



Seguridad en la integración continua de la Metodología ágil y la filosofía DevOps

Universidad de Sevilla
Escuela Técnica Superior de Ingeniería

Máster en Seguridad de la Información y las Comunicaciones

Autor: Eleazar Rubio Sorrentino

Tutor: Juan Manuel Vozmediano Torres





Índice de la presentación



1

Introducción

2

Descripción de la técnica

3

Entorno de trabajo

4

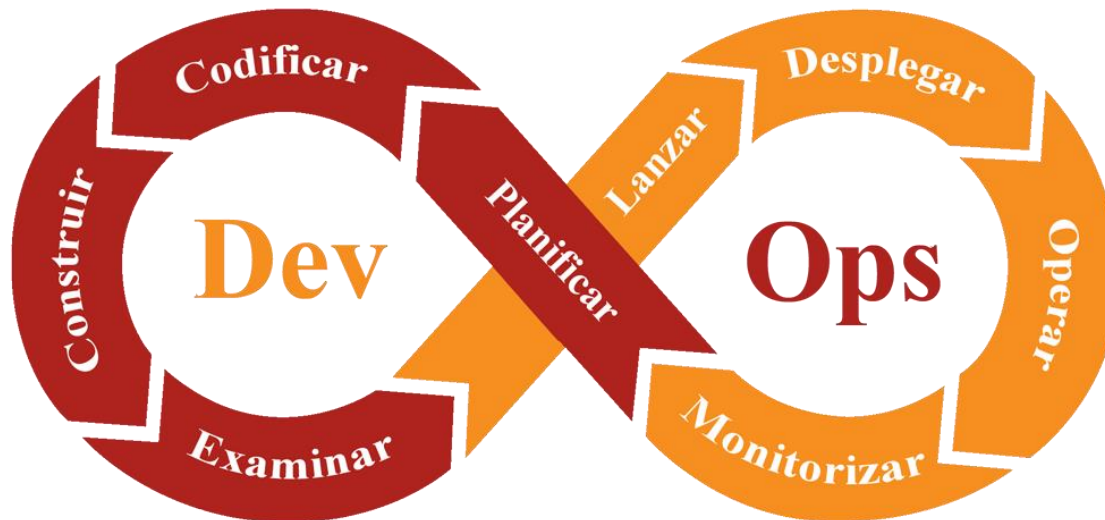
Desarrollo de la solución

5

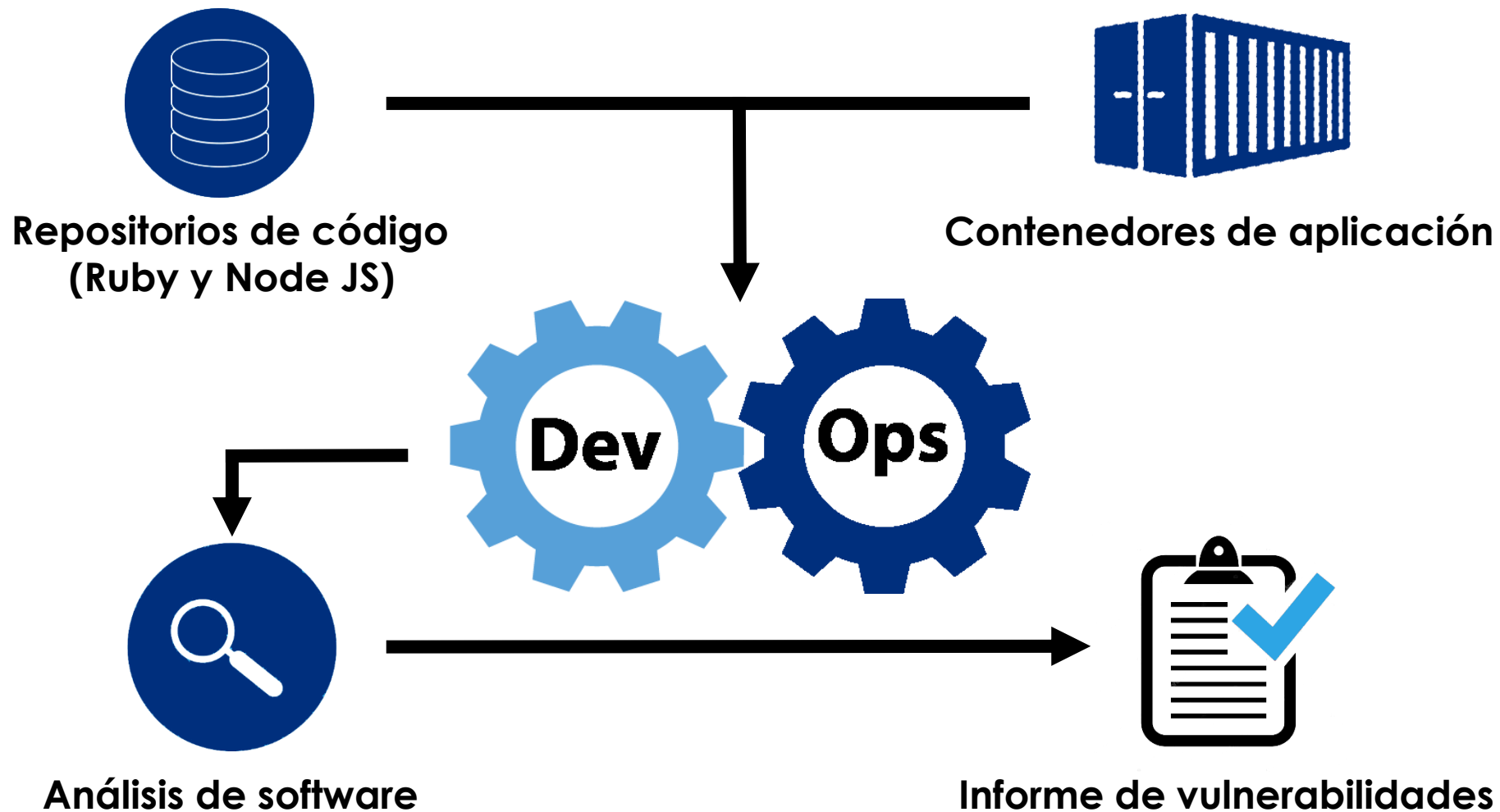
Conclusiones

Contexto y motivación

- Transformación digital de las empresas.
- Desarrollo y operaciones (DevOps).
- Contenedores de aplicación.



Objetivo



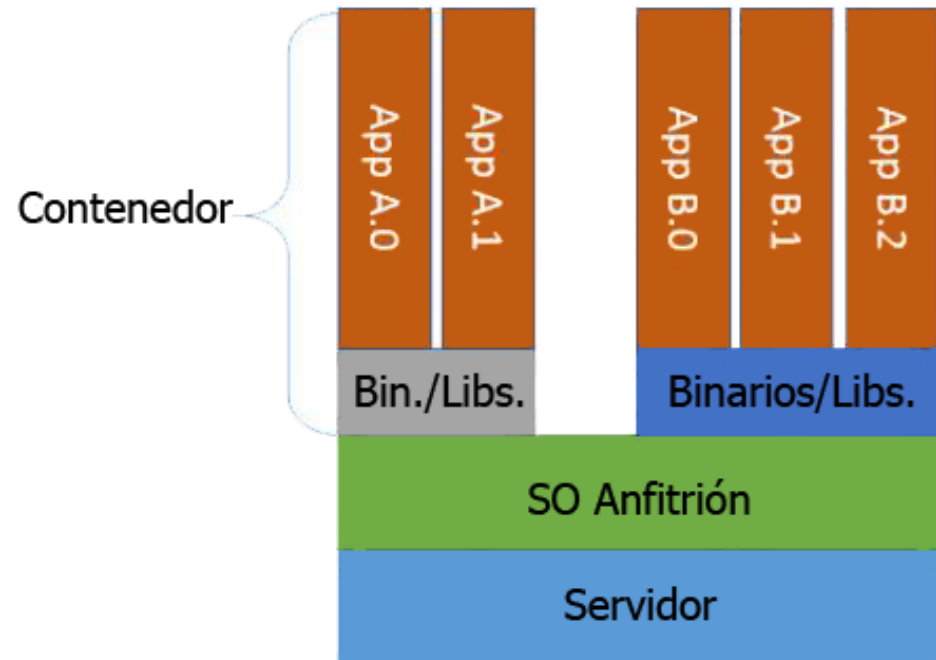
Metodología Ágil



Virtualización de contenedores



Virtualización Tradicional



Basada en contenedores

Integración Continua (IC):

- Varios cambios de código al día.
- Verificación por compilación automática.
- Búsqueda de error muy acotada.

Despliegue Continuo (DC):

- Liberación de código en producción.
- Pruebas continuas y automáticas.
- Estrechamente ligado a IC.

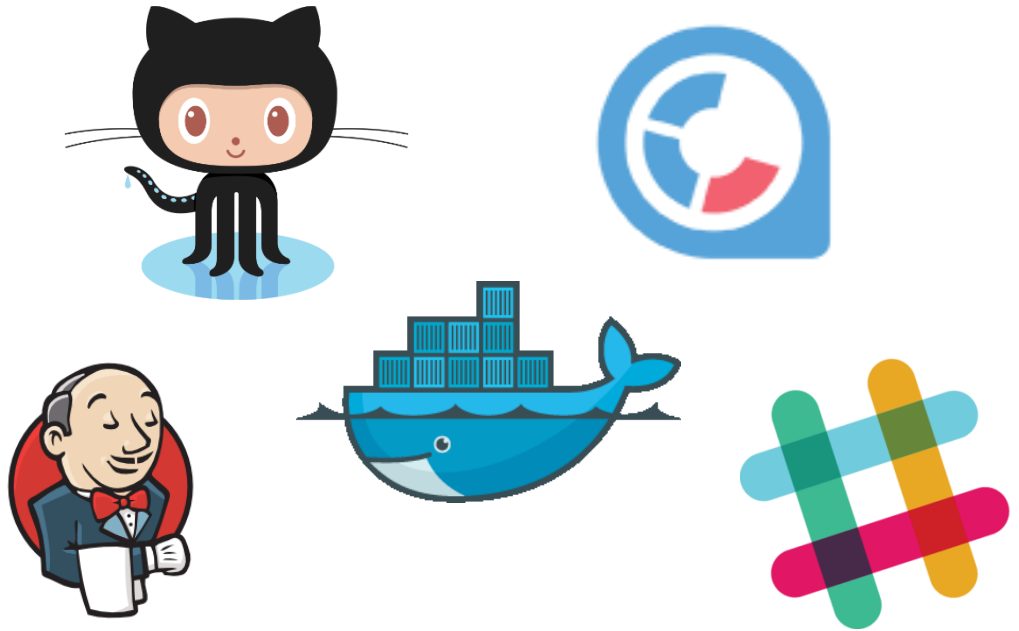
Análisis estático:

- Método de depuración de aplicaciones.
- Código que no está en ejecución.
- Herramientas automatizadas.

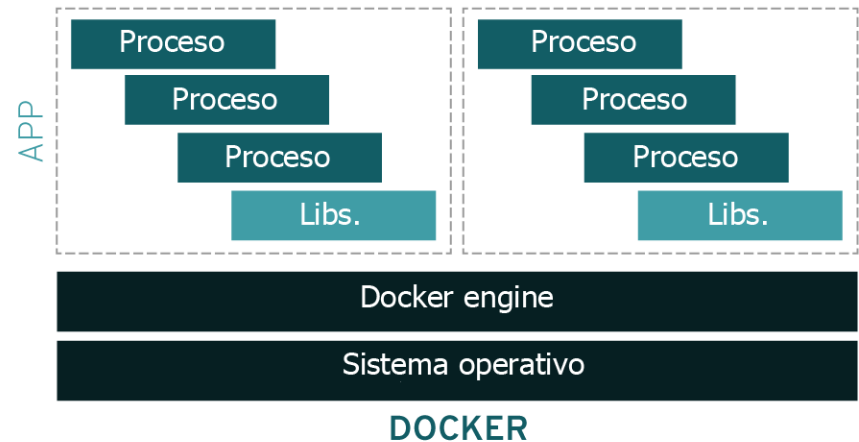
Dependencias de código:

- Aplicación o biblioteca.
- Requerida por la aplicación principal.
- *gemfile.lock* y *package.json*.

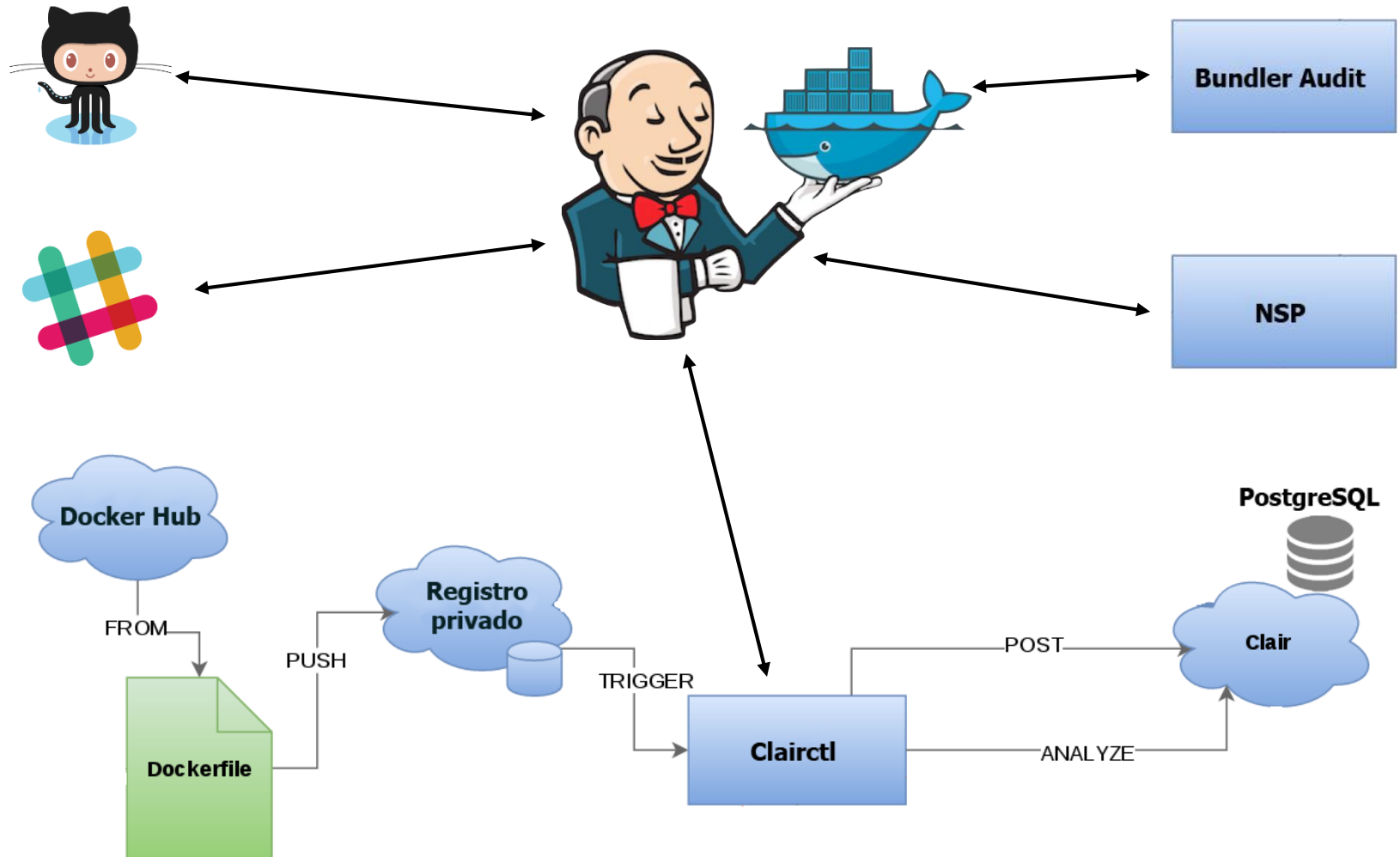
- Git y GitHub.
- Bundler Audit.
- NSP.
- Docker.
- Clair y Clairctl.
- Jenkins.
- Slack.



Contenedores tradicionales Linux vs Docker



Preparación del entorno – Docker Compose



Docker Compose - Clair

```
clair:
  container_name: clair_clair
  image: quay.io/coreos/clair:v2.0.0
  restart: unless-stopped
  depends_on:
    - postgres
  ports:
    - "6060-6061:6060-6061"
  links:
    - postgres
  volumes:
    - /tmp:/tmp
    - ./clair_config:/config
  command: [-config, /config/config.yaml]
postgres:
  container_name: clair_postgres
  image: postgres:9.6
  restart: unless-stopped
  volumes:
    - "data-postgres:/var/lib/postgresql/data"
  environment:
    POSTGRES_PASSWORD: password
```

Docker Compose – Jenkins y Herramientas de análisis

```
jenkins:
  build: ./jenkins
  container_name: jenkins
  ports:
    - "80:8080"
  restart: "always"
  volumes:
    - "data-jenkins:/var/jenkins_home"
    - "reports:/reports"
    - "/usr/bin/docker:/usr/bin/docker"
    - "/var/run/docker.sock:/var/run/docker.sock:ro"
    - "/usr/lib/x86_64-linux-gnu/libltdl.so.7:/usr/lib/x86_64-linux-gnu/libltdl.so.7"
```

```
clairctl:
  build: ./clairctl
  container_name: clair_clairctl
  command: [echo, Hello from clairctl container]

ruby-tool:
  build: ./audit-tools/ruby
  container_name: ruby-tool
  command: [echo, Hello from ruby-tool container]

nodejs-tool:
  build: ./audit-tools/nodejs
  container_name: nodejs-tool
  command: [echo, Hello from nodejs-tool container]
```

Desplegando el entorno

```
eleazarr [~/Master/Master_Ciberseguridad_US/Entorno] (master)$ docker-compose up -d
Creating network "entorno_default" with the default driver
Creating ruby-tool
Creating c_postgres
Creating clairctl
Creating jenkins
Creating nodejs-tool
Creating clair_clair
eleazarr [~/Master/Master_Ciberseguridad_US/Entorno] (master)$
```

```
eleazarr [~/Master/Master_Ciberseguridad_US/Entorno] (master)$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
entorno_ruby-tool	latest	2c03730336ae	2 weeks ago	118MB
entorno_jenkins	latest	2aa7adbb558a	2 weeks ago	844MB
entorno_nodejs-tool	latest	3fe087664545	2 weeks ago	60.7MB
entorno_clairctl	latest	b69f2558be60	2 weeks ago	1.34GB
postgres	9.6	eb0f0e9af6d2	2 weeks ago	266MB
postgres	latest	eb0f0e9af6d2	2 weeks ago	266MB
jenkins/jenkins	lts	aca6340878dd	2 weeks ago	840MB
golang	1.8.3	ec1b36e59395	2 weeks ago	699MB
ruby	2.1.10-alpine	614872f94ade	2 months ago	118MB
alpine	latest	7328f6f8b418	2 months ago	3.97MB
quay.io/coreos/clair	v2.0.0	c5ec68ce85d5	4 months ago	387MB
node	6.10.2-alpine	24d2680547f5	5 months ago	54.1MB

```
eleazarr [~/Master/Master_Ciberseguridad_US/Entorno] (master)$
```

Jenkins CI – Configuración inicial

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/jenkins_home/secrets/initialAdminPassword
```

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

Administrator password

Getting Started

Create First Admin User

Username:	<input type="text" value="eleazar"/>
Password:	<input type="password" value="*****"/>
Confirm password:	<input type="password" value="*****"/>
Full name:	<input type="text" value="Eleazar Rubio Sorrentino"/>
E-mail address:	<input type="text" value="elerubio@us.es"/>

```
eleazarr [~] $ docker exec -ti jenkins bash
jenkins@4f58433cdacf:/$ cat /var/jenkins_home/secrets/initialAdminPassword
4c23c9dad3c74e52b869ef223e635c8c
jenkins@4f58433cdacf:/$
```

The screenshot shows the Jenkins web interface in a browser window. The address bar displays 'jenkins.tfm.com'. The Jenkins logo is at the top left. A sidebar on the left contains links: 'New Item', 'People', 'Build History', 'Manage Jenkins', 'My Views', and 'Credentials'. The main content area features a 'Welcome to Jenkins!' message with a button that says 'Please create new jobs to get started.' Below this, there are two expandable sections: 'Build Queue' (showing 'No builds in the queue.') and 'Build Executor Status' (showing two 'Idle' executors).

Trabajos de Jenkins - Fases

1



Dependencias

2



Análisis

3



Informe HTML

4



Notificación

Dependencias Ruby – Gemfile.lock

Enter an item name

» Required field



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 slaves. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.



External Job

This type of job allows you to record the execution of a process run outside Jenkins, even on a remote machine. This is designed so that you can use Jenkins as a dashboard of your existing automation system.



Multi-configuration project

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



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.

OK

Dependencias Ruby – Gemfile.lock



The screenshot shows the Jenkins configuration interface for a job. The 'General' tab is selected. A parameter named 'RUBY_REPOS' is configured with a 'Default Value' of 'gemfile_vulnerable' and a 'Description' of 'gemfile_vulnerable'. The parameter type is set to 'Plain text'. There is a 'Preview' link and an 'Add Parameter' button at the bottom.

Name	RUBY_REPOS
Default Value	gemfile_vulnerable
Description	gemfile_vulnerable

[Plain text] [Preview](#)

Add Parameter ▾

```
curl https://raw.githubusercontent.com/ElazarWorkshare/${RUBY_REPOS[i]}/  
master/${audit_files[j]} -o ./${RUBY_REPOS[i]}/${audit_files[j]} -f
```

```
sudo docker run --rm -i -v /var/lib/docker/volumes/entorno_data-jenkins/  
_data/workspace/analisis-dependencias-ruby/${RUBY_REPOS[i]}/Gemfile.  
lock:/Gemfile.lock -v /var/lib/docker/volumes/entorno_data-jenkins/  
_data/workspace/analisis-dependencias-ruby/${RUBY_REPOS[i]}/Gemfile:/  
Gemfile entorno_ruby-tool:latest bundle-audit check --update ${ignore  
}
```


Dependencias Ruby – Gemfile.lock



Jenkins > analisis-dependencias-ruby >

[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build with Parameters](#)
[Delete Pipeline](#)
[Configure](#)
[Full Stage View](#)
[HTML Report](#)
[Pipeline Syntax](#)

Pipeline analisis-dependencias-ruby


[Recent Changes](#)

Stage View

Average stage times:

Download dependencies files	Generate Audited repo report	Generate html report	Notify generated report
1s	1s	64ms	748ms
1s	1s	63ms	594ms
1s	1s	46ms	667ms
1s	1s	56ms	602ms



Build History

[trend](#)

find x

#18	12-Sep-2017 15:08
#17	12-Sep-2017 15:08
#16	12-Sep-2017 15:06
#15	12-Sep-2017 15:05
#14	12-Sep-2017 15:04
#13	12-Sep-2017 15:03
#12	12-Sep-2017 15:02
#11	12-Sep-2017 14:58
#10	12-Sep-2017 14:56
#9	12-Sep-2017 14:53

Dependencias Ruby – Gemfile.lock

[Back to analisis-dependencias-ruby](#) [index](#)

Ruby services

gemfile_vulnerable

Updating ruby-advisory-db ...

Skipping update

ruby-advisory-db: 287 advisories

Name: activesupport

Version: 4.1.1

Advisory: CVE-2015-3226

Criticality: Unknown

URL: https://groups.google.com/forum/#!topic/ruby-security-ann/7VIB_pck3hU

Title: XSS Vulnerability in ActiveSupport::JSON.encode

Solution: upgrade to >= 4.2.2, < 4.1.11

Name: activesupport

Version: 4.1.1

Advisory: CVE-2015-3227

Criticality: Unknown



URL: <https://groups.google.com/forum/#!topic/rubyonrails-security/bahr2JLnxvk>

Title: Possible Denial of Service attack in ActiveSupport

Solution: upgrade to >= 4.2.2, < 4.1.11, < 3.2.22


Vulnerabilities found!




Static Analysis  

eleazar.rubio

All Threads


Channels 

- # analisis-dependencias
- # analisis-docker
- # general
- # random

Direct Messages 

- slackbot
- eleazar.rubio (you)

+ Invite People

Apps 

#analisis-dependencias

☆ | 1 | 0 | Add a topic

Today

Jenkins APP 4:04 PM

[FAILED] Analisis Ruby - Encontradas vulnerabilidades!

Repositorios afectados:

gemfile_vulnerable

HTML report:

http://jenkins.tfm.com/job/analisis-dependencias-ruby/17/HTML_Report/

[FAILED] Analisis Ruby - Encontradas vulnerabilidades!

Repositorios afectados:

gemfile_vulnerable

HTML report:

http://jenkins.tfm.com/job/analisis-dependencias-ruby/18/HTML_Report/

+ Message #analisis-dependencias

Clair y Clairctl

General Build Triggers Advanced Project Options Pipeline

String Parameter

Name

DOCKER_REPOS

Default Value

entorno_ruby-tool entorno_jenkins entorno_nodejs-tool entorno_clairctl

Description

entorno_ruby-tool
entorno_jenkins
entorno_nodejs-tool
entorno_clairctl

[Plain text] [Preview](#)

Add Parameter

```
sudo docker run --rm -t -v entorno_reports:/go/src/github.com/jgsquare/clairctl/reports -v /var/run/docker.sock:/var/run/docker.sock:ro --net entorno_default --link clair_clair:clair -p 57330:57330 entorno_clairctl bash -c "cd /go/src/github.com/jgsquare/clairctl/ ; ./clairctl analyze --log-level info --local $repos ; ./clairctl report --log-level info --local $repos"
```

Clair y Clairctl

[Back to analisis-imagenes-docker](#) entorno_nodejs-tool-latest[Zip](#)

CLAIR CONTROL REPORT

Image: entorno_nodejs-tool

Total : 4 vulnerabilities

● Medium : 2

● High : 2



f8dbd94f01f47abe1601b36743b10b4801edb169dc2cfbf728ac13794a9b9f71

zlib 1.2.8-r2 - ▲

○ **CVE-2016-9843**

[Link](#)

○ **CVE-2016-9841**

[Link](#)

○ **CVE-2016-9842**

[Link](#)

○ **CVE-2016-9840**

[Link](#)

Evaluación de la solución

[Back to analisis-dependencias-ruby](#)[index](#)

Ruby services

gemfile_vulnerable

Updating ruby-advisory-db ...
 Skipping update
 ruby-advisory-db: 287 advisories
 Name: activesupport
 Version: 4.1.1
 Advisory: CVE-2015-3226
 Criticality: Unknown
 URL: https://groups.google.com/forum/#!topic/ruby-security-ann/7VIB_pck3hU
 Title: XSS Vulnerability in ActiveSupport::JSON.encode
 Solution: upgrade to >= 4.2.2, ~> 4.1.11

Name: activesupport
 Version: 4.1.1
 Advisory: CVE-2015-3227
 Criticality: Unknown
 URL: <https://groups.google.com/forum/#!topic/rubyonrails-security/bahr2JLnxvk>
 Title: Possible Denial of Service attack in Active Support
 Solution: upgrade to >= 4.2.2, ~> 4.1.11, ~> 3.2.22

Vulnerabilities found!

GEM

```
remote: https://rubygems.org/
specs:
  activesupport (4.2.2)
```

[FAILED] Analisis Ruby - Encontradas vulnerabilidades!

Repositorios afectados:

gemfile_vulnerable

HTML report:

http://jenkins.tfm.com/job/analisis-dependencias-ruby/18/HTML_Report/

[OK] Analisis Ruby - Vulnerabilidades no encontradas!

Repositorios examinados:

gemfile_arreglado

[Back to analisis-dependencias-ruby](#)[index](#)

Ruby services

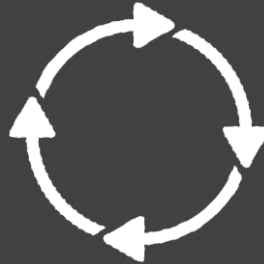


Objetivos cumplidos



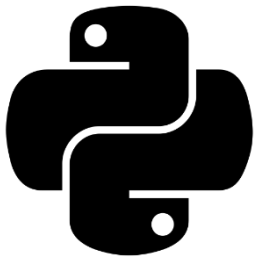
Análisis estático de
forma pasiva

Incluido en el propio
proceso de desarrollo



Utilizando contenedores de
imágenes

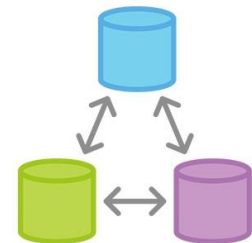
Línea futura de trabajo



Lenguajes de
programación examinados



Preparación del entorno
para producción



Ampliar la cantidad de
repositorios alcanzados

Y ahora... ¿Cómo colaboro?

GitHub, Inc. [US] | <https://github.com/EleazarWorkshare>

Search GitHub Pull requests Issues Marketplace Explore

Overview Repositories 4 Stars 0 Followers 0 Following 0

Eleazar Rubio
EleazarWorkshare
DevOps Engineer

Workshare Ltd.
London, UK.
eleazar.rubio.sorrentino@gmail.com

Organizations

Popular repositories Customize your pinned repositories

- Master_Ciberseguridad_US**
TeX
- gemfile_vulnerable**
Repositorio para la realización de las pruebas del TFM
Ruby
- package_json_vulnerable**
Repositorio para la realización de las pruebas del TFM
- gemfile_arreglado**
Ruby

399 contributions in the last year Contribution settings ▾

Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep

Mon
Wed
Fri

Learn how we count contributions. Less More

Contribution activity Jump to ▾ 2017

September 2017

Created 46 commits in 6 repositories

- [EleazarWorkshare/Master_Ciberseguridad_US](#) 21 commits
- [workshare/ansible](#) 19 commits
- [workshare/haproxy-ingress](#) 3 commits



Seguridad en la integración continua de la Metodología ágil y la filosofía DevOps

Universidad de Sevilla
Escuela Técnica Superior de Ingeniería

Máster en Seguridad de la Información y las Comunicaciones

Autor: Eleazar Rubio Sorrentino

Tutor: Juan Manuel Vozmediano Torres

