Conectividad

- Puente de red en Fedora con nmcli
- Usar resolv.conf directo en Fedora desactivando systemd-resolved

Puente de red en Fedora con nmcli

Este artículo explica cómo configurar un puente de red en Fedora utilizando NetworkManager a través de `nmcli`. La configuración permite que las máquinas virtuales (VMs) se conecten a la red a través del puente.

Pasos principales:

1. **Crear un dispositivo de tipo "bridge"** (br0, por ejemplo).
2. **Configurar la tarjeta de red física** (enp39s0) como esclava del puente.
3. **Asignar la dirección IP y puerta de enlace al puente**, en lugar de hacerlo a la interfaz física.

De esta forma, las VMs podrán conectarse a br0 y el sistema anfitrión seguirá teniendo conexión a la red.

Configuración con nmcli

1. **Eliminar y desactivar la configuración actual** de enp39s0 (Perfil 1) para evitar conflictos:

   ```
   nmcli con down "Perfil 1"
   nmcli con delete "Perfil 1"
   ```

   (Esto desconectará temporalmente la red; tener precaución si se usa SSH.)
2. **Crear el puente**:

   ```
   nmcli con add type bridge ifname br0 con-name br0
   ```

   - Esto genera una interfaz virtual denominada br0.
3. **Configurar una dirección IP estática (opcional)** en br0:

```
nmcli con modify br0 ipv4.method manual \
    ipv4.addresses "192.168.100.130/24" \
    ipv4.gateway "192.168.100.1" \
    ipv4.dns "192.168.100.3 192.168.100.240"
nmcli con modify br0 ipv6.method ignore
```

(Para DHCP, utilizar `ipv4.method auto` y omitir addresses, gateway y DNS.)

4. **Crear la conexión esclava** para la interfaz física enp39s0:

```
nmcli con add type bridge-slave ifname enp39s0 master br0 con-name br0-slave
```

(Este comando asigna enp39s0 al puente br0.)

5. **Activar el puente**:

```
nmcli con up br0
nmcli con up br0-slave
```

Con esta configuración, el sistema anfitrión tendrá la dirección IP en br0, y la interfaz física enp39s0 quedará como parte del puente. Las VMs podrán conectarse a br0 y obtener una dirección IP en la misma red.

Consideraciones adicionales:

- **Precaución**: Realizar cambios en la única interfaz de red puede provocar pérdida de conexión. En entornos SSH, se recomienda tomar precauciones o tener acceso físico a la máquina.
- **Conectividad de las VMs**: Las VMs deben configurarse para utilizar "br0" en lugar de "enp39s0" para conectarse a la red local.

Con esta configuración, el puente de red en Fedora quedará funcional y permitirá la conectividad esperada.

Usar resolv.conf directo en Fedora desactivando systemd-resolved

---

Este apunte documenta cómo forzar que Fedora utilice AdGuardHome como resolutor DNS directo, desactivando `systemd-resolved`, validando DNSSEC correctamente y asegurando que los cambios persistan tras reinicio.

Características

- Desactiva completamente `systemd-resolved`.
- Utiliza un `resolv.conf` estático y personalizado.
- Resuelve nombres DNS a través de AdGuardHome.
- Valida correctamente DNSSEC.
- Compatible con la resolución de nombres `.lan.internal` (o el que quieras) si se combina con reescrituras desde Tailscale.

Requisitos previos

- Fedora instalado y actualizado.
- AdGuardHome configurado como resolutor DNS.
- Haber verificado que AdGuard valida DNSSEC (por ejemplo, usando Cloudflare o NextDNS como upstreams).

Desactivar `systemd-resolved` en Fedora

Fedora utiliza por defecto un stub DNS en `127.0.0.53`, gestionado por `systemd-resolved`, lo cual puede interferir si queremos usar AdGuardHome como resolutor principal.

1. Comprobar estado actual

```
cat /etc/resolv.conf
```

Si ves algo como esto:

```
# This is /run/systemd/resolve/stub-resolv.conf managed by systemd-resolved(8)
nameserver 127.0.0.53
```

Estás usando el stub DNS. También puedes verificar con:

```
resolvectl status
```

Si ves `DNSSEC=no/unsupported`, significa que no se está validando correctamente.

2. Detener y deshabilitar systemd-resolved

```
sudo systemctl disable --now systemd-resolved
```

3. Eliminar el symlink de resolv.conf

```
sudo rm -f /etc/resolv.conf
```

4. Crear un resolv.conf estático personalizado (usa tus DNS locales)

```
sudo tee /etc/resolv.conf > /dev/null <<EOF
nameserver 192.168.1.5
nameserver 192.168.1.155
search lan.internal
options trust-ad edns0 timeout:1 attempts:2 rotate
EOF
```

Este archivo:

- Usa directamente tus resolutores locales (AdGuard).
- Habilita la confianza en firmas DNS (`trust-ad`).
- Permite extensiones modernas (`edns0`).
- Optimiza los tiempos de espera y el reintento.

Verificar funcionamiento

Resolución básica

```
dig google.com
```

DNSSEC fallido (debe dar `SERVFAIL`)

```
dig +dnssec dnssec-failed.org
```

DNSSEC correcto (debe dar `flags: ... ad`)

```
dig +dnssec sigok.verteiltesysteme.net
```

Resultado final

- Fedora ya no intercepta ni redirige peticiones DNS.
- `resolv.conf` permanece inmutable.
- Todo se resuelve a través de AdGuardHome.
- DNSSEC se valida correctamente.
- Puedes resolver hosts de Tailscale si has sincronizado `rewrites:` en AdGuard.
- En caso de que NetworkManager modifique nuestro resolv.conf, podemos aplicarle `sudo chattr +i /etc/resolv.conf` para que sea inmutable.

Enlaces de interés

- Evitar que resolv.conf sea modificado por aplicaciones externas