Sistemas de Gestión Empresarial

Andreu Sanz Sanz

2DAM

2023-24

Tema V. Fail2ban

Sistemes de Gestió Empresarial | 2023-2024

Andreu Sanz Sanz

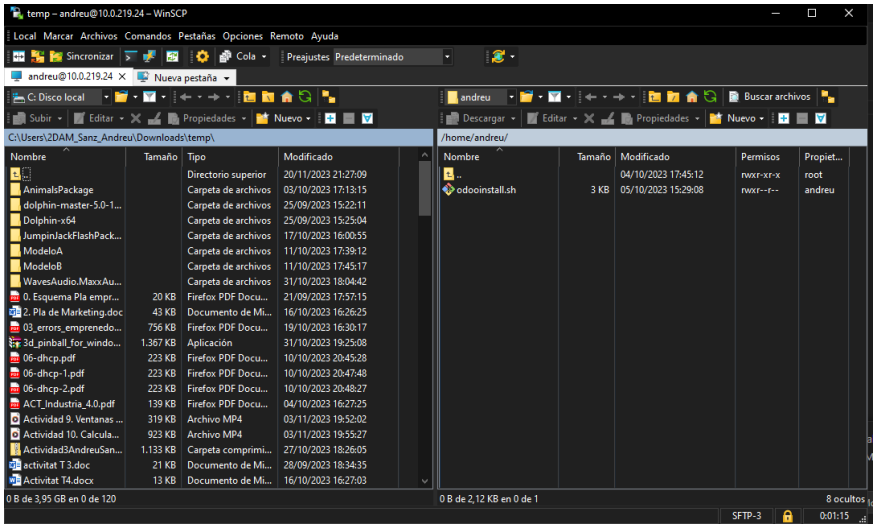
Tabla de continguts

REQUISITOS PREVIOS

1. Comprobar que ssh está instalado (o comprobar que esté instalado)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:13:fc:2b brd ff:ff:ff:ff:ff:ff
    inet 10.0.219.24/24 metric 100 brd 10.0.219.255 scope global dynamic enp0s3
       valid_lft 86362sec preferred_lft 86362sec
    inet6 fe80::a00:27ff:fe13:fc2b/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:f4:47:74 brd ff:ff:ff:ff:ff:ff
andreu@andreu-server:~$ sudo systemctl status ssh
[sudo] password for andreu:
Sorry, try again.
[sudo] password for andreu:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-11-29 15:14:43 UTC; 11min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 657 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 708 (sshd)
      Tasks: 1 (limit: 3398)
     Memory: 4.4M
        CPU: 56ms
     CGroup: /system.slice/ssh.service
             └─708 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

nov 29 15:14:42 andreu-server systemd[1]: Starting OpenBSD Secure Shell server...
nov 29 15:14:43 andreu-server sshd[708]: Server listening on 0.0.0.0 port 22.
nov 29 15:14:43 andreu-server sshd[708]: Server listening on :: port 22.
nov 29 15:14:43 andreu-server systemd[1]: Started OpenBSD Secure Shell server.
andreu@andreu-server:~$ sudo systemctl status ssh
```

2. Probar la conexión a través de ssh desde WIndows a Ubuntu Server (WinSCP, Putty..)



PREGUNTAS CONTEXTUALES FAIL2BAN

3. ¿Qué es un ataque de fuerza bruta?

Un ataque de fuerza bruta es un método en el que un atacante intenta descifrar una contraseña o clave mediante la prueba sistemática de todas las combinaciones posibles. Este enfoque es intensivo en recursos y lleva tiempo.

4. ¿Para qué sirve y qué es FAIL2BAN?

Fail2Ban es una herramienta de prevención de intrusiones en servidores GNU/Linux, escrita en Python. Se utiliza para defender contra ataques de fuerza bruta en servicios abiertos al exterior.

5. ¿Qué hace FAIL2BAN con el fichero de logs?

Fail2Ban monitoriza ficheros de logs, como /var/log/auth.log, en busca de intentos de acceso fallidos. Detecta patrones de autenticación incorrecta y toma medidas como bloquear la IP del atacante.

6. ¿Qué son los jails?

Los "jails" en Fail2Ban son conjuntos de reglas y acciones específicas asociadas a cada servicio que se quiere proteger. Cada jail se configura para defender un servicio particular, como sshd o apache-auth.

7. ¿Qué se puede hacer con FAIL2BAN?

Fail2Ban puede bloquear automáticamente las direcciones IP que superan el umbral de intentos de acceso fallidos, añadiendo reglas al cortafuegos. Aunque no es infalible, sirve como una importante primera línea de defensa contra ataques y puede trabajar en conjunto con otras medidas de seguridad.

CONFIGURACIÓN FAIL2BAN

8. Instala Fail2BAN en Ubuntu Server. (CAPTURA)

comand: sudo apt install fail2ban

```
andreu@andreu-server:~$ systemctl status  fail2ban
♦ fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; disabled; vendor preset: e
     Active: inactive (dead)
       Docs: man:fail2ban(1)
andreu@andreu-server:~$ _
```

9. Habilita Fail2ban para que arranque automáticamente (CAPTURA)

10. Comprobar que el servicio fail2ban está activo (CAPTURA)

Tras ejecutar el comando sudo systemctl enable fail2ban.service he reiniciado el servidor con reboot y despues he ejecutado sudo systemctl status fail2ban.service para comprobar que el Fail2ban estava arrancado.

```
andreu@andreu-server:~$ sudo systemctl status fail2ban.service
[sudo] password for andreu:
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-11-29 16:01:47 UTC; 14s ago
       Docs: man:fail2ban(1)
   Main PID: 647 (fail2ban-server)
      Tasks: 5 (limit: 3398)
     Memory: 15.7M
        CPU: 230ms
     CGroup: /system.slice/fail2ban.service
             └─647 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

nov 29 16:01:47 andreu-server systemd[1]: Started Fail2Ban Service.
nov 29 16:01:49 andreu-server fail2ban-server[647]: Server ready
andreu@andreu-server:~$ _
```

CARACTERÍSTICAS

11. ¿Qué muestra sudo fail2ban-client status? ¡Explícalo! (CAPTURA)

Muestra el numero de jails que estan actualmente habilitados y el detalle de cada uno de ellos.

```
andreu@andreu-server:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

12. ¿Cuál es el archivo de configuración? Explica los parámetros: bantime y maxretry. (CAPTURA)

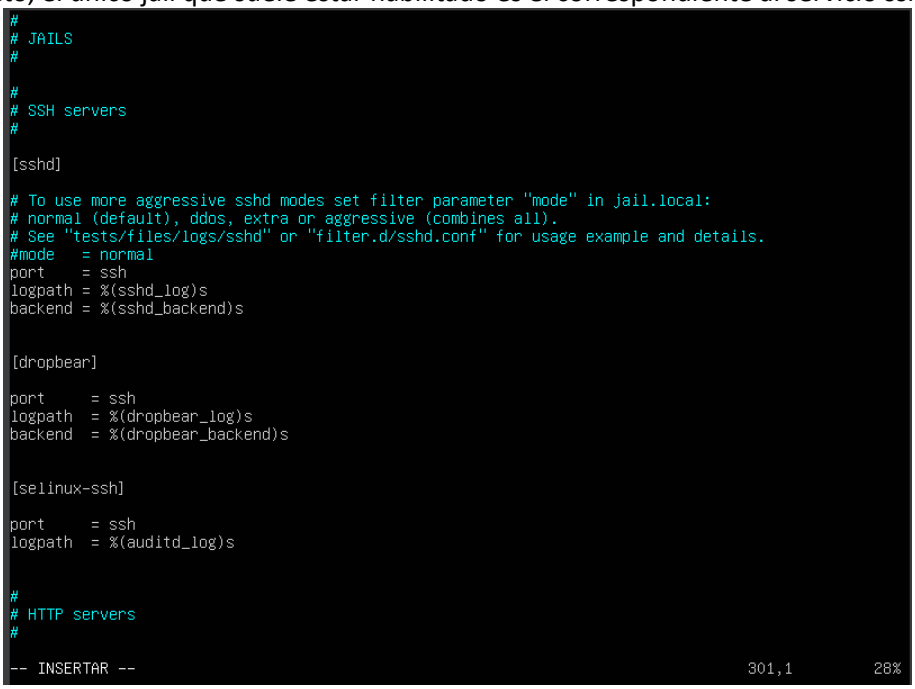
```
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information



# Comments: use '#' for comment lines and ';' (following a space) for inline comments


[INCLUDES]

#before = paths-distro.conf
before = paths-debian.conf
-- INSERTAR --                                                    3,2           Comienzo
```

```
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,

#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#              If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#              If Gamin is not installed, Fail2ban will use auto.
# polling:   uses a polling algorithm which does not require external libraries.
# systemd:   uses systemd python library to access the systemd journal.
#              Specifying "logpath" is not valid for this backend.
#              See "journalmatch" in the jails associated filter config
# auto:      will try to use the following backends, in order:
-- INSERTAR --                                                  95,1          9%
```

El archivo de configuración es /etc/fail2ban/jail.conf.
- bantime es el numero de segundos que el host sea baneado
- maxretry es la cantidad de fallos antes de que se prohíba un host.

13. ¿Cuál es el jail activado por defecto? (CAPTURA)

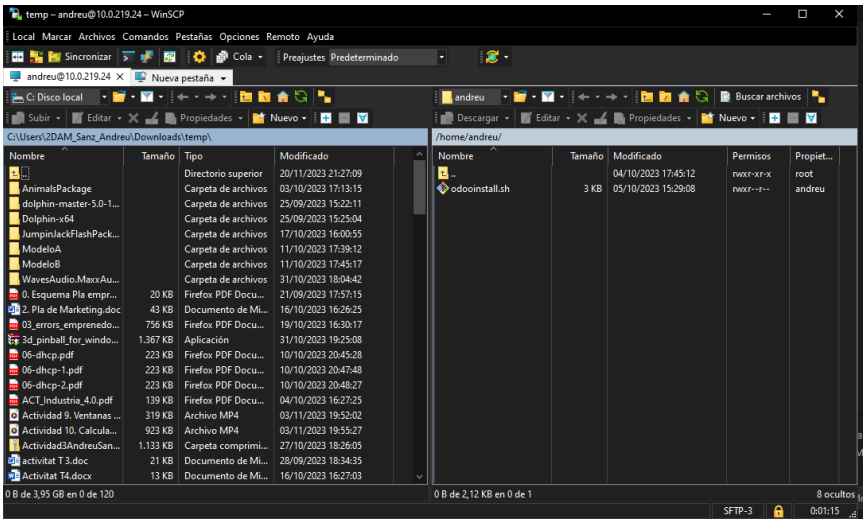
Por defecto, el unico jail que suele estar habilitado es el correspondiente al servicio sshd



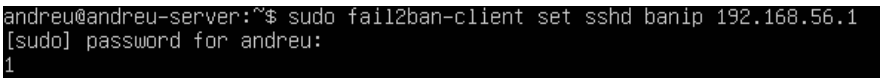
14. Accede al fichero de logs. (CAPTURA)

Ejercicio 1

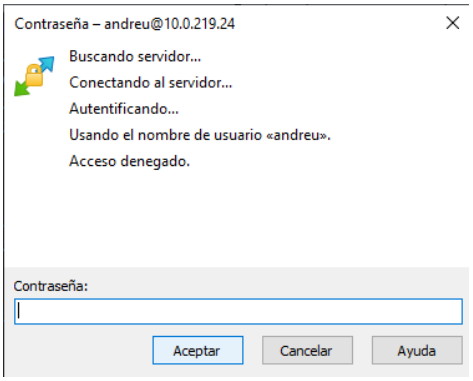
Paso 1



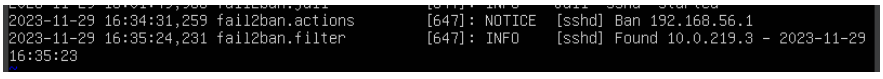
Paso 2



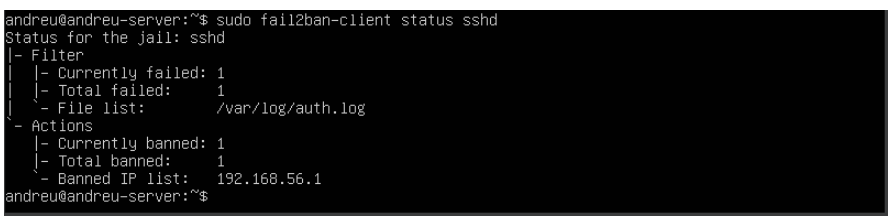
Paso 3



Paso 4



Paso 5



Paso 6

```
andreu@andreu-server:~$ sudo fail2ban-client set sshd unbanip 192.168.56.1
1
```

Ejercicio 2

```
andreu@andreu-server:~$ sudo fail2ban-client set sshd unbanip 192.168.56.1
1
andreu@andreu-server:~$ sudo fail2ban-client set sshd banip 10.0.219.14
1
andreu@andreu-server:~$ 10.0.219.21
10.0.219.21: command not found
andreu@andreu-server:~$ sudo fail2ban-client set sshd banip 10.0.219.21
1
andreu@andreu-server:~$ _
```

Ejercicio 3

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
maxretry = 3
```

```
C:\Users\2DAM_Sanz_Andreu>ssh 10.0.219.24
2dam_sanz_andreu@10.0.219.24's password:
Permission denied, please try again.
2dam_sanz_andreu@10.0.219.24's password:
Permission denied, please try again.
2dam_sanz_andreu@10.0.219.24's password:
ssh_dispatch_run_fatal: Connection to 10.0.219.24 port 22: Connection timed out
```