IMPLEMENTACIÓ D'UN SERVIDOR D'ALT RENDIMENT

Fonaments de Maquinari
Pol Muel Garcia
1r Asix

1. Introducció

En aquesta pràctica portarem a terme un servidor senzill, on crearem un sistema redundant en un CPD virtualitzat (un CPD és un centre de processament de dades). Abans de començar es mostraran la creació de les màquines per tenir una idea de com poder replicar aquesta pràctica.

Els objectius principals és tenir un servidor amb tolerància a falles a part de tenir una seguretat a la xarxa, ja que haurem de tenir obert ports pel servidor de recuperació i haurem d'assegurar-nos que tots els altres estan tancats, i també utilitzarem mecanismes bàsics de monitoratge, simulant així com funciona en un entorn real.

2. Configuració del sistema

2.1 Creació de les màquines virtuals

Haurem de crear dues màquines virtuals amb el sistema operatiu Ubuntu Server instal·lat en elles. La primera màquina tindrà un primer disc dur de 20 GB i un segon amb 50 GB, de maquinari tindrà 2 CPU, 4 GB RAM, en canvi, la segona també tindrà el mateix emmagatzematge, però, amb un maquinari d'1 CPU, 2 GB RAM.

Les dues màquines tindran una connexió a la xarxa amb un adaptador pont.

2.1 Configuració RAID 1 al Servidor-Principal

Per fer un RAID, utilitzarem la comanda “mdadm”, per així poder unir els dos discos i tenir més seguretat en cas de pèrdua d’un disc o de corrupció de dades. Pel que:

```
polmuel@pol:~$ sudo mdadm --create /dev/md0 --level=1 --raid-devices=1 /dev/sdb --force
mdadm: Note: this array has metadata at the start and
    may not be suitable as a boot device.  If you plan to
    store '/boot' on this device please ensure that
    your boot-loader understands md/v1.x metadata, or use
    --metadata=0.90
Continue creating array? y
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
polmuel@pol:~$
```

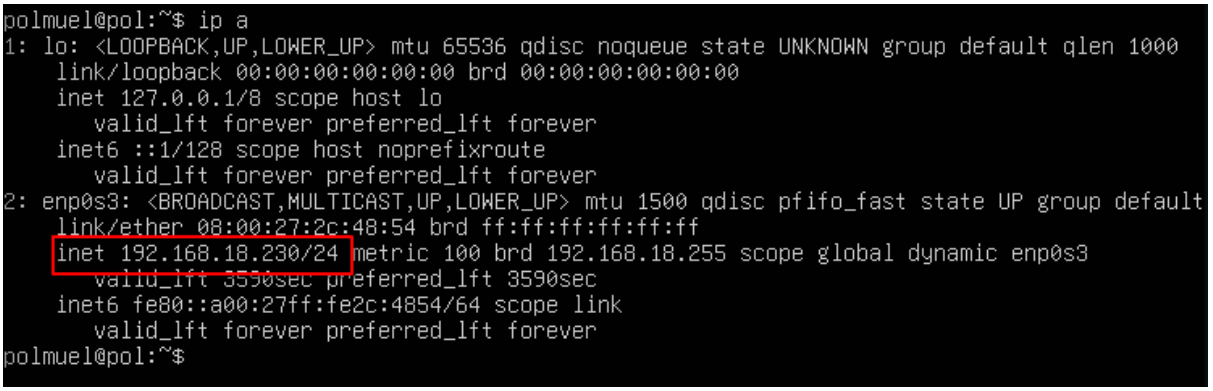
D’aquesta manera ens assegurem de tenir un disc d’emmagatzematge encarregat de salvaguardar les dades del disc principal en cas d'algun error, corrupció o falles del mateix disc.

2.2 Seguretat i protecció de xarxa

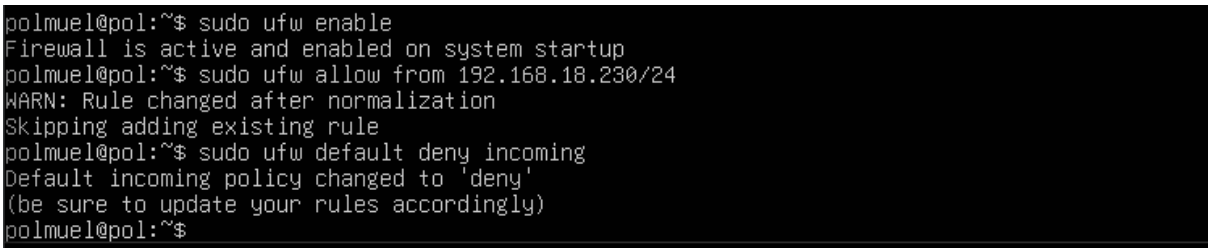
2.2.1 Firewall

En el nostre servidor activarem el firewall per protegir-nos de possibles atacs, però continuarem donant accés al servidor-backup perquè ell tingui accés i es pugui connectar per correcció d'errors o copies/backups de seguretat.

Primer mirarem la IP del servidor-backup amb la comanda "ip a"



I el següent serà activar el firewall i donar accés a l'altre servidor, utilitzarem el següent:



2.2.2 Protecció contra atacs

Per veure si el nostre firewall actua correctament amb el que hem introduït al punt anterior, utilitzarem l'eina fail2ban, amb la qual simularem un atac al servidor, instal·larem l'eina amb la comanda "sudo apt install fail2ban".

Modifiquem la configuració de fail2ban utilitzant "sudo nano /etc/fail2ban/jail.conf" i introduïm el següent en l'apartat sshd.

```
[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
enable = true
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
maxtretry = 3
bantime = 10000
```

Amb el que n'hem introduït nou, farà que es pugui intentar connectar com a molt tres vegades abans de bloquejar la IP.
Una vegada guardat, mirem si està actiu amb "systemctl status fail2ban" per protegir-nos d'atacs per ssh

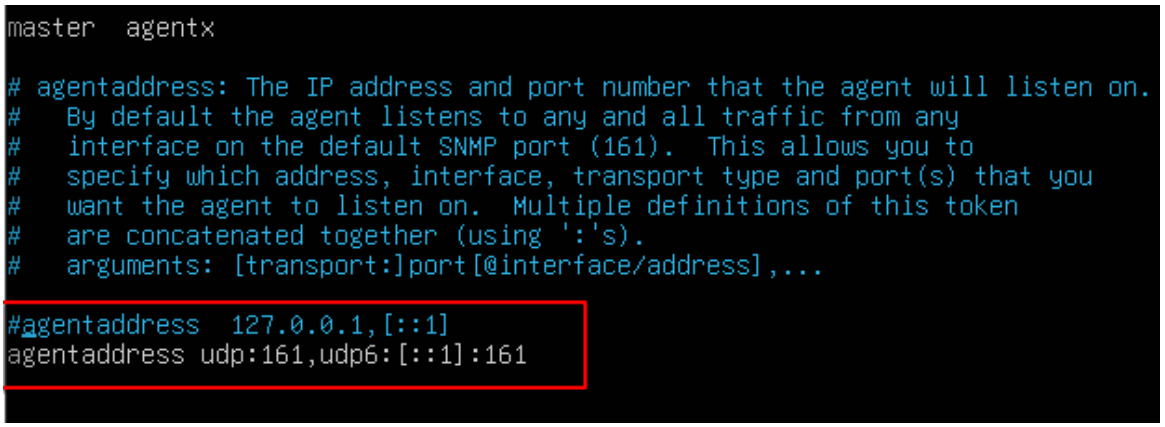
```
polmuel@pol:~$ systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-03-13 13:20:20 UTC; 5min ago
       Docs: man:fail2ban(1)
   Main PID: 2279 (fail2ban-server)
      Tasks: 5 (limit: 4642)
     Memory: 26.1M (peak: 26.6M)
        CPU: 586ms
     CGroup: /system.slice/fail2ban.service
             └─2279 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

mar 13 13:20:20 pol systemd[1]: Started fail2ban.service - Fail2Ban Service.
mar 13 13:20:21 pol fail2ban-server[2279]: 2025-03-13 13:20:21,028 fail2ban.configreader
mar 13 13:20:21 pol fail2ban-server[2279]: Server ready
lines 1-14/14 (END)
```

Com podem veure està activat i el dimoni actuant en el nostre sistema, i per això està fent correctament la seva feina. A part, introduint "sudo fail2ban-client status sshd", ens mostraria les IP's vetades i els intents fallits d'atacs.

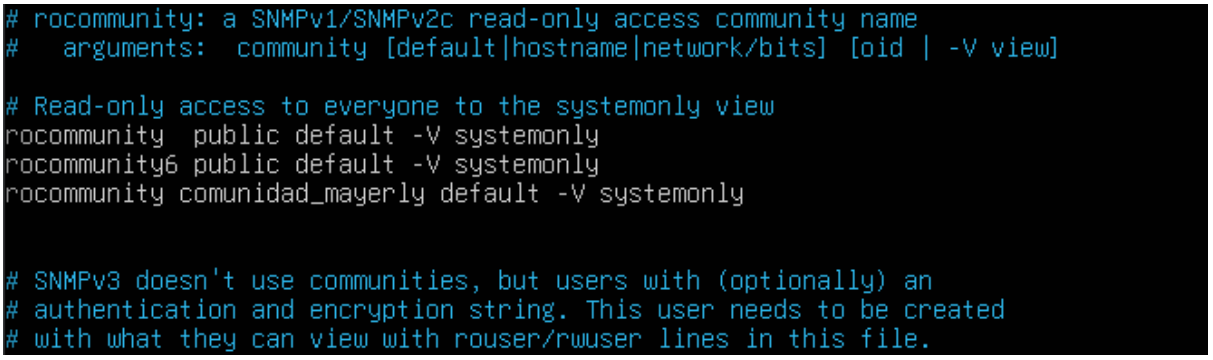
3. Monitoratge bàsic i consulta SNMP

Si es vol tenir un bon control de servidor, necessitem una eina que ens supervisi el rendiment del mateix i que ens digui diferents informacions en temps real del sistema, en el nostre cas, utilitzarem l'eina SNMP, per instal·lar-la farem servir la comanda "sudo apt install snmpd"

Una vegada instal·lat, configurarem el fitxer de configuració de SNMP, el qual es troba a "/etc/snmp/snmpd.conf".



Introduirem el següent perquè escolti a consultes externes en comptes de només locals, i a continuació més a baix...



Per aplicar els canvis, farem un "systemctl restart snmpd"

Una vegada aplicats els canvis mirarem si el servidor-backup pot monitoratge correctament al principal, per fer-ho utilitzarem el següent:

```
polmuel@pol:~$ snmpwalk -v 2c -c comunidad_mayerly 172.16.101.168
iso.3.6.1.2.1.1.1.0 = STRING: "Linux pol 6.8.0-55-generic #57-Ubuntu SMP PREEMPT_DYNAMIC Wed Feb 12 23:42:21 UTC 2025 x8
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (5127) 0:00:51.27
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "pol"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (135162) 0:22:31.62
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E9 03 0E 12 14 1B 00 2B 00 00
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/boot/vmlinuz-6.8.0-55-generic root=UUID=eb2e1e4c-0e5e-4aad-a0ca-db13ff7fda
"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 1
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 115
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
iso.3.6.1.2.1.25.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
polmuel@pol:~$
```

4. Conclusió

Després de completar exitosament la pràctica, hem pogut seguir tot el procés d'implantació d'un servidor d'alt rendiment, i poder observar el seu funcionament i funcionalitat real, per la qual cosa tot i ser un servidor bàsic, es pot representar i aprendre per arribar a implantar servidors més avançats.

A més s'ha après sobre com s'obren els ports i es permet l'accés a un terminal concret, assegurant-nos de poder protegir-nos de possibles atacs externs.