

IMPLEMENTACIÓ D'UN SERVIDOR D'ALT RENDIMENT

Fonaments de Maquinari

Pol Muel Garcia

1r Asix

| | |
|--|-----------|
| 1. Introducció..... | 3 |
| 2. Configuració del sistema..... | 4 |
| 2.1 Creació de les màquines virtuals..... | 4 |
| 2.2 Configuració RAID 1 al Servidor-Principal..... | 4 |
| 2.3 Sincronització automàtica amb rsync..... | 5 |
| 3. Seguretat i protecció de xarxa..... | 6 |
| 3.1 Firewall..... | 6 |
| 3.2 Protecció contra atacs..... | 7 |
| 3. Monitoratge bàsic i consulta SNMP..... | 8 |
| 3.3 Comprovació del monitoratge..... | 9 |
| 3.3.1 Espai lliure:..... | 9 |
| 3.3.2 RAM:..... | 10 |
| 3.3.3 CPU:..... | 10 |
| 4. Simulació de fallades i recuperació..... | 10 |
| 5. Conclusió..... | 11 |

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 oberts 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 40 GB i dos més de 20 GB cada un, de maquinari tindrà 2 CPU, 4 GB RAM, en canvi, la segona també tindrà el mateix , però només un dels dos discos de 20 GB, a part comptarà amb un maquinari d'1 CPU, 2 GB RAM.

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

2.2 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:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda          8:0    0   40G  0 disk
├─sda1       8:1    0    1M  0 part
└─sda2       8:2    0   40G  0 part /
sdb          8:16   0   20G  0 disk
sdc          8:32   0   20G  0 disk
sr0         11:0    1 1024M  0 rom
polmuel@pol:~$ sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdb /dev/sdc
[sudo] password for polmuel:
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? yes
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
polmuel@pol:~$
```

Amb la primera comanda mirarem els discos que tenim i quin nom tenen, per així saber quins utilitzarem per fer el Raid.

A més d'aquesta manera ens assegurem de tenir dos discos d'emmagatzematge encarregats de salvaguardar les dades del disc principal en cas d'algun error, corrupció o falles del mateix disc.

El següent que farem serà formatar /dev/md0 per convertir-ho en un format ext4, i muntar-la a /mnt/dades

```
polmuel@pol:~$ sudo mkdir -p /mnt/dades
polmuel@pol:~$ sudo mkfs.ext4 /dev/md0
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 5238528 4k blocks and 1310720 inodes
Filesystem UUID: a5a1e5c5-37ca-4e0a-8037-79d754e5c1f4
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

polmuel@pol:~$ sudo mount /dev/md0 /mnt/dades/
polmuel@pol:~$
```

I posar-hem que es munta automàticament en iniciar l'ordinador, així ens facilitarà el següent pas per la sincronització amb el servidor de backup.

2.3 Sincronització automàtica amb rsync

Farem que les dades es vagin copiant automàticament al servidor de backup cada 6 hores, per així assegurar una possible recuperació, ja sigui amb el raid o amb el propi servidor secundari, pel que estem oferint una seguretat molt alta en cas de possibles fallides de discs, dades, etc

```
polmuel@pol:~$ sudo rsync -avz -e ssh polmuel@172.16.101.168:/mnt/dades /mnt/backup/
polmuel@172.16.101.168's password:
receiving incremental file list
dades/
dades/backup/
dades/lost+found/

sent 36 bytes  received 150 bytes  74,40 bytes/sec
total size is 0  speedup is 0,00
polmuel@pol:~$ _
```

Amb aquesta comanda hem enviat les dades que hem guardat a la carpeta, i ara farem que aquest procés es faci cada 6 hores. Per fer-ho utilitzarem el crontab (per obrir

```
#
# m h dom mon dow   command
0 */6 * * * /usr/bin/rsync -avz -e ssh polmuel@172.16.101.168:/mnt/dades /mnt/backup
```

3. Seguretat i protecció de xarxa

3.1 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 còpies/backups de seguretat.

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

```
polmuel@pol:~$ ip a
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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2c:48:54 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.144/24 metric 100 brd 172.16.101.255 scope global dynamic enp0s3
        valid_lft 7170sec preferred_lft 7170sec
    inet6 fe80::a00:27ff:fe2c:4854/64 scope link
        valid_lft forever preferred_lft forever
```

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

```
polmuel@pol:~$ sudo ufw enable
Firewall is active and enabled on system startup
polmuel@pol:~$ sudo ufw allow from 172.16.101.144/24
WARN: Rule changed after normalization
Rule added
polmuel@pol:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
polmuel@pol:~$ _
```

3.2 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
maxretry = 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 mostraran 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”.

```
master agentx

# agentaddress: The IP address and port number that the agent will listen on.
# By default the agent listens to any and all traffic from any
# interface on the default SNMP port (161). This allows you to
# specify which address, interface, transport type and port(s) that you
# want the agent to listen on. Multiple definitions of this token
# are concatenated together (using ':'s).
# arguments: [transport:]port[@interface/address],...

#agentaddress 127.0.0.1,[:,1]
agentaddress udp:161,udp6:[::1]:161
```

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

```
# rocommunity: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity public default -V systemonly
rocommunity6 public default -V systemonly
rocommunity comunidad_mayerly default -V systemonly

# SNMPv3 doesn't use communities, but users with (optionally) an
# authentication and encryption string. This user needs to be created
# with what they can view with rouser/rwuser lines in this file.
```

Per aplicar els canvis, farem un “systemctl restart snmpd”

```
polmuel@pol:~$ sudo systemctl restart snmpd
polmuel@pol:~$ _
```


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-db13ff7fde
"
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:~$
```

3.3 Comprovació del monitoratge

Ara mirarem si ens donen les mateixes respostes, el sistema i el servidor de backup amb el snmpd, mirarem la ram, la cpu i l'espai lliure en el disc

3.3.1 Espai lliure:

Servidor :

```
polmuel@pol:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           395M  1,1M  393M   1% /run
/dev/sda2       40G   24G   14G  64% /
tmpfs           2,0G     0  2,0G   0% /dev/shm
tmpfs           5,0M     0  5,0M   0% /run/lock
tmpfs           395M  12K  394M   1% /run/user/1000
/dev/md127      20G   28K   19G   1% /mnt/dades
polmuel@pol:~$
```

Backup:

```
polmuel@pol:~$ snmpget -v 2c -c comunidad_mayerly 172.16.101.168 .1.3.6.1.4.1.2021.9.1.7.1
iso.3.6.1.4.1.2021.9.1.7.1 = INTEGER: 14092664
polmuel@pol:~$
```

3.3.2 RAM:

Servidor:

```
polmuel@pol:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:           3,8Gi        502Mi        1,5Gi         1,1Mi         2,1Gi         3,4Gi
Swap:          3,8Gi         268Ki         3,8Gi
polmuel@pol:~$ _
```

Backup:

```
polmuel@pol:~$ snmpget -v 2c -c comunidad_mayerly 172.16.101.168 .1.3.6.1.4.1.2021.4.5.0
iso.3.6.1.4.1.2021.4.5.0 = INTEGER: 4034648
```

3.3.3 CPU:

Servidor:

```
top - 18:12:28 up 1:54, 1 user, load average: 0,00, 0,00, 0,00
Tasks: 118 total, 1 running, 117 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,0 us, 0,3 sy, 0,0 ni, 99,5 id, 0,0 wa, 0,0 hi, 0,2 si, 0,0 st
MiB Mem : 3940,1 total, 1571,4 free, 505,9 used, 2145,3 buff/cache
MiB Swap: 3940,0 total, 3939,7 free, 0,3 used. 3434,2 avail Mem
```

Backup:

```
polmuel@pol:~$ snmpget -v 2c -c comunidad_mayerly 172.16.101.168 .1.3.6.1.4.1.2021.11.9.0
iso.3.6.1.4.1.2021.11.9.0 = INTEGER: 0
```

4. Simulació de fallades i recuperació

Per acabar, simularem una fallada en un dels discos del servidor per veure si està la RAID montada correctament i funcionant, pel que la primera comanda sera per fer-li entendre que un dels discos esta fallant

```
polmuel@pol:~$ sudo mdadm /dev/md127 --fail /dev/sdb
[ 2219.102883] md/raid1:md127: Disk failure on sdb, disabling device.
[ 2219.102883] md/raid1:md127: Operation continuing on 1 devices.
mdadm: set /dev/sdb faulty in /dev/md127
polmuel@pol:~$
```

I a continuació mirarem si efectivament està fent la raid només un dels dos discos que teniem

```
polmuel@pol:~$ cat /proc/mdstat
Personalities : [raid1] [raid0] [raid6] [raid5] [raid4] [raid10]
md127 : active raid1 sdc[1] sdb[0](F)
      20954112 blocks super 1.2 [2/1] [_U]

unused devices: <none>
polmuel@pol:~$
```

Una vegada que hem concluit que no esta funcionant el disco que hem fet fallar, el treurem de la RAID per evitar possibles errors a l'hora d'extreure'n físicament el disc.

```
polmuel@pol:~$ sudo mdadm /dev/md127 --remove /dev/sdb
mdadm: hot removed /dev/sdb from /dev/md127
polmuel@pol:~$
```

Per verificar que les dades continuen intactes ja que teniem un altre disc de repost, tornarem a fer la comanda per copiar les dades al servidor de backup, i mirarem si realment hi han dades

```
polmuel@pol:~$ sudo rsync -avz -e ssh polmuel@172.16.101.168:/mnt/dades /mnt/backup/
[sudo] password for polmuel:
polmuel@172.16.101.168's password:
receiving incremental file list

sent 27 bytes  received 141 bytes  48,00 bytes/sec
total size is 0  speedup is 0,00
polmuel@pol:~$ ll /mnt/backup/
total 12
drwxrwxrwx 3 polmuel polmuel 4096 mar 21 16:41 ./
drwxr-xr-x 3 root     root    4096 mar 19 19:35 ../
drwxrwxrwx 4 polmuel polmuel 4096 mar 19 19:51 dades/
polmuel@pol:~$ _
```

5. 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.