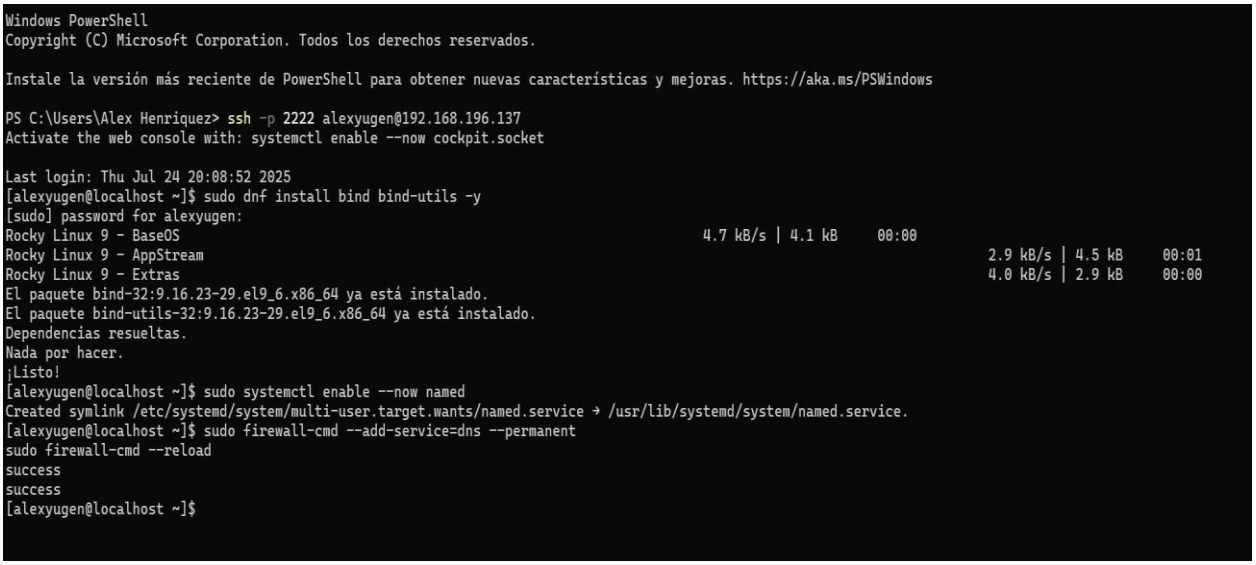
Desarrollo del Desafío: Seguridad y Configuración de BIND

1. Instalación y Configuración Básica de BIND

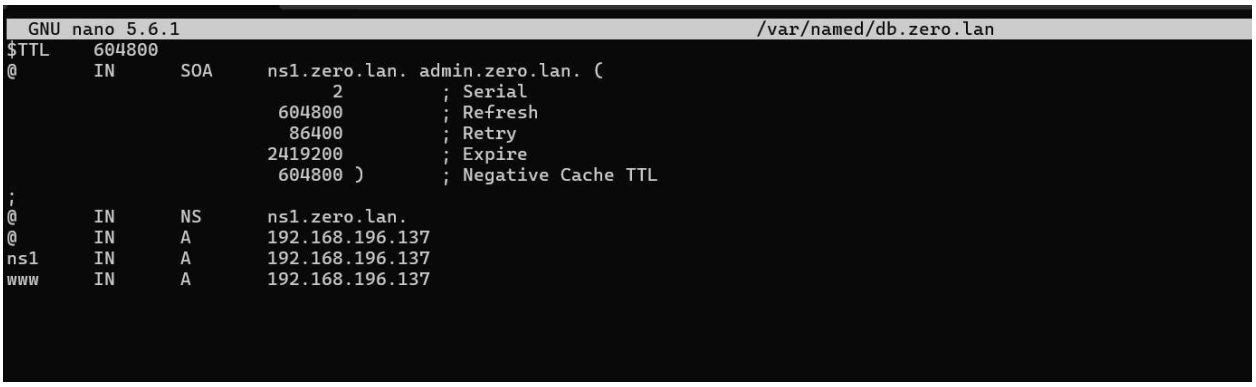
1.1. Instalación de BIND y Configuración del Firewall

Se procede a instalar los paquetes bind y bind-utils en el servidor Rocky Linux. Posteriormente, se habilita el servicio named para que inicie con el sistema y se configura firewall para permitir el tráfico DNS (puerto 53 TCP/UDP).



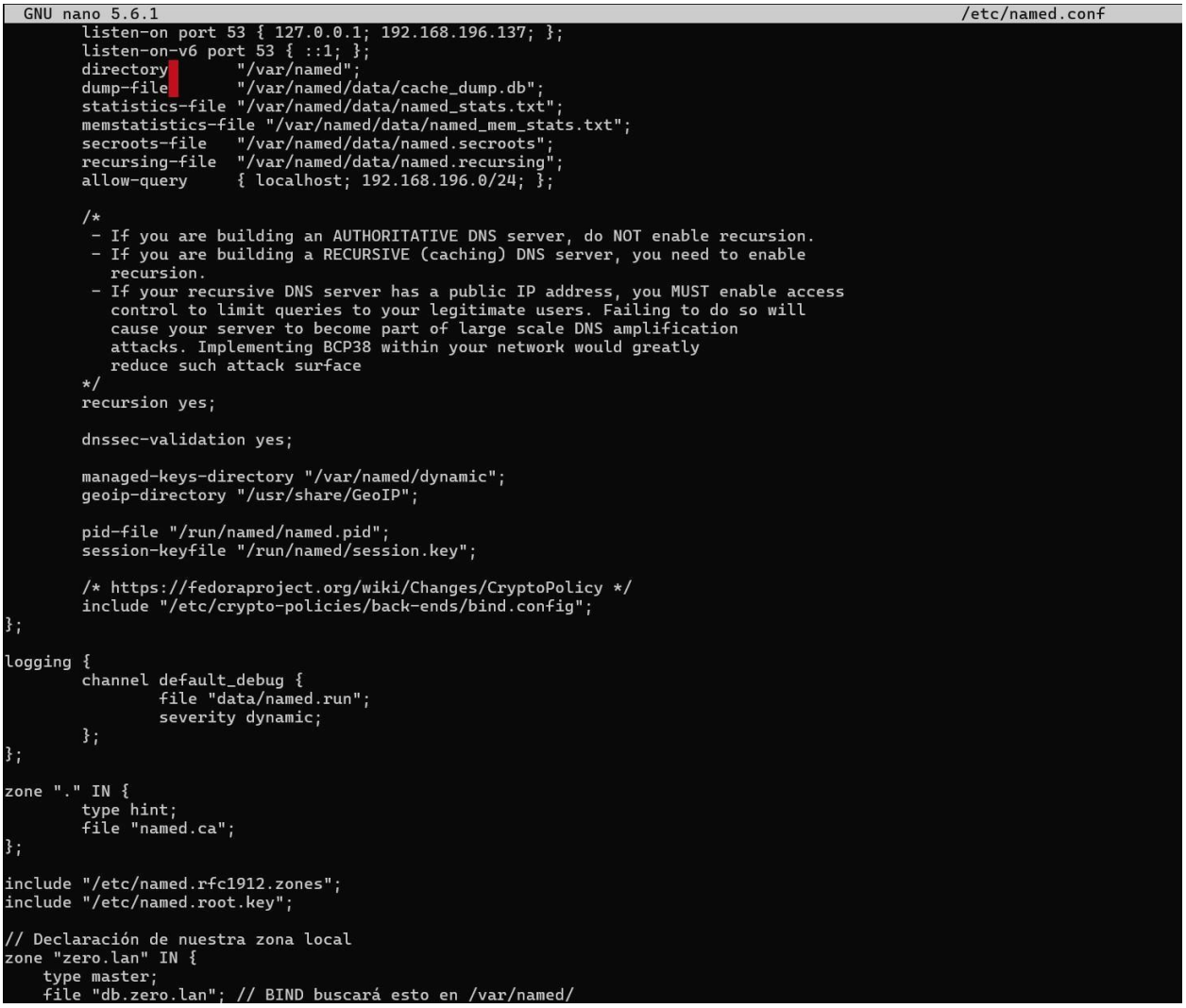
1.2. Configuración del Dominio Ficticio zero.lan

Se crea el archivo de zona /var/named/db.zero.lan con los registros SOA, NS y A necesarios, apuntando a la IP del servidor local (192.168.196.137). Se ajustan los permisos del archivo para el grupo named.



1.3. Configuración del Archivo Principal named.conf

Se modifica el archivo /etc/named.conf para que el servidor escuche en la IP de la red local y permita consultas desde la misma. Finalmente, se añade la declaración de la zona zero.lan para que BIND la reconozca como una zona maestra.



```
 GNU nano 5.6.1                                                    /etc/named.conf
        listen-on port 53 { 127.0.0.1; 192.168.196.137; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 192.168.196.0/24; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-validation yes;

        managed-keys-directory "/var/named/dynamic";
        geoip-directory "/usr/share/GeoIP";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";

        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

// Declaración de nuestra zona local
zone "zero.lan" IN {
    type master;
    file "db.zero.lan"; // BIND buscará esto en /var/named/
```

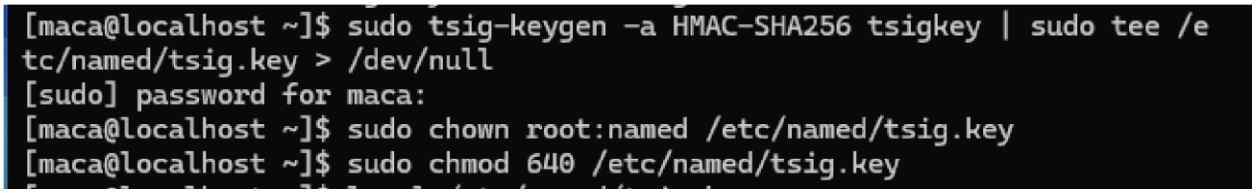
2. Implementación de Medidas de Seguridad

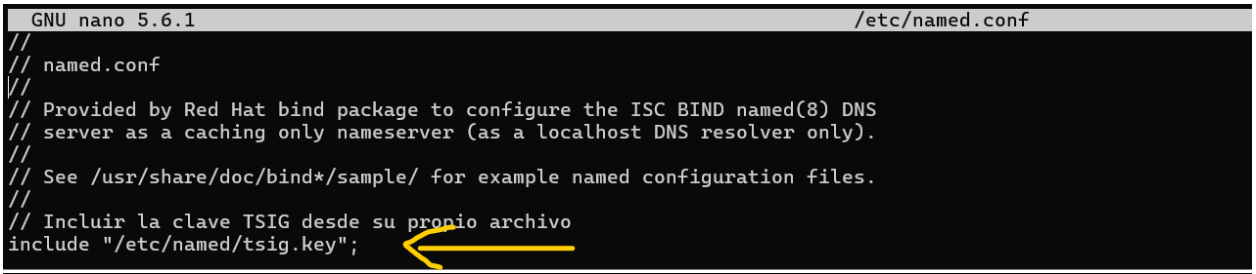
2.1. Restricción de Acceso a la Resolución Recursiva

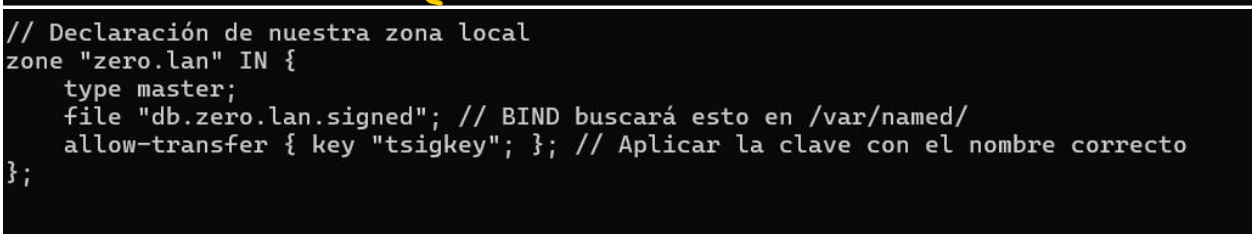
Para prevenir que el servidor sea utilizado en ataques de amplificación, se añade la directiva allow-recursion al bloque options en named.conf, permitiendo consultas recursivas únicamente a la red local.

2.2. Control de Acceso a Transferencia de Zona mediante TSIG

Se utiliza la herramienta tsig-keygen para generar una clave criptográfica simétrica. Esta clave se guarda en /etc/named/tsig.key y se incluye en la configuración principal mediante una directiva include. Posteriormente, se modifica la zona zero.lan para permitir transferencias (allow-transfer) únicamente a quienes presenten una solicitud firmada con dicha clave (tsigkey).







2.3. Configuración de Logs de Auditoría

Se reemplaza el bloque logging por defecto por una configuración personalizada que guarda los eventos de seguridad y transferencias en un archivo de texto plano

(/var/log/bind/security.log). Se crea el directorio de logs, se le asigna el propietario named:named y se ajusta el contexto de SELinux para permitir la escritura.

```
[root@localhost named]#
[root@localhost named]# ls -ld /var/log/bind
drwxr-xr-x. 2 named named 26 jul 24 22:26 /var/log/bind
[root@localhost named]# sudo semanage fcontext -l | grep "/var/log/bind"
/var/log/bind(/.*)?                               all files          system_u:object_r:named_log_t:s0
[root@localhost named]# ls -Zld /var/log/bind
drwxr-xr-x. 2 named named unconfined_u:object_r:named_log_t:s0 26 jul 24 22:26 /var/log/bind
[root@localhost named]#
```

(se muestran con comando de vista los directorios creados y permitidos)

```
 GNU nano 5.6.1                                                    /etc/named.conf

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";

        /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
        include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
    channel security_log {
        file "/var/log/bind/security.log" versions 3 size 5m;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category security { security_log; };
    category xfer-in { security_log; };
    category xfer-out { security_log; };
    category general { security_log; };
};
```

3. Validación de Configuración y Aplicación de DNSSEC

3.1. Validación de la Sintaxis de Configuración

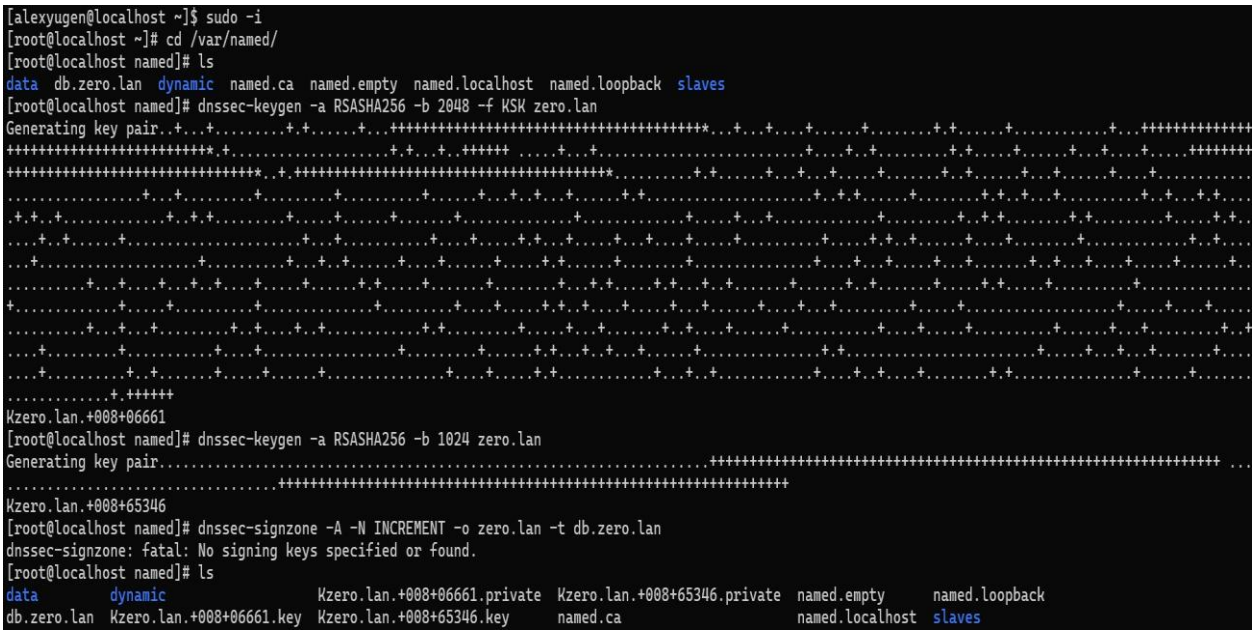
Antes de aplicar los cambios más complejos, se utilizan las herramientas named-checkconf y named-checkzone para verificar que no existan errores de sintaxis en los archivos de configuración y de zona. Ambas validaciones se completaron exitosamente.

```
[alexyugen@localhost ~]$ sudo named-checkconf
[alexyugen@localhost ~]$ sudo named-checkzone zero.lan /var/named/db.zero.lan
zone zero.lan/IN: loaded serial 2
OK
[alexyugen@localhost ~]$
```

3.2. Implementación de DNSSEC: Generación de Claves y Firma de Zona

Se procede a asegurar la zona con DNSSEC. Primero, se habilita la booleana de SELinux named_write_master_zones. Luego, se generan las claves KSK (Key Signing Key) y ZSK (Zone Signing Key). Se añaden las claves públicas al archivo de zona

db.zero.lan y finalmente se firma la zona con dnssec-signzone, creando el archivo db.zero.lan.signed.



3.3. Validación de la Firma de Registros DNSSEC

Se actualiza la configuración en named.conf para que apunte al nuevo archivo de zona firmado (db.zero.lan.signed). Tras reiniciar el servicio named, se realiza una consulta final con dig solicitando los registros DNSKEY y la validación DNSSEC (+dnssec). La respuesta del servidor incluye el flag ad (Authenticated Data), confirmando que la firma de la zona es válida y ha sido verificada criptográficamente por el servidor.

```
[root@localhost named]# ls
data        db.zero.lan.signed  dynamic               Kzero.lan.+008+06661.private  Kzero.lan.+008+65346.private  named.empty      named.loopback
db.zero.lan  dsset-zero.lan.    Kzero.lan.+008+06661.key  Kzero.lan.+008+65346.key      named.ca                      named.localhost  slaves
[root@localhost named]# chown root:named /var/named/db.zero.lan.signed
[root@localhost named]# sudo nano /etc/named.conf
[root@localhost named]# systemctl restart named
[root@localhost named]# sudo systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-07-24 22:26:28 -04; 7s ago
    Process: 3777 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking>
    Process: 3779 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 3780 (named)
      Tasks: 8 (limit: 10723)
     Memory: 21.6M
        CPU: 67ms
```

```
[root@localhost named]# dig @localhost zero.lan DNSKEY +dnssec

; <<>> DiG 9.16.23-RH <<>> @localhost zero.lan DNSKEY +dnssec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43306
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 0ecad252de0aaf6d010000006882ed1693e646282bb86dbc (good)
;; QUESTION SECTION:
;zero.lan.                      IN      DNSKEY

;; ANSWER SECTION:
zero.lan.               604800  IN      DNSKEY  257 3 8 AwEAAZe2Mmum4JAuAK0hE7wp+Iqie63Fj7dEbStrfIPj1eMLvfrq/U4f DKjRPxU7VJeB6/ryBqU1pWb2FYDFG03y3ot8fXfG1HA
v7QJv7CTcQyzd H0gmbzUgjD4+TcO+M1NnjdyIgxurEtBWVxHDajHUTCnvB40lK9H5rojd 9XwPJHCQfGHl6o8mAxxuPFxBHrgySh26GITt0DmOXUe6JyLoljFAs67X Y30Bz79Jy4J9CgMKgzujKA5j1tyF
7pItCurqZNzD3DWZdCFhlK0Aqpey oFViVm8vM36lFsqHflcddNXNevP+WExvRcEH6CeCIU5sIvk1ZS2JxILJ Glon2APcQrU=
zero.lan.               604800  IN      DNSKEY  256 3 8 AwEAAdGnETRWlaOpulkJOhG8gDKyfRfcbczAM7cwfdzoVKXoMZPa09LF xOyzy3rLRR5iZAuqC5A4FNgGN9ywFCSCr8dKygM3H72
qrxBlE5H8eKCR PGD3FMyPWRnIS9hatmdz6Ru/r6Jg+yEHrRYjl+vdcJ7rfye+vqxyus6z U7dazHJD
zero.lan.               604800  IN      RRSIG   DNSKEY 8 2 604800 20250824010856 20250725010856 6661 zero.lan. gmGjf96f7DVTz/1/bVMsTZu3j6yAvN/vq6e+AnM2GS2hG
kxb4t92RBvf vA6X0Tsw1O70EInc7e2MPM7oTPVbvIAS0VqRSdg6peR3SLCpZiO9dBYH 2PjtXGH8g96rt+ykDyw+GxG/k5j5R6Za/fujZ6TMTYeywbREAGSWOZRO 5qlVanBfeUo4/p5SGnlPygRnbCPPgL
mW2SRurbLRo9o/Ccw/+IGhTarc r56gnNrltMIG4u2nljWLg0Hi8GrnCCOtIdZmSYMFERDGcNv2GKs9HVS4 0skSEIDuHKsU494rzD2k0tmva0AOx89MZbzC9V9xcM3QvsemERrPNn16 YjUTbw==
zero.lan.               604800  IN      RRSIG   DNSKEY 8 2 604800 20250824010856 20250725010856 65346 zero.lan. YiRFI/VKjtzaJPr8mmQjhaJj4PdzYi8sO7azWn3mJnAL
8HfoHZoA3of2 80242zGF1Id+CBGaRi0kAuhA6pbt9ia8/g8XMQev1p7IxJwiNuAJ65Kl hFpadhca0P6aURvjAB9AKLxBQzridm17goh7XQBMoYbmqUhwrjhaQuDM Kko=

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Thu Jul 24 22:33:58 -04 2025
;; MSG SIZE  rcvd: 953
```