

DOCUMENTACIÓN – srv-router

Información general

El servidor **srv-router** actúa como gateway principal de la infraestructura interna de MillorNet.

Su función es:

- Proporcionar salida a Internet mediante NAT
- Segmentar la red en diferentes zonas
- Ofrecer servicios de red centrales (DNS y DHCP)
- Aplicar políticas de seguridad perimetral
- Preparar la infraestructura para futuras ampliaciones (DMZ, MGMT, VPN)

Este servidor constituye el punto de interconexión entre la red interna (ZONA 3) y la red externa.

La arquitectura ha sido diseñada siguiendo principios de:

- Segmentación de red
- Seguridad por defecto (deny by default)
- Escalabilidad
- Centralización de servicios

Configuración de red

El router dispone de cuatro interfaces de red configuradas en VirtualBox:

Interfaz	Tipo	Función
----------	------	---------

enp0s3	Adaptador puente	Conexión a Internet
enp0s8	Red interna	LAN (ZONA 3)
enp0s9	Red interna	DMZ (preparada)
enp0s1 0	Red interna	MGMT (preparada)

Direccionamiento IP

Se definió un rango profesional independiente de la red física:

Red interna LAN: 10.0.0.0/24

Configuración:

Router LAN: 10.0.0.1

DMZ: 10.0.1.1/24

MGMT: 10.0.2.1/24

El uso de una red distinta a la red física evita conflictos de enrutamiento y permite una correcta implementación de NAT.

Hostname

Se configuró el hostname:

srv-router

Esto permite:

- Identificación clara del rol del servidor
- Mejora en la trazabilidad de logs
- Integración futura con DNS interno

Enrutamiento y NAT

Se habilitó el reenvío de paquetes (IP forwarding), permitiendo al sistema actuar como router entre interfaces.

Se implementó NAT mediante iptables para permitir que los equipos de la red interna accedan a Internet utilizando la IP del adaptador puente.

La regla aplicada realiza enmascaramiento (MASQUERADE) sobre el tráfico saliente de la red 10.0.0.0/24.

Este mecanismo permite:

- Aislar la red interna
- Ocultar direcciones privadas
- Permitir acceso controlado al exterior

```
GNU nano 7.2 /etc/netplan/00-installer-config.yaml
network:
  version: 2
  renderer: networkd
  ethernets:

    enp0s3:
      dhcp4: true

    enp0s8:
      dhcp4: no
      addresses:
        - 10.0.0.1/24

    enp0s9:
      dhcp4: no
      addresses:
        - 10.0.1.1/24

    enp0s10:
      dhcp4: no
      addresses:
        - 10.0.2.1/24_

[ Wrote 22 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-G Copy

ikervp@millornet:~$ sudo netplan apply
ikervp@millornet:~$ 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 pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c0:60:32 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.39/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 43187sec preferred_lft 43187sec
    inet6 fe80::a00:27ff:fec0:6032/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:50:2c:e8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe50:2ce8/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6d:9f:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.1/24 brd 10.0.1.255 scope global enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe6d:9ff7/64 scope link
        valid_lft forever preferred_lft forever
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c4:9e:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.1/24 brd 10.0.2.255 scope global enp0s10
        valid_lft forever preferred_lft forever
```

```
GNU nano 7.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
net.ipv4.ip_forward=1
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set Mark
^X Exit      ^R Read File ^N Replace   ^U Paste     ^D Justify   ^_/ Go To Line M-E Redo     M-G Copy
```

```
ikervp@millornet: ~
ikervp@millornet:~$ sudo nano /etc/sysctl.conf
ikervp@millornet:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
ikervp@millornet:~$ cat /proc/sys/net/ipv4/ip_forward
1
ikervp@millornet:~$
```

Firewall

Se implementó una política de firewall restrictiva utilizando iptables.

Política por defecto

- INPUT → DROP
- FORWARD → DROP
- OUTPUT → ACCEPT

Reglas permitidas

- Tráfico loopback
- Conexiones establecidas y relacionadas
- SSH desde la red interna

- DNS desde la red interna
- DHCP desde la red interna
- Forwarding LAN → Internet

Este enfoque sigue el principio de mínimo privilegio y reduce la superficie de ataque del gateway.

```
1
ikervp@millornet:~$ sudo apt install iptables-persistent -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  netfilter-persistent
The following packages will be REMOVED:
```

```
ikervp@millornet:~$ sudo iptables -F
sudo iptables -t nat -F
ikervp@millornet:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o enp0s3 -j MASQUERADE
sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state ESTABLISHED,RELATED -j ACCEPT
ikervp@millornet:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
ikervp@millornet:~$
```

```
ikervp@millornet:~$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
0 upgraded, 0 newly installed, 0 to remove and 141 not upgraded.
ikervp@millornet:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
ikervp@millornet:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
ikervp@millornet:~$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
ikervp@millornet:~$ sudo ufw allow in on enp0s8
Rules updated
Rules updated (v6)
ikervp@millornet:~$
```

```
GNU nano 7.2 /etc/default/ufw
# /etc/default/ufw
#
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPv6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="ACCEPT"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"

# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
Wrote 47 lines
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set Mark
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo     M-G Copy

ikervp@millornet:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
ikervp@millornet:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
Anywhere on enp0s8 ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
Anywhere (v6) on enp0s8 ALLOW Anywhere (v6)

ikervp@millornet:~$
```

Servicio DNS interno

Se instaló y configuró **BIND** como servidor DNS autoritativo interno.

Dominio interno

millornet.local

El router actúa como:

- Servidor DNS autoritativo para la zona interna
- Servidor DNS recursivo con forwarders externos

Registros configurados

Nombre	IP
srv-router	10.0.0.1

srv-core	10.0.0.1
	0
srv-db	10.0.0.2
	0
srv-backup	10.0.0.3
	0
srv-logs	10.0.0.4
	0

También se configuró zona inversa para resolución IP → nombre.

```
ikervp@millornet:~$ sudo apt update
sudo apt install bind9 bind9-utils bind9-dnsutils -y
```

```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    recursion yes;
    allow-recursion { 10.0.0.0/24; };
    allow-query { 10.0.0.0/24; };

    forwarders {
        8.8.8.8;
        1.1.1.1;
    };

    dnssec-validation auto;
    listen-on { 10.0.0.1; };
};

[ Wrote 15 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line M-E Redo      M-C Copy
```

```
ikervp@millornet:~$ sudo apt install isc-dhcp-server -y
Reading package lists... Done
```

```
GNU nano 7.2 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s8"
INTERFACESv6=""

Read 18 lines
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-G Copy
```

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
# BOOTP or DHCP.  Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
# hardware ethernet 08:00:07:26:c0:a5;
# fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.  The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
# match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.100 10.0.0.200;
    option routers 10.0.0.1;
    option domain-name-servers 10.0.0.1;
    option domain-name "millornet.local";
}
}
```

```
ikervp@millornet: ~
ikervp@millornet:~$ sudo iptables -F
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
[sudo] password for ikervp:
ikervp@millornet:~$ sudo iptables -A INPUT -i lo -j ACCEPT
ikervp@millornet:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
ikervp@millornet:~$ sudo iptables -A INPUT -i enp0s8 -p tcp --dport 22 -j ACCEPT
ikervp@millornet:~$ sudo iptables -P INPUT DROP
ikervp@millornet:~$ sudo iptables -A INPUT -i enp0s8 -p tcp --dport 22 -j ACCEPT
ikervp@millornet:~$ sudo iptables -A INPUT -i enp0s8 -p udp --dport 53 -j ACCEPT
ikervp@millornet:~$ sudo iptables -A INPUT -i enp0s8 -p tcp --dport 53 -j ACCEPT
ikervp@millornet:~$ sudo iptables -A INPUT -i enp0s8 -p udp --dport 67:68 --sport 67:68 -j ACCEPT
ikervp@millornet:~$ sudo iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o enp0s3 -j MASQUERADE
ikervp@millornet:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
ikervp@millornet:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state ESTABLISHED,RELATED -j ACCEPT
ikervp@millornet:~$ sudo netfilter-persistent save
sudo: netfilter-persistent: command not found
ikervp@millornet:~$
```

```

iker@millornet:~$ sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify whois
0 upgraded, 4 newly installed, 0 to remove and 147 not upgraded.
Need to get 496 kB of archives.
After this operation, 2,572 kB of additional disk space will be used.
Get:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 496 kB in 0s (1,080 kB/s)
Selecting previously unselected package python3-pyasyncore.
(Reading database ... 90%

```

```

GNU nano 7.2 /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 22
maxretry = 5

```

```

GNU nano 7.2 /etc/rsyslog.conf
#####
# Filter duplicated messages
$RepeatedMsgReduction on
#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*. * @10.0.0.40:514
[ Wrote 54 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-6 Copy

```

```

GNU nano 7.2 /etc/bind/named.conf.local
zone "millornet.local" {
    type master;
    file "/etc/bind/db.millornet.local";
};
[ Wrote 4 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-6 Copy

```

```

GNU nano 7.2 /etc/bind/db.millornet.local *
$TTL      604800
@          IN      SOA      ns1.millornet.local. admin.millornet.local. (
                        2026021701 ; Serial
                        604800      ; Refresh
                        86400        ; Retry
                        2419200      ; Expire
                        604800 )     ; Negative Cache TTL

; Servidor DNS
@          IN      NS       ns1.millornet.local.

; Registro A del DNS
ns1        IN      A        10.0.0.1

; Servidores internos
srv-core   IN      A        10.0.0.10
srv-db     IN      A        10.0.0.20
srv-backup IN      A        10.0.0.30
srv-logs   IN      A        10.0.0.40
srv-router IN      A        10.0.0.1

^G Help      ^O Write Out ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-G Copy

```

```

GNU nano 7.2 /etc/bind/named.conf.local *
zone "millornet.local" {
    type master;
    file "/etc/bind/db.millornet.local";
};
zone "0.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.0.0";
};

```

```

GNU nano 7.2 /etc/bind/db.10.0.0
$TTL      604800
@          IN      SOA      ns1.millornet.local. admin.millornet.local. (
                        2026021701
                        604800
                        86400
                        2419200
                        604800 )

@          IN      NS       ns1.millornet.local.

1          IN      PTR      srv-router.millornet.local.
10         IN      PTR      srv-core.millornet.local.
20         IN      PTR      srv-db.millornet.local.
30         IN      PTR      srv-backup.millornet.local.
40         IN      PTR      srv-logs.millornet.local.

[ Wrote 15 lines ]
^G Help      ^O Write Out ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-G Copy

```

```

ikervp@millornet:~$ ikervp@millornet:~$ sudo named-checkconf
ikervp@millornet:~$ sudo named-checkzone millornet.local /etc/bind/db.millornet.local
sudo named-checkzone 0.0.10.in-addr.arpa /etc/bind/db.10.0.0
zone millornet.local/IN: loaded serial 2026021701
OK
zone 0.0.10.in-addr.arpa/IN: loaded serial 2026021701
OK
ikervp@millornet:~$

sudo named-checkzone 0.0.10.in-addr.arpa /etc/bind/db.10.0.0
zone millornet.local/IN: loaded serial 2026021701
OK
zone 0.0.10.in-addr.arpa/IN: loaded serial 2026021701
OK
ikervp@millornet:~$ sudo systemctl restart bind9
sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Tue 2026-02-17 15:32:46 UTC; 27ms ago
     Docs: man:named(8)
  Main PID: 1494 (named)
    Status: "running"
   Tasks: 6 (limit: 2267)
  Memory: 22.9M (peak: 23.3M)
     CPU: 53ms
  CGroup: /system.slice/named.service
          └─1494 /usr/sbin/named -f -u bind

Feb 17 15:32:46 millornet named[1494]: zone 0.0.10.in-addr.arpa/IN: loaded serial 2026021701
Feb 17 15:32:46 millornet named[1494]: zone 127.in-addr.arpa/IN: loaded serial 1
Feb 17 15:32:46 millornet named[1494]: zone localhost/IN: loaded serial 2
Feb 17 15:32:46 millornet named[1494]: zone 255.in-addr.arpa/IN: loaded serial 1
Feb 17 15:32:46 millornet named[1494]: zone millornet.local/IN: loaded serial 2026021701
Feb 17 15:32:46 millornet systemd[1]: Started named.service - BIND Domain Name Server.
Feb 17 15:32:46 millornet named[1494]: all zones loaded
Feb 17 15:32:46 millornet named[1494]: running
Feb 17 15:32:46 millornet named[1494]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complet
Feb 17 15:32:46 millornet named[1494]: managed-keys-zone: Key 38696 for zone . is now trusted (acceptance timer complet
lines 1-22/22 (END)

Feb 17 15:32:46 millornet named[1494]: running
Feb 17 15:32:46 millornet named[1494]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complet
Feb 17 15:32:46 millornet named[1494]: managed-keys-zone: Key 38696 for zone . is now trusted (acceptance timer complet

ikervp@millornet:~$ dig @10.0.0.1 srv-core.millornet.local

; <<>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <<>> @10.0.0.1 srv-core.millornet.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50464
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: bd362973befab0a70100000069948a32dca1f09b681bf3d3 (good)
;; QUESTION SECTION:
;srv-core.millornet.local.      IN      A

;; ANSWER SECTION:
srv-core.millornet.local. 604800 IN      A      10.0.0.10

;; Query time: 0 msec
;; SERVER: 10.0.0.1#53(10.0.0.1) (UDP)
;; WHEN: Tue Feb 17 15:33:06 UTC 2026
;; MSG SIZE rcvd: 97

ikervp@millornet:~$

```

Beneficios

- Resolución por nombre en vez de IP
- Preparación para LDAP
- Escalabilidad

- Mejora en auditoría y logs
-

Servicio DHCP interno

Se implementó servidor DHCP para la red 10.0.0.0/24.

Rango dinámico asignado:

10.0.0.100 – 10.0.0.200

Parámetros entregados a los clientes:

- Gateway: 10.0.0.1
- DNS: 10.0.0.1
- Dominio: millornet.local

Esto permite:

- Gestión centralizada de direcciones IP
 - Simplificación del despliegue de nuevos equipos
 - Reducción de errores manuales
-

Seguridad adicional

Se reforzó la seguridad del router mediante:

- Fail2Ban para protección frente a intentos de acceso SSH
 - Envío de logs al servidor central srv-logs
 - Segmentación preparada para futuras DMZ
-

Segmentación preparada

El router dispone de redes adicionales preparadas:

10.0.1.0/24 → DMZ

10.0.2.0/24 → Gestión

Aunque actualmente no están en uso, esta estructura permite:

- Publicación futura de servicios externos
 - Separación de tráfico administrativo
 - Arquitectura escalable y profesional
-

Resultado final

La infraestructura cuenta ahora con:

- Gateway con NAT funcional
- Firewall restrictivo
- DNS interno autoritativo
- DHCP centralizado
- Arquitectura segmentada
- Preparación para ampliación

El servidor srv-router constituye el núcleo de la infraestructura de red de MillorNet, proporcionando conectividad segura, controlada y escalable.

DOCUMENTACIÓN – srv-proxy

DOCUMENTACIÓN – srv-core

Información general

El servidor srv-core actúa como servidor central de la red interna (ZONA 3) de MillorNet. Su función principal es proporcionar servicios críticos compartidos al resto de servidores internos, sirviendo como punto de referencia para autenticación, sincronización horaria y servicios base.

Se ha configurado el servidor con una dirección IP fija dentro de la red interna
LAN: Red: 192.168.1.0/24 IP del servidor: 192.168.1.10

El uso de IP fija garantiza:

- Estabilidad en la comunicación entre servidores
- Posibilidad de aplicar reglas de seguridad basadas en origen
- Facilidad para integrar posteriormente DNS interno

Esta red está aislada del exterior, lo que incrementa la seguridad al tratarse de una zona interna de servidores.

Configuración de red

```
GNU nano 7.2 /etc/netplan/01-int-lan.yaml *
network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.10/24

ikervp@millornet:~$ sudo netplan apply
ikervp@millornet:~$
```

Hostname

```
ikervp@millornet:~$ sudo hostnamectl set-hostname srv-core
ikervp@millornet:~$
```

Asignar un hostname coherente:

- Facilita la administración

- Mejora la legibilidad de logs
 - Permite una futura integración limpia con DNS y LDAP
-

Firewall

```
ikervp@millornet:~$ sudo apt update
sudo apt install -y ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing

# SSH interno
sudo ufw allow from 192.168.1.0/24 to any port 22

# LDAP
sudo ufw allow 389
sudo ufw allow 636

# NTP
sudo ufw allow 123/udp

sudo ufw enable
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Se ha configurado un **firewall local** utilizando **ufw** con una política restrictiva por defecto:

- **Denegar todo el tráfico entrante**
- **Permitir todo el tráfico saliente**

Posteriormente, se han habilitado **únicamente los servicios necesarios**, como:

- Acceso SSH desde la red interna
- Servicios LDAP
- Sincronización horaria (NTP)
- Servicios internos futuros

Este enfoque reduce la superficie de ataque y cumple el principio de **mínimo privilegio**

Servicio de sincronización horaria

Para la sincronización de la hora se ha utilizado **systemd-timesyncd**, el servicio NTP nativo de Ubuntu Server.

Este servicio:

- Garantiza que el servidor mantenga la hora sincronizada
- Evita conflictos con otros demonios NTP
- Reduce la complejidad del sistema

La sincronización horaria es crítica para:

- Logs
- Autenticación (LDAP)
- Auditorías y correlación de eventos

```
ikervp@millornet:~$ sudo apt install -y slapd ldap-utils samba bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr bind9-utils dns-root-data ibverbs-providers libattr1 libavahi-client3 libavahi-common-data libavahi-common3
  libboost-iostreams1.83.0 libboost-locale1.83.0 libboost-thread1.83.0 libcephfs2 libcups2t64 libibverbs1
  libldap-common libldap2 libldb2 libltdl7 libodbc2 librados2 librdmacm1t64 libtalloc2 libtdb1 libtevent0t64 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb
  samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
```

Servicio de directorio (LDAP)

Se ha instalado **OpenLDAP** para proporcionar un **servicio centralizado de autenticación y gestión de usuarios**.

LDAP permitirá:

- Centralizar usuarios y grupos
- Facilitar el control de accesos
- Preparar la infraestructura para una gestión unificada de identidades

Este servicio será consumido por otros servidores internos y, potencialmente, por estaciones de trabajo.

```
ikervp@millornet:~$ sudo apt install -y slapd ldap-utils samba bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr bind9-utils dns-root-data ibverbs-providers libattr1 libavahi-client3 libavahi-common-data libavahi-common3
  libboost-iostreams1.83.0 libboost-locale1.83.0 libboost-thread1.83.0 libcephfs2 libcups2t64 libibverbs1
  libldap-common libldap2 libldb2 libltdl7 libodbc2 librados2 librdmacm1t64 libtalloc2 libtdb1 libtevent0t64 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb
  samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
```

Servidor de archivos interno

Se ha instalado **Samba** para ofrecer un **servicio de archivos compartidos** dentro de la red interna.

El servidor de archivos permitirá:

- Centralizar documentación y recursos internos
- Facilitar el intercambio seguro de archivos
- Integrarse posteriormente con autenticación LDAP

```
ikervp@millornet:~$ sudo apt install -y slapd ldap-utils samba bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr bind9-utils dns-root-data ibverbs-providers libattr1 libavahi-client3 libavahi-common-data libavahi-common3
  libboost-iostreams1.83.0 libboost-locale1.83.0 libboost-thread1.83.0 libcephfs2 libcups2t64 libibverbs1
  libldap-common libldap2 libldb2 libltdl7 libodbc2 librados2 librdmacm1t64 libtalloc2 libtdb1 libtevent0t64 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb
  samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
```

Servicio DNS interno (preparado)

Se ha instalado **Bind9** como base para un **DNS interno**, aunque su configuración definitiva se realizará en una fase posterior.

Disponer de un DNS interno permitirá:

- Resolver nombres de servidores internos
- Eliminar la dependencia de direcciones IP
- Mejorar la escalabilidad de la infraestructura

```
ikervp@millornet:~$ sudo apt install -y slapd ldap-utils samba bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr bind9-utils dns-root-data ibverbs-providers libattr1 libavahi-client3 libavahi-common-data libavahi-common3
  libboost-iostreams1.83.0 libboost-locale1.83.0 libboost-thread1.83.0 libcephfs2 libcups2t64 libibverbs1
  libldap-common libldap2 libldb2 libltdl7 libodbc2 librados2 librdmacm1t64 libtalloc2 libtdb1 libtevent0t64 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb
  samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
```

Servicio NTP interno

El servidor **srv-core** actúa como servidor de sincronización horaria para la red interna (ZONA 3).

Centralizar la hora permite coherencia en logs, autenticación LDAP y auditorías.

El servicio utiliza **systemd-timesyncd** y expone NTP únicamente en la red interna.

```
GNU nano 7.2 /etc/systemd/timesyncd.conf *
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it under the
# terms of the GNU Lesser General Public License as published by the Free
# Software Foundation; either version 2.1 of the License, or (at your option)
# any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file (or a copy of it placed in
# /etc/ if the original file is shipped in /usr/), or by creating "drop-ins" in
# the /etc/systemd/timesyncd.conf.d/ directory. The latter is generally
# recommended. Defaults can be restored by simply deleting the main
# configuration file and all drop-ins located in /etc/.
#
# Use 'systemd-analyze cat-config systemd/timesyncd.conf' to display the full config.
# See timesyncd.conf(5) for d

[Time]
NTP=0.pool.ntp.org 1.pool.ntp.org
FallbackNTP=
#NTP=
#FallbackNTP=ntp.ubuntu.com
#RootDistanceMaxSec=5
#PollIntervalMinSec=32

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo     M-G Copy
```

```
GNU nano 7.2 /etc/systemd/timesyncd.conf.d/server.conf *
[Time]
PollIntervalMinSec=16
PollIntervalMaxSec=1024

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo     M-G Copy
```

```
ikervp@srv-core:~$ sudo ufw allow 123/udp
sudo ufw reload
Skipping adding existing rule
Skipping adding existing rule (v6)
Firewall reloaded
ikervp@srv-core:~$
```

```
ikervp@srv-core:~$ timedatectl status
          Local time: Mon 2026-02-09 14:48:33 UTC
          Universal time: Mon 2026-02-09 14:48:33 UTC
              RTC time: Mon 2026-02-09 14:43:00
              Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
ikervp@srv-core:~$
```

DOCUMENTACIÓN – srv-db

El servidor **srv-db** actúa como **servidor de bases de datos** de la infraestructura interna de MillorNet.

Su función principal es alojar y gestionar las bases de datos utilizadas por los servicios corporativos, manteniendo estos datos **aislados y protegidos** del resto de la red.

Este servidor **no expone servicios directamente a usuarios finales**, sino que únicamente acepta conexiones desde el servidor central **srv-core**.

Información general

El servidor se ha configurado con una **dirección IP fija** dentro de la red interna LAN

- **Red:** 192.168.1.0/24
- **IP del servidor:** 192.168.1.20

El uso de IP fija permite:

- Controlar el acceso mediante reglas de firewall
- Garantizar conectividad estable con **srv-core**
- Facilitar la administración y futura integración con DNS interno

La máquina se encuentra conectada exclusivamente a la red interna, sin acceso directo desde el exterior.

Configuración de red

```
GNU nano 7.2 /etc/netplan/01-int-lan.yaml *
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.20/24_
```

```
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set Mark
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/_ Go To Line M-E Redo     M-6 Copy
```

Hostname

El nombre de host configurado para esta máquina es:

srv-db

Este identificador:

- Permite diferenciar claramente el rol del servidor
- Mejora la trazabilidad en logs y auditorías

```
ikervp@millornet: ~$ sudo hostnamectl set-hostname srv-db
ikervp@millornet: ~$
```

Firewall

Se ha implementado un firewall local mediante **ufw** siguiendo un enfoque **altamente restrictivo**:

- Todo el tráfico entrante está **denegado por defecto**
- Solo se permiten conexiones explícitas desde **srv-core**

Reglas principales:

- Acceso SSH únicamente desde la IP del servidor central
- Acceso al servicio de base de datos solo desde **srv-core**

Este diseño garantiza que:

- Ningún otro servidor o equipo pueda acceder a la base de datos
- Se reduzca drásticamente la superficie de ataque
- Se cumpla el principio de **segmentación y mínimo privilegio**

```
ikervp@millornet:~$ sudo apt install -y ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing

# SSH solo desde srv-core
sudo ufw allow from 192.168.1.10 to any port 22

# PostgreSQL
sudo ufw allow from 192.168.1.10 to any port 5432

sudo ufw enable
```

Base de datos

En el servidor se ha instalado un sistema de gestión de bases de datos relacional (PostgreSQL).

Este servicio se utiliza para:

- Almacenar datos críticos de aplicaciones internas
- Separar la capa de datos de la lógica de negocio

- Facilitar copias de seguridad y tareas de mantenimiento

El servicio se ha configurado para:

- Escuchar únicamente en la interfaz interna
- Aceptar conexiones exclusivamente desde **srv-core**

```
ikervp@millornet:~$ sudo apt install -y postgresql postgresql-contrib
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcommon-sense-perl libjson-perl libjson-xs-perl libllvm17t64 libpq5 libtypes-serialiser-perl postgresql-16
  postgresql-client-16 postgresql-client-common postgresql-common ssl-cert
Suggested packages:
  postgresql-doc postgresql-doc-16
```

Gestión de copias de seguridad locales

El servidor mantiene copias de seguridad **temporales y locales** de las bases de datos.

Estas copias:

- Permiten una recuperación rápida ante errores lógicos
- Sirven como paso previo a los backups centralizados
- Se transfieren posteriormente al servidor **srv-backup**

DOCUMENTACIÓN – srv-backup

Información general

El servidor **srv-backup** actúa como **servidor central de copias de seguridad** de la infraestructura interna de MillorNet.

Su función principal es:

- Recibir backups de los servidores críticos (**srv-core** y **srv-db**)
- Almacenar versiones históricas de los datos
- Facilitar la recuperación ante fallos, errores humanos o incidentes de seguridad

Este servidor no presta servicios directos a usuarios finales

El servidor se encuentra conectado exclusivamente a la **red interna LAN (ZONA 3)** y dispone de una dirección IP fija:

- **Red:** 192.168.1.0/24
- **IP del servidor:** 192.168.1.30

El uso de IP fija permite:

- Controlar el acceso desde servidores autorizados
 - Garantizar estabilidad en los procesos de backup
 - Facilitar la integración con servicios internos como DNS
-

Configuración de red

```
GNU nano 7.2 /etc/netplan/01-int-lan.yaml *
network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.30/24
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy

Firewall

Se ha configurado un firewall local con una política restrictiva:

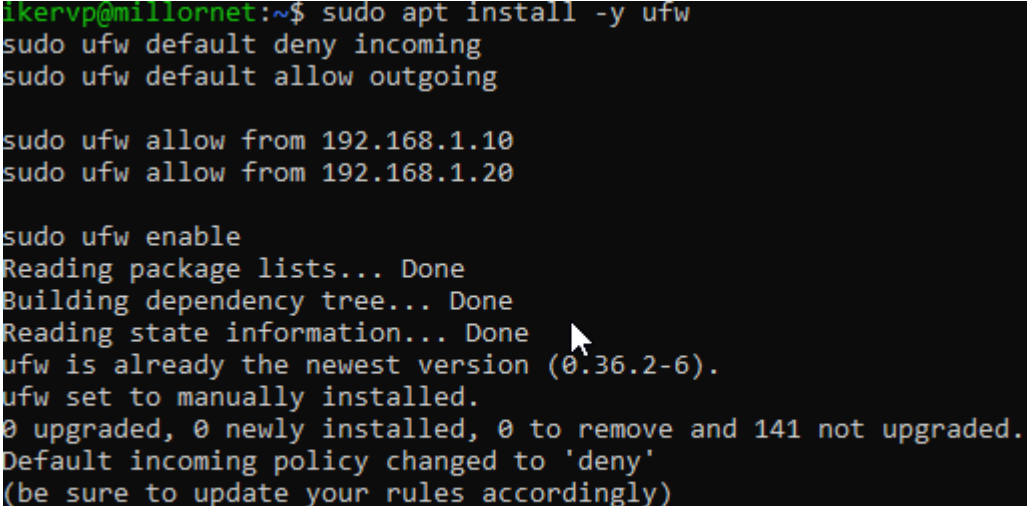
- Todo el tráfico entrante está **denegado por defecto**
- Solo se permiten conexiones desde los servidores autorizados

Concretamente:

- `srv-core`
- `srv-db`

Este enfoque garantiza que:

- Ningún otro equipo de la red pueda acceder a los datos de backup
- Se minimice el riesgo de accesos no autorizados
- El servidor quede protegido frente a movimientos laterales



```
ikervp@millornet:~$ sudo apt install -y ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing

sudo ufw allow from 192.168.1.10
sudo ufw allow from 192.168.1.20

sudo ufw enable
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 141 not upgraded.
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Servicios

El servidor utiliza herramientas de backup basadas en sincronización y versionado, como **rsync** y **borgbackup**.

Estos servicios permiten:

- Realizar copias incrementales eficientes
- Mantener múltiples versiones de los datos
- Optimizar el uso de espacio en disco

El diseño está orientado a la **fiabilidad y recuperación**, no al rendimiento inmediato.

```
ikervp@millornet:~$ sudo apt install -y rsync borgbackup
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsync is already the newest version (3.2.7-1ubuntu1.2).
rsync set to manually installed.
The following additional packages will be installed:
  python3-msgpack python3-packaging
Suggested packages:
  python3-pyfuse3 borgbackup-doc
The following NEW packages will be installed:
  borgbackup python3-msgpack python3-packaging
0 upgraded, 3 newly installed, 0 to remove and 141 not upgraded.
Need to get 955 kB of archives.
After this operation, 3,834 kB of additional disk space will be used.
Get:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-msgpack amd64 1.0.3-3build2 [80.1 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-packaging all 24.0-1 [41.1 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu noble/universe amd64 borgbackup amd64 1.2.8-1 [833 kB]
24% [3 borgbackup 1,524 B/833 kB 0%]
```

DOCUMENTACIÓN – srv-logs

Información general

El servidor **srv-logs** actúa como **servidor centralizado de registros y monitorización** de la infraestructura interna de MillorNet.

Su función principal es:

- Centralizar los logs generados por los servidores internos
- Detectar eventos anómalos o incidentes de seguridad

- Servir como base para auditorías y análisis forense

El servidor se encuentra conectado a la red interna LAN (ZONA 3) con una IP fija:

- Red: 192.168.1.0/24
- IP del servidor: 192.168.1.40

Esta configuración:

- Garantiza conectividad estable con el resto de servidores
 - Permite aplicar reglas de seguridad basadas en origen
 - Facilita una futura integración con DNS interno
-

Configuración de red

```
GNU nano 7.2 /etc/netplan/01-int-lan.yaml *
network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.40/24_
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-G Copy

Firewal

El firewall del servidor se ha configurado siguiendo una política restrictiva:

- Todo el tráfico entrante denegado por defecto
- Se permite únicamente el tráfico necesario para la recepción de logs

Concretamente:

- Recepción de logs remotos mediante syslog
- Comunicación interna con servidores autorizados

Este enfoque protege el servidor frente a accesos no deseados y limita su exposición.

```
ikervp@millornet:~$ sudo apt install -y ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing

# Syslog
sudo ufw allow 514/udp

sudo ufw enable
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 141 not upgraded.
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
Rules updated
Rules updated (v6)
Command may disrupt existing ssh connections. Proceed with operation (y|n)? _
```

Servicios

El servidor utiliza **rsyslog** como sistema de centralización de logs.

Esto permite:

- Recibir logs desde **srv-core**, **srv-db** y **srv-backup**
- Unificar registros en un único punto
- Facilitar la detección de incidencias

La centralización mejora la capacidad de respuesta ante problemas y ataques.

Se ha instalado **Fail2Ban** como sistema básico de protección frente a accesos no autorizados.

Fail2Ban:

- Analiza logs en tiempo real
- Bloquea automáticamente direcciones sospechosas
- Refuerza la seguridad del entorno interno

```
ikervp@millornet:~$ sudo apt install -y rsyslog fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyasyncore python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl
  | rsyslog-gnutls rsyslog-gssapi rsyslog-relp
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify whois
The following packages will be upgraded:
  rsyslog
1 upgraded, 4 newly installed, 0 to remove and 140 not upgraded.
Need to get 1,007 kB of archives.
After this operation, 2,572 kB of additional disk space will be used.
Get:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 rsyslog amd64 8.2312.0-3ubuntu9.1 [511 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0.2-2 [10.1 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1.0.2-3ubuntu0.1 [409 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.6-2ubuntu1 [25.0 kB]
Get:5 http://es.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 1,007 kB in 1s (978 kB/s)
(Reading database ... 80%
```
