[update-center]] Hosted inventory of plugins and plugin metadata to enable plugin installation from within Jenkins. Upstream:: [[upstream]] A configured

Pipeline or Project which triggers a separate Pipeline or Project as part of its execution. Workspace:: [[workspace]] A disposable directory on the file system of a Node where work can be done by a Pipeline or Project. Workspaces are typically left in place after a Build or Pipeline run completes unless specific Workspace cleanup policies have been put in place on the Jenkins Master.

Architecting for Manageability

Introduction

With over 1,000 plugins and countless versions of said plugins in the open-source community, testing for all possible conflicts before upgrading one or more production Jenkins instances is simply not feasible. While Jenkins itself will warn of potential incompatibility if it detects that a plugin requires a newer version of the Jenkins core, there is no automatic way to detect conflicts between plugins or to automatically quantifying the impact of upgrading a plugin before doing the upgrade.

Instead, Jenkins administrators should be made responsible for manually testing their own instance's plugin and core version updates before performing them on the production instance. This kind of testing requires a copy or "test instance" of the production server to act as the sandbox for such tests and can prevent production master downtime.

Test Instances

A test master is a Jenkins master used solely for testing configurations and plugins in a non-production environment. For organizations with a mission-critical Jenkins instance, having a test master is highly recommended.

Upgrading or downgrading either the Jenkins core or any plugins can sometimes have the unintended side effect of crippling another plugin's functionality or even crashing a master. As of today, there is no better way to pre-test for such catastrophic conflicts than with a test master.

Test masters should have identical configurations, jobs, and plugins as the production master so that test upgrades will most closely resemble the outcomes of a similar change on your production master. For example, installing the Folders plugin while running a version of the Jenkins core older than 1.554.1 will cause the instance crash and be inaccessible until the plugin is manually uninstalled from the *plugin* folder.

Setting up a test instance

There are many methods for setting up a test instance, but the commonality between them all is that the _$JENKINS*HOME* between them is nearly identical. Whether this means that most all of the production masters' _$JENKINS*HOME* folder is version controlled in a service like GitHub and mounted manually or programmatically to a test server or Docker container, the result is nearly the same.

It is ideal to first ensure sure the master is idle (no running or queued jobs) before attempting to create a test master.

With GitHub + manual commands

You will simply need to open up your command-line interface and "cd" to the folder that contains the _$JENKINS*HOME* directory for your production master and run the "git init" command. For the location of this folder, please refer to section 3.

It is recommended that before running the "git add" command that you create a good *.gitignore* file. This file will prevent you from accidentally version-controlling a file that is too large to be stored in GitHub (anything >50 MB).

Here is an example *.gitignore* file for a Jenkins master running on OS X:

```
.DS_Store
.AppleDouble
.LSOverride
Icon
._*
.Spotlight-V100
.Trashes
.AppleDB
.AppleDesktop
Network Trash Folder
Temporary Items
.apdisk
*.log
*.tmp
*.old
*.jar
*.son
.Xauthority
.bash_history
.bash_profile
.fontconfig
.gitconfig
.gem
.lesshst
.mysql_history
.owner
.ri
.rvm
.ssh
.viminfo
```

```
.vnc
bin/
tools/
**/.owner
**/queue.xml
**/fingerprints/
**/shelvedProjects/
**/updates/
**/jobs/*/workspace/
**/war/
/tools/
**/custom_deps/
**/slave/workspace/
**/slave-slave.log.*
cache/
fingerprints/
**/wars/jenkins*.war
*.log
*.zip
*.rrd
*.gz
```

Once you have a good *.gitignore* file, you can run the follow git commands to commit your _-$JENKINS*HOME* to a git repository like GitHub:

```
git add --all
git commit -m "first commit"
git push
```

Now you can install Jenkins to a fresh instance and "git clone" this _$JENKINS*HOME* from the git repository to your new instance. You will need to replace the files in the new instance with your version-controlled files to complete the migration, whether through scripts or through a drag-and-drop process.

Once this is done, you will need to restart the new test master's Jenkins service or reload its configuration from the Jenkins UI ("Manage Jenkins" >> "Reload Configuration").

With GitHub + Docker (Linux-only)

When it comes to version controlling your $JENKINS_HOME, just follow the instructions in the previous section.

The next step will be to create a Docker image with identical configurations to your production instance's - operating system (Linux-only), installed libraries/tools, and open ports. This can be accomplished through Dockerfiles.

You will then just need to create mounted storage on your Docker server with a clone of your version-controlled _$JENKINS*HOME* home and a simple image to clone the _$JENKINS*HOME* into.

For example, we can create a Docker image called *jenkins-storage* and version control our _$JENKINS*HOME* in a Github repository known as "demo-joc". The "jenkins-storage" Docker image can be built from a Dockerfile similar to this:

```
FROM debian:jessie
RUN apt-get update && apt-get -y upgrade
RUN apt-get install -y --no-install-recommends \
    openjdk-7-jdk \
    openssh-server \
    curl \
    ntp \
    ntpdate  \
    git  \
    maven  \
    less  \
    vim
RUN printf "AddressFamily inet" >> /etc/ssh/ssh_config
ENV MAVEN_HOME /usr/bin/mvn
ENV GIT_HOME /usr/bin/git
# Install Docker client
RUN curl https://get.docker.io/builds/Linux/x86_64/docker-latest -o /usr/local/bin/d\
ocker
RUN chmod +x /usr/local/bin/docker
RUN groupadd docker
# Create Jenkins user
RUN useradd jenkins -d /home/jenkins
RUN echo "jenkins:jenkins" | chpasswd
RUN usermod -a -G docker jenkins
# Make directories for [masters] JENKINS_HOME, jenkins.war lib and [slaves] remote F\
S root, ssh privilege separation directory
RUN mkdir /usr/lib/jenkins /var/lib/jenkins /home/jenkins /var/run/sshd
# Set permissions
RUN chown -R jenkins:jenkins /usr/lib/jenkins /var/lib/jenkins /home/jenkins
#create data folder for cloning
RUN ["mkdir", "/data"]
RUN ["chown", "-R", "jenkins:jenkins", "/data"]
USER jenkins
VOLUME ["/data"]
WORKDIR /data
# USER jenkins
```

```
CMD ["git", "clone", "https://github.com/[your-github-id]/docker-jenkins-storage.git\
", "."]
```

Creating mounted storage for containers would just require something similar to the following command:

```
docker run --name storage [your-dockerhub-id]/jenkins-storage git clone https://gith\
ub.com/[your-github-id]/docker-jenkins-storage.git .
```

And Jenkins images that rely on the mounted storage for their _$JENKNIS*HOME* will then need to point to the mounted volume:

```
docker run -d --dns=172.17.42.1 --name joc-1 --volumes-from storage -e JENKINS_HOME=\
/data/var/lib/jenkins/jenkins [your-dockerhub-id]/jenkins --prefix=""
```

.Test master slaves

Test masters can be connected to test slaves, but this will require further configurations. Depending on your implementation of a test instance, you will either need to create a Jenkins Docker slave image or a slave VM. Of course, open-source plugins like the EC2 plugin also the option of spinning up new slaves on-demand.

The slave connection information will also need to be edited in the config.xml located in your test master's _$JENKINS*HOME*.

.Rolling back plugins that cause failures

If you discover that a plugin update is causing conflict within the test master, you can rollback in several ways:

- For bad plugins, you can rollback the plugin from the UI by going to the plugin manager ("Manage Jenkins" >> "Manage Plugins") and going to the "Available" tab. Jenkins will show a "downgrade" button next to any plugins that can be downgraded.
- If the UI is unavailable, then enter your _$JENKINS

HOME folder and go to
the plugins folder. From there, delete the .hpi or .jpi file for the offending plugin, then restart Jenkins. If you need to rollback to an older version, you will need to manually copy in an older version of that .jpi or .hpi. To do this, go to the plugin's page on the Jenkins wiki[103] and download one of its archived versions.

[103]https://updates.jenkins-ci.org/download/plugins

Troubleshooting for Stability

Jenkins masters can suffer instability problems when the master is not properly sized for its hardware or a buggy plugin wastes resources. To combat this, Jenkins administrators should begin their troubleshooting by identifying which components are behaving abnormally and which resources are insufficient. The administrator can take thread dumps[104] and head dumps to get some of this information, but in some cases where the instance has become non-operational and taking a thread dump is impossible, it is useful to have a persistent record outside of Jenkins itself to reference when such troubleshooting is required.

Using the Jenkins Metrics Plugin

The Jenkins Metrics Plugin[105] is an open-source plugin which exposes metrics on a Jenkins instance. Metrics are exposed using the Dropwizard Metrics API[106]

.Metrics exposed

The exact list of exposed metrics varies depending on your installed plugins. To get a full list of available metrics for your own master, run the following script on https://wiki.jenkins-ci.org/display/JENKINS/Jenkins+Script+Console[your master's script console]:

```
for (j in Jenkins.instance.getExtensionList(jenkins.metrics.api.MetricProvider.class\
)) {
     for (m in j.getMetricSet()) {
          for (i in m.metrics)
               { println i.getKey() }
     }
}
```

CloudBees has documented[107] the full list of exposed metrics, along with in-depth explanations of each.

.Metrics Usage

Metrics are protected by a set of permissions for viewing, accessing the thread dump, and posting a health check. The Metrics Operational Menu can be access via the web UI by visiting <jenkins-url>/metrics/currentUser, and the 4 menu options (Metrics, Ping, Threads, Healthcheck) lead to a JSON string containing the requested metrics or thread dump.

Access to the Metrics Servlet can also be provided by issuing API keys. API keys can be configured from the Jenkins global configuration screen (<jenkins-url>/configure) under the "Metrics" section. Multiple access can be generated and permissions associated with those keys can also be restricted at this level.

[104]https://wiki.jenkins-ci.org/display/JENKINS/Obtaining+a+thread+dump
[105]https://wiki.jenkins-ci.org/display/JENKINS/Metrics+Plugin
[106]https://dropwizard.github.io/metrics/3.1.0
[107]https://documentation.cloudbees.com/docs/cje-user-guide/monitoring-sect-reference.html#monitoring-sect-reference-metrics

More information on Metrics basic and advanced usages can be found here[108].

Architecting for Scale

Introduction

As an organization matures from a continuous delivery standpoint, its Jenkins requirements will similarly grow. This growth is often reflected in the Jenkins master's architecture, whether that be "vertical" or "horizontal" growth.

Vertical growth is when a master's load is increased by having more configured jobs or orchestrating more frequent builds. This may also mean that more teams are depending on that one master.

Horizontal growth is the creation of additional masters within an organization to accommodate new teams or projects, rather than adding these things to an existing single master.

There are potential pitfalls associated with each approach to scaling Jenkins, but with careful planning, many of them can be avoided or managed. Here are some things to consider when choosing a strategy for scaling your organization's Jenkins instances:

- **Do you have the resources to run a distributed build system?** If possible,
- **Do you have the resources to maintain multiple masters?** Jenkins masters
- **How mission critical are each team's projects?** Consider segregating the
- **How important is a fast start-up time for your Jenkins instance?** The more
  it is recommended set up dedicated build nodes that run separately from the Jenkins master. This frees up resources for the master to improve its scheduling performance and prevents builds from being able to modify any potentially sensitive data in the master's _$JENKINS*HOME*. This also allows for a single master to scale far more vertically than if that master were both the job builder and scheduler. will require regular plugin updates, semi-monthly core upgrades, and regular backups of configurations and build histories. Security settings and roles will have to be manually configured for each master. Downed masters will require manual restart of the Jenkins master and any jobs that were killed by the outage. most vital projects to separate masters to minimize the impact of a single downed master. Also consider converting any mission-critical project pipelines to Pipeline jobs, which have the ability to survive a master-agent connection interruptions. jobs a master has configured, the longer it takes to load Jenkins after an upgrade or a crash. The use of folders and views to organize jobs can limit the number of that need to be rendered on start up.

Distributed Builds Architecture

A Jenkins master can operate by itself both managing the build environment and executing the builds with its own executors and resources. If you stick with this "standalone" configuration you will most likely run out of resources when the number or the load of your projects increase.

[108] https://documentation.cloudbees.com/docs/cje-user-guide/monitoring-sect-getting-started.html

To come back up and running with your Jenkins infrastructure you will need to enhance the master (increasing memory, number of CPUs, etc). The time it takes to maintain and upgrade the machine, the master together with all the build environment will be down, the jobs will be stopped and the whole Jenkins infrastructure will be unusable.

Scaling Jenkins in such a scenario would be extremely painful and would introduce many "idle" periods where all the resources assigned to your build environment are useless.

Moreover, executing jobs on the master's executors introduces a "security" issue: the "jenkins" user that Jenkins uses to run the jobs would have full permissions on all Jenkins resources on the master. This means that, with a simple script, a malicious user can have direct access to private information whose integrity and privacy could not be, thus, guaranteed.

For all these reasons Jenkins supports the "master/agent" mode, where the workload of building projects are delegated to multiple agents.

An agent is a machine set up to offload projects from the master. The method with which builds are scheduled depends on the configuration given to each project. For example, some projects may be configured to "restrict where this project is run" which ties the project to a specific agent or set of labeled agents. Other projects which omit this configuration will select an agent from the available pool in Jenkins.

In a distributed builds environment, the Jenkins master will use its resources to only handle HTTP requests and manage the build environment. Actual execution of builds will be delegated to the agents. With this configuration it is possible to horizontally scale an architecture, which allows a single Jenkins installation to host a large number of projects and build environments.

Master/agent communication protocols

In order for a machine to be recognized an agent, it needs to run a specific agent program to establish bi-directional communication with the master.

There are different ways to establish a connection between master and agent:

- *The SSH connector*: Configuring an agent to use the SSH connector is the

preferred and the most stable way to establish master-agent communication. Jenkins has a built-in SSH client implementation. This means that the Jenkins master can easily communicate with any machine with an SSH server installed. The only requirement is that the public key of the master is part of the set of the authorized keys on the agent. Once the host and SSH key is defined for a new agent, Jenkins will establish a connection to the machine and bootstrap the agent process.

- *The JNLP-TCP connector*: In this case the communication is established
  starting the agent through Java Web Start (JNLP). With this connector the Java Web Start program has to be launched in the machine in 2 different ways:

. Manually: by navigating to the Jenkins master URL in a browser on the agent. Once the Java Web Start icon is clicked, the agent will be launched on the machine. The downside of this approach is that the agents cannot be centrally managed by the Jenkins master and each/stop/start/update of the agent needs to be executed manually on the agent's machine in versions of Jenkins older than 1.611. This approach is convenient when the master cannot instantiate the connection with the client, for example: with agents running inside a firewalled network connecting to a master located outside the firewall.

. As a service: First you'll need to manually launch the agent using the above method. After manually launching it, *jenkins-slave.exe* and *jenkins-slave.xml* will be created in the slave's work directory. Now go to the command line to execute the following command:

[source, width="300"] —- sc.exe create "<serviceKey>" start= auto binPath= "<path to jenkins-slave.exe>" DisplayName= "<service display name>" —-

<serviceKey> is the name of the registry key to define this agent service and <service display name> is the label that will identify the service in the Service Manager interface.

To ensure that restarts are automated, you will need to download a agent jar newer than v 2.37 and copy it to a permanent location on the machine. The *.jar* file can be found at:

[source, width="350"] —- http://<your-jenkins-host>/jnlpJars/slave.jar —-

If running a version of Jenkins newer than 1.559, the *.jar* will be kept up to date each time it connects to the master.

* *The JNLP-HTTP connector*: This approach is quite similar to the JNLP-TCP Java Web Start approach, with the difference in this case being that the agent is executed as headless and the connection can be tunneled via HTTP(s). The exact command can be found on your JNLP gaent's configuration page:

[[jnlp_agent]] .JNLP agent launch command image::hardware-recommendations/jnlp-slave.png[scaledwidth=90%]

This approach is convenient for an execution as a daemon on Unix.

- *Custom-script*: It is also possible to create a custom script to initialize
  the communication between master and agent if the other solutions do not provide enough flexibility for a specific use-case. The only requirement is that the script runs the java program as a *java -jar slave.jar* on the agent.

Windows agent set-up can either follow the standard SSH and JNLP approach or use a more Windows-specific configuration approach. Windows agents have the following options:

- *SSH-connector approach with Putty*
- *SSH-connector approach with Cygwin and OpenSSH*:
- *Remote management facilities (WMI + DCOM)*: With this approach, which

- *JNLP-connector approach*: With https://wiki.jenkins-ci.org/display/JENKINS/SSH+slaves+and+Cygwin[This] is the easiest to setup and recommended approach. utilizes the https://wiki.jenkins-ci.org/display/JENKINS/Windows+Slaves+ Slave plugin]), the Jenkins master will register the slave agent on the windows slave machine creating a Windows service. The Jenkins master can control the slaves, issuing stops/restarts/updates of the same. However this is difficult to set-up and not recommended. https://wiki.jenkins-ci.org/display/JENKINS/Installing+Jenkins+as+a+Windows+service[this approach] it is possible to manually register the slave as Windows service, but it will not be possible to centrally manage it from the master. Each stop/start/update of the slave agent needs to be executed manually on the slave machine, unless running Jenkins 1.611 or newer.

Creating fungible slaves

Configuring tools location on slaves

The Jenkins Global configuration page let you specify the tools needed during the builds (i.e. Ant, Maven, Java, etc).

When defining a tool, it is possible to create a pointer to an existing installation by giving the directory where the program is expected to be on the slave. Another option is to let Jenkins take care of the installation of a specific version in the given location. It is also possible to specify more than one installation for the same tool since different jobs may need different versions of the same tool.

The pre-compiled "Default" option calls whatever is already installed on the slave and exists in the machine PATH, but this will return a failure if the tool was not already installed and its location was not added to the PATH system variable.

One best practice to avoid this failure is to configure a job with the assumption that the target slave does not have the necessary tools installed, and to include the tools' installation as part of the build process.

Define a policy to share slave machines

As mentioned previously, slaves should be interchangeable and standardized in order to make them sharable and to optimize resource usage. Slaves should not be customized for a particular set of jobs, nor for a particular team.

Lately Jenkins has become more and more popular not only in CI but also in CD, which means that it must orchestrate jobs and pipelines which involve different teams and technical profiles: developers, QA people and Dev-Ops people.

In such a scenario, it might make sense to create customized and dedicated slaves: different tools are usually required by different teams (i.e. Puppet/Chef for the Ops team) and teams' credentials are usually stored on the slave in order to ensure their protection and privacy.

In order to ensure the execution of a job on a single/group of slaves only (i.e. iOS builds on OSX slaves only), it is possible to tie the job to the slave by specifying the slave's label in the job configuration page. Note that the restriction has to be replicated in every single job to be tied and that the slave won't be protected from being used by other teams.

Setting up cloud slaves

Cloud build resources can be a solution for a case when it is necessary to maintain a reasonably small cluster of slaves on-premise while still providing new build resources when needed.

In particular it is possible to offload the execution of the jobs to slaves in the cloud thanks to ad-hoc plugins which will handle the creation of the cloud resources together with their destruction when they are not needed anymore:

- The https://wiki.jenkins-ci.org/display/JENKINS/Amazon+EC2+Plugin[EC2 Plugin]
- The https://wiki.jenkins-ci.org/display/JENKINS/JClouds+Plugin[JCloud plugin]
  let Jenkins use AWS EC2 instances as cloud build resources when it runs out of on-premise slaves. The EC2 slaves will be dynamically created inside an AWS network and de-provisioned when they are not needed. creates the possibility of executing the jobs on any cloud provider supported by JCloud libraries

Right-sizing Jenkins masters

Master division strategies

Designing the best Jenkins architecture for your organization is dependent on how you stratify the development of your projects and can be constrained by limitations of the existing Jenkins plugins.

The 3 most common forms of stratifying development by masters is:

1. **By environment (QA, DEV, etc)** - With this strategy, Jenkins masters are populated by jobs based on what environment they are deploying to.

- **Pros**

** Can tailor plugins on masters to be specific to that environment's needs ** Can easily restrict access to an environment to only users who will be using that environment

- **Cons**

** Reduces ability to create pipelines ** No way to visualize the complete flow across masters ** Outage of a master will block flow of all products

2. **By org chart** - This strategy is when masters are assigned to divisions within an organization.

- **Pros**

** Can tailor plugins on masters to be specific to that team's needs ** Can easily restrict access to a division's projects to only users who are within that division

- **Cons**

** Reduces ability to create cross-division pipelines ** No way to visualize the complete flow across masters ** Outage of a master will block flow of all products

3. **Group masters by product lines** - When a group of products, with on only critical product in each group, gets its own Jenkins masters.

- **Pros**

** Entire flows can be visualized because all steps are on one master ** Reduces the impact of one master's downtime on only affects a small subset of products

- **Cons**

** A strategy for restricting permissions must be devised to keep all users from having access to all items on a master.

When evaluating these strategies, it is important to weigh them against the vertical and horizontal scaling pitfalls discussed in the introduction.

Another note is that a smaller number of jobs translates to faster recovery from failures and more importantly a higher mean time between failures.

Calculating how many jobs, masters, and executors are needed

Having the best possible estimate of necessary configurations for a Jenkins installation allows an organization to get started on the right foot with Jenkins and reduces the number of configuration iterations needed to achieve an optimal installation. The challenge for Jenkins architects is that true limit of vertical scaling on a Jenkins master is constrained by whatever hardware is in place for the master, as well as harder to quantify pieces like the types of builds and tests that will be run on the build nodes.

There is a way to estimate roughly how many masters, jobs and executors will be needed based on build needs and number of developers served. These equations assume that the Jenkins master will have 5 cores with one core per 100 jobs (500 total jobs/master) and that teams will be divided into groups of 40.

If you have information on the actual number of available cores on your planned master, you can make adjustments to the "number of masters" equations accordingly.

The equation for *estimating the number of masters and executors needed* when the number of configured jobs is known is as follows:

[source, width="350"] —- masters = number of jobs/500 executors = number of jobs * 0.03 —-

The equation for *estimating the maximum number of jobs, masters, and executors needed* for an organization based on the number of developers is as follows:

[source, width="350"] —- number of jobs = number of developers * 3.333 number of masters = number of jobs/500 number of executors = number of jobs * 0.03 —-

These numbers will provide a good starting point for a Jenkins installation, but adjustments to actual installation size may be needed based on the types of builds and tests that an installation runs.

Scalable storage for masters

It is also recommended to choose a master with consideration for future growth in the number of plugins or jobs stored in your master's _$JENKINS*HOME*. Storage is cheap and Jenkins does not require fast disk access to run well, so it is more advantageous to invest in a larger machine for your master over a faster one.

Different operating systems for the Jenkins master will also allow for different approaches to expandable storage:

- *Spanned Volumes on Windows* - On NTFS devices like Windows, you can create a
- *Logical Volume Manager for Linux* - LVM manages disk drives and allows
- *ZFS for Solaris* - ZFS is even more flexible than LVM and spanned volumes
- *Symbolic Links* - For systems with existing Jenkins installations and who
  spanned volume that allows you to add new volumes to an existing one, but have them behave as a single volume. To do this, you will have to ensure that Jenkins is installed on a separate partition so that it can be converted to a spanned volume later. logical volumes to be resized on the fly. Many distributions of Linux use LVM when they are installed, but Jenkins should have its our LVM setup. and just requires that the _$JENKINS*HOME* be on its own filesystem. This makes it easier to create snapshots, backups, etc. cannot use any of the above-mentioned methods, symbolic links (symlinks) may be used instead to store job folders on separate volumes with symlinks to those directories.

Additionally, to easily prevent a _$JENKINS*HOME* folder from becoming bloated, make it mandatory for jobs to discard build records after a specific time period has passed and/or after a specific number of builds have been run. This policy can be set on a job's configuration page.

Setting up a backup policy

It is a best practice to take regular backups of your $JENKINS_HOME. A backup ensures that your Jenkins instance can be restored despite a misconfiguration, accidental job deletion, or data corruption.

Finding your $JENKINS_HOME

Windows

If you install Jenkins with the Windows installer, Jenkins will be installed as a service and the default _$JENKINS*HOME* will be "C:Program Files (x86)\jenkins".

You can edit the location of your _$JENKINS*HOME* by opening the jenkins.xml file and editing the _$JENKINS*HOME* variable, or going to the "Manage Jenkins" screen, clicking on the "Install as Windows Service" option in the menu, and then editing the "Installation Directory" field to point to another existing directory.

Mac OSX

If you install Jenkins with the OS X installer, you can find and edit the location of your _-$JENKINS*HOME* by editing the "Macintosh HD/Library/LaunchDaemons" file's _$JENKINS*HOME* property.

By default, the _$JENKINS*HOME* will be set to "Macintosh HD/Users/Shared/Jenkins".

Ubuntu/Debian

If you install Jenkins using a Debian package, you can find and edit the location of your _$JENKINS*HOME* by editing your "/etc/default/jenkins" file.

By default, the _$JENKINS*HOME* will set to "/var/lib/jenkins" and your $JENKINS_WAR will point to "/usr/share/jenkins/jenkins.war".

Red Hat/CentOS/Fedora

If you install Jenkins as a RPM package, the default _$JENKINS*HOME* will be "/var/lib/jenkins".

You can edit the location of your _$JENKINS*HOME* by editing the "/etc/sysconfig/jenkins" file.

openSUSE

If installing Jenkins as a package using zypper, you'll be able to edit the _$JENKINS*HOME* by editing the "/etc/sysconfig/jenkins" file.

The default location for your _$JENKINS*HOME* will be set to "/var/lib/jenkins" and the $JENKINS_-WAR home will be in "/usr/lib/jenkins".

FreeBSD

If installing Jenkins using a port, the _$JENKINS*HOME* will be located in whichever directory you run the "make" command in. It is recommended to create a "/usr/ports/devel/jenkins" folder and compile Jenkins in that directory.

You will be able to edit the _$JENKINS*HOME* by editing the "/usr/local/etc/jenkins".

OpenBSD

If installing Jenkins using a package,the _$JENKINS*HOME* is set by default to "/var/jenkins".

If installing Jenkins using a port, the _$JENKINS*HOME* will be located in whichever directory you run the "make" command in. It is recommended to create a "/usr/ports/devel/jenkins" folder and compile Jenkins in that directory.

You will be able to edit the _$JENKINS*HOME* by editing the "/usr/local/etc/jenkins" file.

Solaris/OpenIndiana

The Jenkins project voted on September 17, 2014 to discontinue Solaris packages.

Anatomy of a $JENKINS_HOME

The folder structure for a _$JENKINS*HOME* directory is as follows:

```
JENKINS_HOME
 +- config.xml     (Jenkins root configuration file)
 +- *.xml          (other site-wide configuration files)
 +- identity.key   (RSA key pair that identifies an instance)
 +- secret.key     (deprecated key used for some plugins' secure operations)
 +- secret.key.not-so-secret  (used for validating _$JENKINS_HOME_ creation date)
 +- userContent    (files served under your https://server/userContent/)
 +- secrets        (root directory for the secret+key for credential decryption)
     +- hudson.util.Secret   (used for encrypting some Jenkins data)
     +- master.key           (used for encrypting the hudson.util.Secret key)
     +- InstanceIdentity.KEY (used to identity this instance)
 +- fingerprints   (stores fingerprint records, if any)
 +- plugins        (root directory for all Jenkins plugins)
     +- [PLUGINNAME]   (sub directory for each plugin)
         +- META-INF       (subdirectory for plugin manifest + pom.xml)
         +- WEB-INF        (subdirectory for plugin jar(s) and licenses.xml)
     +- [PLUGINNAME].jpi   (.jpi or .hpi file for the plugin)
 +- jobs           (root directory for all Jenkins jobs)
     +- [JOBNAME]      (sub directory for each job)
         +- config.xml     (job configuration file)
         +- workspace      (working directory for the version control system)
         +- latest         (symbolic link to the last successful build)
         +- builds         (stores past build records)
             +- [BUILD_ID]     (subdirectory for each build)
                 +- build.xml      (build result summary)
                 +- log            (log file)
                 +- changelog.xml  (change log)
     +- [FOLDERNAME]   (sub directory for each folder)
         +- config.xml     (folder configuration file)
         +- jobs           (sub directory for all nested jobs)
```

Segregating pure configuration from less durable data

[[segrate-data]]

CAUTION: No data migration is handled by Jenkins when using those settings. So you either want to use them from the beginning, or make sure you take into consideration which data you would like to be moved to the right place before using the following switches.

It is possible to separate customize some of the layout to better separate pure job configurations from less durable data, like build data or logs. footnote:[These switches are used to configure out of the box Jenkins Essentials[109] instances.]

Configure a different *jobs build data* layout

Historically, the configuration of a given job is located under `$JENKINS_HOME/jobs/[JOB_NAME]/config.xml` and its builds are under `$JENKINS_HOME/jobs/[JOB_NAME]/builds`.

This typically makes it more impractical to set up a different backup policy, or set up a quicker disk for making builds potentially faster.

For instance, if you would like to move builds under a different root, you can use the following value: `+$JENKINS_VAR/${ITEM*FULL*NAME}/builds+`.

Note that starting with Jenkins 2.119, the User Interface for this was replaced by the `jenkins.model.Jenkins.buildsD` system property. See the dedicated *Features Controlled with System Properties* wiki page[110] for more details.

Choosing a backup strategy

All of your Jenkins-specific configurations that need to be backed up will live in the _$JENKINS*HOME*, but it is a best practice to back up only a subset of those files and folders.

Below are a few guidelines to consider when planning your backup strategy.

.Exclusions

When it comes to creating a backup, it is recommended to exclude archiving the following folders to reduce the size of your backup:

[literal] /war (the exploded Jenkins war directory) /cache (downloaded tools) /tools (extracted tools)

These folders will automatically be recreated the next time a build runs or Jenkins is launched.

.Jobs and Folders

Your job or folder configurations, build histories, archived artifacts, and workspace will exist entirely within the *jobs* folder.

The *jobs* directory, whether nested within a folder or at the root level is as follows:

[109] https://jenkins.io/blog/2018/04/06/jenkins-essentials/
[110] https://wiki.jenkins.io/display/JENKINS/Features+controlled+by+system+properties

```
+- jobs            (root directory for all Jenkins jobs)
    +- [JOBNAME]      (sub directory for each job)
        +- config.xml     (job configuration file)
        +- workspace      (working directory for the version control system)
        +- latest         (symbolic link to the last successful build)
        +- builds         (stores past build records)
            +- [BUILD_ID]     (subdirectory for each build)
                +- build.xml      (build result summary)
                +- log            (log file)
                +- changelog.xml  (change log)
```

If you only need to backup your job configurations, you can opt to only backup the *config.xml* for each job. Generally build records and workspaces do not need to be backed up, as workspaces will be re-created when a job is run and build records are only as important as your organizations deems them.

.System configurations

Your instance's system configurations exist in the root level of the _$JENKINS*HOME* folder:

[literal] +- config.xml (Jenkins root configuration file) +- *.xml (other site-wide configuration files)

The *config.xml* is the root configuration file for your Jenkins. It includes configurations for the paths of installed tools, workspace directory, and slave agent port.

Any .xml other than that *config.xml* in the root Jenkins folder is a global configuration file for an installed tool or plugin (i.e. Maven, Git, Ant, etc). This includes the *credentials.xml* if the Credentials plugin is installed.

If you only want to backup your core Jenkins configuration, you only need to back up the *config.xml*.

.Plugins

Your instance's plugin files (.hpi and .jpi) and any of their dependent resources (help files, *pom.xml* files, etc) will exist in the *plugins* folder in $JENKINS_HOME.

[literal] +- plugins (root directory for all Jenkins plugins) +- [PLUGINNAME] (sub directory for each plugin) +- META-INF (subdirectory for plugin manifest + pom.xml) +- WEB-INF (subdirectory for plugin jar(s) and licenses.xml) +- [PLUGINNAME].jpi (.jpi or .hpi file for the plugin)

It is recommended to back up the entirety of the plugins folder (.hpi/.jpis + folders).

.Other data

Other data that you are recommended to back up include the contents of your *secrets* folder, your *identity.key*, your *secret.key*, and your *secret.key.not-so-secret* file.

[literal] +- identity.key (RSA key pair that identifies an instance) +- secret.key (used for various secure Jenkins operations) +- secret.key.not-so-secret (used for validating _$JENKINS*HOME* creation date) +- userContent (files served in https://server/userContent/) +- secrets (directory for the

secret+key decryption) +- hudson.util.Secret (used for encrypting some Jenkins data) +- master.key (used for encrypting the hudson.util.Secret key) +- InstanceIdentity.KEY (used to identity this instance)

The *identity.key* is an RSA key pair that identifies and authenticates the current Jenkins instance.

The *secret.key* is used to encrypt plugin and other Jenkins data, and to establish a secure connection between a master and slave.

The *secret.key.not-so-secret* file is used to validate when the _$JENKINS*HOME* was created. It is also meant to be a flag that the secret.key file is a deprecated way of encrypting information.

The files in the secrets folder are used by Jenkins to encrypt and decrypt your instance's stored credentials, if any exist. Loss of these files will prevent recovery of any stored credentials. *hudson.util.Secret* is used for encrypting some Jenkins data like the credentials.xml, while the *master.key* is used for encrypting the hudson.util.Secret key. Finally, the *InstanceIdentity.KEY* is used to identity this instance and for producing digital signatures.

Define a Jenkins instance to rollback to

In the case of a total machine failure, it is important to ensure that there is a plan in place to get Jenkins both back online and in its last good state.

If a high availability set up has not been enabled and no back up of that master's filesystem has been taken, then an corruption of a machine running Jenkins means that all historical build data and artifacts, job and system configurations, etc. will be lost and the lost configurations will need to be recreated on a new instance.

1. Backup policy - In addition to creating backups using the previous section's backup guide, it is important to establish a policy for selecting which backup should be used when restoring a downed master. 2. Restoring from a backup - A plan must be put in place on whether the backup should be restored manually or with scripts when the primary goes down.

Resilient Jenkins Architecture

Administrators are constantly adding more and more teams to the software factory, making administrators in the business of making their instances resilient to failures and scaling them in order to onboard more teams.

Adding build nodes to a Jenkins instance while beefing up the machine that runs the Jenkins master is the typical way to scale Jenkins. Said differently, administrators scale their Jenkins master vertically. However, there is a limit to how much an instance can be scaled. These limitations are covered in the introduction to this chapter.

Ideally, masters will be set up to automatically recover from failures without human intervention. There are proxy servers monitoring active masters and re-routing requests to backup masters if the active master goes down. There are additional factors that should be reviewed on the path to continuous delivery. These factors include componetizing the application under development, automating the entire pipeline (within reasonable limits) and freeing up contentious resources.

.Step 1: Make each master highly available

Each Jenkins master needs to be set up such that it is part of a Jenkins cluster.

A proxy (typically HAProxy or F5) then fronts the primary master. The proxy's job is to continuously monitor the primary master and route requests to the backup if the primary goes down. To make the infrastructure more resilient, you can have multiple backup masters configured.

.Step 2: Enable security

Set up an authentication realm that Jenkins will use for its user database.

TIP: If you are trying to set up a proof-of-concept, it is recommended to use the https://wiki.jenkins-ci.org/display/JENKINS/Mock+Security+Realm+Plugin[Mock Security Realm plugin] for authentication.

.Step 3: Add build nodes (slaves) to master

Add build servers to your master to ensure you are conducting actual build execution off of the master, which is meant to be an orchestration hub, and onto a “dumb” machine with sufficient memory and I/O for a given job or test.

.Step 4: Setup a test instance

A test instance is typically used to test new plugin updates. When a plugin is ready to be used, it should be installed into the main production update center.

Hardware Recommendations

Introduction

Sizing a Jenkins environment depends on a number of factors, which makes it a very inexact science. Achieving an optimal configuration requires some experience and experimentation. It is, however, possible to make a smart approximation to start - especially when designing with Jenkins' best practices in mind.

The following outlines these factors and how you can account for them when sizing your configuration. You are also provided sample configurations and the hardwares behind some of the largest Jenkins installations presented in a Jenkins Scalability Summit.

Choosing the Right Hardware for Masters

One of the greatest challenges of properly setting up a Jenkins instance is that there is no *one size fits all* answer - the exact specifications of the hardware that you will need will depend heavily on your organization's current and future needs.

Your Jenkins master will be serving HTTP requests and storing all of the important information for your Jenkins instance in its _$JENKINS*HOME* folder (configurations, build histories and plugins).

More information on sizing masters based organizational needs can be found in the Architecting for Scale section.

Memory Requirements for the Master

The amount of memory Jenkins needs is largely dependent on many factors, which is why the RAM allotted for it can range from 200 MB for a small installation to 70+ GB for a single and massive Jenkins master. However, you should be able to estimate the RAM required based on your project build needs.

Each build node connection will take 2-3 threads, which equals about 2 MB or more of memory. You will also need to factor in CPU overhead for Jenkins if there are a lot of users who will be accessing the Jenkins user interface.

It is generally a bad practice to allocate executors on a master, as builds can quickly overload a master's CPU/memory/etc and crash the instance, causing unnecessary downtime. Instead, it is advisable to set up agents that the Jenkins master can delegate jobs to, keeping the bulk of the work off of the master itself.

Choosing the Right Build Machines

The backbone of Jenkins is its ability to orchestrate builds, but installations which do not leverage Jenkins' distributed builds architecture are artificially limiting the number of builds that their masters can orchestrate. More information on a more distributed architecture can be found in the Architecting for Scale section.

Requirements for a Machine to be an agent

[[fungibility]] Agents are typically generic x86 machines with enough memory to run specific build types. The agent's configuration depends on the builds it will be used for and on the tools required by the same builds.

Configuring a machine to act as an agent inside your infrastructure can be tedious and time consuming. This is especially true when the same set-up has to be replicated on a large pool of agents. Because of this, is ideal to have fungible agents, which are agents that are easily replaceable. Agents should be generic for all builds rather customized for a specific job or a set of jobs. The more generic the agents, the more easily they are interchanged, which in turn allows for a better use of resources and a reduced impact on productivity if some agents suffer an outage. Andrew Bayer introduced this concept of "fungibility" as applied to agents during his presentation https://www.slideshare.net/andrewbayer/seven-habits-of-highly-effective-jenkins-users-2014-edition["Seven Habits of Highly Effective Jenkins Users" at the Jenkins User Conference (Europe, 2014)].

The more automated the environment configuration is, the easier it is to replicate a configuration onto a new agent machine. Tools for configuration management or a pre-baked image can be excellent solutions to this end. Containers and virtualization are also popular tools for creating generic agent environments.

More information on estimating the number of executors needed in a given environment can be found in the Architecting for Scale section.

Pipeline as Code

Introduction

Pipeline as Code describes a set of features that allow Jenkins users to define pipelined job processes with code, stored and versioned in a source repository. These features allow Jenkins to discover, manage, and run jobs for multiple source repositories and branches – eliminating the need for manual job creation and management.

To use *Pipeline as Code*, projects must contain a file named `Jenkinsfile` in the repository root, which contains a "Pipeline script."

Additionally, one of the enabling jobs needs to be configured in Jenkins:

- *Multibranch Pipeline*: build multiple branches of a

single repository automatically

- *Organization Folders*: scan a *GitHub Organization* or *Bitbucket Team* to discover an organization's repositories, automatically creating managed *Multibranch Pipeline* jobs for them

Fundamentally, an organization's repositories can be viewed as a hierarchy, where each repository may have child elements of branches and pull requests.

.Example Repository Structure .... +— GitHub Organization +— Project 1 +— master +— feature-branch-a +— feature-branch-b +— Project 2 +— master +— pull-request-1 +— etc... ....

Prior to *Multibranch Pipeline* jobs and *Organization Folders*, Folders[111] could be used to create this hierarchy in Jenkins by organizing repositories into folders containing jobs for each individual branch.

Multibranch Pipeline and *Organization Folders* eliminate the manual process by detecting branches and repositories, respectively, and creating appropriate folders with jobs in Jenkins automatically.

[111]https://wiki.jenkins-ci.org/display/JENKINS/CloudBees+Folders+Plugin

The Jenkinsfile

Presence of the `Jenkinsfile` in the root of a repository makes it eligible for Jenkins to automatically manage and execute jobs based on repository branches.

The `Jenkinsfile` should contain a Pipeline script, specifying the steps to execute the job. The script has all the power of Pipeline available, from something as simple as invoking a Maven builder, to a series of interdependent steps, which have coordinated parallel execution with deployment and validation phases.

A simple way to get started with Pipeline is to use the *Snippet Generator* available in the configuration screen for a Jenkins *Pipeline* job. Using the *Snippet Generator*, you can create a Pipeline script as you might through the dropdowns in other Jenkins jobs.

Folder Computation

Multibranch Pipeline projects and *Organization Folders* extend the existing folder functionality by introducing 'computed' folders. Computed folders automatically run a process to manage the folder contents. This computation, in the case of *Multibranch Pipeline* projects, creates child items for each eligible branch within the child. For *Organization Folders*, computation populates child items for repositories as individual *Multibranch Pipelines*.

Folder computation may happen automatically via webhook callbacks, as branches and repositories are created or removed. Computation may also be triggered by the *Build Trigger* defined in the configuration, which will automatically run a computation task after a period of inactivity (this defaults to run after one day).

[role="image-border"] image::folder-computation-build-trigger-schedule.png[scaledwidth="75%"]

Information about the last execution of the folder computation is available in the *Folder Computation* section.

[role="image-border"] image::folder-computation-main.png[scaledwidth="75%",width="75%"]

The log from the last attempt to compute the folder is available from this page. If folder computation doesn't result in an expected set of repositories, the log may have useful information to diagnose the problem.

[role="image-border"] image::folder-computation-log.png[scaledwidth="75%",width="75%"]

Configuration

Both *Multibranch Pipeline* projects and *Organization Folders* have configuration options to allow precise selection of repositories. These features also allow selection of two types of credentails to use when connecting to the remote systems:

*

scan credentials, which are used for accessing the GitHub or Bitbucket APIs

*
checkout credentials, which are used when the repository is cloned from the
 remote system; it may be useful to choose an SSH key or ”- *anonymous* -“, which uses the default credentials configured for the OS user

IMPORTANT: If you are using a *GitHub Organization*, you should create a GitHub access token[112] to use to avoid storing your password in Jenkins and prevent any issues when using the GitHub API. When using a GitHub access token, you must use standard *Username with password* credentials, where the username is the same as your GitHub username and the password is your access token.

Multibranch Pipeline Projects

Multibranch Pipeline projects are one of the fundamental enabling features for *Pipeline as Code*. Changes to the build or deployment procedure can evolve with project requirements and the job always reflects the current state of the project. It also allows you to configure different jobs for different branches of the same project, or to forgo a job if appropriate. The `Jenkinsfile` in the root directory of a branch or pull request identifies a multibranch project.

NOTE: *Multibranch Pipeline* projects expose the name of the branch being built with the `BRANCH_-NAME` environment variable and provide a special `checkout scm` Pipeline command, which is guaranteed to check out the specific commit that the Jenkinsfile originated. If the Jenkinsfile needs to check out the repository for any reason, make sure to use `checkout scm`, as it also accounts for alternate origin repositories to handle things like pull requests.

To create a *Multibranch Pipeline*, go to: *New Item -> Multibranch Pipeline*. Configure the SCM source as appropriate. There are options for many different types of repositories and services including Git, Mercurial, Bitbucket, and GitHub. If using GitHub, for example, click *Add source*, select GitHub and configure the appropriate owner, scan credentials, and repository.

Other options available to *Multibranch Pipeline* projects are:

- *API endpoint* - an alternate API endpoint to use a self-hosted GitHub Enterprise
- *Checkout credentials* - alternate credentials to use when checking out the code (cloning)
- *Include branches* - a regular expression to specify branches to include
- *Exclude branches* - a regular expression to specify branches to exclude; note that this will take precedence over includes
- *Property strategy* - if necessary, define custom properties for each branch

After configuring these items and saving the configuration, Jenkins will automatically scan the repository and import appropriate branches.

[112]https://github.com/settings/tokens/new?scopes=repo,public_repo,admin:repo_hook,admin:org_hook&amp;description=Jenkins+Access

Organization Folders

Organization Folders offer a convenient way to allow Jenkins to automatically manage which repositories are automatically included in Jenkins. Particularly, if your organization utilizes *GitHub Organizations* or *Bitbucket Teams*, any time a developer creates a new repository with a `Jenkinsfile`, Jenkins will automatically detect it and create a *Multibranch Pipeline* project for it. This alleviates the need for administrators or developers to manually create projects for these new repositories.

To create an *Organization Folder* in Jenkins, go to: *New Item -> GitHub Organization* or *New Item -> Bitbucket Team* and follow the configuration steps for each item, making sure to specify appropriate *Scan Credentials* and a specific *owner* for the GitHub Organization or Bitbucket Team name, respectively.

Other options available are:

- *Repository name pattern* - a regular expression to specify which repositories are *included*
- *API endpoint* - an alternate API endpoint to use a self-hosted GitHub Enterprise
- *Checkout credentials* - alternate credentials to use when checking out the code (cloning)

After configuring these items and saving the configuration, Jenkins will automatically scan the organization and import appropriate repositories and resulting branches.

Orphaned Item Strategy

Computed folders can remove items immediately or leave them based on a desired retention strategy. By default, items will be removed as soon as the folder computation determines they are no longer present. If your organization requires these items remain available for a longer period of time, simply configure the Orphaned Item Strategy appropriately. It may be useful to keep items in order to examine build results of a branch after it's been removed, for example.

[role="image-border"] image::orphaned-item-strategy.png[scaledwidth="75%"]

Icon and View Strategy

You may also configure an icon to use for the folder display. For example, it might be useful to display an aggregate health of the child builds. Alternately, you might reference the same icon you use in your GitHub organization account.

[role="image-border"] image::folder-icon.png[scaledwidth="75%"]

Example

To demonstrate using an Organization Folder to manage repositories, we'll use the fictitious organization: CloudBeers, Inc..

Go to *New Item*. Enter 'cloudbeers' for the item name. Select *GitHub Organization* and click *OK*.

[role="image-border"] image::screenshot1.png[scaledwidth="75%"]

Optionally, enter a better descriptive name for the *Description*, such as 'CloudBeers GitHub'. In the *Repository Sources* section, complete the section for "GitHub Organization". Make sure the *owner* matches the GitHub Organization name exactly, in our case it must be: *cloudbeers*. This defaults to the same value that was entered for the item name in the first step. Next, select or add new "Scan credentials" - we'll enter our GitHub username and access token as the password.

[role="image-border"] image::screenshot2.png[scaledwidth="75%"]

After saving, the "Folder Computation" will run to scan for eligible repositories, followed by multibranch builds.

[role="image-border"] image::screenshot3.png[scaledwidth="75%"]

Refresh the page after the job runs to ensure the view of repositories has been updated.

[role="image-border"] image::screenshot4.png[scaledwidth="75%"]

A this point, you're finished with basic project configuration and can now explore your imported repositories. You can also investigate the results of the jobs run as part of the initial *Folder Computation*.

[role="image-border"] image::screenshot5.png[scaledwidth="75%"]

Continuous Delivery with Pipeline

Introduction

Continuous delivery allows organizations to deliver software with lower risk. The path to continuous delivery starts by modeling the software delivery pipeline used within the organization and then focusing on the automation of it all. Early, directed feedback, enabled by pipeline automation enables software delivery more quickly over traditional methods of delivery.

Jenkins is the Swiss army knife in the software delivery toolchain. Developers and operations (DevOps) personnel have different mindsets and use different tools to get their respective jobs done. Since Jenkins integrates with a huge variety of toolsets, it serves as the intersection point between development and operations teams.

Many organizations have been orchestrating pipelines with existing Jenkins plugins for several years. As their automation sophistication and their own Jenkins experience increases, organizations inevitably want to move beyond simple pipelines and create complex flows specific to their delivery process.

These Jenkins users require a feature that treats complex pipelines as a first-class object, and so the Pipeline plugin[113] was developed .

[113]https://wiki.jenkins-ci.org/display/JENKINS/Pipeline+Plugin

Pre-requisites

Continuous delivery is a process - rather than a tool - and requires a mindset and culture that must percolate from the top-down within an organization. Once the organization has bought into the philosophy, the next and most difficult part is mapping the flow of software as it makes its way from development to production.

The root of such a pipeline will always be an orchestration tool like a Jenkins, but there are some key requirements that such an integral part of the pipeline must satisfy before it can be tasked with enterprise-critical processes:

- *Zero or low downtime disaster recovery*: A commit, just as a mythical hero,
- *Audit runs and debug ability*: Build managers like to see the exact execution
  encounters harder and longer challenges as it makes its way down the pipeline. It is not unusual to see pipeline executions that last days. A hardware or a Jenkins failure on day six of a seven-day pipeline has serious consequences for on-time delivery of a product. flow through the pipeline, so they can easily debug issues.

To ensure a tool can scale with an organization and suitably automate existing delivery pipelines without changing them, the tool should also support:

- *Complex pipelines*: Delivery pipelines are typically more complex than
  canonical examples (linear process: Dev->Test->Deploy, with a couple of operations at each stage). Build managers want constructs that help parallelize parts of the flow, run loops, perform retries and so forth. Stated differently, build managers want programming constructs to define pipelines.
- *Manual interventions*: Pipelines cross intra-organizational boundaries
  necessitating manual handoffs and interventions. Build managers seek capabilities such as being able to pause a pipeline for a human to intervene and make manual decisions.

The Pipeline plugin allows users to create such a pipeline through a new job type called Pipeline. The flow definition is captured in a Groovy script, thus adding control flow capabilities such as loops, forks and retries. Pipeline allows for stages with the option to set concurrencies, preventing multiple builds of the same pipeline from trying to access the same resource at the same time.

Concepts

.Pipeline Job Type

There is just one job to capture the entire software delivery pipeline in an organization. Of course, you can still connect two Pipeline job types together if you want. A Pipeline job type uses a Groovy-based DSL for job definitions. The DSL affords the advantage of defining jobs programmatically:

```
node('linux'){
  git url: 'https://github.com/jglick/simple-maven-project-with-tests.git'
  def mvnHome = tool 'M3'
  env.PATH = "${mvnHome}/bin:${env.PATH}"
  sh 'mvn -B clean verify'
}
```

.Stages

Intra-organizational (or conceptual) boundaries are captured through a primitive called "stages." A deployment pipeline consists of various stages, where each subsequent stage builds on the previous one. The idea is to spend as few resources as possible early in the pipeline and find obvious issues, rather than spend a lot of computing resources for something that is ultimately discovered to be broken.

[[throttled-concurrent]] .Throttled stage concurrency with Pipeline image::stage-concurrency.png[scaledwidth="90

Consider a simple pipeline with three stages. A naive implementation of this pipeline can sequentially trigger each stage on every commit. Thus, the deployment step is triggered immediately after the Selenium test steps are complete. However, this would mean that the deployment from commit two overrides the last deployment in motion from commit one. The right approach is for commits two and three to wait for the deployment from commit one to complete, consolidate all the changes that have happened since commit one and trigger the deployment. If there is an issue, developers can easily figure out if the issue was introduced in commit two or commit three.

Pipeline provides this functionality by enhancing the stage primitive. For example, a stage can have a concurrency level of one defined to indicate that at any point only one thread should be running through the stage. This achieves the desired state of running a deployment as fast as it should run.

```
 stage name: 'Production', concurrency: 1
 node {
     unarchive mapping: ['target/x.war' : 'x.war']
     deploy 'target/x.war', 'production'
     echo 'Deployed to http://localhost:8888/production/'
 }
```

.Gates and Approvals

Continuous delivery means having binaries in a release ready state whereas continuous deployment means pushing the binaries to production - or automated deployments. Although continuous deployment is a sexy term and a desired state, in reality organizations still want a human to give the final approval before bits are pushed to production. This is captured through the "input" primitive in Pipeline. The input step can wait indefinitely for a human to intervene.

```
input message: "Does http://localhost:8888/staging/ look good?"
```

.Deployment of Artifacts to Staging/Production

Deployment of binaries is the last mile in a pipeline. The numerous servers employed within the organization and available in the market make it difficult to employ a uniform deployment step. Today, these are solved by third-party deployer products whose job it is to focus on deployment of a particular stack to a data center. Teams can also write their own extensions to hook into the Pipeline job type and make the deployment easier.

Meanwhile, job creators can write a plain old Groovy function to define any custom steps that can deploy (or undeploy) artifacts from production.

```
def deploy(war, id) {
    sh "cp ${war} /tmp/webapps/${id}.war"
}
```

.Restartable flows

All Pipelines are resumable, so if Jenkins needs to be restarted while a flow is running, it should resume at the same point in its execution after Jenkins starts back up. Similarly, if a flow is running a lengthy sh or bat step when an agent unexpectedly disconnects, no progress should be lost when connectivity is restored.

There are some cases when a flow build will have done a great deal of work and proceeded to a point where a transient error occurred: one which does not reflect the inputs to this build, such as source code changes. For example, after completing a lengthy build and test of a software component, final deployment to a server might fail because of network problems.

.Pipeline Stage View

When you have complex builds pipelines, it is useful to see the progress of each stage and to see where build failures are occurring in the pipeline. This can enable users to debug which tests are failing at which stage or if there are other problems in their pipeline. Many organization also want to make their pipelines user-friendly for non-developers without having to develop a homegrown UI, which can prove to be a lengthy and ongoing development effort.

The Pipeline Stage View feature offers extended visualization of Pipeline build history on the index page of a flow project. This visualization also includes helpful metrics like average run time by stage and by build, and a user-friendly interface for interacting with input steps.

.Pipeline Stage View plugin image::workflow-big-responsive.png[scaledwidth="90%"]

The only prerequisite for this plugin is a pipeline with defined stages in the flow. There can be as many stages as you desired and they can be in a linear sequence, and the stage names will be displayed as columns in the Stage View interface.

Artifact traceability and with fingerprints

Traceability is important for DevOps teams who need to be able to trace code from commit to deployment. It enables impact analysis by showing relationships between artifacts and allows for visibility into the full lifecycle of an artifact, from its code repository to where the artifact is eventually deployed in production.

Jenkins and the Pipeline feature support tracking versions of artifacts using file fingerprinting, which allows users to trace which downstream builds are using any given artifact. To fingerprint with Pipeline, simply add a “fingerprint: true” argument to any artifact archiving step. For example:

```
archiveArtifacts artifacts: '**', fingerprint: true
```

will archive any WAR artifacts created in the Pipeline and fingerprint them for traceability. This trace log of this artifact and a list of all fingerprinted artifacts in a build will then be available in the left-hand menu of Jenkins:

To find where an artifact is used and deployed to, simply follow the “more details” link through the artifact’s name and view the entires for the artifact in its “Usage” list.

[[fingerprinting]] .Fingerprint of a WAR image::fingerprinting.png[scaledwidth=”90%”]

For more information, visit the https://wiki.jenkins-ci.org/display/JENKINS/Fingerprint[fingerprint documentation] to learn more about how fingerprints work.

License

Code

Content

[114]https://creativecommons.org/licenses/by-sa/4.0/
[115]https://creativecommons.org/licenses/by-sa/4.0/
[116]https://creativecommons.org/licenses/by-sa/4.0/legalcode