TP : Sécurisation de la Machine Linux

Objectifs :

Créer des ACL pour contrôler les accès aux fichiers et répertoires.

Générer un certificat auto-signé pour sécuriser les communications HTTPS sur Apache2.

Configurer l'authentification SSH par clé publique.

Utiliser journalctl pour surveiller les journaux système.

Étapes :

1. Création d'ACL :

Utilisez les commandes setfacl et getfacl pour ajouter des ACL à un fichier ou répertoire, en accordant des autorisations spécifiques à certains utilisateurs ou groupes.

Correction:

Pour donner des droits spécifiques à un user:

setfacl -m u:user:rwx /chemin/vers/le/fichier

Pour verifier:

getfacl /chemin/vers/le/fichier

2. Génération d'un Certificat Auto-Signé :

Utilisez OpenSSL pour générer un certificat auto-signé à des fins de test ou de développement. Assurez-vous de spécifier les détails du certificat, tels que le nom de l'organisation, le nom de domaine, etc.

```
(base) vladislavyaromiy@EPORRED367 ~ % openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.............................+++++
e is 65537 (0x010001)
(base) vladislavyaromiy@EPORRED367 ~ % openssl req -new -key server.key -out ser
ver.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Paris
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dauphine
Organizational Unit Name (eg, section) []:Dauphine
Common Name (e.g. server FQDN or YOUR name) []:psl
Email Address []:mail@mail

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:none
An optional company name []:none
(base) vladislavyaromiy@EPORRED367 ~ % openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Signature ok
subject=C = FR, ST = Paris, L = Paris, O = Dauphine, OU = Dauphine, CN = psl, emailAddress = mail@mail
Getting Private key
(base) vladislavyaromiy@EPORRED367 ~ %
```

3. Configuration de l'Authentification SSH par Clé Publique :

Générez une paire de clés SSH (publique/privée) sur votre machine locale à l'aide de ssh-keygen.

Copiez la clé publique (id_rsa.pub) sur le serveur distant dans le fichier ~/.ssh/authorized_keys pour chaque utilisateur qui doit se connecter via SSH.

Pour generer ssh key:

```
(base) vladislavyaromiy@EPORRED367 .ssh % ssh-keygen -t ed25519 -C "vlad.yaromiy@gmail.com"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/vladislavyaromiy/.ssh/id_ed25519): server_env
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in server_env
Your public key has been saved in server_env.pub
The key fingerprint is:
SHA256:DsVq/I+GVe2VoVSJgb/0r5Z5KRb8L6QsRCBAEv3Zeao vlad.yaromiy@gmail.com
The key's randomart image is:
+--[ED25519 256]--+
|  o+o.     ..+.. |
|   .. ... . o o  |
|     . +oo + . o |
|     .ooo + = o  |
|      = S= o.+   |
|     . +o . ooo  |
|       +o. . oo+.|
|      E .o. oo=oo|
|       .. ....o+o|
+----[SHA256]-----+
(base) vladislavyaromiy@EPORRED367 .ssh % cat server_env.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINi8O5nv9h5yKmIXK9tFYovXPLvIedFgFJn2t0FEMeoP vlad.yaromiy@gmail.com
(base) vladislavyaromiy@EPORRED367 .ssh %
```

On l’ajoute sur serveur

```
(base) vladislavyaromiy@EPORRED367 .ssh % ssh-copy-id -i ~/.ssh/server_env.pub vlad@192.168.64.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/Users/vladislavyaromiy/.ssh/server_env.p
b"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already
installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install t
he new keys
vlad@192.168.64.2's password:

Number of key(s) added:        1

Now try logging into the machine, with:   "ssh 'vlad@192.168.64.2'"
and check to make sure that only the key(s) you wanted were added.

(base) vladislavyaromiy@EPORRED367 .ssh %
```

```
vlad@vlad-ubuntu:~/.ssh$ ls
authorized_keys
vlad@vlad-ubuntu:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINi8O5nv9h5yKmIXK9tFYovXPLvIedFgFJn2t0FEMeoP vlad.yaromiy@gmail.com
vlad@vlad-ubuntu:~/.ssh$
```

Donc on peut se connecter en utilisant notre public key

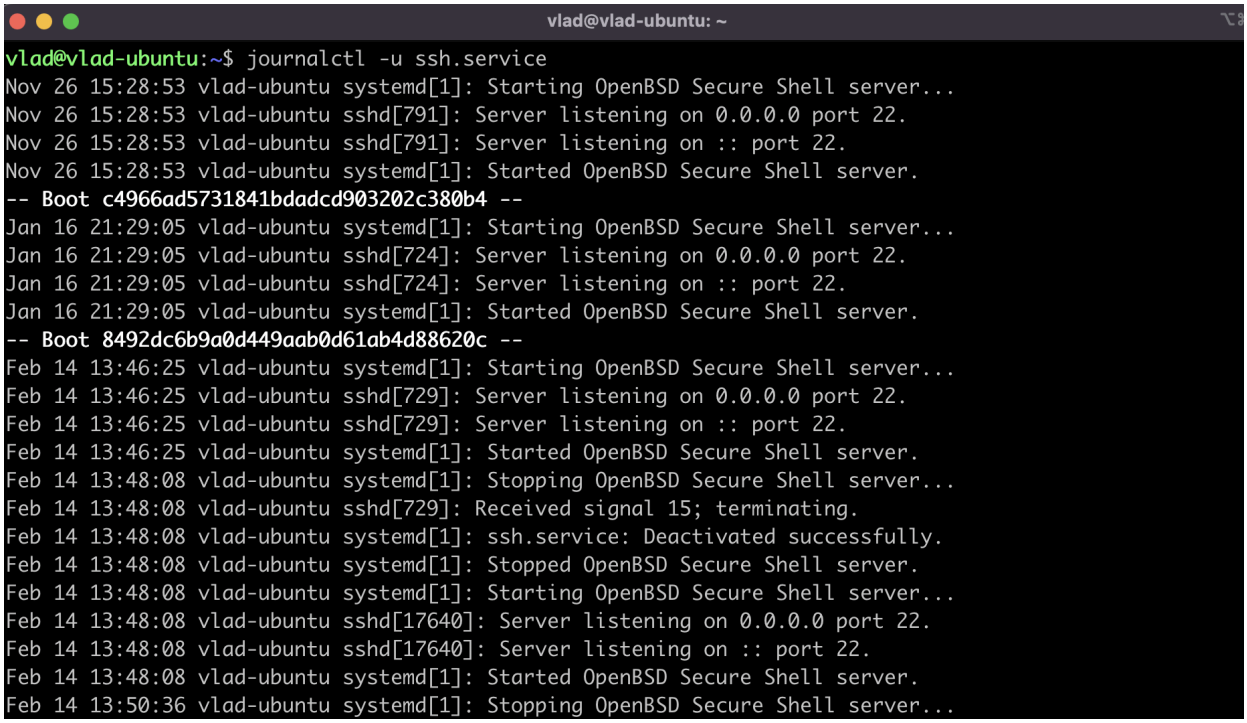
```
base) vladislavyaromiy@EPORRED367 .ssh % ssh -i ~/.ssh/server_env vlad@192.168.64.2
elcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic aarch64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

 System information as of Thu Feb 15 11:12:18 AM UTC 2024

 System load:             0.0
 Usage of /:              48.0% of 18.01GB
 Memory usage:            5%
 Swap usage:              0%
 Processes:               121
 Users logged in:         1
 IPv4 address for enp0s1: 192.168.64.2
 IPv6 address for enp0s1: fdc7:c2cd:2b0:3488:5ce7:fff:fed8:caf1


xpanded Security Maintenance for Applications is not enabled.

 updates can be applied immediately.

 additional security update can be applied with ESM Apps.
earn more about enabling ESM Apps service at https://ubuntu.com/esm


ast login: Thu Feb 15 11:08:26 2024 from 192.168.64.1
lad@vlad-ubuntu:~$
```

4. Utilisation de journalctl :

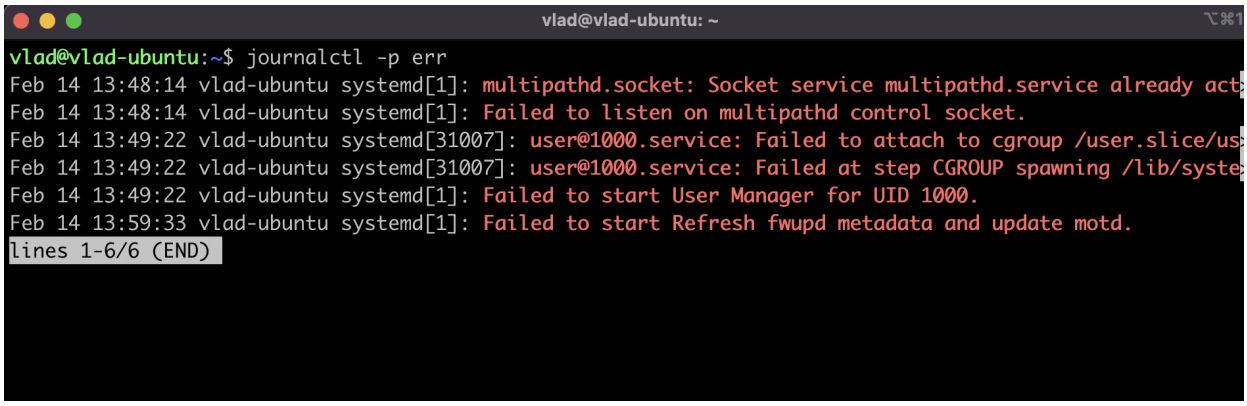
Utilisez journalctl pour surveiller les journaux système. Explorez différentes options de journalctl pour filtrer les journaux par service, priorité, plage de dates, etc.

Examinez les journaux pour détecter d'éventuelles anomalies ou activités suspectes.

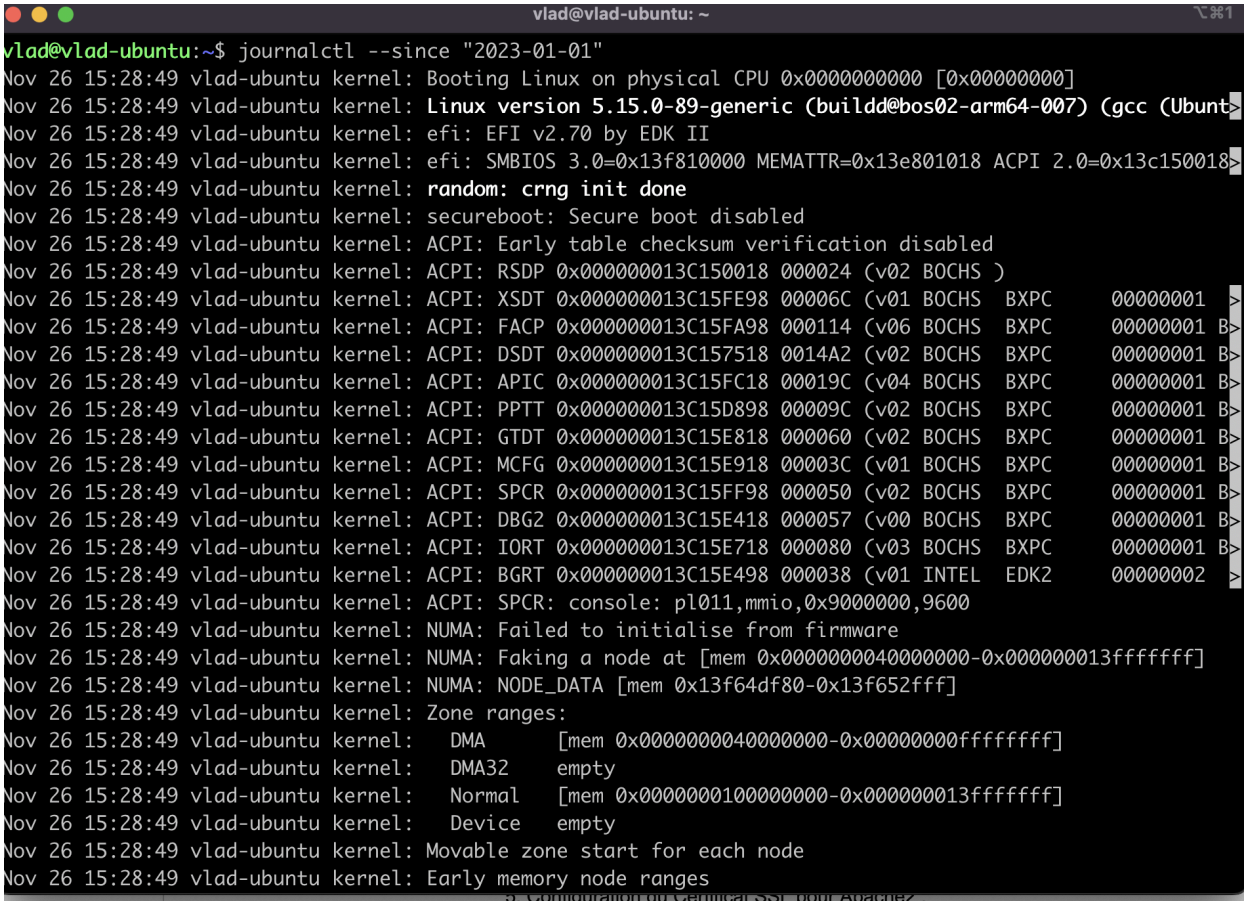
On a filtre par service (par exemple ssh.service)



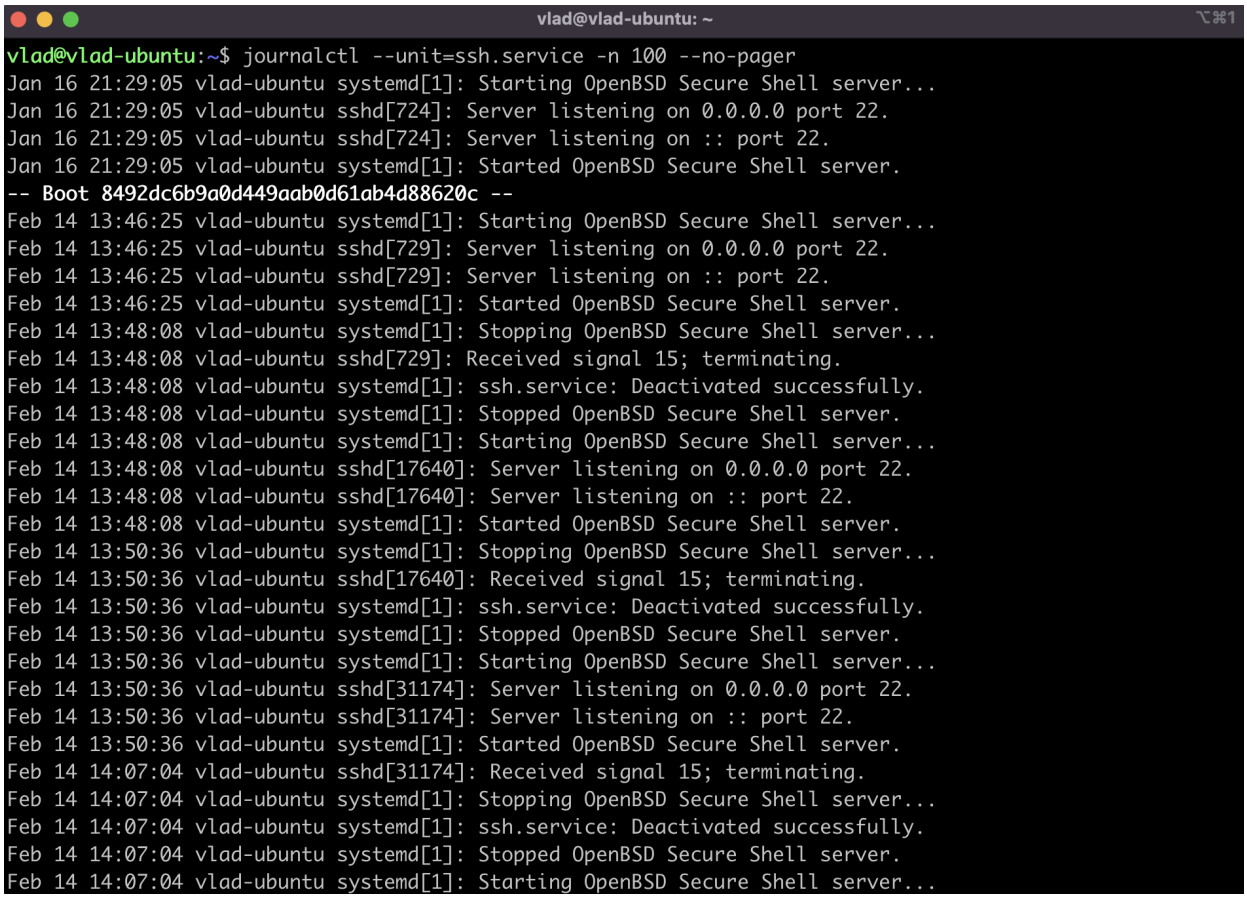
Filtre par priorité (par exemple filtre par erreur)



On peut aussi voir des logs par certain timelapse



Ce qui est très utile lors du développement c’est la possibilité de voir les derniers logs du service pour détecter des erreurs éventuelles.



5. Configuration du Certificat SSL pour Apache2 :

Utilisez le certificat auto-signé généré pour sécuriser les communications HTTPS sur Apache2.

Configurez Apache2 pour utiliser le certificat SSL en ajoutant les directives appropriées dans les fichiers de configuration Apache.