EXPLANATORY DOCUMENTATION

Debusschere Antoine
Tridon Quentin
PANDRAUD Nicolas
SCHERPEREEL Clement
CHATEAU Nicolas

Summary

Grub-2 (BOOTHOLE) (Hack)

Hacking part

In the boot grub menu select option to edit.

```
      CentOS Linux (3.10.0-123.6.3.el7.x86_64) 7 (Core)
      CentOS Linux, with Linux 3.10.0-123.el7.x86_64
      CentOS Linux, with Linux 0-rescue-ebd92ba39a774cabbf86e507be71d952

      Use the ↑ and ↓ keys to change the selection.
      Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Select Option to edit (e).

```
        insmod xfs                                                          ↑
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  d40e2af5-c\
463-4e94-ba7f-464ad2055ef1
        else
          search --no-floppy --fs-uuid --set=root d40e2af5-c463-4e94-ba7f-464a\
d2055ef1
        fi
        linux16 /vmlinuz-3.10.0-123.6.3.el7.x86_64 root=/dev/mapper/centos-roo\
t ro rd.lvm.lv=centos/swap vconsole.font=latarcyrheb-sun16 rd.lvm.lv=centos/ro\
ot crashkernel=auto  vconsole.keymap=us rhgb quiet LANG=en_US.UTF-8
        initrd16 /initramfs-3.10.0-123.6.3.el7.x86_64.img
_

      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

Go to the line of Linux 16 and change ro with rw init=/sysroot/bin/sh.

```
            insmod xfs                                                          ↑
            set root='hd0,msdos1'
            if [ x$feature_platform_search_hint = xy ]; then
              search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  d40e2af5-c\
463-4e94-ba7f-464ad2055ef1
            else
              search --no-floppy --fs-uuid --set=root d40e2af5-c463-4e94-ba7f-464a\
d2055ef1
            fi
            linux16 /vmlinuz-3.10.0-123.6.3.el7.x86_64 root=/dev/mapper/centos-roo\
t rw init=/sysroot/bin/sh  rd.lvm.lv=centos/swap vconsole.font=latarcyrheb-sun\
16 rd.lvm.lv=centos/root crashkernel=auto  vconsole.keymap=us rhgb quiet LANG=\
en_US.UTF-8
            initrd16 /initramfs-3.10.0-123.6.3.el7.x86_64.img                   ↓

          Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
          discard edits and return to the menu. Pressing Tab lists
          possible completions.
```

Now press Control+x to start on single user mode.

```
[  OK  ] Started Show Plymouth Boot Screen.
[  OK  ] Reached target Paths.
[  OK  ] Reached target Basic System.
         Starting File System Check on /dev/mapper/centos-root...
[    1.062057] sd 0:0:0:0: [sda] Assuming drive cache: write through
[    1.063004] sd 0:0:0:0: [sda] Assuming drive cache: write through
[    1.063978] sd 0:0:0:0: [sda] Assuming drive cache: write through
systemd-fsck[394]: fsck: error 2 (No such file or directory) while executing fsck.ext2 for /dev/mapper/centos-root
[  OK  ] Started File System Check on /dev/mapper/centos-root.
[  OK  ] Started dracut initqueue hook.
         Mounting /sysroot...
[  OK  ] Mounted /sysroot.
[  OK  ] Reached target Initrd Root File System.
         Starting Reload Configuration from the Real Root...
[  OK  ] Started Reload Configuration from the Real Root.
[  OK  ] Reached target Initrd File Systems.
[  OK  ] Reached target Initrd Default Target.

Generating "/run/initramfs/rdsosreport.txt"


Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.


:/# _
```

Now access the system with this command.

chroot /sysroot

Reset the password.

passwd root

Update selinux information

touch /.autorelabel

Exit chroot

exit

Reboot your system

Reboot

Nagios recover admin password

```
[root@localhost ~]# docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS                                   NAMES
e1ec5de2d636        nagiosxi:5.5.6      "/usr/local/bin/run.…"   13 months ago       Up 30 minutes       0.0.0.0:80->80/tcp                      nostalgic_ganguly
ab1349a18882        mysql:5.7           "docker-entrypoint.s…"   13 months ago       Up 30 minutes       0.0.0.0:3306->3306/tcp, 33060/tcp       dev_db
[root@localhost ~]#
```

You need to go in :

docker exec -it e1ec5de2d636 /bin/bash

then

/usr/local/nagiosxi/scripts/reset_nagiosadmin_password.php --password=newpassword

Portainer recover soupeladmin password

Admin n'existe pas, sur le fichier de portainer.db nous avons trouvé l'utilisateur suivant :


```
{"Id":2,"Username":"soupeladmin","Password":"$2a$10$QftFvTx5yBpf06iOoqT6G.Nmc0CFB6GPiHVbCBq4MbcfxsQV
pect":true,"PortainerEndpointList":true,"PortainerExtensionList":true,"PortainerMOTD":true,"PortainerRegistryInspect":true,"PortainerRegistryList":
```

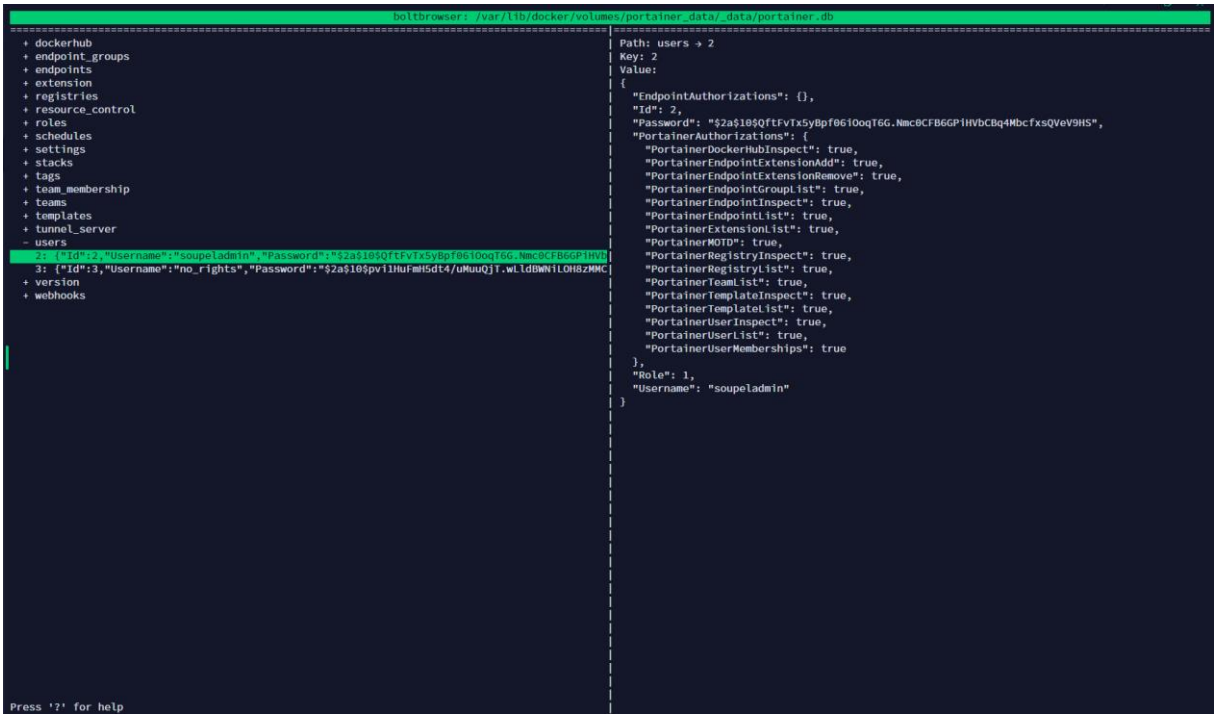

Pour recouvrer son mot de passe

yum install unzip && yum install curl
curl -sSL https://git.bullercodeworks.com/brian/boltbrowser/releases/download/2.0/boltbrowser.linux64.zip -o bolt.zip
unzip bolt.zip
docker volume ls
docker stop portainer
docker run --rm httpd:2.4-alpine htpasswd -nbB soupeladmin 'password'

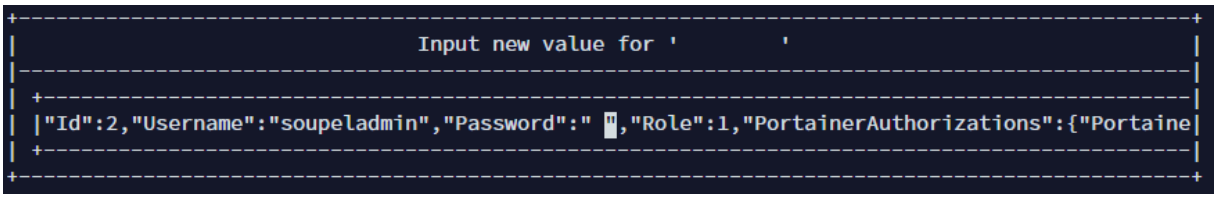
```
[root@localhost recover]# docker run --rm httpd:2.4-alpine htpasswd -nbB soupeladmin 'password'
Unable to find image 'httpd:2.4-alpine' locally
2.4-alpine: Pulling from library/httpd
f84cab65f19f: Pull complete
bb2b121e3f63: Pull complete
5b78361913e7: Pull complete
32af7daef0d3: Pull complete
b9d08706c705: Pull complete
Digest: sha256:8c16a28de3e8a715c613bc84868f8ccb984eca1027800f18bfc7a0fab377f475
Status: Downloaded newer image for httpd:2.4-alpine
soupeladmin:$2y$05$DFHzEnhtkiiLUJFjE8uvXOwMvDr8n6o8kMqgRfNr/2JwLqFI4MrIO
```

Copy the hash and

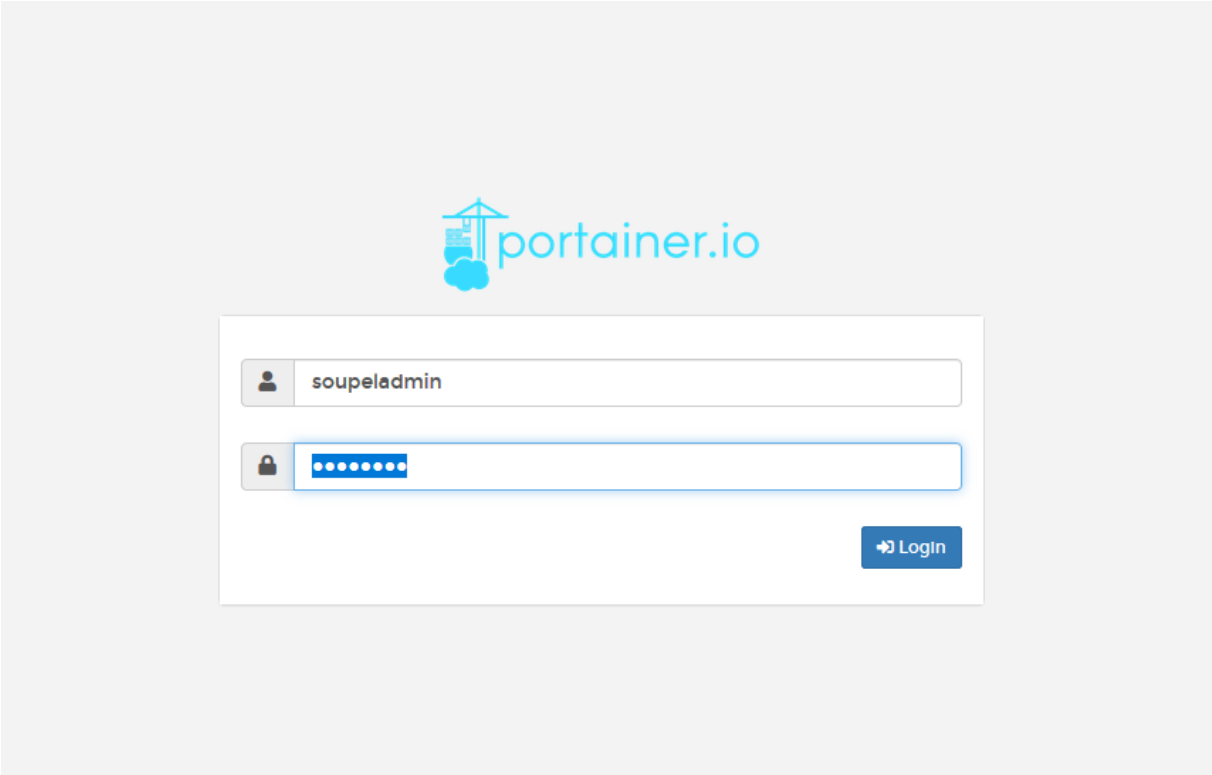
./boltbrowser.linux64 /var/lib/docker/volumes/portainer_data/_data/portainer.db



Press enter on the user

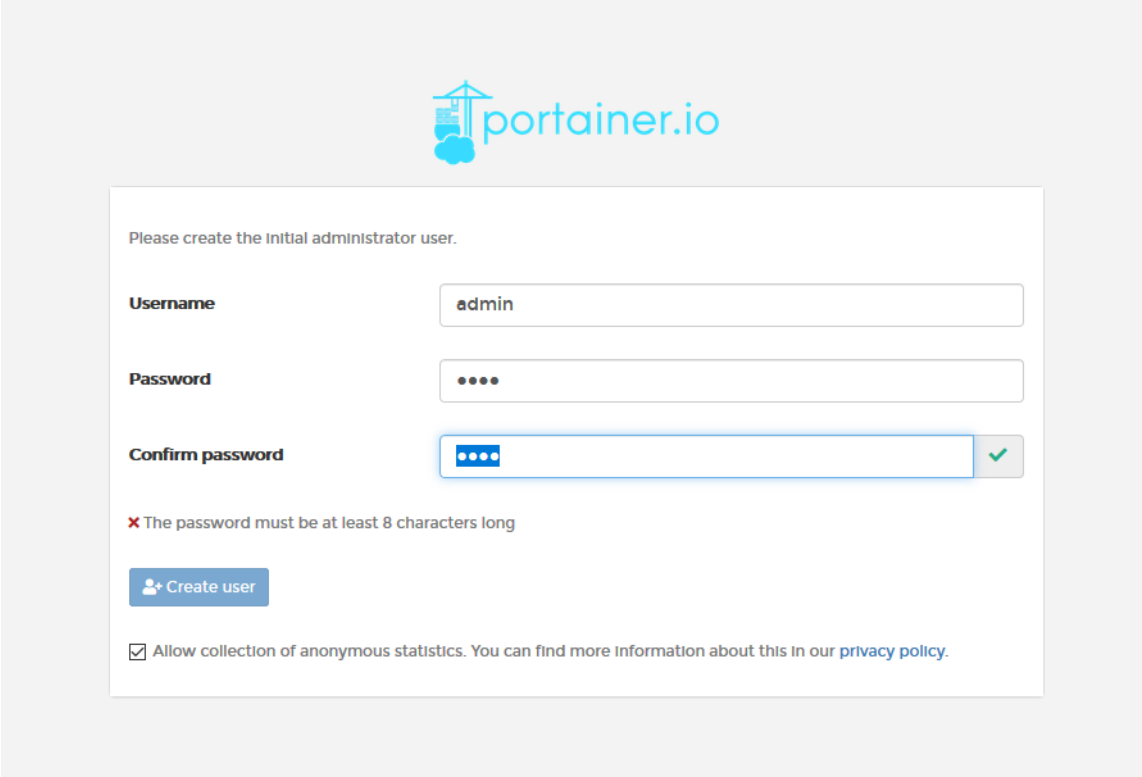


Past your hash here, press Q and restart your docker,



Portainer recover admin password (BRUTE)

docker stop portainer
docker volume prune
docker rm (ID container bloquant)
docker volume rm portainer_data
docker volume create portainer_dsata
docker run -d -p 9000:9000 --name portainer --restart always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce



Install Gitlab with docker

You need to stop the Gitea container before to install Gitlab.

Then you can run the following command :

sudo docker run --detach --hostname gitlab.example.com --publish 443:443 --publish 80:80 --publish 44:22 --name gitlab --restart always --volume $GITLAB_HOME/config:/etc/gitlab --volume $GITLAB_HOME/logs:/var/log/gitlab --volume $GITLAB_HOME/data:/var/opt/gitlab gitlab/gitlab-ee:latest

The initialization process may take a long time, you can track this process with this command :

sudo docker logs -f gitlab

Gitlab runner

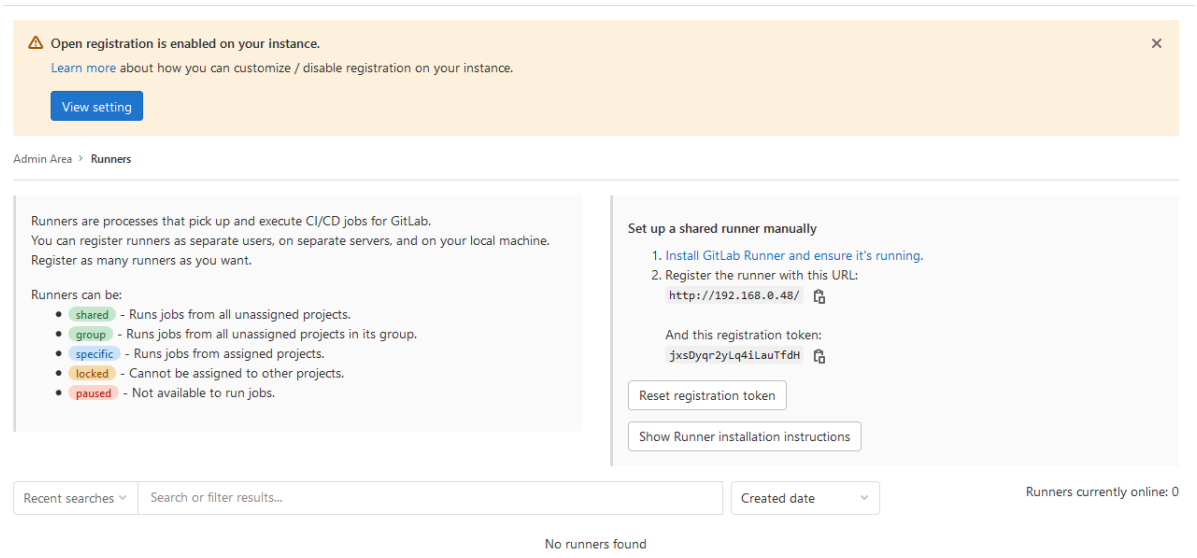
To install the gitlab runner you need to run the following command :

docker run -d --name gitlab-runner --restart always -v /srv/gitlab runner/config:/etc/gitlab-runner -v /var/run/docker.sock:/var/run/docker.sock gitlab/gitlab-runner:latest

Then to configure it run :

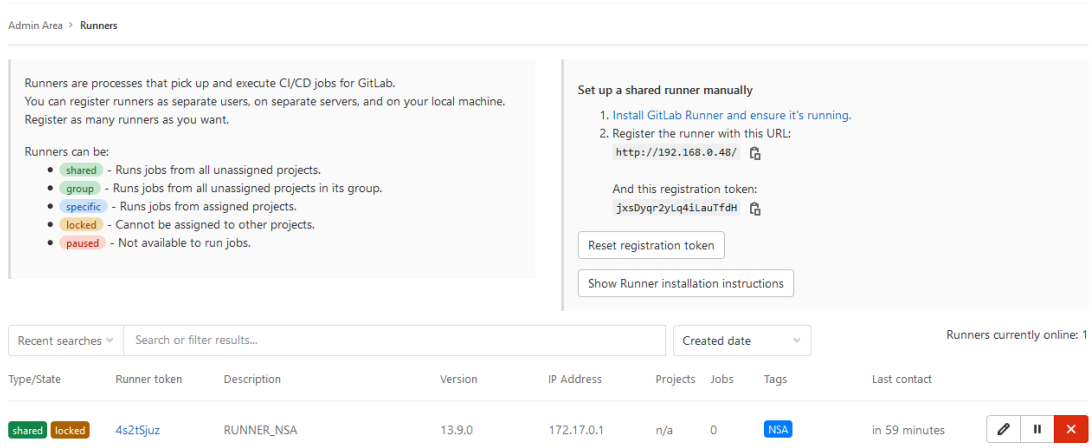
docker run --rm -it -v /srv/gitlab-runner/config:/etc/gitlab-runner gitlab/gitlab-runner register

And go to your gitlab web site in admin area, runners, and you will find the URL and the Registration Token for the runner.

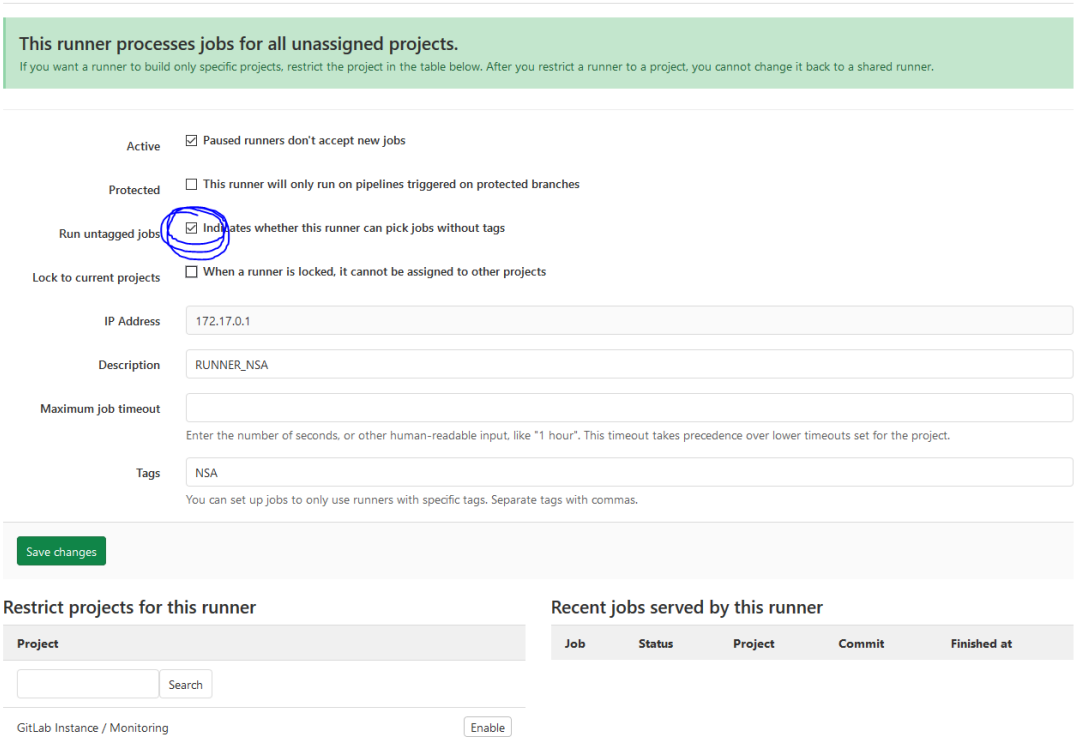


```
Enter the GitLab instance URL (for example, https://gitlab.com/):
http://192.168.0.48/
Enter the registration token:
jxsDyqr2yLq4iLauTfdH
Enter a description for the runner:
[29a3d0620c09]: RUNNER_NSA
Enter tags for the runner (comma-separated):
NSA
Registering runner... succeeded                     runner=jxsDyqr2
Enter an executor: ssh, docker-ssh+machine, kubernetes, docker-ssh, shell, parallels, virtualbox, docker+machine, custom, docker:
docker
Enter the default Docker image (for example, ruby:2.6):
ruby:2.6
Runner registered successfully. Feel free to start it, but if it's running already the config should be automatically reloaded!
```

Refresh your browser and you will get something like that :



You need to edit your fresh pipeline by clicking on the pen left to the redcross.



You need to uncheck the “lock to current projects” and check the “Run untagged jobs” if you want it to work.

How to install NRPE AGENT (Nagios)

Client Side

Supported Distributions

The Linux agent installation is currently supported on RHEL/CentOS/Oracle Linux/CloudLinux 5+, Fedora14+, SLES 11+, OpenSUSE 11+, Ubuntu 12+, and Debian 6+.

Installing The Agent

Download the Linux NRPE agent to the /tmp directory on the Linux server you wish to monitor.

cd /tmp

wget https://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz

Unpack the installation archive you just downloaded:

tar xzf linux-nrpe-agent.tar.gz

Enter the newly created agent subdirectory:

cd linux-nrpe-agent

Run the wrapper script **as root** (if using *Ubuntu* you'll need to either run sudo -i to run as root or run the

command with sudo in front):

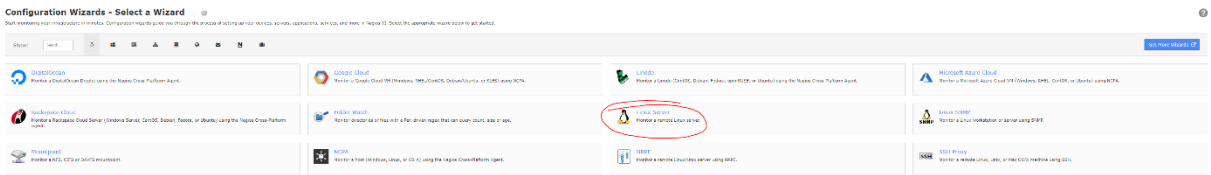
./fullinstall

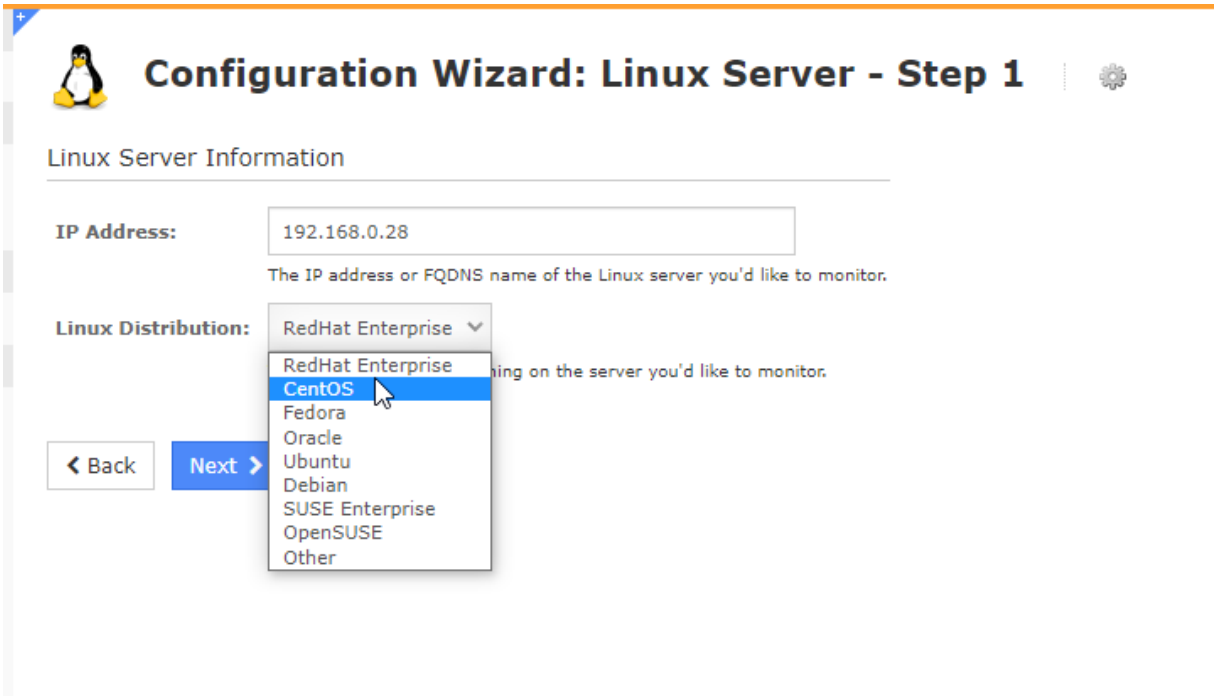
This will automatically take care of a number of things for you, including:

- Modifying the distro's package manager repositories
- Installing prerequisite packages
- Creating required users and groups
- Defining services for xinetd
- Compiling and installing the agent and plugins
- Configuring the firewall
- Configuring the agent

At the end of the execution of the script, you need to enter the **IP address** of the Nagios server.

Server side





Enter the IP address of your target VM and enter the distribution.

After that you can add a lot of parameters to monitor your linux VM. You can add warning and critical threshold. To not generate a lot of warnings you are free to add your own values.

Configuration Wizard: Linux Server - Step 2

Linux Server Details

IP Address: 192.168.0.28

Operating System: CentOS

Host Name: 192.168.0.28

The name you'd like to have associated with this Linux server.

Linux Agent

You will need to install an agent on the Linux server in order to monitor its metrics.

Agent Download: Download Agent

Agent Install Instructions: Agent Installation Instructions

SSL Encryption: Enabled (Default)

Determines whether or not data between the Nagios XI server and Linux agent is encrypted.
Note: Legacy NRPE installations may require that SSL support be disabled.

Server Metrics

Specify which services you'd like to monitor for the Linux server.

- [x] **Ping**
  Monitors the server with an ICMP ping. Useful for watching network latency and general uptime.
- [x] **Yum Update Status**
  Monitors the server to ensure it's up to date with the latest RPM packages.
- [x] **Load**
  Monitors the load on the server (1,5,15 minute values).
  15,10,5 30,20,10
- [x] **CPU Statistics**
  Monitors the server CPU statistics (% user, system, iowait, and idle)
  85 % 95 %
- [x] **Memory Usage**
  Monitors the memory usage on the server.
  80 % 90 %
- [x] **Swap Usage**
  Monitors the swap usage on the server.
  50 % 80 %
- [x] **Open Files**
  Monitors the number of open files on the server.
  30 50
- [x] **Users**
  Monitors the number of users currently logged in to the server.
  5 10
- [x] **Total Processes**
  Monitors the total number of processes running on the server.

You can monitor services, but you can do it on the configuration wizards

Services

Specify any services normally started by the init process that should be monitored to ensure they're in a running state.

	init.d Service	Display Name
☑	sshd	SSH Server
☑	crond	Cron Scheduling Daemon
☐	syslog	System Logging Daemon
☐	httpd	Apache Web Server
☐	mysqld	MySQL Server
☐	sendmail	Sendmail Mail Transfer Agent
☐	dovecot	Dovecot Mail Server

Add Row | Delete Row

Processes

Specify any process names that should be monitored to ensure they're running.

	Linux Process	Display Name
☐	sendmail	Sendmail
☐		
☐		
☐		
☐		

Add Row | Delete Row

You can deepen check the problems by configuring "When a potential problem is first detected"

Configuration Wizard: Linux Server - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:

Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.

Back | Next | Finish

Install Grafana & Prometheus

Grafana install with docker

Run the following command :

docker run -d -p 3000:3000 grafana/grafana
If you want to run an another port grafana you can launch the following command:

docker run -d --name=grafana -p 3456:3000 grafana/grafana
After that you need to go on the IP address of your web browser, enter admin and a random password, it will ask you to modify it and it's over.

Prometheus install with Node Explorer

With Prometheus you can monitor multiple services, here we will explain to you how to monitor a VM with Node Explorer:

First you need to create a file, prometheus.yml at /tmp/ then paste this.

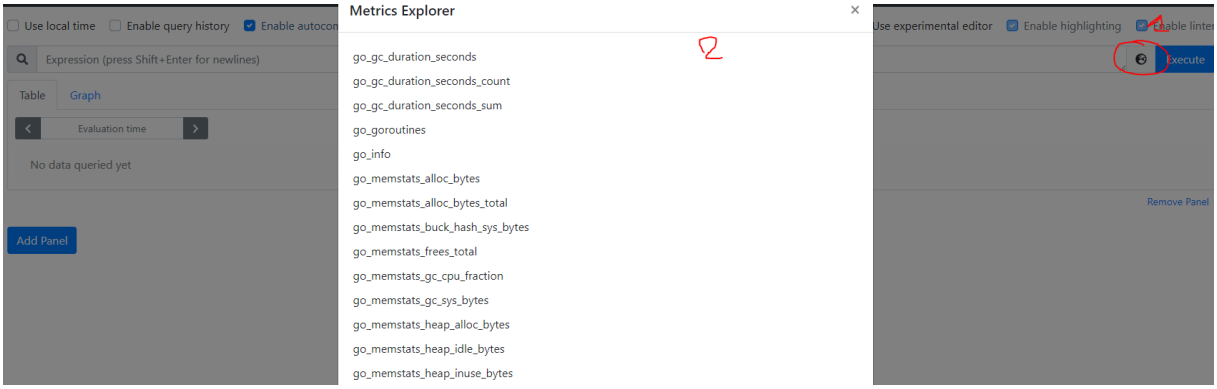
Nano /tmp/prometheus.yml

```
"global:
  scrape_interval: 5s
  external_labels:
    monitor: 'node'
scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['xxx.xxx.xxx.xxx:9090'] ## IP Address of the localhost
  - job_name: 'node-exporter'
    static_configs:
      - targets: ['xxx.xxx.xxx.xxx:9100'] ## IP Address of the localhost"
```

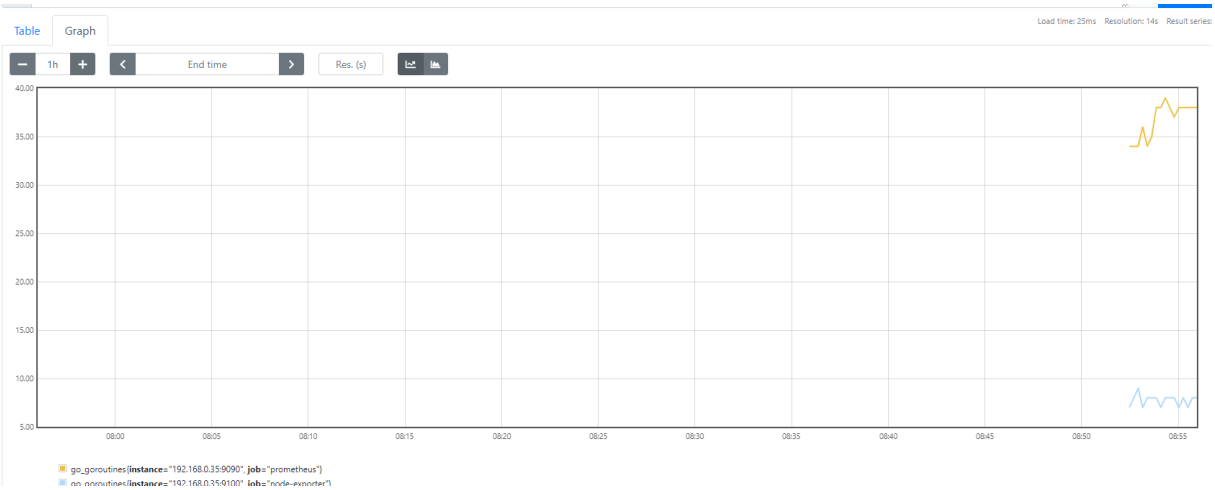
After that you need to run :

docker run -d --name prometheus -p 9090:9090 -v /tmp/prometheus.yml:/etc/prometheus/prometheus.yml prom/prometheus

When you are on prometheus you can select the request that you need. And execute it.

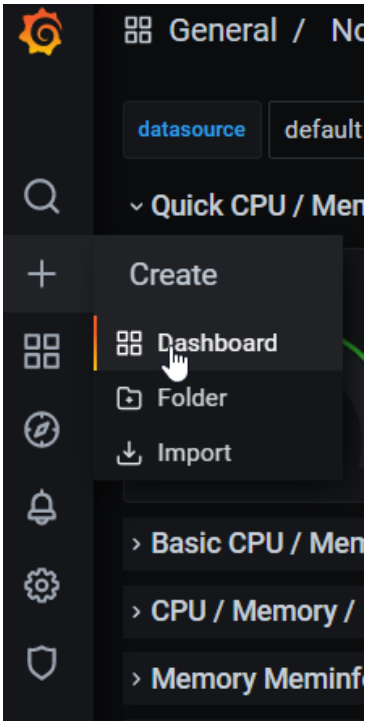


After that you can select “Graph” and you will get a graph of the command how’s running.

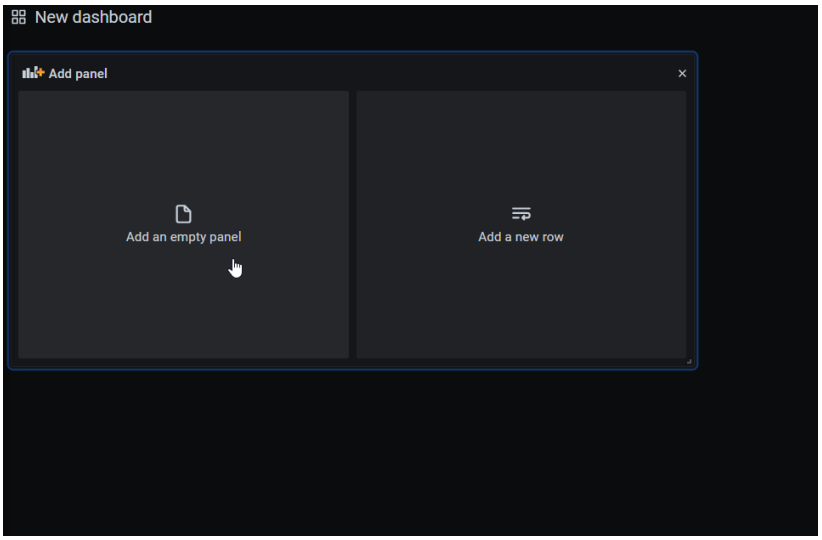


Now we will link prometheus to grafana :

Click on the +, then dashboard :

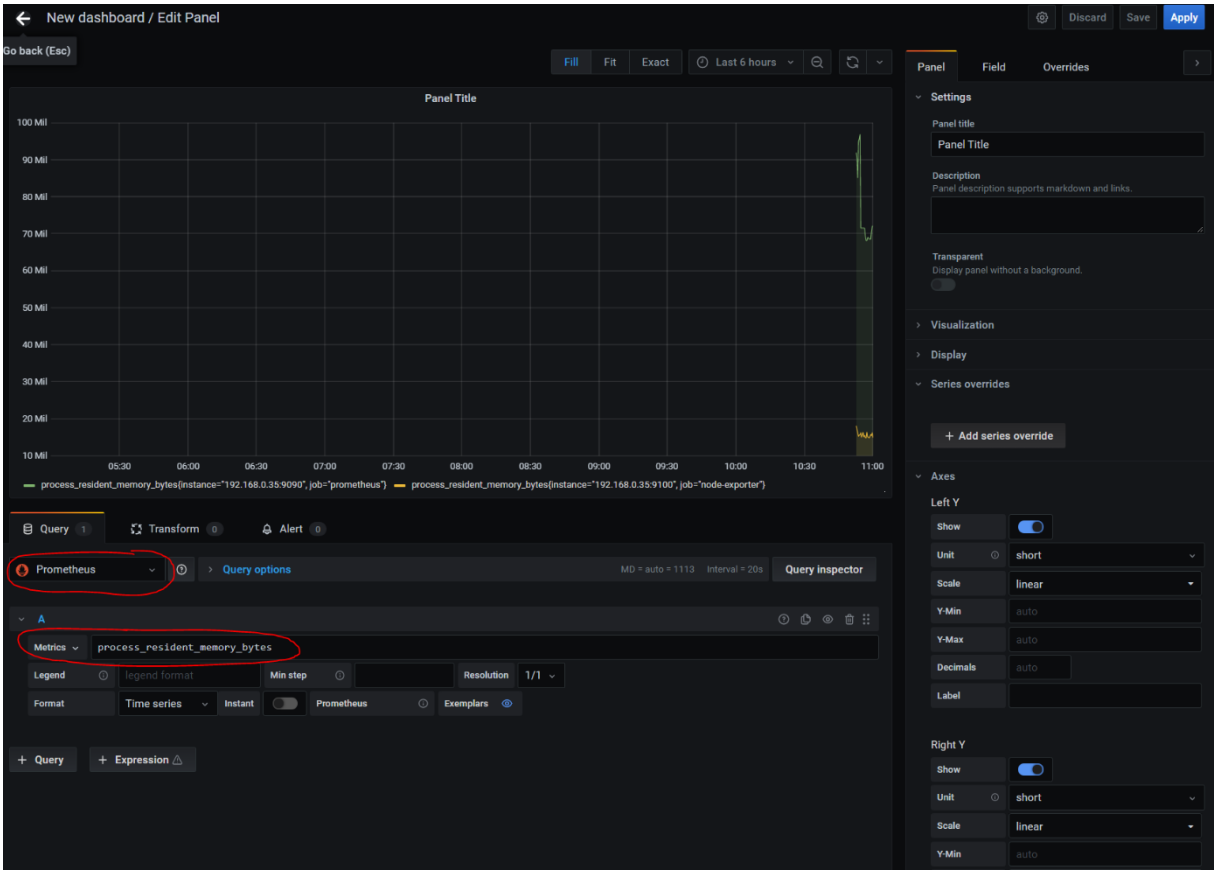


Then add an empty panel :

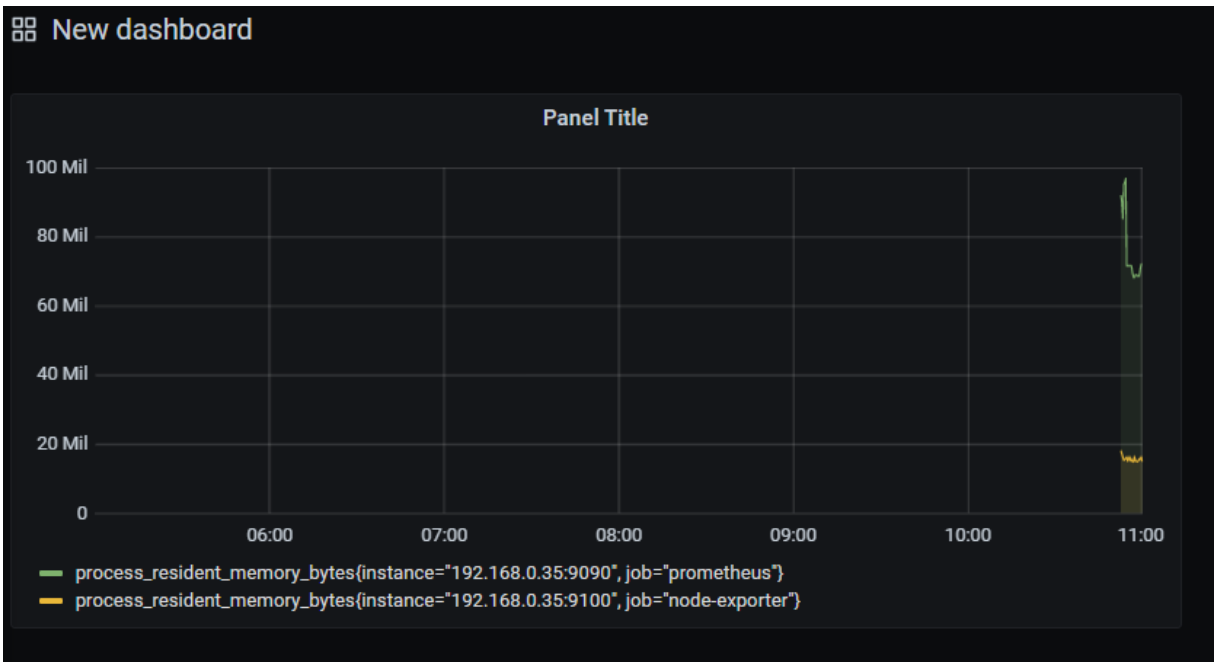


And you will get a new page with a lot of parameters, you need to select prometheus, and the metrics that you need to supervise.

You can add X metrics by clicking on Query at the bottom of the page.



After that you will get this :



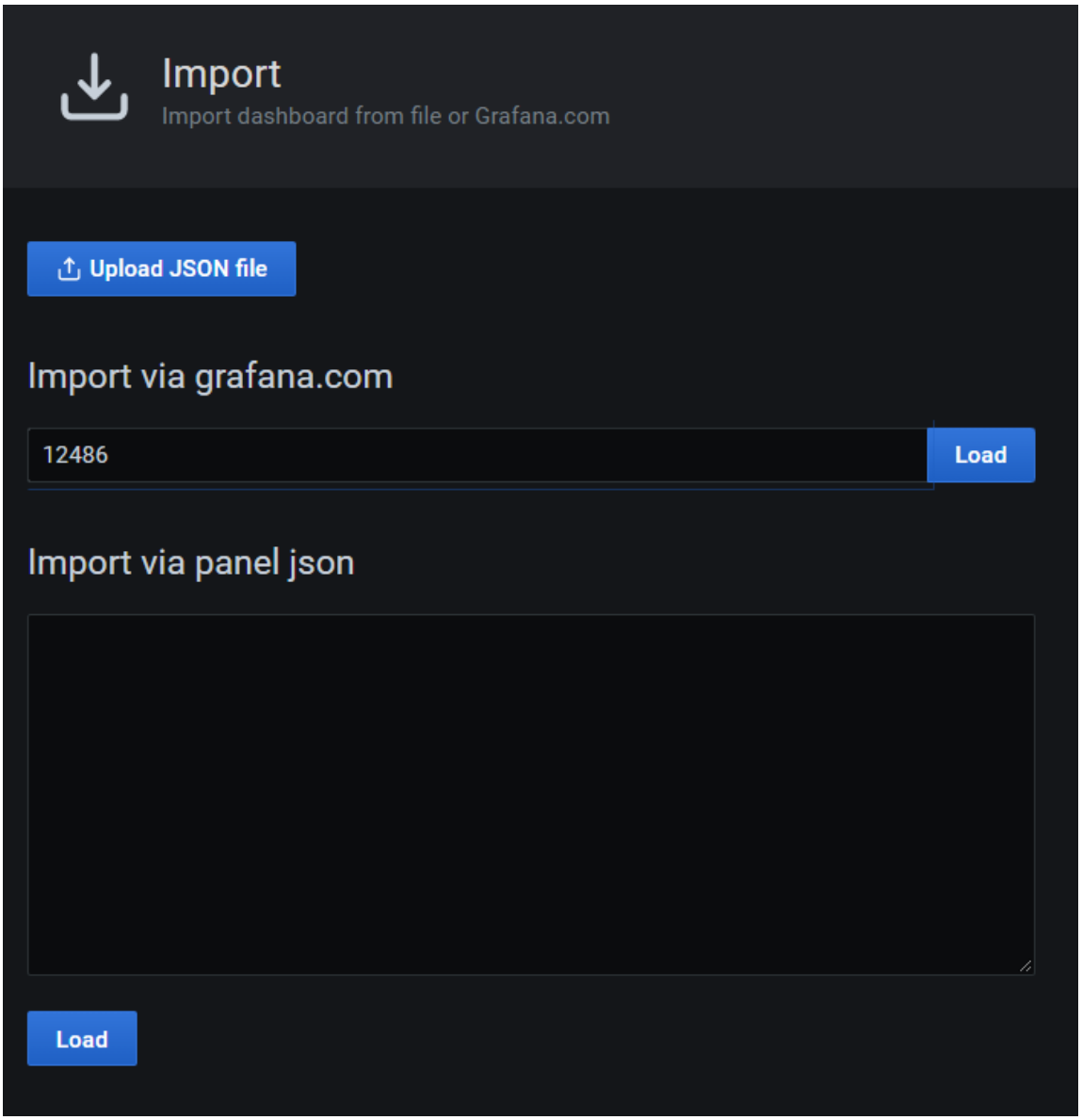
Your panel with the specifics metrics running.

Import specific Dashboard

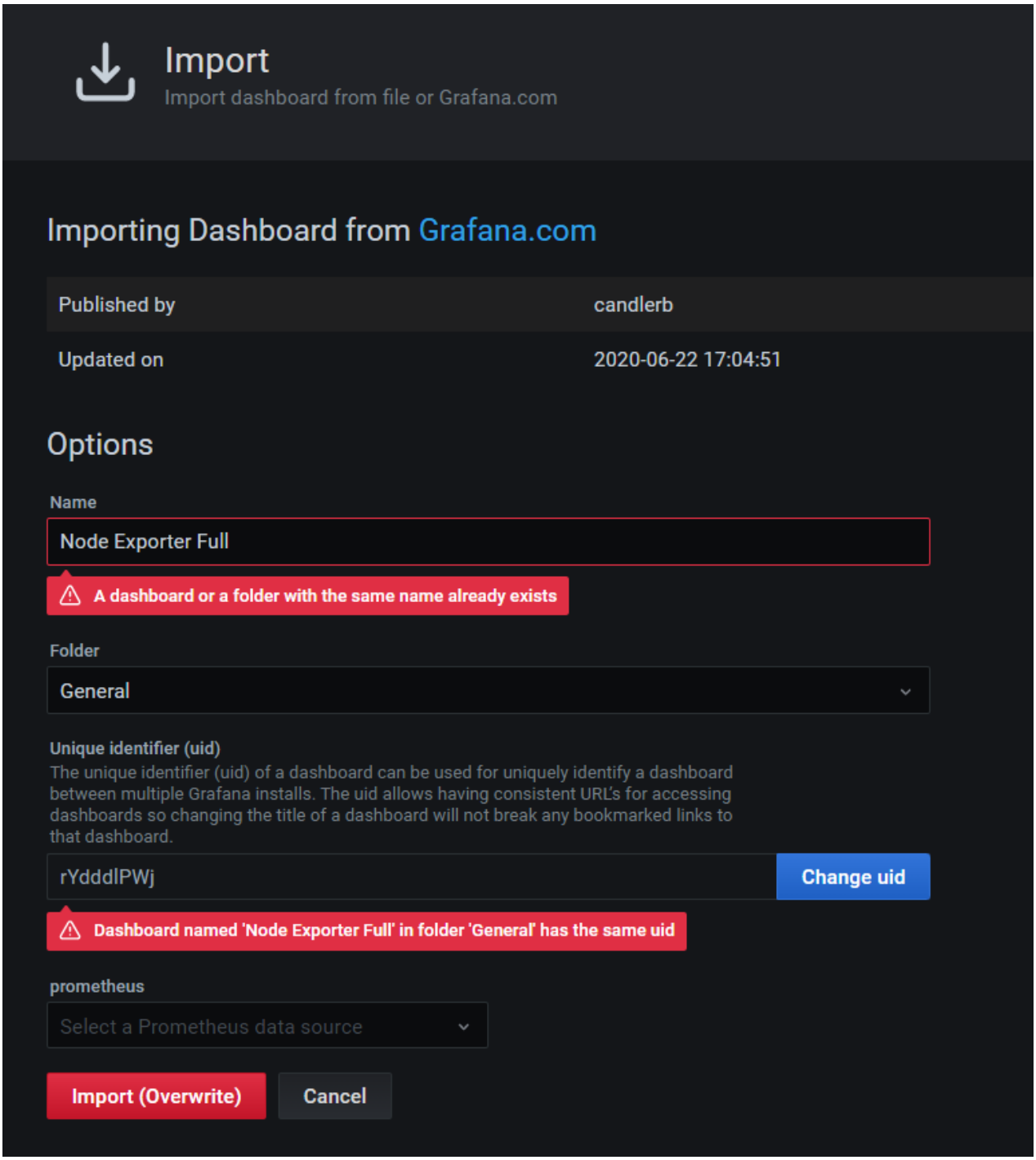
You can also import specific Dashboar, by clicking on +, then import. You will have something like that. You need to enter the number of the dashboard, of it's URL :

https://grafana.com/grafana/dashboards

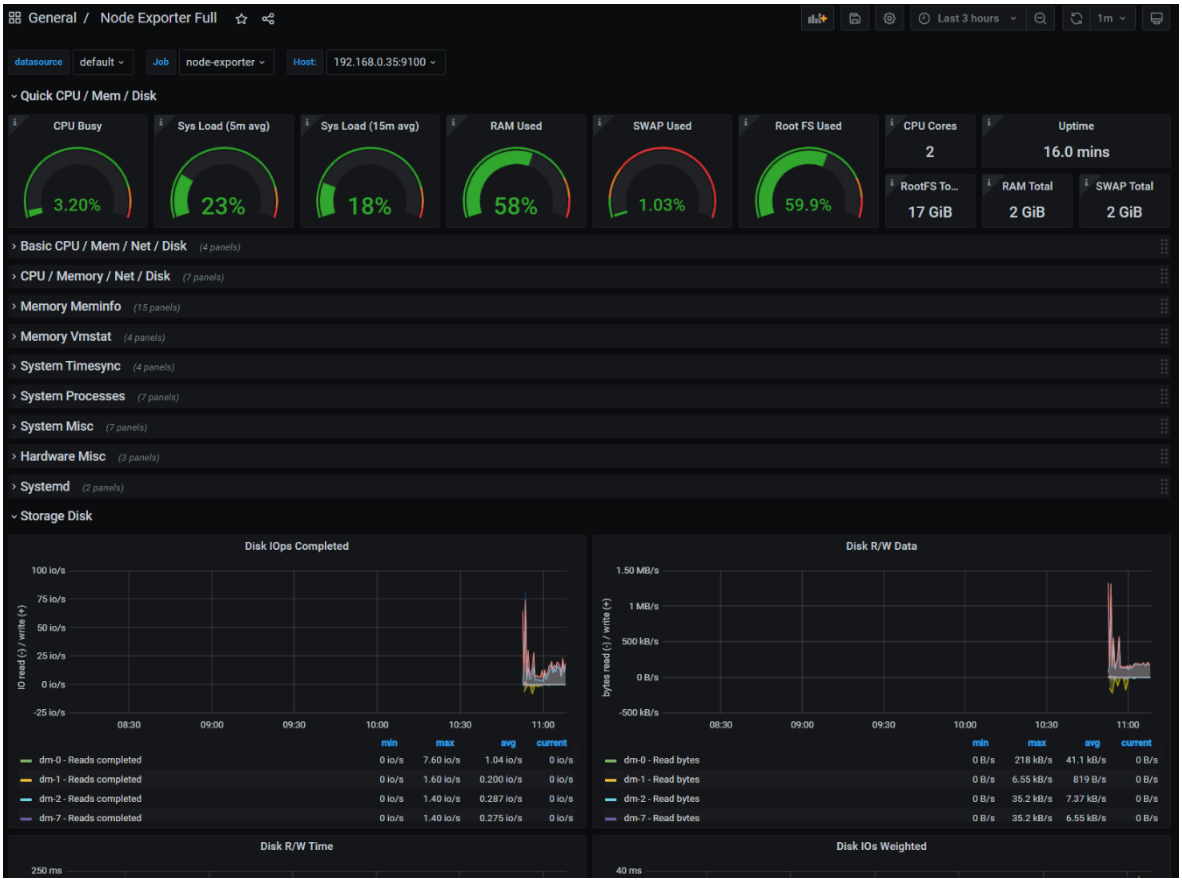
Here we will use the Dashboard number "12486", Then click on Load.



If your dashboard already exist, you will get the red warnings, but here it’s not important, you will then have to click on "import" and you will get your new dashboard



Normally will get something like that.



Install Mysql Exporter

First you need to go in your database :

docker exec -it <db_container> mysql -uroot -p

And create the following user :

mysql> CREATE USER 'exporter'@'%' IDENTIFIED BY 'exporterpassword' WITH MAX_USER_CONNECTIONS 3;
mysql> GRANT PROCESS, REPLICATION CLIENT, SELECT ON *.* TO 'exporter'@'%';
Then run :

```
docker run -d \
--name mysql80-exporter \
--publish 9104 \
--restart always \
--env DATA_SOURCE_NAME="exporter:exporterpassword@(<IP_ADDRESS>:3306)/" \
prom/mysqld-exporter:latest \
--collect.info_schema.processlist \
--collect.info_schema.innodb_metrics \
--collect.info_schema.tablestats \
--collect.info_schema.tables \
--collect.info_schema.userstats \
--collect.engine_innodb_status
```

After that you need to modify the prometheus.yml file with the following lines :

```
  - job_name: 'mysql'
    static_configs:
      - targets: ['192.168.0.35:32770']
```

Then you need to stop the prometheus container and erase it, after that you need to run :

```
docker run \
   -p 9090:9090 \
   -v /tmp/prometheus.yml:/etc/prometheus/prometheus.yml \
   prom/prometheus
```

normally you will get something like this on prometheus.

If you want to import the dashboard related of mysql-exporter in grafana, the number of the dashboard is 7362.

Firewall configuration

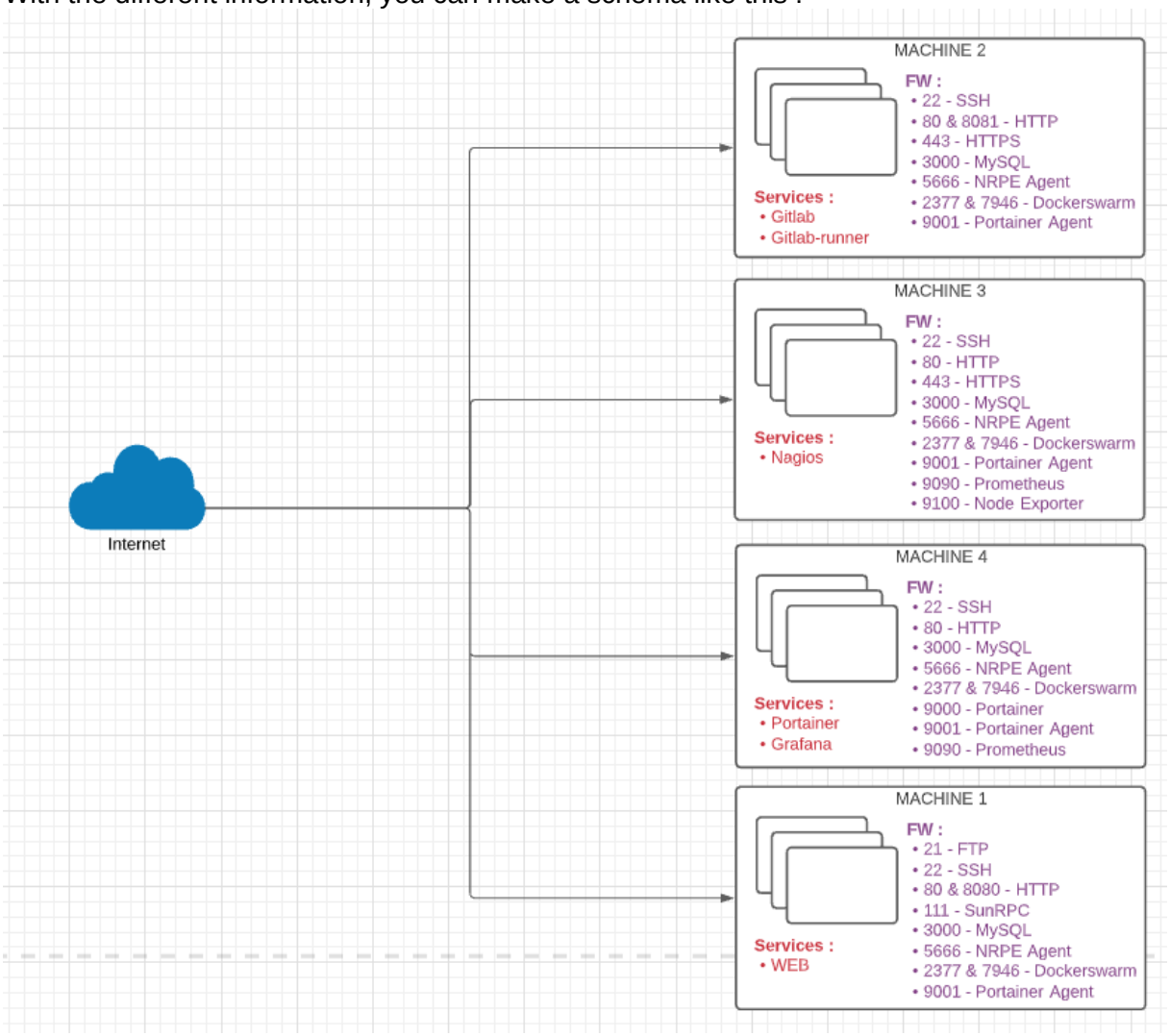
Matrice de Flux

Firstly, you need to install “lsof” packager, to launch the following command :

lsof -i -P -n | grep LISTEN.
And you will get the following output :

```
[root@localhost ~]# lsof -i -P -n | grep LISTEN.
sshd         944 root    3u  IPv4  27456      0t0  TCP *:22 (LISTEN)
sshd         944 root    4u  IPv6  27462      0t0  TCP *:22 (LISTEN)
xinetd       953 root    5u  IPv6  27478      0t0  TCP *:5666 (LISTEN)
master      1134 root   13u  IPv4  28288      0t0  TCP 127.0.0.1:25 (LISTEN)
master      1134 root   14u  IPv6  28289      0t0  TCP [::1]:25 (LISTEN)
dockerd     1185 root   29u  IPv6  31550      0t0  TCP *:2377 (LISTEN)
dockerd     1185 root   39u  IPv6  32310      0t0  TCP *:7946 (LISTEN)
docker-pr   1545 root    4u  IPv4  29488      0t0  TCP *:9000 (LISTEN)
docker-pr   2518 root    4u  IPv4  38734      0t0  TCP *:9001 (LISTEN)
docker-pr  17569 root    4u  IPv4 128689      0t0  TCP *:3000 (LISTEN)
docker-pr 115416 root    4u  IPv4 703607      0t0  TCP *:80 (LISTEN)
[root@localhost ~]#
```

With the different information, you can make a schema like this :



Installation

sudo yum install firewalld

sudo systemctl enable firewalld

sudo systemctl start firewalld

sudo firewall-cmd --state

Flow Blockage

Suppression of services and ports

firewall-cmd - -permanent --remove-port=444/tcp

firewall-cmd - -permanent --remove-service=mysql

Add an exception

Add a service or a port in exception

firewall-cmd --permanent --add-port=22/TCP

firewall-cmd - -permanent --add-service=https

Restart FirewallD

You need to restart the firewall if you want It to take effect.

firewall-cmd –reload

Revert to default (for reset)

revert to default (pour reset de base) firewall-cmd --set-target=default --zone=public fi
rewall-cmd --reload

Docker restart always

docker update --restart unless-stopped <container_name>

NTP synchronized : yes

systemctl stop ntpd
ntpd -gq
systemctl start ntpd

Update root password on mysql

If we want to show every user, we need to run the following command :

select * from mysql_user;

We changed all the passwords of the different root user with this following commands:

ALTER USER 'root'@'%' IDENTIFIED BY ‘password’;
ALTER USER 'root'@'172.18.0.1' IDENTIFIED BY ‘password’;
ALTER USER 'root'@'localhost' IDENTIFIED BY ‘password’;

We saw 3 differents root on 3 differents hosts, so we changed everything.

```
mysql> select Host User from mysql.user;
+------------+
| User       |
+------------+
| %          |
| 172.18.0.1 |
| localhost  |
| localhost  |
| localhost  |
+------------+
5 rows in set (0.00 sec)

mysql> select Host User Password from mysql.user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
 syntax to use near 'Password from mysql.user' at line 1
mysql> select User from mysql.user;
+---------------+
| User          |
+---------------+
| root          |
| root          |
| mysql.session |
| mysql.sys     |
| root          |
+---------------+
5 rows in set (0.00 sec)

mysql> ALTER USER 'root'@'%' IDENTIFIED BY 't5JrMOUOCbr5zl0syXf0';
Query OK, 0 rows affected (0.00 sec)

mysql> ALTER USER 'root'@'172.18.0.1' IDENTIFIED BY 't5JrMOUOCbr5zl0syXf0';
Query OK, 0 rows affected (0.00 sec)

mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 't5JrMOUOCbr5zl0syXf0';
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Change a user password

You can run the following command to see every users:

cat /etc/passwd

```
[root@localhost ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:998:996:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
admin:x:1000:1000:admin:/home/admin:/bin/bash
dockerroot:x:996:993:Docker User:/var/lib/docker:/sbin/nologin
service-web:x:1002:1002::/home/service-web:/bin/bash
nagios:x:1003:1003::/home/nagios:/bin/bash
saslauth:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin
gitlab-runner:x:1004:1005:GitLab Runner:/home/gitlab-runner:/bin/bash
```

You will see every users by the following caracteristic **“:/bin/bash”**

If you want to change the password of a user, you need to run the following command :
sudo -u <username> passwd *// OR //* ***sudo passwd <username>Docker restart always***