

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 vérifier:

`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 server.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 ~ % █
```

```

(base) vladislavyaromiy@EPORRED367 ~ % cat server
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2Q
QyNTUxOQAAACByrnptaK0ibDecH2BdIbiu/c9Y4kEsIdxq+4ErczliDAAAAKDwQhg68
0gAAAAAtzc2gtZWQyNTUxOQAAACByrnptaK0ibDecH2BdIbiu/c9Y4kEsIdxq+4ErczT
AAAEb8uhDF1CwuZvm+uUHx38q5pziFwDCI9fjB+xS1mrLI3Kuem1orSJsN5wfYF0hu
z1jiQSwH3Gr7gStzOWIMAAAAFnZsYWQueWFyb21peUBnbWFpbC5jb20BAGMEBQYH
-----END OPENSSH PRIVATE KEY-----
(base) vladislavyaromiy@EPORRED367 ~ % cat server.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxB/wx7EXLjHYu7Zbf+JRElnzEYkMIwNydZUde8wSh7g0opqJ
u4fItRjtVpvh2BG6nPTF5gXJhwaPEc8BZPIFo3yHoqpx8TScKe8z/oB8G11Ib1xW
Y3C42Qcm74/DIJUpXE2haagKMxf8RDLbSDk1L17pXDz8H3hF/waLxko36PidbeVY
yhYpQFrFuul76GQRri8otHCnZbPc5xWvQlRf+b870hrmUeMFqtbkEwgjMKqtEN1J
4M4Gf/CioK4qLqadES/Azpp1J3lhguKS9vL+Ql8UnAUs/R3jcUnTc/pb5FctJcL9
LaaZC/u/Uz2qW7sZBoRx1oJPXJZrJ2vPS3XfIwIDAQABAoIBABZIpknRNVC4gNbD
ZBVC5p2I4Bz8od5n4yAAeMyYQL2o2TtFmPkIvYKNWzw+HMNuXi+HYwW708LtyPaw
EZc2f+p8rsha7kJHHBRvjDYiXBEVvKXMR0NiL9MtYLRROChE4vBXFb6hNAvmDZC6
gXUNqbohWPy3EJpdsdTinp3vXq40yPqdXHiYrFo0vesQ/ZY6t8f0Wq1Ebmd5q+Bt
qlp2mecPvGItnLIjYKGp20LG1yV2R372caGVi8Yg5kMUimjJ8LDTgnz2tSynKuU
aajCqgb8K+SaNypESpCxLUZSAUNevkFIp2I89vWeSv/YwqRPesIq6VVvHXgCZI+8
u+7mt1ECgYEA4q89Ca2NCS0D8ZPSvA4HRc+4ztp61HkooDRPVfsXBxy+6WJp43yy
hXzDrYlfbSxkdHEHvGqtkTN0NoGkwsuzqLgaeqpxwZVBcWWStJi8aUmdNWYSy5L
xIJyUlZi8dAAIA5FF645fY4MaMIj2UTj9m1gdg304VsW+7saGK9NzZkCgYEA1HQe
TDX9NLCrYVCCyxdCxvda/gXq0hQ2cRhswfFk6IY3xbGEec1RYuUlnd3Yh7UERMjs
6eUWnofa9FEQJ/W4C2bMod3ub8jqApA/rT6SIkiywhyOuVy9Ddn2Z6CqY80s8hLZ
Yq6J7Dd840ZZnGw2sza3HDBdmAwe9XhYlVkosBsCgYEA30dFbGLE0+rrnr6gnEdr
X6BgVVKLQYspY545Tb5TW4DnTzKJ7LZmYqVnuxiZkKGMewfFShNzlfAyYcHEabVK
sCsW654pHQ+MnTQKmIzwYkJGWqW8A2yo3kds/se405uXjnoZJJQGcWSRvD+PiaoI
m2WbBKS5XHmpd1ug3jxJRvkCgYBmtuEzDWMmx0eEXA1wLQX09iYa7Dcq7zzG/v0N
4yxbMxDh1opq7PYtLwY5xdj6+2xd6RqJlOWSDbKxLkP2XdkmQgQr0gYeK2/f32e5
1aeHQqQRrwb3VVVzgxQW6AlcjwJqU1KZYIvH0CVDR0kADmN+aUbztJhQXLyUMXb
JukCAwKBgQCIL/7jybZ0qczPCgwtbQvFqYcmvMiI8sW0/n16I+vBo2TK5naHcuk/
Ty0aTLBxhFzREqpF/zYXaxJN55BoJutmf44stnJjarchET6MyFFAxSujOSB+0acp
FdHcEDBkG4U1ldMoQRkhdPQPYLqCLrx9WE2a4y6evbAOiVlt68YBwQ==
-----END RSA 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/0r5Z5KRb8L6QsRCBAEv3Zea0 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 AAAAC3NzaC1lZDI1NTE5AAAAINi805nv9h5yKmIXK9tFYovXPLvIedFgFJn2t0FEMeoP 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
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:~$ cd ~/.ssh
vlad@vlad-ubuntu:~/.ssh$ ls
authorized_keys
vlad@vlad-ubuntu:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINI805nv9h5yKmIXK9tFYovXPLvIedFgFJn2t0FEMeoP vlad.yaromiy@gmail.com
vlad@vlad-ubuntu:~/.ssh$
```

Donc on peut se connecter en utilisant notre public key

```
(base) vladi@vlad-ubuntu:~$ ssh -i ~/.ssh/server_env vlad@192.168.64.2
Welcome 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 18.0GB
Memory usage:         5%
Swap usage:           0%
Processes:            121
Users logged in:      1
IPv4 address for enp0s1: 192.168.64.2
IPv6 address for enp0s1: fd7:c2cd:2b0:3488:5ce7:fff:fed8:caf1

Expanded Security Maintenance for Applications is not enabled.

No updates can be applied immediately.

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

Last login: Thu Feb 15 11:08:26 2024 from 192.168.64.1
vlad@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)

```

vlad@vlad-ubuntu: ~$ journalctl -u ssh.service
Nov 26 15:28:53 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Nov 26 15:28:53 vlad-ubuntu sshd[791]: Server listening on 0.0.0.0 port 22.
Nov 26 15:28:53 vlad-ubuntu sshd[791]: Server listening on :: port 22.
Nov 26 15:28:53 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.
-- Boot c4966ad5731841bdadcd903202c380b4 --
Jan 16 21:29:05 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Jan 16 21:29:05 vlad-ubuntu sshd[724]: Server listening on 0.0.0.0 port 22.
Jan 16 21:29:05 vlad-ubuntu sshd[724]: Server listening on :: port 22.
Jan 16 21:29:05 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.
-- Boot 8492dc6b9a0d449aab0d61ab4d88620c --
Feb 14 13:46:25 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Feb 14 13:46:25 vlad-ubuntu sshd[729]: Server listening on 0.0.0.0 port 22.
Feb 14 13:46:25 vlad-ubuntu sshd[729]: Server listening on :: port 22.
Feb 14 13:46:25 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...
Feb 14 13:48:08 vlad-ubuntu sshd[729]: Received signal 15; terminating.
Feb 14 13:48:08 vlad-ubuntu systemd[1]: ssh.service: Deactivated successfully.
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Stopped OpenBSD Secure Shell server.
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Feb 14 13:48:08 vlad-ubuntu sshd[17640]: Server listening on 0.0.0.0 port 22.
Feb 14 13:48:08 vlad-ubuntu sshd[17640]: Server listening on :: port 22.
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Feb 14 13:50:36 vlad-ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...

```

Filtre par priorité (par exemple filtre par erreur)

```

vlad@vlad-ubuntu: ~$ journalctl -p err
Feb 14 13:48:14 vlad-ubuntu systemd[1]: multipathd.socket: Socket service multipathd.service already act
Feb 14 13:48:14 vlad-ubuntu systemd[1]: Failed to listen on multipathd control socket.
Feb 14 13:49:22 vlad-ubuntu systemd[31007]: user@1000.service: Failed to attach to cgroup /user.slice/us
Feb 14 13:49:22 vlad-ubuntu systemd[31007]: user@1000.service: Failed at step CGROUP spawning /lib/syste
Feb 14 13:49:22 vlad-ubuntu systemd[1]: Failed to start User Manager for UID 1000.
Feb 14 13:59:33 vlad-ubuntu systemd[1]: Failed to start Refresh fwupd metadata and update motd.
lines 1-6/6 (END)

```

On peut aussi voir des logs par certain timelapse

```

vlad@vlad-ubuntu: ~
vlad@vlad-ubuntu:~$ journalctl --since "2023-01-01"
Nov 26 15:28:49 vlad-ubuntu kernel: Booting Linux on physical CPU 0x0000000000 [0x00000000]
Nov 26 15:28:49 vlad-ubuntu kernel: Linux version 5.15.0-89-generic (buildd@bos02-arm64-007) (gcc (Ubuntu
Nov 26 15:28:49 vlad-ubuntu kernel: efi: EFI v2.70 by EDK II
Nov 26 15:28:49 vlad-ubuntu kernel: efi: SMBIOS 3.0=0x13f810000 MEMATTR=0x13e801018 ACPI 2.0=0x13c150018
Nov 26 15:28:49 vlad-ubuntu kernel: random: crng init done
Nov 26 15:28:49 vlad-ubuntu kernel: secureboot: Secure boot disabled
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: Early table checksum verification disabled
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: RSDP 0x0000000013C150018 000024 (v02 BOCHS )
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: XSDT 0x0000000013C15FE98 00006C (v01 BOCHS BXPC 00000001
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: FACP 0x0000000013C15FA98 000114 (v06 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: DSDT 0x0000000013C157518 0014A2 (v02 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: APIC 0x0000000013C15FC18 00019C (v04 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: PPTT 0x0000000013C15D898 00009C (v02 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: GTDT 0x0000000013C15E818 000060 (v02 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: MCFG 0x0000000013C15E918 00003C (v01 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: SPCR 0x0000000013C15FF98 000050 (v02 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: DBG2 0x0000000013C15E418 000057 (v00 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: IORT 0x0000000013C15E718 000080 (v03 BOCHS BXPC 00000001 B
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: BGRT 0x0000000013C15E498 000038 (v01 INTEL EDK2 00000002
Nov 26 15:28:49 vlad-ubuntu kernel: ACPI: SPCR: console: pl011,mmio,0x9000000,9600
Nov 26 15:28:49 vlad-ubuntu kernel: NUMA: Failed to initialise from firmware
Nov 26 15:28:49 vlad-ubuntu kernel: NUMA: Faking a node at [mem 0x0000000040000000-0x0000000013ffffff]
Nov 26 15:28:49 vlad-ubuntu kernel: NUMA: NODE_DATA [mem 0x13f64df80-0x13f652fff]
Nov 26 15:28:49 vlad-ubuntu kernel: Zone ranges:
Nov 26 15:28:49 vlad-ubuntu kernel: DMA [mem 0x0000000040000000-0x00000000ffffff]
Nov 26 15:28:49 vlad-ubuntu kernel: DMA32 empty
Nov 26 15:28:49 vlad-ubuntu kernel: Normal [mem 0x0000000010000000-0x0000000013ffffff]
Nov 26 15:28:49 vlad-ubuntu kernel: Device empty
Nov 26 15:28:49 vlad-ubuntu kernel: Movable zone start for each node
Nov 26 15:28:49 vlad-ubuntu kernel: Early memory node ranges

```

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


```
vlad@vlad-ubuntu: ~  
vlad@vlad-ubuntu:~$ journalctl --unit=ssh.service -n 100 --no-pager  
Jan 16 21:29:05 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...  
Jan 16 21:29:05 vlad-ubuntu sshd[724]: Server listening on 0.0.0.0 port 22.  
Jan 16 21:29:05 vlad-ubuntu sshd[724]: Server listening on :: port 22.  
Jan 16 21:29:05 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.  
-- Boot 8492dc6b9a0d449aab0d61ab4d88620c --  
Feb 14 13:46:25 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...  
Feb 14 13:46:25 vlad-ubuntu sshd[729]: Server listening on 0.0.0.0 port 22.  
Feb 14 13:46:25 vlad-ubuntu sshd[729]: Server listening on :: port 22.  
Feb 14 13:46:25 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.  
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...  
Feb 14 13:48:08 vlad-ubuntu sshd[729]: Received signal 15; terminating.  
Feb 14 13:48:08 vlad-ubuntu systemd[1]: ssh.service: Deactivated successfully.  
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Stopped OpenBSD Secure Shell server.  
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...  
Feb 14 13:48:08 vlad-ubuntu sshd[17640]: Server listening on 0.0.0.0 port 22.  
Feb 14 13:48:08 vlad-ubuntu sshd[17640]: Server listening on :: port 22.  
Feb 14 13:48:08 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.  
Feb 14 13:50:36 vlad-ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...  
Feb 14 13:50:36 vlad-ubuntu sshd[17640]: Received signal 15; terminating.  
Feb 14 13:50:36 vlad-ubuntu systemd[1]: ssh.service: Deactivated successfully.  
Feb 14 13:50:36 vlad-ubuntu systemd[1]: Stopped OpenBSD Secure Shell server.  
Feb 14 13:50:36 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...  
Feb 14 13:50:36 vlad-ubuntu sshd[31174]: Server listening on 0.0.0.0 port 22.  
Feb 14 13:50:36 vlad-ubuntu sshd[31174]: Server listening on :: port 22.  
Feb 14 13:50:36 vlad-ubuntu systemd[1]: Started OpenBSD Secure Shell server.  
Feb 14 14:07:04 vlad-ubuntu sshd[31174]: Received signal 15; terminating.  
Feb 14 14:07:04 vlad-ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...  
Feb 14 14:07:04 vlad-ubuntu systemd[1]: ssh.service: Deactivated successfully.  
Feb 14 14:07:04 vlad-ubuntu systemd[1]: Stopped OpenBSD Secure Shell server.  
Feb 14 14:07:04 vlad-ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
```

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.