#CyberCamp19

Entornos SecDevOps Dockerizados

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índice

1.

$Whoami

Antonio Juanilla(Specter)

$WHOAMI

Antonio Juanilla

1. Autodidacta
2. Desarrollador de Software
3. SecDevOps
4. Co-Organizador de HackMadrid%27
5. Miembro del equipo de FlagHunters
6. Amante del Hacking y la Seguridad informática
7. Amante de la tecnología
8. Defensor de la democratización de la tecnología la mejora de la sociedad

Redes

Instragram, Twitter, Telegram,Github

@spectertj

#CyberCamp19

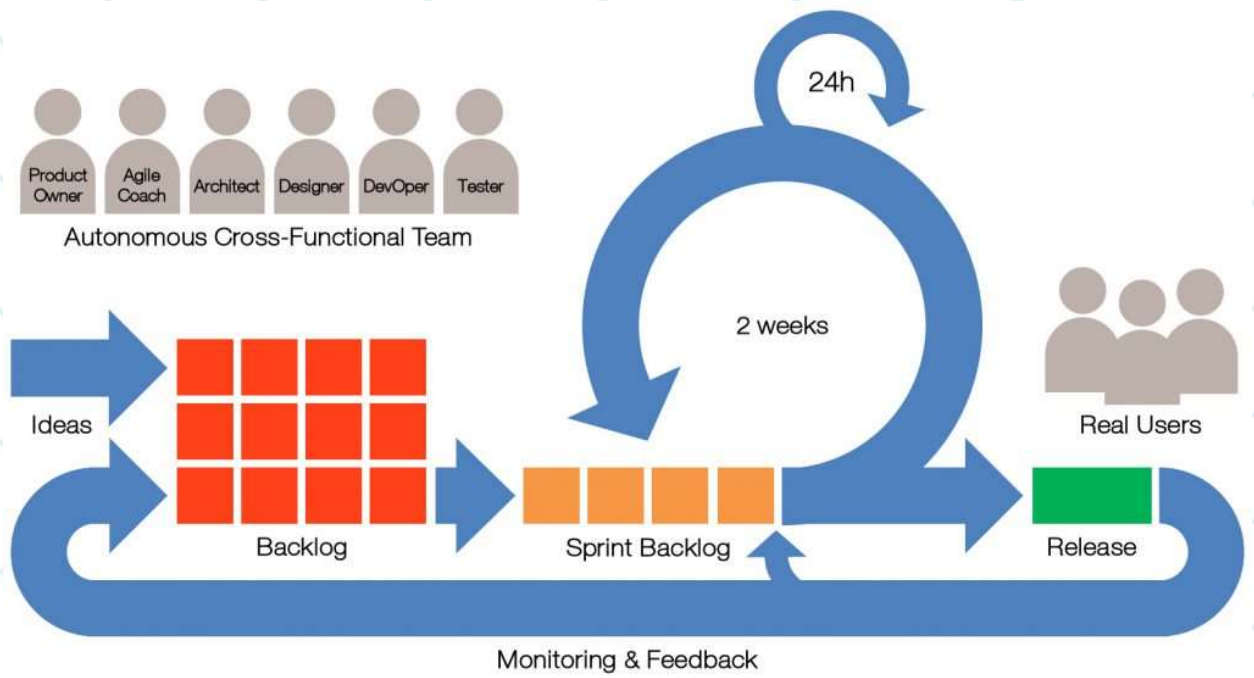
2.

Flujo del agilismo

Antonio Juanilla(Specter)

cyber camp
CYBERSECURITY EVENT
2019
TALENTO · FAMILIAS · TÉCNICOS

Flujo del agilismo



#CyberCamp19

3.

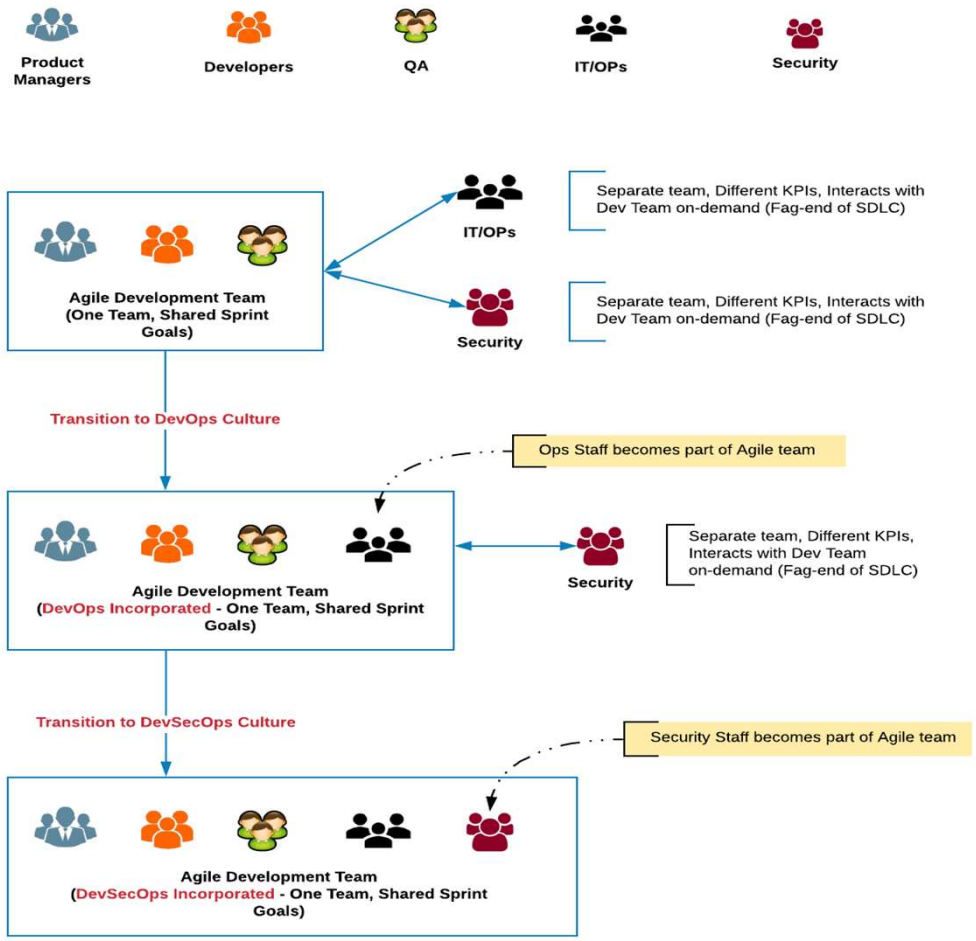
Transición

Antonio Juanilla(Specter)

cyber camp
CYBERSECURITY EVENT
2019
TALENTO FAMILIAS TÉCNICOS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Transición


Product Managers
Developers
QA
IT/OPs
Security
Agile Development Team (One Team, Shared Sprint Goals)
IT/OPs
Separate team, Different KPIs, Interacts with Dev Team on-demand (Fag-end of SDLC)
Security
Separate team, Different KPIs, Interacts with Dev Team on-demand (Fag-end of SDLC)
Transition to DevOps Culture
Ops Staff becomes part of Agile team
Agile Development Team (DevOps Incorporated - One Team, Shared Sprint Goals)
Security
Separate team, Different KPIs, Interacts with Dev Team on-demand (Fag-end of SDLC)
Transition to DevSecOps Culture
Security Staff becomes part of Agile team
Agile Development Team (DevSecOps Incorporated - One Team, Shared Sprint Goals)

#CyberCamp19

4.

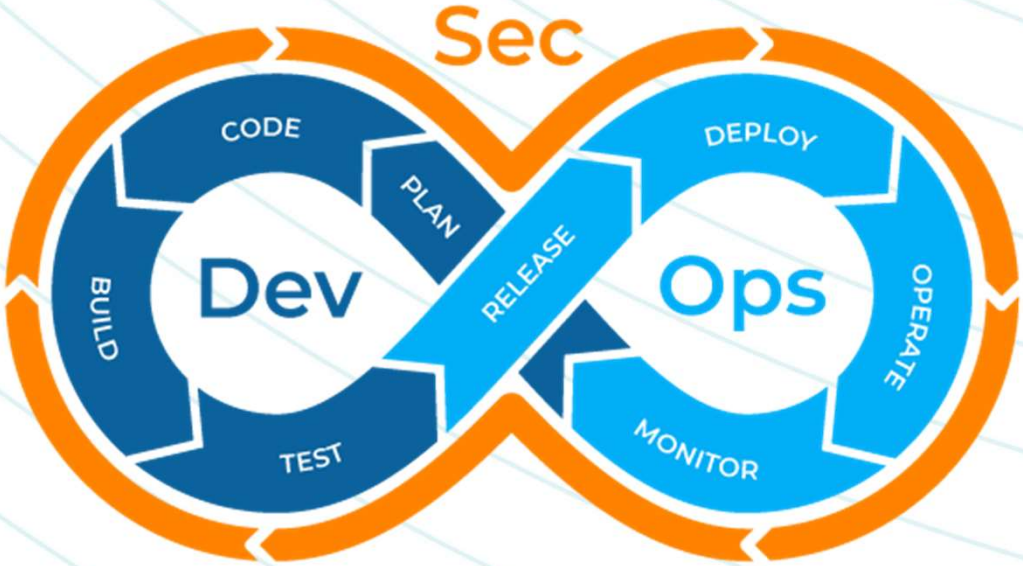
SecDevOps(DevSecOps)

Antonio Juanilla(Specter)

cyber camp
CYBERSECURITY EVENT
2019
TALENTO FAMILIAS TÉCNICOS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SecDevOps(DevSecOps)



#CyberCamp19

5.

Cultura DevOps y contenerización

Antonio Juanilla(Specter)

cyber camp
CYBERSECURITY EVENT
2019
TALENTO · FAMILIAS · TÉCNICOS

Cultura DevOps y contenerización

#CyberCamp19

6.

Taller

Antonio Juanilla(Specter)

cyber camp
CYBERSECURITY EVENT
2019

TALENTO · FAMILIAS · TÉCNICOS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Imágenes Usadas

Gitea
Jenkins
Nginx
Owasp/Sonarqube
Traefik:v1.7
Portainer
Swarmpit
stefanprodan/swarmprom-grafana:5.3.4
ELK stack y filebeat:7.4.1

Comandos iniciales

Docker pull

Docker ps -a

Docker image ls

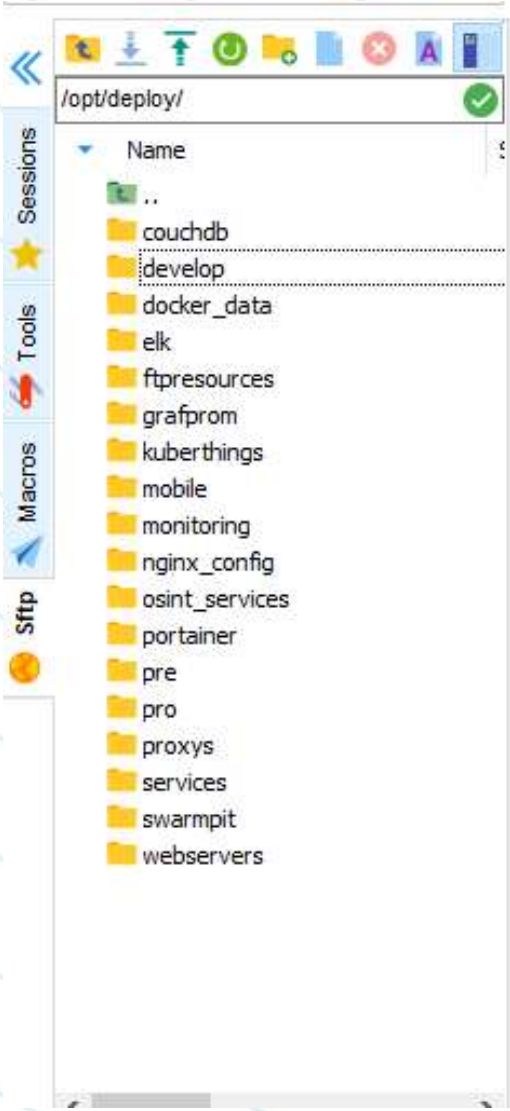
Docker *swarm init*

Docker stack deploy –c archivo.yml nombre de servicio

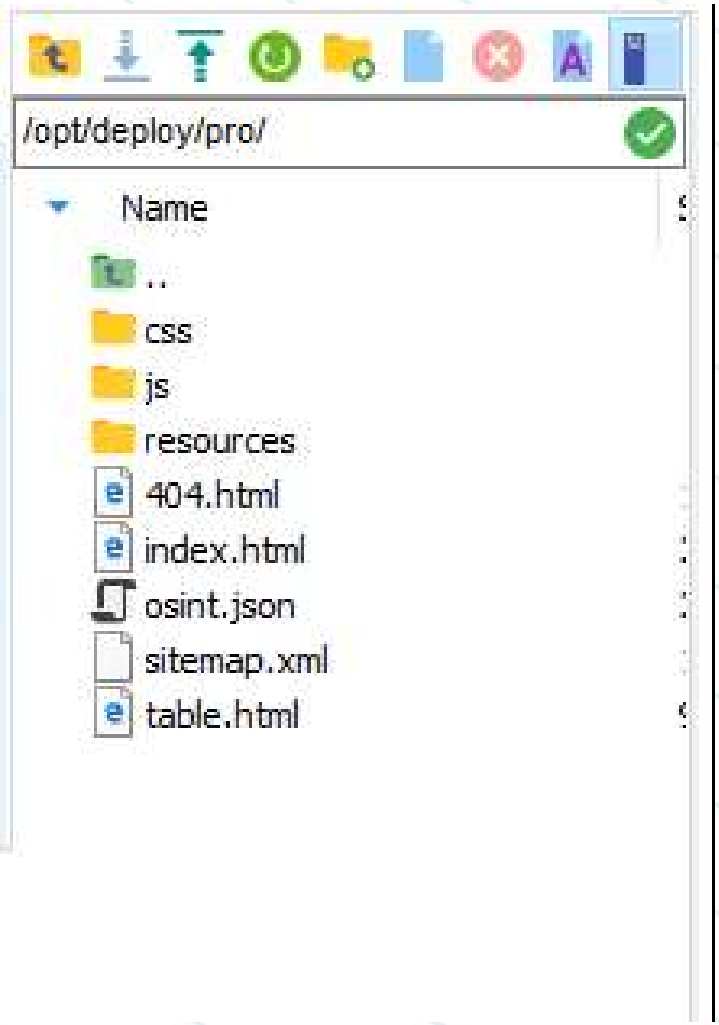
Docker stack ps servicio

Docker *swarm join {token}*

Organización



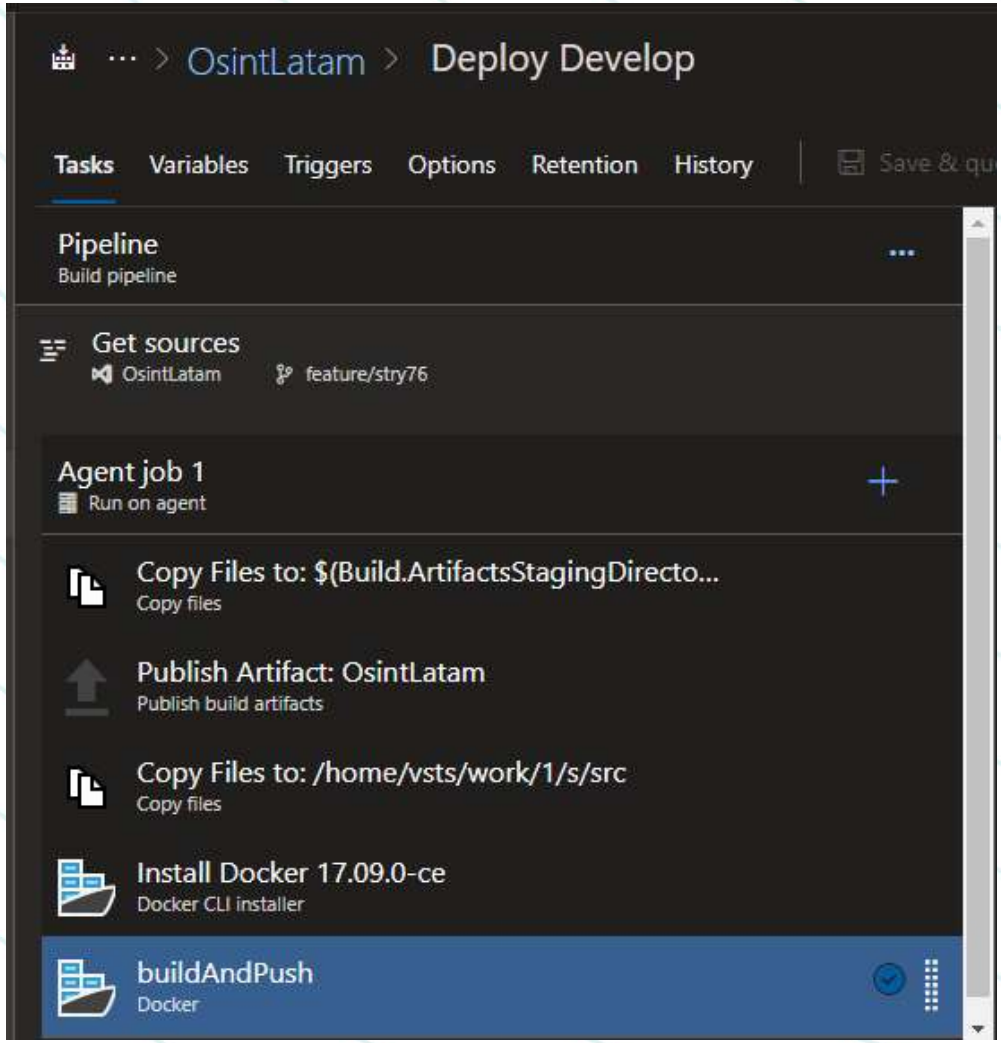
Organización



Docker-compose.yml

```yaml
version: '3.3'
services:
  dev:
    image: registry.gitlab.com/cyberitosint/osintlatam/framework-web:latest
    networks:
     - osint-net
     - traefik-public
     - default
    logging:
      driver: json-file
    deploy:
      labels:
        traefik.tags: traefik-public
        traefik.redirectorservice.frontend.redirect.entryPoint: https
        traefik.webservice.frontend.entryPoints: https
        traefik.redirectorservice.frontend.entryPoints: http
        traefik.docker.network: traefik-public
        traefik.enable: 'true'
        traefik.port: '80'
        traefik.frontend.rule: Host:dev.ciberinteligencia-osintlatinoamerica.com
      restart_policy:
        condition: on-failure
      resources:
        limits:
          cpus: '0.1'
          memory: 500M
  mobile:
    image: nginx:latest
    volumes:
     - /opt/deploy/mobile:/usr/share/nginx/html:ro
    networks:
     - osint-net
     - traefik-public
     - default
    logging:
      driver: json-file
```

Pipeline


OsintLatam > Deploy Develop
Tasks
Variables
Triggers
Options
Retention
History
Pipeline
Build pipeline
Get sources
OsintLatam
feature/stry76
Agent job 1
Run on agent
Copy Files to: $(Build.ArtifactsStagingDirecto...
Copy files
Publish Artifact: OsintLatam
Publish build artifacts
Copy Files to: /home/vsts/work/1/s/src
Copy files
Install Docker 17.09.0-ce
Docker CLI installer
buildAndPush
Docker

Pipeline.yml

OsintLatam CI

master / OsintLatam / azure-pipelines.yml

```yaml
trigger:
  - develop
pr:
  - master
  - pre

jobs:

- job: Scan
  pool:
    name: Hosted VS2017
  steps:
```

Settings

```yaml
  - task: SonarSource.sonarqube.15B84CA1-B62F-4A2A-A403-89B77A063157.SonarQubePrepare@4
    displayName: 'Prepare analysis on SonarQube'
    inputs:
      SonarQube: Sonar
      scannerMode: CLI
      configMode: manual
      cliProjectKey: OsintLatam
      cliProjectName: OsintLatam
      cliSources: src/front
```

Settings

Pipeline.yml

OsintLatam CI

master / OsintLatam / azure-pipelines.yml

```yaml
- job: Development_Deploy
  steps:
  Settings
  - task: CopyFilesOverSSH@0
    displayName: 'Securely copy files to the remote machine'
    inputs:
      sshEndpoint: 'vps ppal'
      sourceFolder: src/front
      targetFolder: /opt/deploy/develop
  condition: and(succeeded(),eq(variables['Build.SourceBranch'],'refs/heads/develop'))

- job: PRE_Deploy
  steps:
  Settings
  - task: CopyFilesOverSSH@0
    displayName: 'Securely copy files to the remote machine'
    inputs:
      sshEndpoint: 'vps ppal'
      sourceFolder: src/front
      targetFolder: /opt/deploy/pre
  condition: and(succeeded(),eq(variables['Build.SourceBranch'],'refs/heads/pre'))
```

Dockerfile

You updated feature/stry76 4 months ago — Create a pull request

Contents History Compare Blame Edit Rename Delete Download

```
1 FROM nginx:alpine
2 LABEL Author = Specter
3 COPY /front/. /usr/share/nginx/html
4 EXPOSE 80
```

Herramientas contenerizadas

1. Portainer
2. Swarmpit
3. Grafana
4. Prometheus
5. Nginx
6. Traefik

1. Elastic Search
2. Kibana
3. Logstash
4. Filebeat
5. Sonarqube

Traefik

PROVIDERS HEALTH V1.7.16 / MAROILLES DOCUMENTATION

28 FRONTENDS

frontend-redirectorservice-logging-kibana-redirectorservice

Main | Details

Route Rule

`Host:kibana.ciberinteligencia-osintlatinoamerica.com`

Entry Points: http

Backend: backend-logging-kibana-redirectorservice

frontend-redirectorservice-monitoring-alertmanager-redirectorservice

Main | Details

Route Rule

`Host:alertmanager.ciberinteligencia-osintlatinoamerica.com`

Entry Points: http

28 BACKENDS

backend-logging-kibana-redirectorservice

Main | Details

Server	Weight
http://10.0.0.94:5601	1

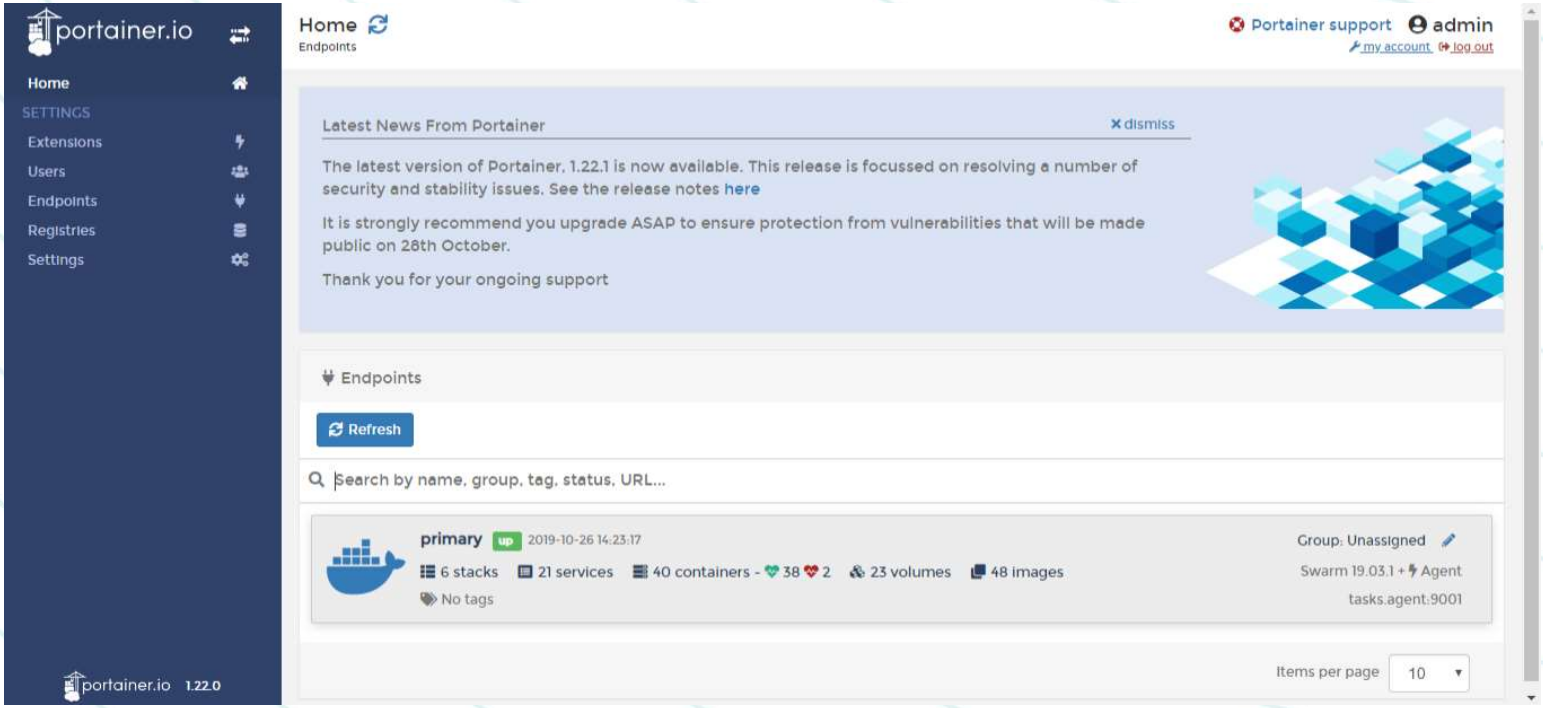
backend-logging-kibana-webservice

Main | Details

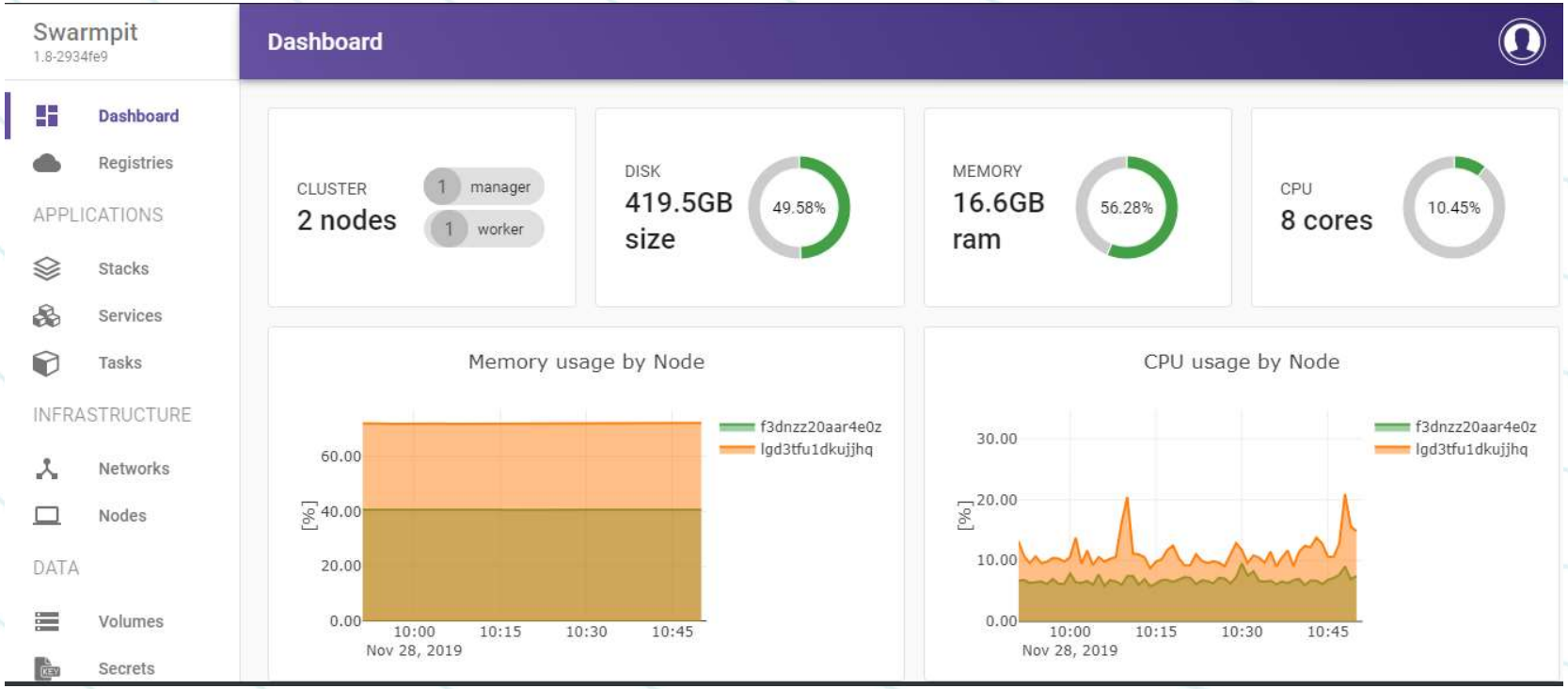
Server	Weight
http://10.0.0.94:5601	1

backend-monitoring-alertmanager-redirectorservice

Portainer


portainer.io
Home
SETTINGS
Extensions
Users
Endpoints
Registries
Settings
portainer.io 1.22.0
Home
Endpoints
Portainer support
admin
my account
log out
Latest News From Portainer
dismiss
The latest version of Portainer, 1.22.1 is now available. This release is focussed on resolving a number of security and stability issues. See the release notes here
It is strongly recommend you upgrade ASAP to ensure protection from vulnerabilities that will be made public on 28th October.
Thank you for your ongoing support
Endpoints
Refresh
Search by name, group, tag, status, URL...
primary
up
2019-10-26 14:23:17
6 stacks
21 services
40 containers - 38 2
23 volumes
48 images
No tags
Group: Unassigned
Swarm 19.03.1 + Agent
tasks.agent:9001
Items per page
10

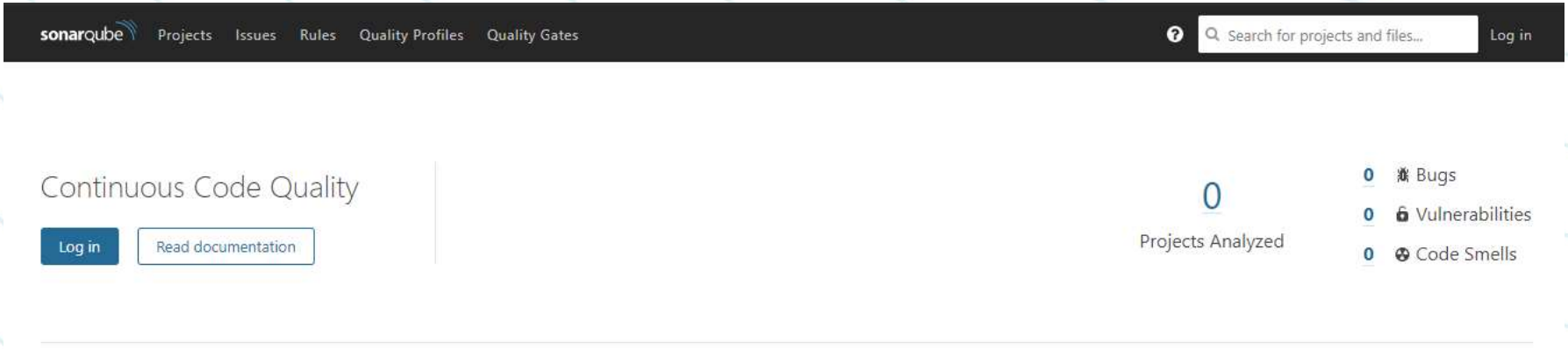
Swarmpit


Swarmpit
1.8-2934fe9
Dashboard
Registries
APPLICATIONS
Stacks
Services
Tasks
INFRASTRUCTURE
Networks
Nodes
DATA
Volumes
Secrets
Dashboard
CLUSTER
2 nodes
1 manager
1 worker
DISK
419.5GB
size
49.58%
MEMORY
16.6GB
ram
56.28%
CPU
8 cores
10.45%
Memory usage by Node
f3dnzz20aar4e0z
lgd3tfu1dkujjhq
[%]
60.00
40.00
20.00
0.00
10:00
10:15
10:30
10:45
Nov 28, 2019
CPU usage by Node
f3dnzz20aar4e0z
lgd3tfu1dkujjhq
[%]
30.00
20.00
10.00
0.00
10:00
10:15
10:30
10:45
Nov 28, 2019

Grafana


Docker Swarm Nodes
0
12:06
12:08
12:10
12:12
12:14
12:16
12:18
20%
0%
Total Memory
16.6 GB
Available Memory
39%
Total swap mem...
0 B
Used swap memory
N/A
Swap used / tota...
0%
Memory usage by Node
10 GB
8 GB
6 GB
4 GB
2 GB
Used leader.ciberinteligenc
Used worker.ciberinteligen

Sonarqube


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Search for projects and files...
Log in
Continuous Code Quality
Log in
Read documentation
0
Projects Analyzed
0 Bugs
0 Vulnerabilities
0 Code Smells

ELK stack

Discover

New Save Open Share Inspect

Search KQL Last 15 minutes Show dates Refresh

+ Add filter

logstash*

Selected fields

? _source

Available fields

@timestamp
t @version
t _id
t _index
_score
t _type
t host
t message
port

61,985 hits

Nov 28, 2019 @ 12:07:36.736 - Nov 28, 2019 @ 12:22:36.736 — Auto

Time	_source
> Nov 28, 2019 @ 12:22:09.538	message: \xCB\xED`\x8A\x87\xC27\xA8xd\a\xC5\xC3v\u0015\x8F\x8F#\xA7\xB0\xFB\x9F^\xEF\xE2\xE1\xE5\x94OI\x80\b\b[\xB5\xBFv 嚇/\xB0\u0015\xEF\u0016f\xD9ɴldNCV\xED\xDAG0\xDE4K\xF7g\xBF\xB2[\x9Eg\x8BFJ\x99\u0011B\xE5F(/Fc\x93h\xE3\xAA\u001DLnI\xE5\xEC\u000F\x8B~:\x8B\x96\xB3\x87\xE9t\xC3V\x81c\xACB3^\xA4/\u0017\u0000\xFF\xAC\v\xDC\u0019\xA4;\x95\x9A*bd\xEF\x93\xD5\u0005\u0015\x9C\xC9\xFE)%L~E\xE6\xE4\x84U\xEE\xF6!d2lG\xBD\xBF\"\u000F0M\xC3\xFF~\xC8\u0010\x80

Cloudflare como capa de seguridad

Your SSL/TLS encryption mode is Full

This setting was last changed a few seconds ago

- Off (not secure)
  No encryption applied
- Flexible
  Encrypts traffic between the browser and Cloudflare
- **Full**
  Encrypts end-to-end, using a self signed certificate on the server
- Full (strict)
  Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server

Learn more about End-to-end encryption with Cloudflare

API ▸ Help ▸

Traffic Served Over TLS

Last 24 hours

None (not secure)	TLS v1.2	TLS v1.3
15	9	65

None (not secure) 17% | TLS v1.2 10% | TLS v1.3 75%

Help ▸

Always Use HTTPS

Redirect all requests with scheme "http" to "https". This applies to all http requests to the zone.

This setting was last changed 3 months ago

On

API ▸ Help ▸

HTTP Strict Transport Security (HSTS)

Enforce web security policy for your website.

Status: On
Max-Age: 6 months (Recommended)
Include subdomains: On
Preload: Off

This setting was last changed a month ago

Change HSTS Settings

API ▸ Help ▸

Minimum TLS Version

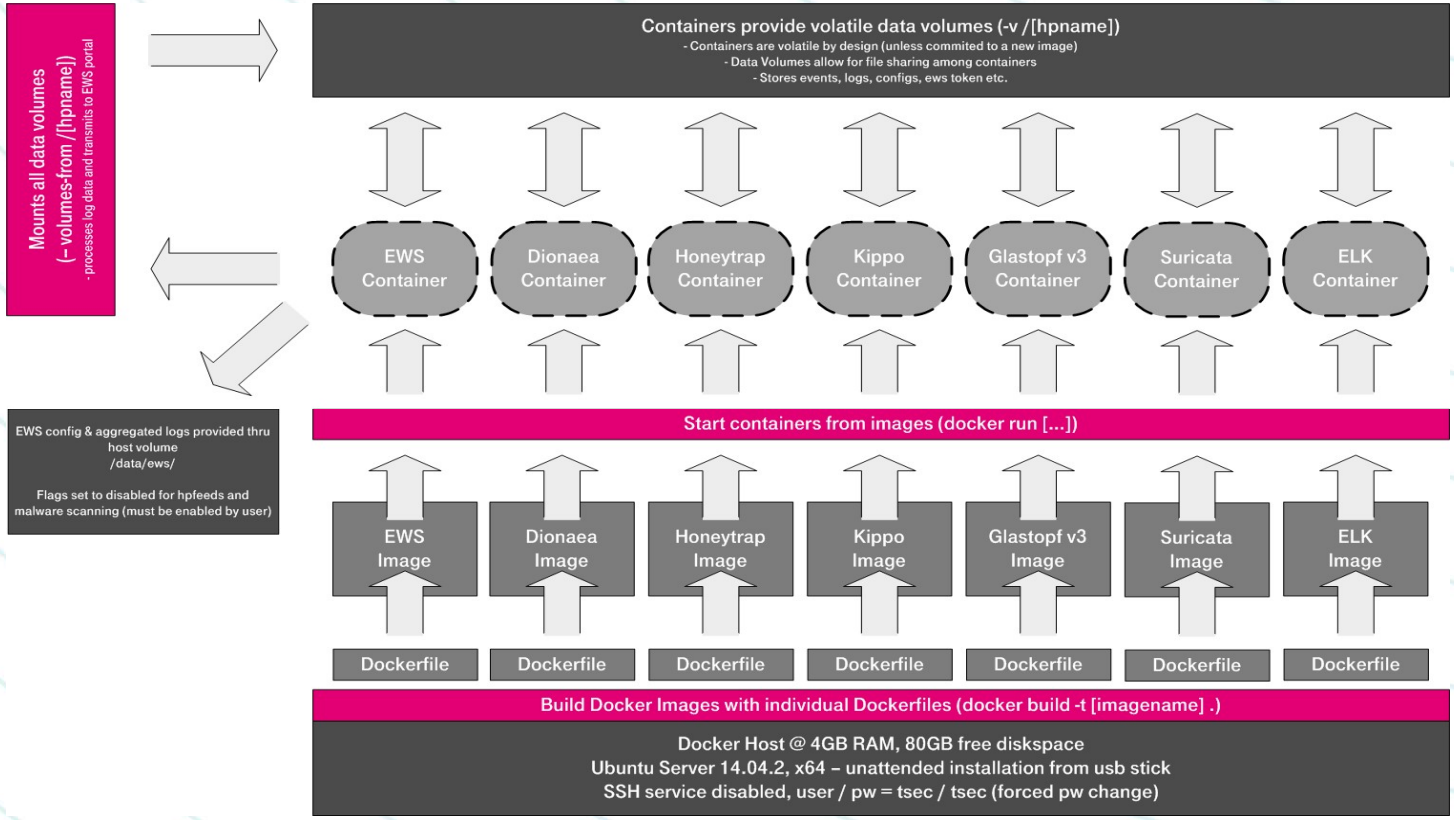
Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.

TLS 1.2

API ▸ Help ▸

Help ▸

Ejemplo de lo ejercitado



GRACIAS

LMB1

@CybercampES

Diapositiva 37

LMB1 Completar con tus perfiles sociales

Leticia Morán Barrientos; 13/11/2019