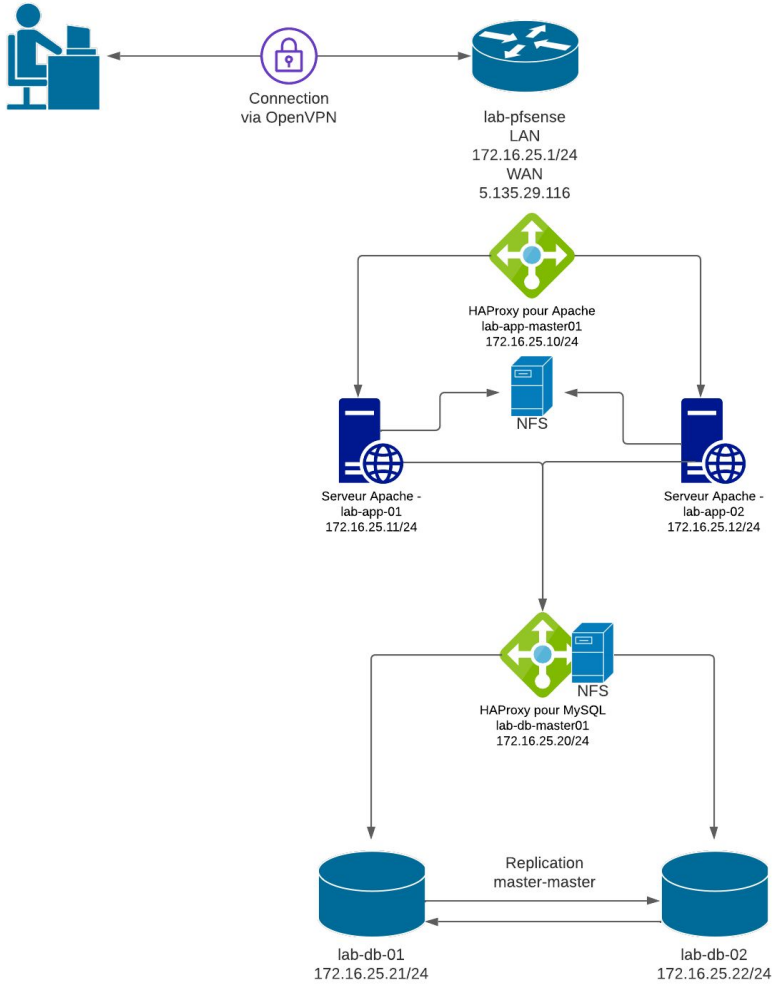
Document 3LPIC

Anthony NGUYEN

Diagramme


Connection
via OpenVPN
lab-pfsense
LAN
172.16.25.1/24
WAN
5.135.29.116
HAProxy pour Apache
lab-app-master01
172.16.25.10/24
NFS
Serveur Apache -
lab-app-01
172.16.25.11/24
Serveur Apache -
lab-app-02
172.16.25.12/24
NFS
HAProxy pour MySQL
lab-db-master01
172.16.25.20/24
Replication
master-master
lab-db-01
172.16.25.21/24
lab-db-02
172.16.25.22/24

ESXI

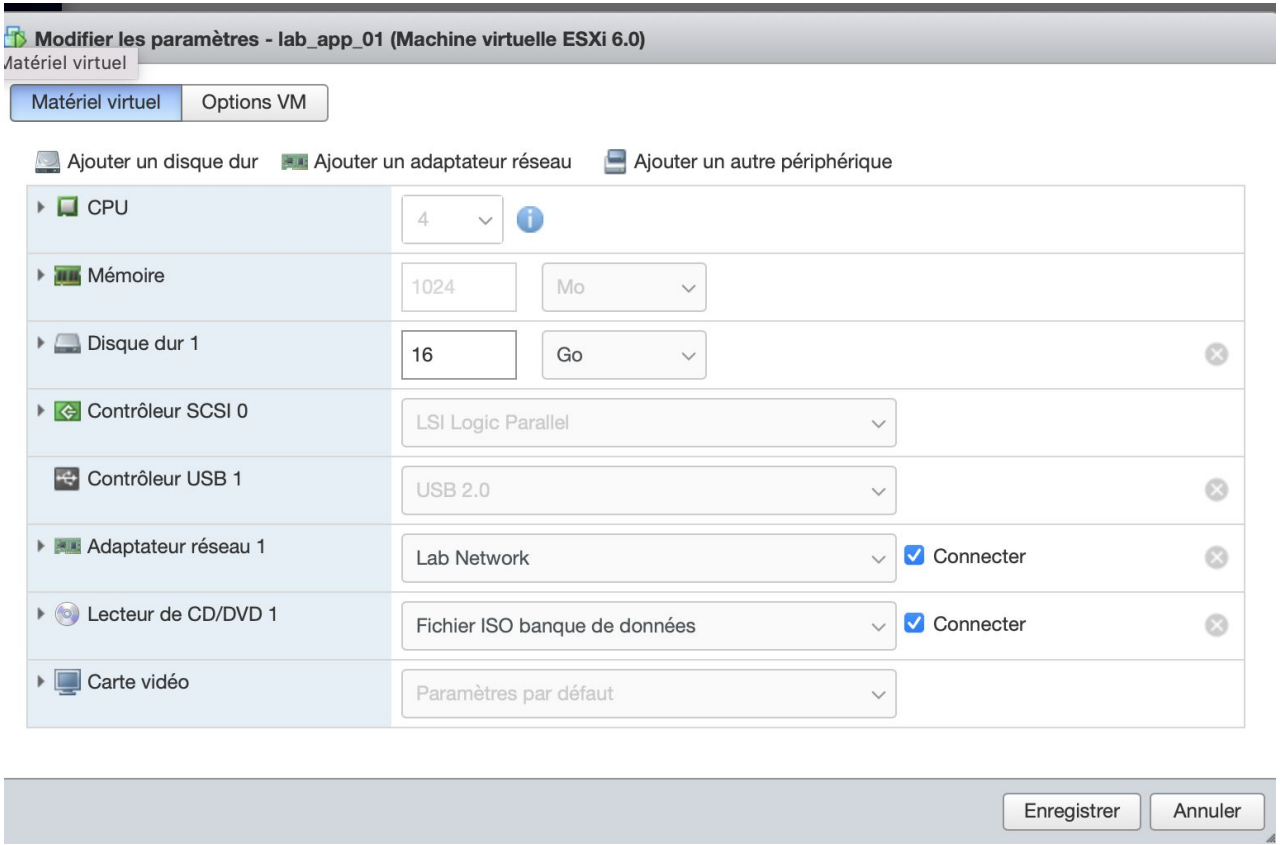
Liste des machines utilisées

lab_pfsense	Normale	8,6 Go	Autre Linux (64 bits)	Inconnu	44 MHz	400 Mo
lab_app_01	Normale	17,22 Go	Autre Linux (64 bits)	Inconnu	3 MHz	47 Mo
lab_app_02	Normale	1,22 Go	Autre Linux (64 bits)	Inconnu	2 MHz	47 Mo
lab_db_01	Normale	1,22 Go	Autre Linux (64 bits)	Inconnu	1 MHz	48 Mo
lab_db_02	Normale	1,22 Go	Autre Linux (64 bits)	Inconnu	2 MHz	48 Mo
lab_db_master_01	Normale	1,22 Go	Autre Linux (64 bits)	Inconnu	2 MHz	47 Mo
lab_app_master_01	Normale	1,22 Go	Autre Linux (64 bits)	Inconnu	3 MHz	47 Mo

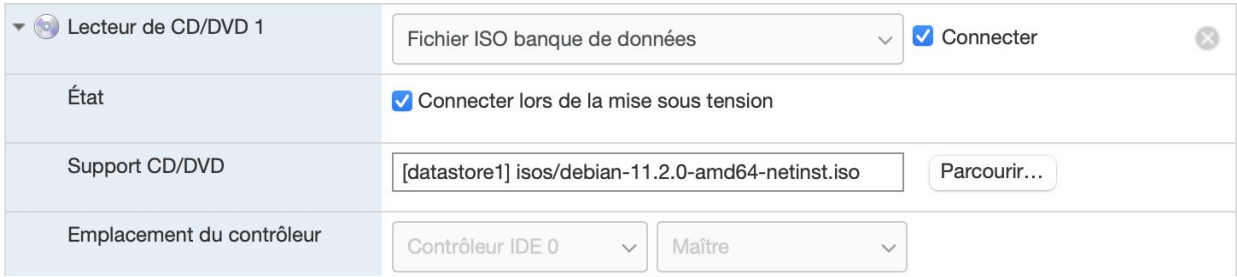
Filtres rapides…

12 éléments

Paramètres sur toutes les machines



Sélectionner l’ISO de Debian



Évaluer le nombre de vCPUs

(procLog x cores) x sockets = vcpus

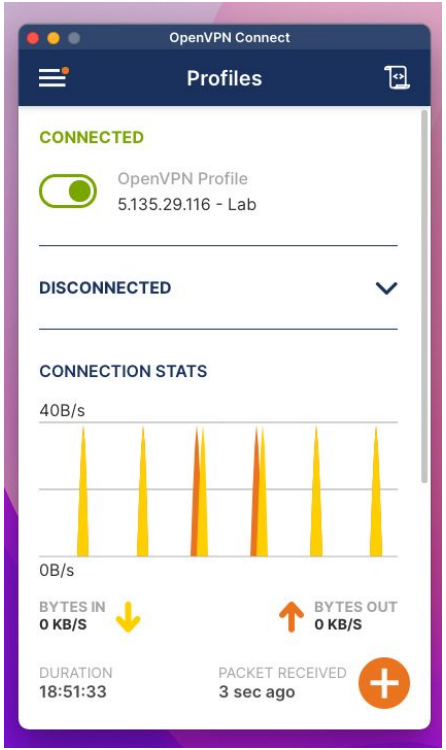
(8 x 4) x 1 = 32 vCPUs

CPU	
Processeurs logiques	8
Type de processeur	Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz
Sockets	1
Cœurs par socket	4
Hyperthreading	Oui, activé
Mémoire	31,91 Go

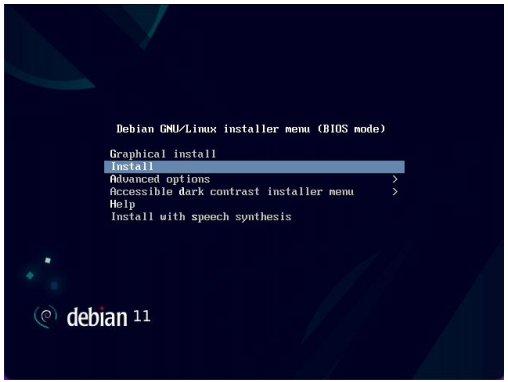
pfSense


VMware Virtual Machine - Netgate Device ID: 41d097d179356cfebb1e
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4: 5.135.29.116/24
LAN (lan) -> em1 -> v4: 172.16.25.1/24

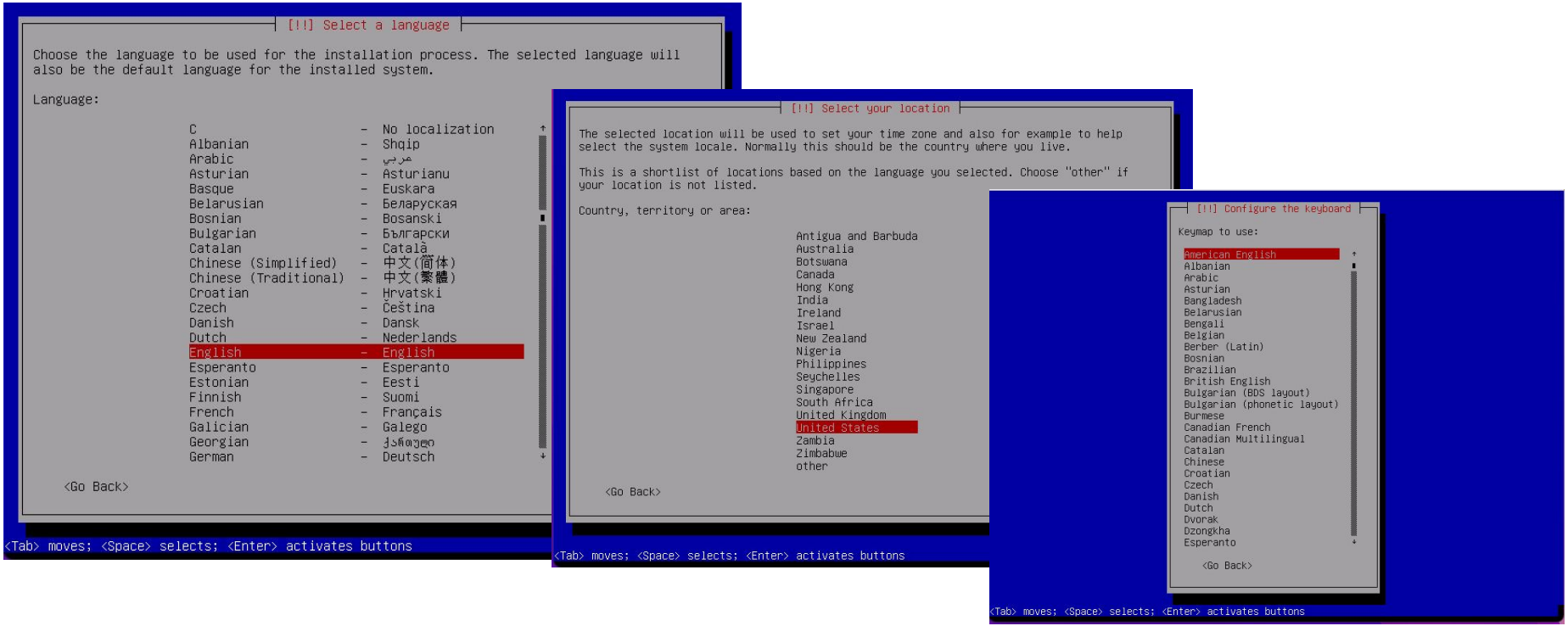
OpenVPN


OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
5.135.29.116 - Lab
DISCONNECTED
CONNECTION STATS
40B/s
0B/s
BYTES IN
0 KB/S
BYTES OUT
0 KB/S
DURATION
18:51:33
PACKET RECEIVED
3 sec ago

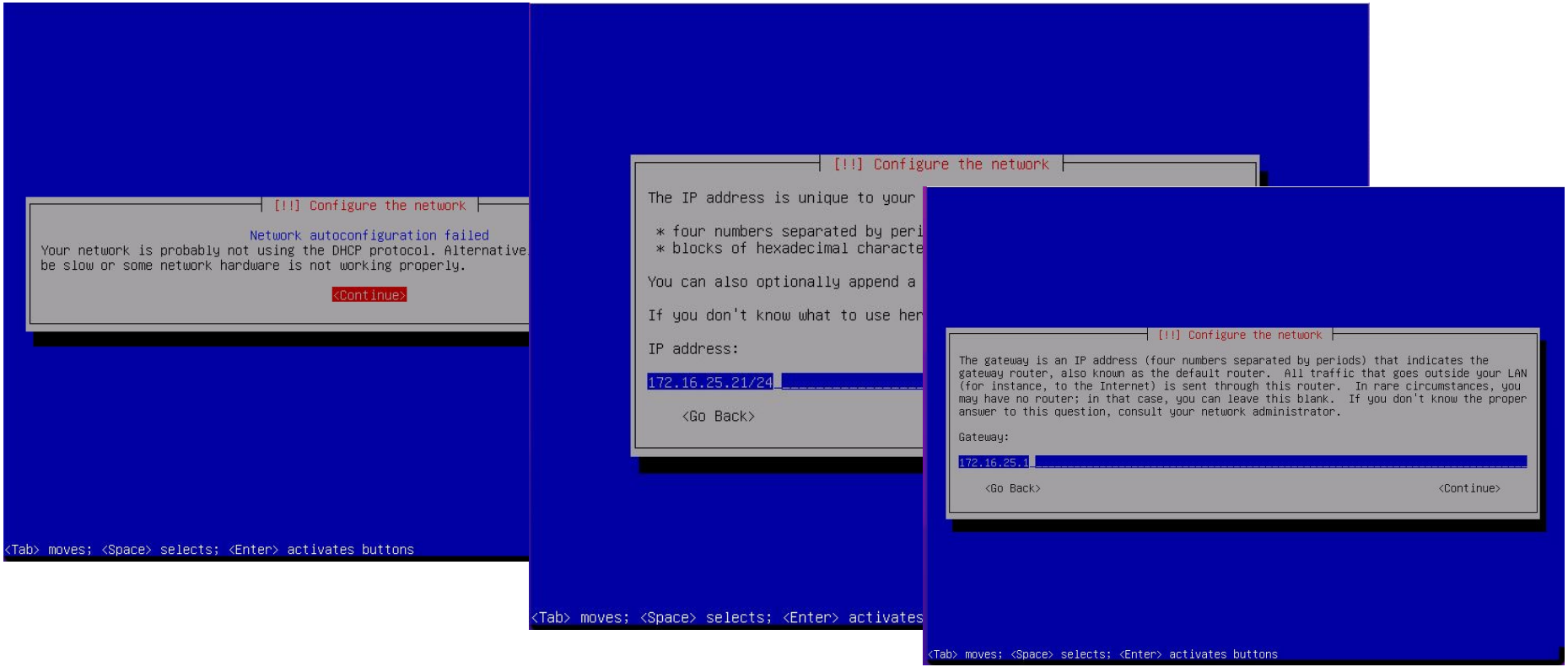
Installation Debian (sur 6 VMs)



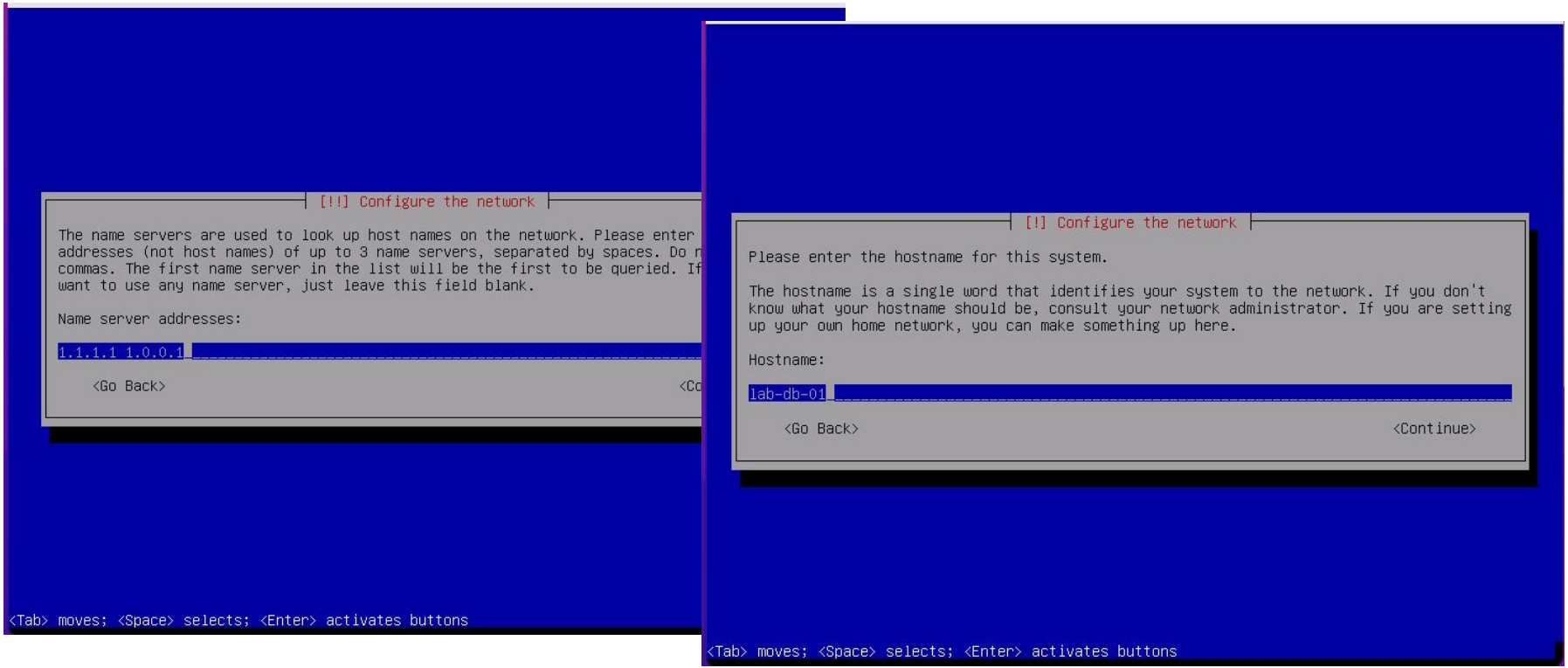
Language/Lieu/Keyboard par défaut



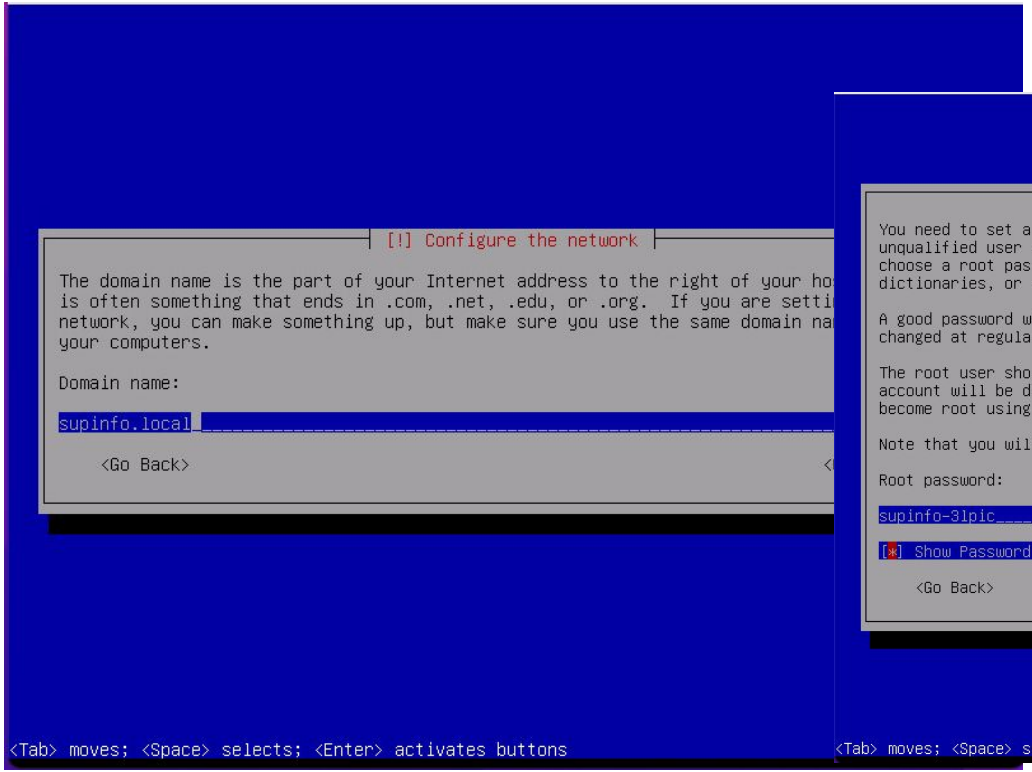
Configuration de l’IP statique

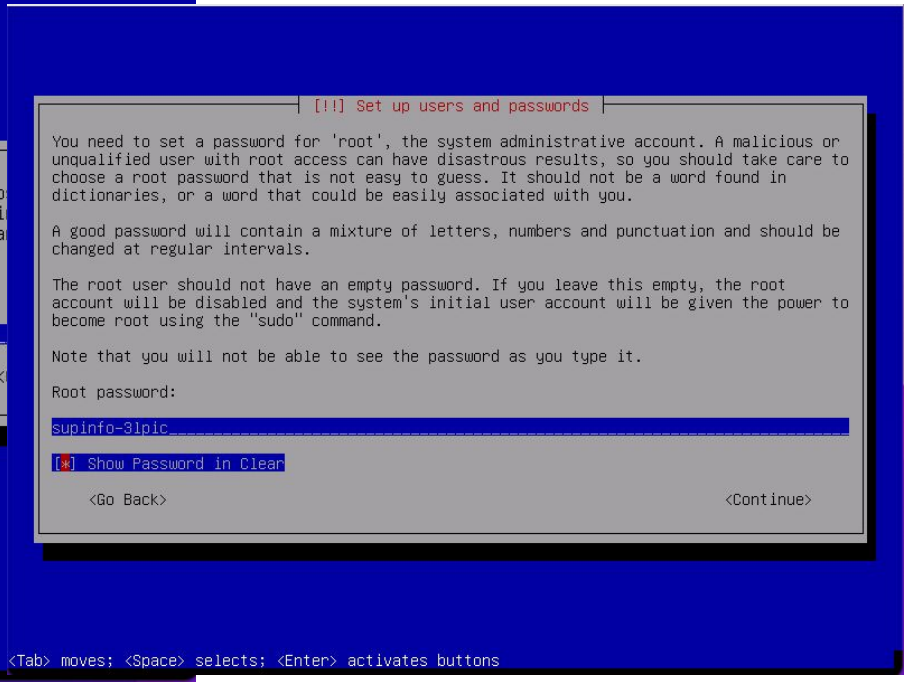


Setup DNS et Hostname

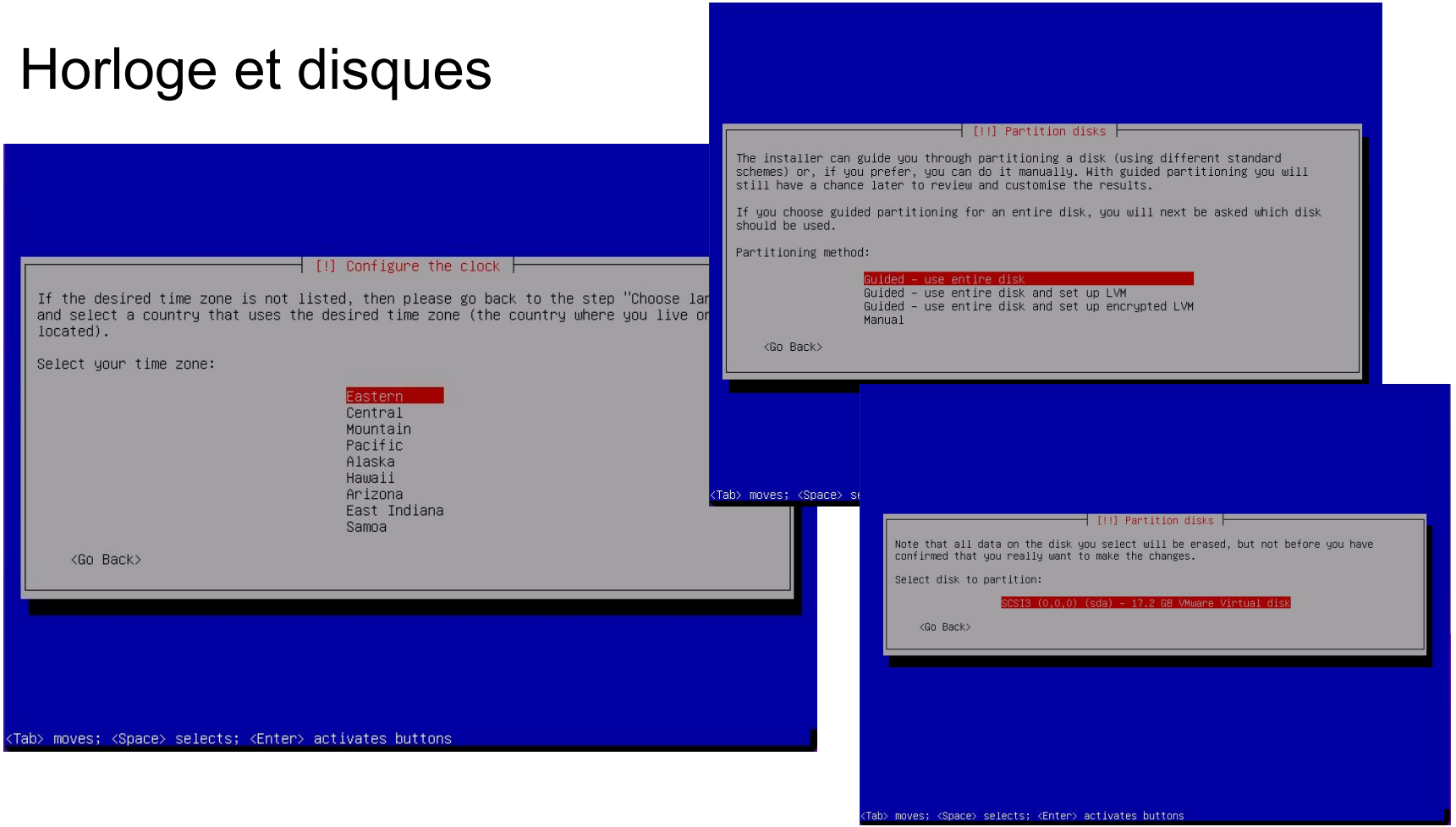


Domain name et mdp

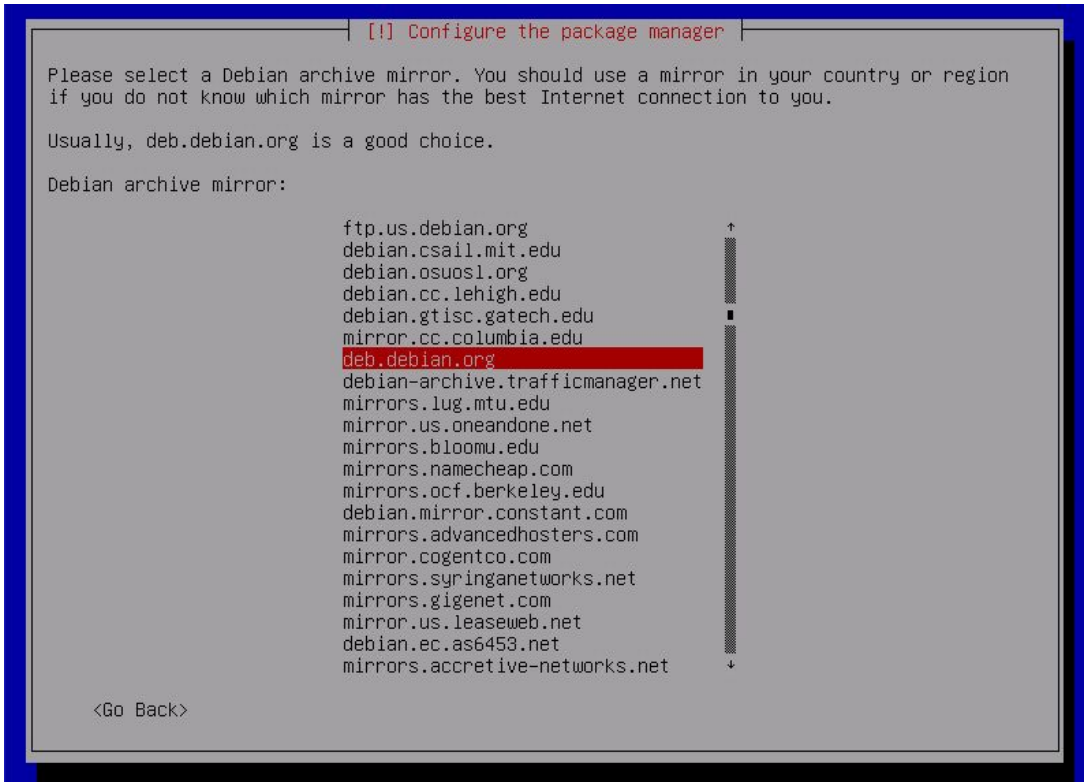




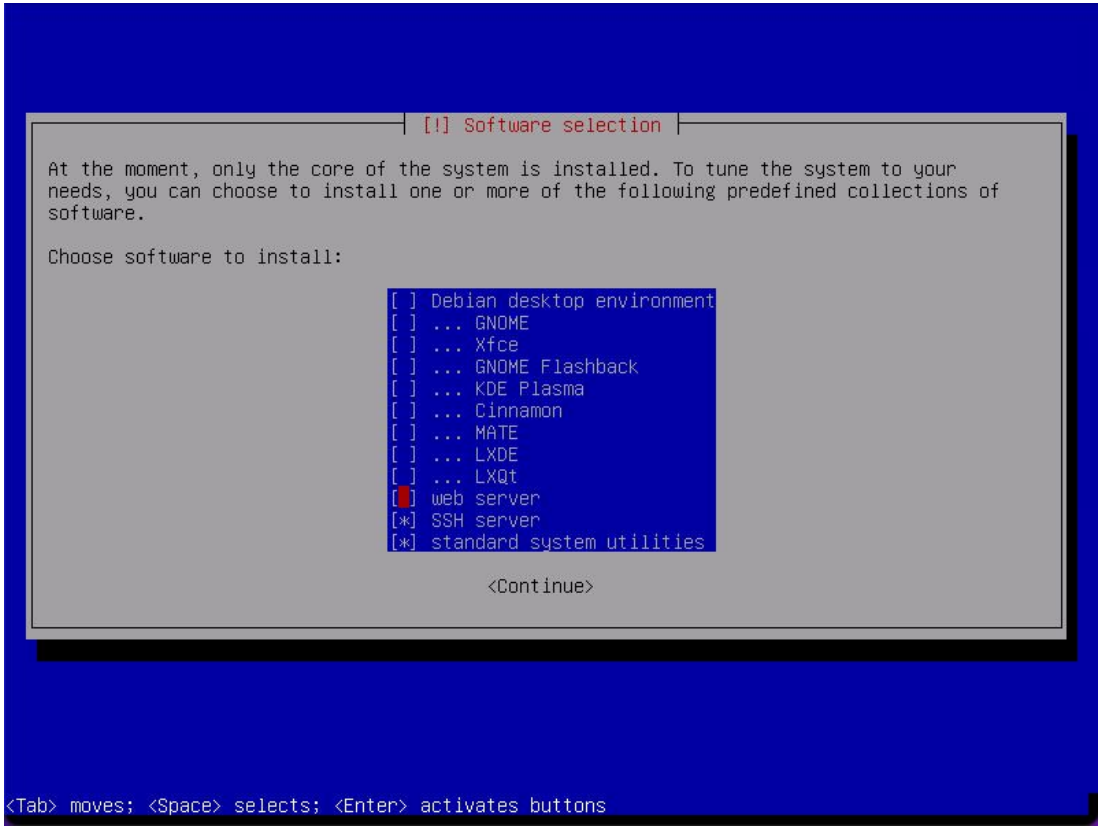
Horloge et disques



Package Manager



Services


[!] Software selection
At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.
Choose software to install:
[ ] Debian desktop environment
[ ] ... GNOME
[ ] ... Xfce
[ ] ... GNOME Flashback
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] web server
[*] SSH server
[*] standard system utilities
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

Config SSH Client

config

```
Host lab-app-master-01
  User root
  Hostname 172.16.25.10

Host lab-app-01
  User root
  Hostname 172.16.25.11

Host lab-app-02
  User root
  Hostname 172.16.25.12

Host lab-db-master-01
  User root
  Hostname 172.16.25.20

Host lab-db-01
  User root
  Hostname 172.16.25.21

Host lab-db-02
  User root
  Hostname 172.16.25.22

```

Config SSH Serveur

Autoriser le login SSH en root

```
root@lab-db-01:~# nano /etc/ssh/sshd_config
```

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
```

```
root@lab-db-01:~# systemctl restart sshd
```

SSH Client

```
(base) ngyanthony@MacBook-Pro-de-Anthony ~ % ssh lab-db-01
The authenticity of host '172.16.25.21 (172.16.25.21)' can't be established.
ED25519 key fingerprint is SHA256:mUvCWAleWY0ql6Z+A0VRR7e1tUTj8Bfe+sgCIahNmGA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

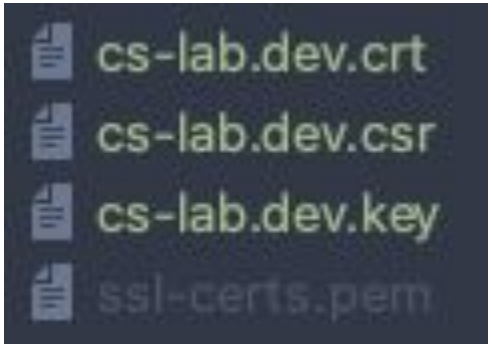
```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.25.21' (ED25519) to the list of known hosts.
root@172.16.25.21's password:
Linux lab-db-01 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb 13 10:02:18 2022
root@lab-db-01:~#
```

HTTPS

Trousseau MacOS - Root CA

HAProxy - ssl-certs

OpenSSL
Cryptography and SSL/TLS Toolkit




```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwIBAgIBATANBgkqhkiG9w0BAQ0FADBbMRAwDgYDVQQKDAdTVVBJ
TkZPMQ0wCwYDVQQHDARMWU9OMRQwEgYDVQQIDAtSSE9ORS1BTFBFUzELMAkGA1UE
BhMCRlIxFTATBgNVBAMMDCouY3MtbGFiLmRldjAeFw0yMjAyMTkxNjExNDZaFw0y
NDAyMTkxNjExNDZaMEoxCzAJBgNVBAYTAkZSMRQwEgYDVQQIDAtSSE9ORS1BTFBF
UzEQMA4GA1UECgwHU1VQSU5GTzETMBEGA1UEAwwKY3MtbGFiLmRldjCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAL6FyfL6dM71UyHXJuEH7G3X3ZTGP6Q2
JPd7A8cRurbh/4jzevdA2z1GbtPjyh4SMt1wRq7ygeDSuQrDpfAKIPg1HRoWdkvZ
3elmVgOjVoL46JIqzQ9elkdgZ/wVXduCavfkZW3u3xQJCmREibGtViWxQQC7DgWw
neJmUYw2UKnK2AEQVWzH2E8GMubUmOD6pc5imr3uAvwpk2jLfAyoDTovdrFnBtrC
74WxKOOQvWFXARR5NLxWPv3lfUxH/iNTs+a6SKKt1joCPEioPT4vSw44jufxxn11
ul5zxm8BLDmxETE72D7uAcrX/TMBjtZF1tcBWcrs1DsLCQdMR4L+HrsCAwEAAaOB
iTCBhjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBQYi7mwO1/bR/BsNl7mQOo2JgXU
LjALBgNVHQ8EBAMCBPAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MCgGA1UdEQEB/wQeMByCCmNzLWxhYi5kZXaCDnd3dy5jcy1sYWIuZGV2MA0GCSqG
SIb3DQEBDQUAA4IBAQCUOqXidCpG/MxNOpBkBBkjwbWfwQyGmhsJDz5/5f+dEByn
7H4CGD1ZlWXCJPs+NM3Dk6I0pKGE/4KeuK2+KNSa0Hd0GIgjgKc7u8DT5DxdQgic
b5i9C92w1sBbhn/QTQX7ee7c/3KS5LKubXDOkkITWK50coF/1ibHWCYtCZ33NTGT
NU/KlFQ0rkllnl0CJIFqaOCOslgGz+nzqjLmAnA6WPauwyAUXF2xx6paIqAadoU3
BJdD6rpPfAj0X9bxOIiaKK1JrxYYhbz83T1cq+DV9jgPJVmQMHevWjGoEWXIuYPJ
yMNfTJ7nvW3Ev8PUqA8UiOV6TMt4JSIh5TlDtLvH
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIDOTCCAiECAQAwWTEQMA4GA1UECgwHU1VQSU5GTzENMAsGA1UEBwwETFlPTjEU
MBIGA1UECAwLUkhPTkUtQUxQRVMxCzAJBgNVBAYTAkZSMRMwEQYDVQQDDApjcy1s
YWIuZGV2MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvoXJ8vp0zvVT
Idcm4QfsbdfdlMY/pDYk93sDxxG6tuH/iPN690DbPUZu0+PKHhIy3XB6rvKB4NK5
CsOl8Aog+DUdGhZ2S9nd6WZWA6NWgvjokirND16WR2Bn/BVd24Jq9+Rlbe7fFAkK
ZESJsa1WJbFBALsOBbCd4mZRjDZQqcrYARBVbMfYTwYy5tSY4PqlzmKave4C/CmT
aMt8DKgNOi92sWcG2sLvhbEo45C9YVcBFHk0vFY+/eV9TEf+I1Oz5rpIoq3WOgI8
SKg9Pi9LDjiO5/H6fXW6XnPGbwEsObERMTvYPu4Bytf9MwGO1kXW1wFZyuzUOwsJ
```

HAProxy - Redirection HTTPS + Cert

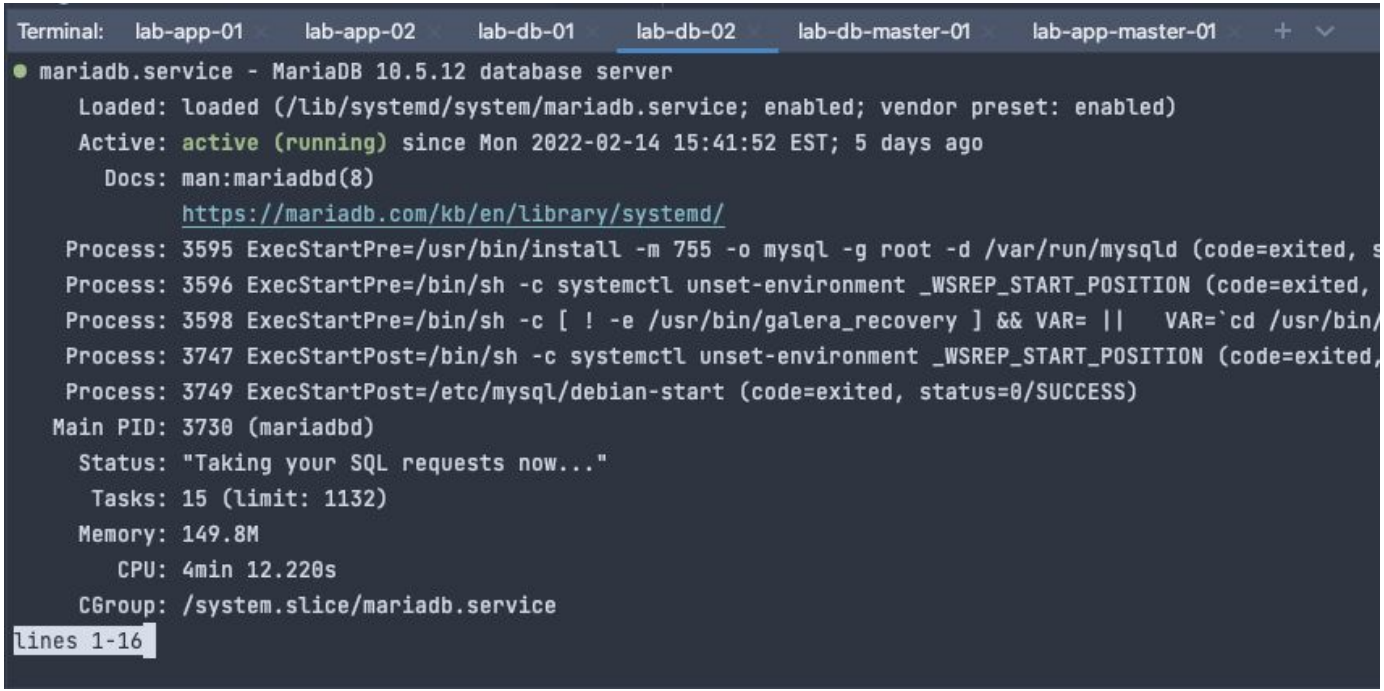
```
frontend main
    bind *:80
    bind *:443 ssl crt /etc/haproxy/certs/ssl-certs.pem
    redirect scheme https if !{ ssl_fc }
    mode http
    default_backend             app
```

HAProxy - Redirection HTTPS + Cert

```
    # utilize system-wide crypto-policies
    # ssl-default-bind-ciphers PROFILE=SYSTEM
    # ssl-default-server-ciphers PROFILE=SYSTEM
```

MySQL HA

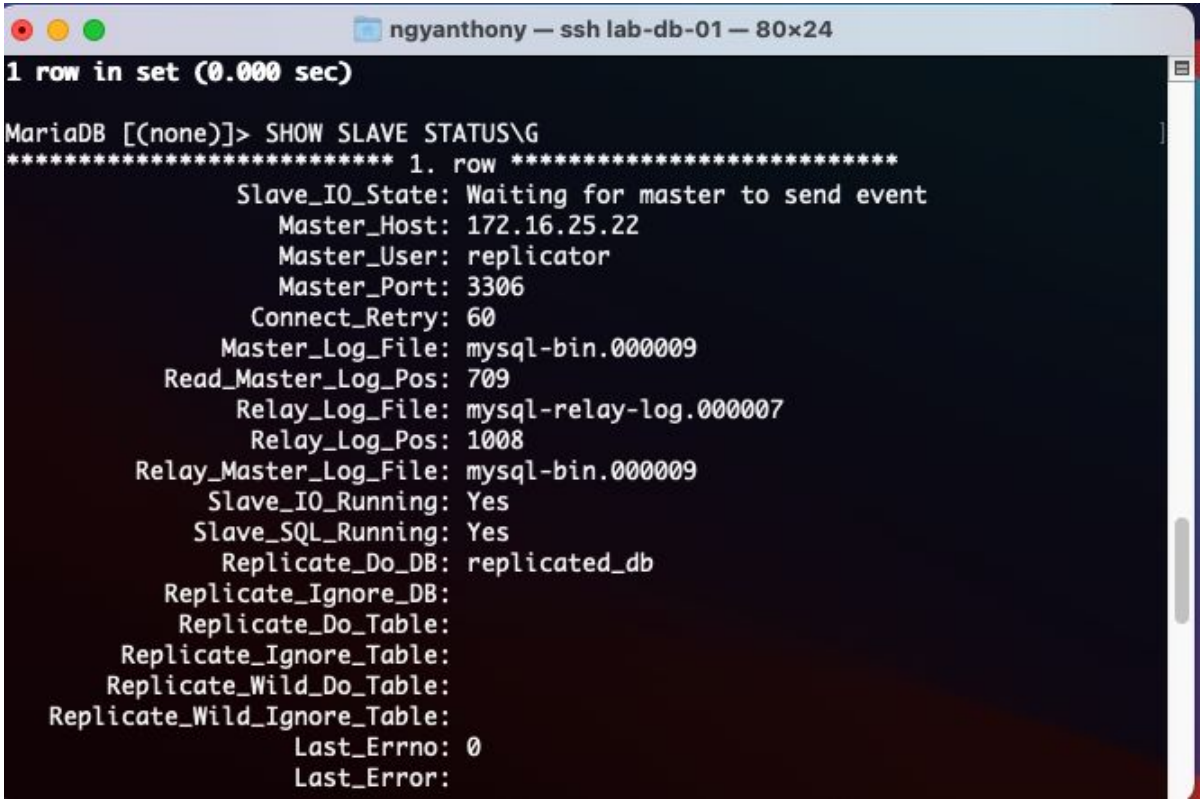
MySql Process



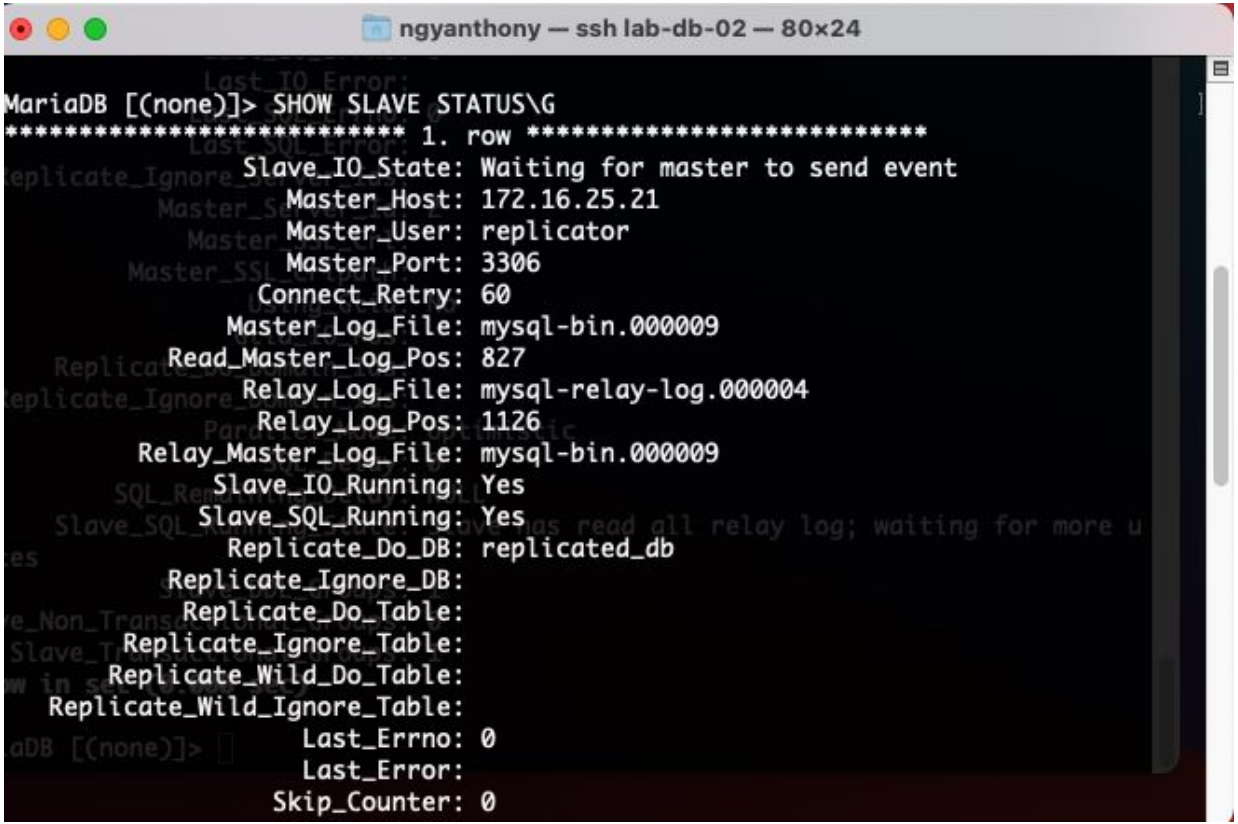
HAProxy - Load balancing MySQL

```
listen mysql-cluster
    bind *:3306
    mode tcp
    balance roundrobin
    option mysql-check
    default-server fastinter 1000
    server mysql-1 172.16.25.21:3306 check
    server mysql-2 172.16.25.22:3306 check
```

HAProxy - Load balancing MySQL



HAProxy - Load balancing MySQL

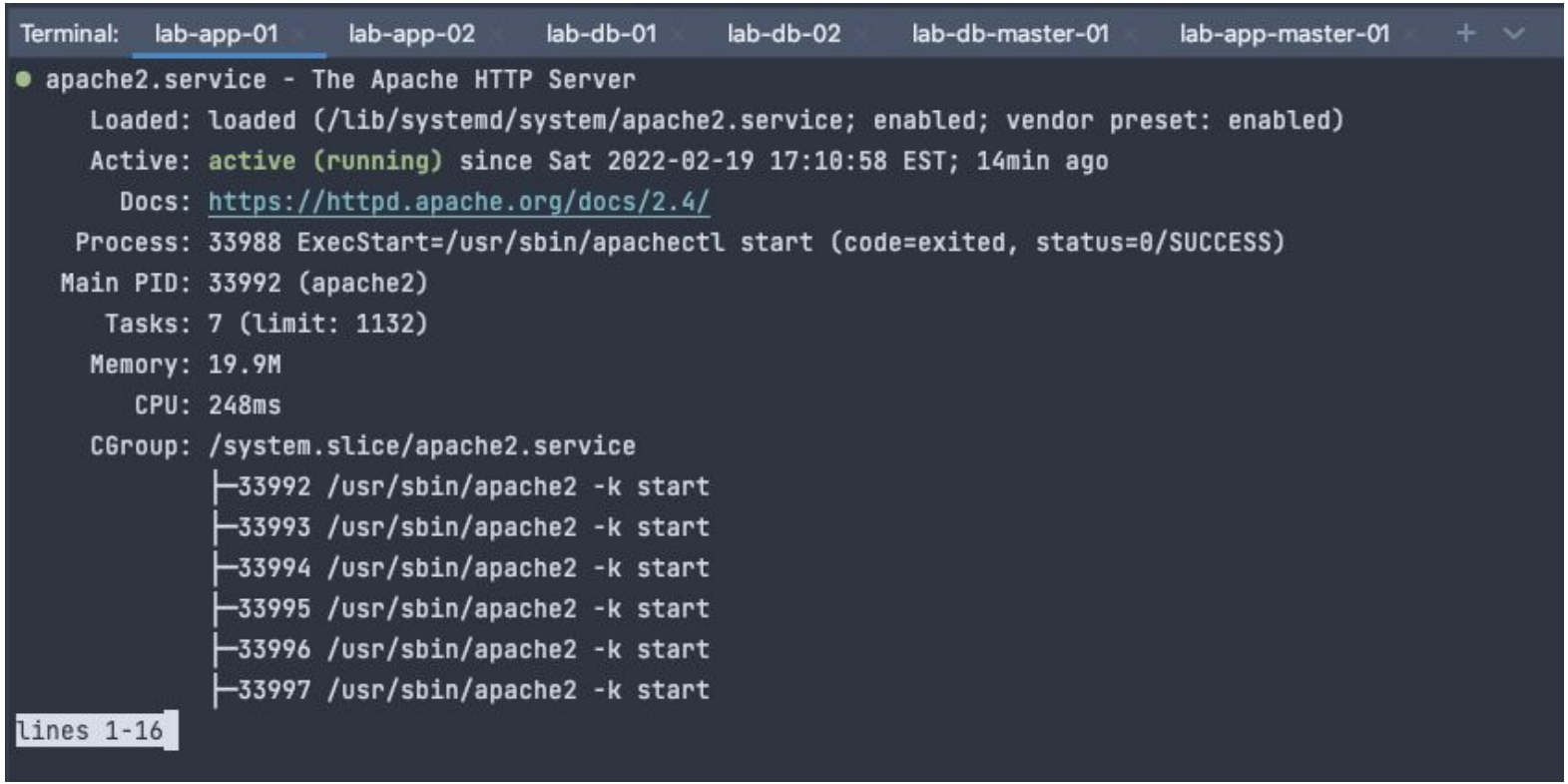


Apache HA

HAProxy - Redirection HTTPS + Cert

```
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend main
    bind *:80
    bind *:443 ssl crt /etc/haproxy/certs/ssl-certs.pem
    redirect scheme https if !{ ssl_fc }
    mode http
    default_backend             app

#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    balance     roundrobin
    server app1 172.16.25.11:80 check
    server app2 172.16.25.12:80 check
```

HAProxy - Redirection HTTPS + Cert



Ça fonctionne !

NFS

Serveurs NFS sur DB-Master et App-Master

```
root@lab-db-master-01:~# showmount -e
Export list for lab-db-master-01:
/data/nfs 172.16.25.0/255.255.255.0
```

```
root@lab-app-master-01:/data/nfs/www/filegator# showmount -e
Export list for lab-app-master-01:
/data/nfs 172.16.25.0/255.255.255.0
```

```
root@lab-app-02:~# mount | grep nfs
172.16.25.10:/data/nfs on /data/nfs_mounted type nfs4 (rw,relatime,vers=4.2,rsize=131072,wsize=131072,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.16.25.12,local_lock=none,addr=172.16.25.10)
172.16.25.10:/data/nfs on /mnt/shared_data type nfs4 (rw,relatime,sync,vers=4.2,rsize=131072,wsize=131072,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=172.16.25.12,local_lock=none,addr=172.16.25.10)
```

Filegator

Filegator - Interface

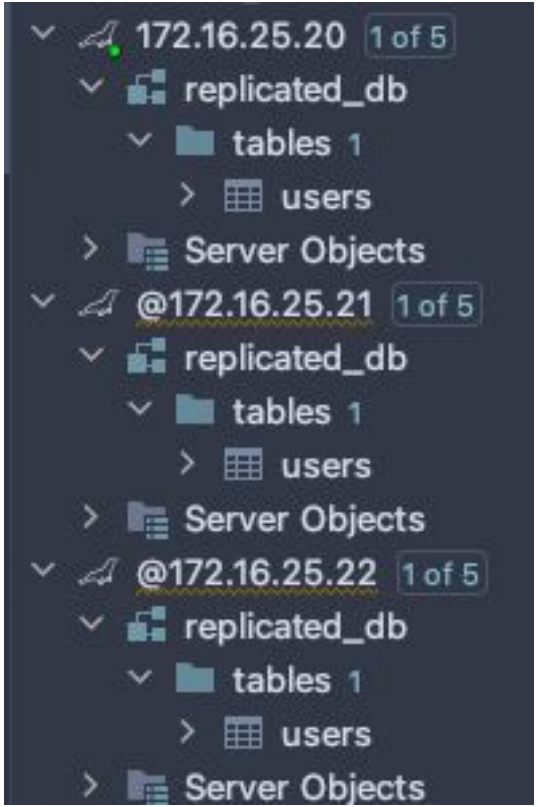
Filegator - Path utilisés

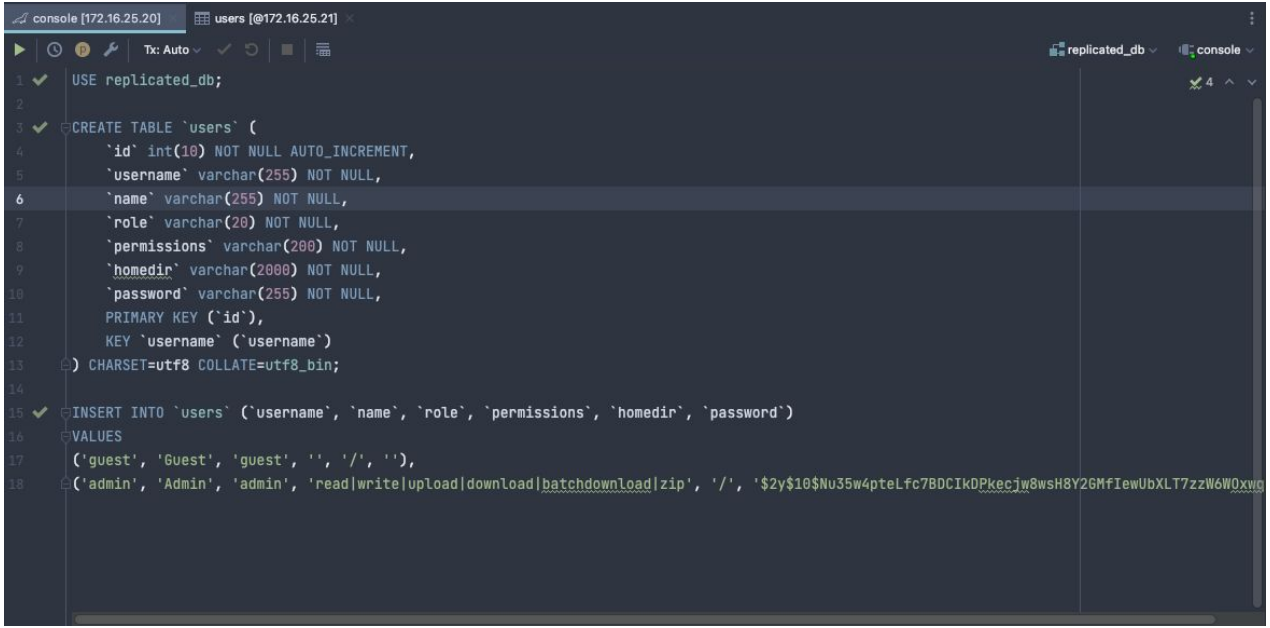
```
root@lab-app-02:/mnt/shared_data/www/filegator# ls
backend      CHANGELOG.md        composer.json  configuration.php         CONTRIBUTING.md  docker     LICENSE       package-lock.json  repository  SECURITY.md
BACKERS.md   CODE_OF_CONDUCT.md  composer.lock  configuration_sample.php  dist             index.php  package.json  private            robots.txt  vendor
```

```
root@lab-app-master-01:/data/nfs/www/filegator# ls
BACKERS.md     CODE_OF_CONDUCT.md  LICENSE       backend        composer.lock      configuration_sample.php  docker     package-lock.json  private     robots.txt
CHANGELOG.md   CONTRIBUTING.md     SECURITY.md   composer.json  configuration.php  dist                      index.php  package.json       repository  vendor
```

```
root@lab-app-02:/mnt/shared_data/www/filegator/repository# ls
test
```

Filegator - Utilisation de la DB



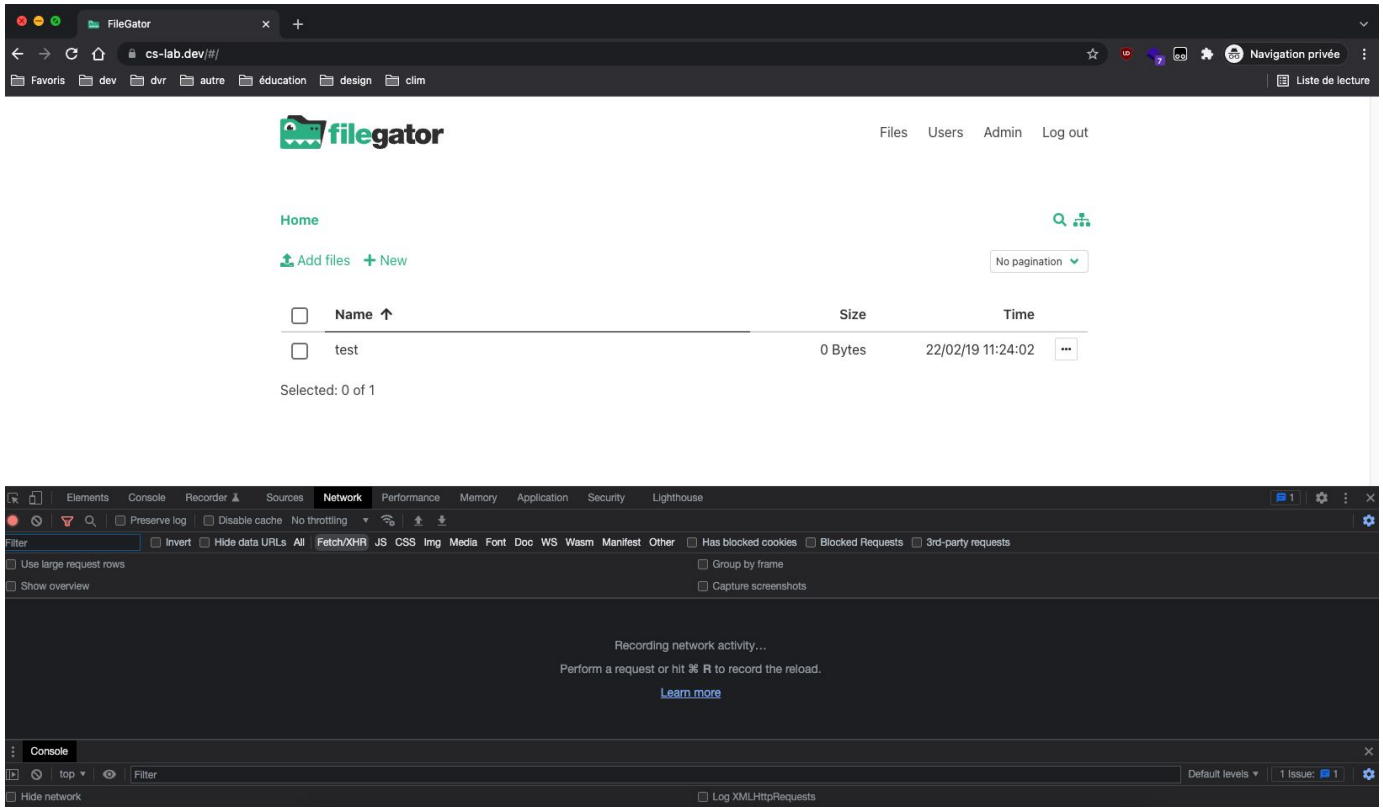


Filegator - Configuration PHP

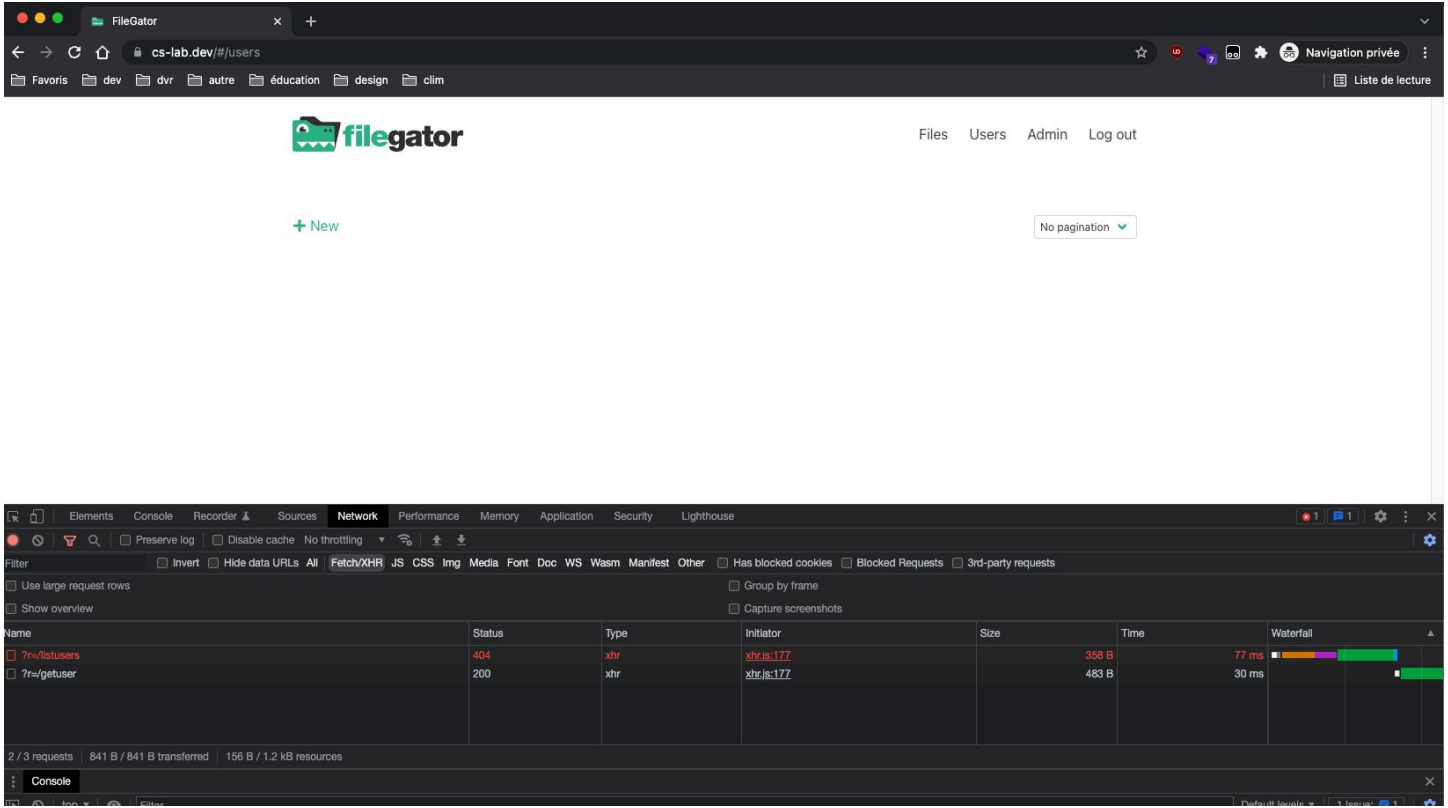
```
'Filegator\Services\Auth\AuthInterface' => [
    'handler' => '\Filegator\Services\Auth\Adapters\Database',
    'config' => [
        'driver' => 'mysqli',
        'host' => '172.16.25.20',
        'username' => 'supinfo',
        'password' => 'supinfo-3lpic',
        'database' => 'replicated_db',
    ],
],
```

```
apt install php-fpm
a2enmod proxy_fcgi setenvif
a2enconf php7.4-fpm

apt-get install php-mysql
```

Accès via HAProxy… ça marche !



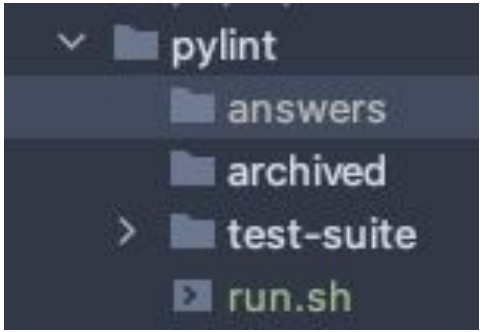
… ou pas.


FileGator
cs-lab.dev/#/users
Navigation privée
Favoris
dev
dvr
autre
éducation
design
clim
Liste de lecture
filegator
Files
Users
Admin
Log out
+ New
No pagination
Elements
Console
Recorder
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
All
Fetch/XHR
JS
CSS
Img
Media
Font
Doc
WS
Wasm
Manifest
Other
Has blocked cookies
Blocked Requests
3rd-party requests
Use large request rows
Group by frame
Show overview
Capture screenshots
Name
Status
Type
Initiator
Size
Time
Waterfall
?r=/listusers
404
xhr
xhr.js:177
358 B
77 ms
?r=/getuser
200
xhr
xhr.js:177
483 B
30 ms
2 / 3 requests
841 B / 841 B transferred
156 B / 1.2 kB resources
Console

Script/Watch

Lint Python

https://github.com/PyCQA/pylint



standard/run.sh | pylint/run.sh

```
echo "RUNNING SCRIPT"

#CURRENT_DIR=$(pwd)
CURRENT_DIR="/data/nfs/www/filegator/repository/pylint"
TEST_DIR="${CURRENT_DIR}/test-suite"
ARCHIVE_DIR="${CURRENT_DIR}/archived"
ANSWERS_DIR="${CURRENT_DIR}/answers"

cd "$TEST_DIR"
# Get all files with python extension
FILES=$(ls | egrep '\.py$')

for f in $FILES
do
    echo "Processing $f"
    now=$(date +"%FT%T")

    # get results
    result_path="${ANSWERS_DIR}/${now}-${f}-results.txt"
    pylint "$f" > "$result_path"

    # archive script files
    archive_path="${ARCHIVE_DIR}/$f"
    mv "$f" "$archive_path"
done

echo "END OF SCRIPT"
```

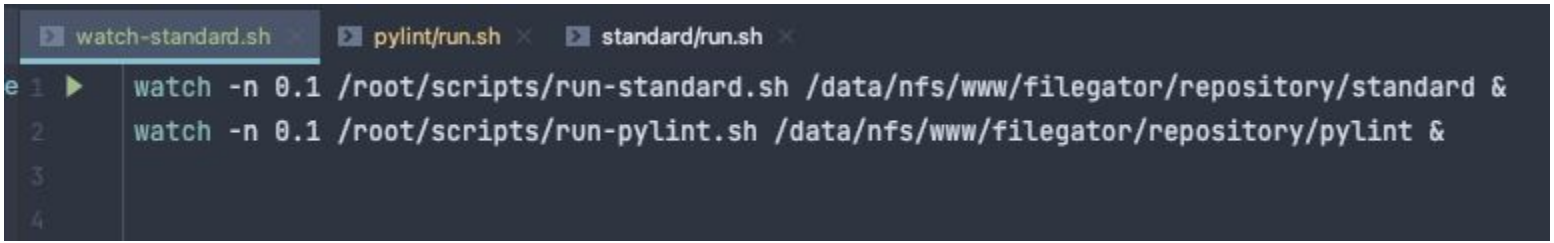
Lint Javascript

https://github.com/standard/standard

run.sh

```
echo "RUNNING SCRIPT"

#CURRENT_DIR=$(pwd)
CURRENT_DIR="/data/nfs/www/filegator/repository/standard"
TEST_DIR="${CURRENT_DIR}/test-suite"
ARCHIVE_DIR="${CURRENT_DIR}/archived"
ANSWERS_DIR="${CURRENT_DIR}/answers"

cd "$TEST_DIR"
# Get all files with javascript extension
FILES=$(ls | egrep '\.js$')

for f in $FILES
do
    echo "Processing $f"
    now=$(date +"%FT%T")

    # get results
    result_path="${ANSWERS_DIR}/${now}-${f}-results.txt"
    standard "$f" > "$result_path"
#    npx standard "$f" > "$result_path"

    # archive script files
    archive_path="${ARCHIVE_DIR}/$f"
    mv "$f" "$archive_path"
done

echo "END OF SCRIPT"
```

Watch


watch-standard.sh
pylint/run.sh
standard/run.sh
watch -n 0.1 /root/scripts/run-standard.sh /data/nfs/www/filegator/repository/standard &
watch -n 0.1 /root/scripts/run-pylint.sh /data/nfs/www/filegator/repository/pylint &

FIN.