
ResumenIA: LPIC-2 Objetivo 205.3 - Resolución de Problemas de Red

Peso del Objetivo: 3

Descripción General

El objetivo 205.3 de LPIC-2 se enfoca en la capacidad de un administrador de sistemas Linux para diagnosticar y resolver problemas de red complejos. Esto va más allá de la configuración básica, requiriendo un conocimiento profundo de las utilidades de monitoreo, análisis y solución de problemas, así como la comprensión de cómo los diferentes componentes del sistema (archivos de configuración, registros, hardware, firewalls) impactan la conectividad.

Áreas de Conocimiento Clave Desarrolladas

1. Ubicación y Contenido de los Archivos de Restricción de Acceso

La seguridad a nivel de host es crucial para la resolución de problemas, ya que las restricciones de acceso pueden bloquear conexiones legítimas.

- `hosts.allow` y `hosts.deny` (`/etc/hosts.allow`, `/etc/hosts.deny`): Estos archivos controlan el acceso a los servicios de red basados en TCP Wrappers. TCP Wrappers es un sistema de seguridad de bajo nivel que puede permitir o denegar el acceso a servicios que lo soportan (como `sshd`, `vsftpd`, etc.) basándose en la dirección IP del cliente.
- Prioridad: Si ambos archivos contienen reglas para un servicio, `hosts.deny` suele tener prioridad, pero la implementación exacta puede variar. Por lo general, se evalúa `hosts.allow` primero; si hay una coincidencia de permiso, se concede el acceso. Si no, se evalúa `hosts.deny`; si hay una coincidencia de denegación, se niega el acceso. Si no hay ninguna coincidencia, el acceso se permite.
- Sintaxis: `daemon_list : client_list [: option : option ...]`
- `daemon_list`: Lista de servicios (ej. `sshd`, `vsftpd`, `ALL`).
- `client_list`: Lista de hosts, IPs, rangos de red, o `ALL`, `LOCAL`.
- Ejemplo:
- Permitir SSH solo desde la red 192.168.1.0/24:

```
# /etc/hosts.allow
sshd : 192.168.1.
# /etc/hosts.deny
sshd : ALL
```

- Bloquear todo excepto localhost para vsftpd:

```
# /etc/hosts.allow
```

```
vsftpd : LOCAL
# /etc/hosts.deny
vsftpd : ALL
```

- Impacto en la resolución de problemas: Si un servicio no es accesible, revisar estos archivos es fundamental. Un acceso denegado puede manifestarse como un "Connection refused" o "Host unreachable" desde el cliente, incluso si el servicio está corriendo y el firewall permite el tráfico.

2. Utilidades para Configurar y Manipular Interfaces de Red Ethernet

Aunque cubiertas en el 205.1, su dominio es vital para el diagnóstico, ya que una configuración incorrecta puede ser la raíz de un problema.

- `ip`: La herramienta preferida para configurar y manipular interfaces, direcciones y rutas.
- `ip link show [dev <interface>]`: Muestra el estado físico y lógico de la interfaz (UP/DOWN, errores RX/TX).
- `ip addr show [dev <interface>]`: Muestra las direcciones IP (IPv4 e IPv6) asignadas.
- `ip link set <interface> up/down`: Para habilitar/deshabilitar una interfaz y verificar si el problema es físico o de configuración.
- `ifconfig` (Legado): Similar a `ip addr`/`ip link` para la configuración y visualización de interfaces.
- `ifconfig <interface> [up/down]`: Configuración básica y estado.

3. Utilidades para Gestionar Tablas de Enrutamiento

Un enrutamiento incorrecto es una causa común de "Host unreachable" o "Destination Net Unreachable".

- `ip route`: La herramienta principal para visualizar y manipular la tabla de enrutamiento.
- `ip route show`: Muestra todas las rutas. Indispensable para verificar si el gateway por defecto está correctamente configurado y si existen rutas específicas hacia subredes remotas.
- `ip -6 route show`: Para rutas IPv6.
- `route` (Legado): Muestra y permite la manipulación de la tabla de enrutamiento IPv4.
- `route -n`: Muestra la tabla de enrutamiento numéricamente (útil para evitar problemas de resolución de DNS).

4. Utilidades para Producir Listados con los Estados de la Red

Para identificar conexiones activas, puertos en escucha y estadísticas.

- `ss`: Rápido y eficiente para listar sockets (conexiones).
- `ss -tuln`: Muestra todos los sockets TCP y UDP en estado de escucha (`LISTEN`) de forma numérica (IPs y puertos, no nombres). Útil para ver si un servicio esperado está realmente escuchando.
- `ss -tunap`: Muestra todas las conexiones TCP y UDP (incluyendo establecidas, cerrando, etc.),

junto con los nombres de los programas (`p`) y los números de proceso (`n`). Ayuda a identificar qué aplicación está usando qué conexión.

- `netstat` (Legado): Proporciona información similar a `ss`.
- `netstat -tulnp`: Funcionalidad equivalente a `ss -tulnp`.
- `netstat -r`: Muestra la tabla de enrutamiento, similar a `route -n`.

5. Utilidades para Obtener Información sobre la Configuración de la Red

Conocer la configuración actual es el primer paso para detectar desviaciones.

- `hostname`: Muestra o establece el nombre de host del sistema.
- `hostname`: Muestra el nombre de host actual.
- `hostname -f`: Muestra el FQDN (Fully Qualified Domain Name).
- Archivos asociados:
- `/etc/hostname`: Contiene el nombre de host estático del sistema (usado por `systemd`).
- `/etc/HOSTNAME`: Usado por algunos sistemas más antiguos o específicos.
- `ping`, `ping6`: Prueban la conectividad a nivel de IP (Capa 3) y miden la latencia.
- `ping <IP_destino>`: Confirma si un host es alcanzable. Si falla, el problema es de red o firewall.
- `ping6 <IPv6_destino>`: Lo mismo para IPv6.
- `traceroute`, `traceroute6`: Muestran la ruta (los "saltos" o routers) que toman los paquetes para llegar a un destino. Útil para identificar dónde se detiene la conectividad.
- `traceroute <IP_destino>`: Muestra la ruta IPv4.
- `traceroute6 <IPv6_destino>`: Muestra la ruta IPv6.
- Ejemplo: Si `ping` falla, `traceroute` puede mostrar si el problema está en el router local, en un ISP intermedio, o en el destino.
- `mtr` (My Traceroute): Combina la funcionalidad de `ping` y `traceroute` en una herramienta interactiva, mostrando estadísticas de latencia y pérdida de paquetes para cada salto.
- `mtr <IP_destino>`: Proporciona una vista en tiempo real y más detallada de la conectividad y la calidad de la ruta.
- Archivos de configuración de red:
- `/etc/network/`: Contiene configuraciones de red en sistemas basados en Debian/Ubuntu (ej. `/etc/network/interfaces`).
- `/etc/sysconfig/network-scripts/`: Contiene configuraciones de red en sistemas basados en Red Hat/Rocky (ej. `ifcfg-eth0`).
- NetworkManager: Un gestor de red dinámico común en distribuciones modernas. Sus

configuraciones se encuentran en `/etc/NetworkManager/system-connections/` y se gestionan con `nmcli` o `nmtui`. Comprender su impacto es clave, ya que puede sobrescribir configuraciones manuales.

- `/etc/resolv.conf`: Configura los servidores de nombres DNS.
- `nameserver <IP_DNS>`: Lista los servidores DNS a usar.
- `search <dominio>`: Dominio de búsqueda.
- Impacto en la resolución de problemas: Si las IPs funcionan pero los nombres de host no (`ping google.com` falla pero `ping 8.8.8.8` funciona), el problema es de resolución DNS.
- `/etc/hosts`: Archivo de mapeo de nombres de host a direcciones IP estáticas. Tiene prioridad sobre DNS para la resolución de nombres.
- Ejemplo: `127.0.0.1 localhost`, `192.168.1.10 rocky.example.com rocky`.
- Impacto en la resolución de problemas: Un `hosts` mal configurado puede hacer que un nombre de host se resuelva a una IP incorrecta.

6. Métodos para Obtener Información sobre los Dispositivos de Hardware Reconocidos y Usados

Para diagnosticar problemas a nivel de hardware.

- `dmesg`: Muestra los mensajes del búfer del kernel. Contiene información sobre el hardware detectado durante el arranque, incluyendo tarjetas de red, errores de controlador, etc.
- `dmesg | grep -i eth`: Filtrar mensajes relacionados con Ethernet.
- `dmesg | grep -i firmware`: Ver si hay problemas con firmware de dispositivos.

7. Archivos de Inicialización del Sistema y su Contenido (Systemd y SysV init)

La forma en que se inician los servicios de red es crucial para la persistencia de la configuración.

- Systemd: El sistema de inicio moderno y gestor de servicios.
- `systemctl status <service>`: Verifica el estado de un servicio (ej. `NetworkManager.service`, `systemd-networkd.service`).
- `journalctl -u <service>`: Muestra los logs de un servicio específico.
- `systemctl is-enabled <service>`: Comprueba si un servicio está configurado para iniciarse al arrancar.
- SysV init (Legado): Sistema de inicio más antiguo.
- Scripts en `/etc/init.d/` y enlaces simbólicos en `/etc/rcX.d/`.
- `service <service> status/start/stop/restart`.

8. Conocimientos sobre NetworkManager y su Impacto en la Configuración de la Red

NetworkManager es el gestor de red por defecto en muchas distribuciones modernas (Red Hat, Rocky, Fedora, Ubuntu Desktop).

- Impacto: Puede sobrescribir configuraciones manuales si no se le instruye correctamente. Gestiona interfaces alámbricas, inalámbricas, VPNs, etc., de forma dinámica.
- Utilidades:
- `nmcli` (NetworkManager Command Line Interface): Herramienta de línea de comandos para interactuar con NetworkManager.
- `nmcli device show`: Muestra el estado de los dispositivos de red.
- `nmcli connection show`: Muestra las conexiones configuradas (perfiles).
- `nmcli connection up <nombre_conexion>`: Activa una conexión.
- `nmtui` (NetworkManager Text User Interface): Interfaz de usuario basada en texto para configurar NetworkManager.

Archivos de Registro del Sistema

Los logs son tu mejor amigo para la resolución de problemas.

- `/var/log/syslog` (Debian/Ubuntu) y `/var/log/messages` (Red Hat/Rocky): Contienen mensajes generales del sistema, incluyendo eventos de red, errores de interfaces, mensajes del kernel (similar a `dmesg`), etc.
- Diario de Systemd (`journalctl`): El sistema de registro unificado de Systemd.
- `journalctl -xe`: Muestra los mensajes más recientes con detalles.
- `journalctl -k`: Muestra los mensajes del kernel (similar a `dmesg`).
- `journalctl -u <servicio_red>`: Filtra mensajes por unidad de servicio de red (ej. `systemd-networkd.service`, `NetworkManager.service`).
