LPIC2 2021 Sesión 12 (2021-03-11)

Documentación relacionada:

- Manual Certificacion LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

NFS

- DOC: (pag 219)
- DOC: Material Practicas LPIC-2/LPIC-202/3-File Sharing/2-NFS/1-Configuración de servidor NFS en RedHat 7.pdf
- no enrutable
- `nfstat`
- NFS v4: ACLs y Kerberos
- `yum -y install nfs-utils`
- `systemctl start rpcbind nfs-server`
- `systemctl enable rpcbind nfs-server`
- **/etc/exports**
- `rpcinfo`
- `showmount -a`: clientes conectados ¿?
  - `showmount –exports`
- `showmount –exports <ip>`: para ver que ofrece la máquina <ip>
- `exportfs`: que estoy ofreciendo
  - **-v**: lista compartidos con opciones
  - **-a**: exporta todos los directorios en /etc/exports
  - **-u**: un-export
  - **-r**: re-export (después de una modificación)

Laboratorio

- DOC: Material Practicas LPIC-2/LPIC-202/3-File Sharing/2-NFS/Configuracion NFS.txt
- server:

  /etc/exports

  ```
  /usuarios 192.168.2.152(rw,no_root_squash)
  ```

- cliente:
  - mount:

    ```
    mount -t nfs 192.168.2.5:/usuarios /mnt
    ```

  - fstab:

/etc/fstab

```
192.168.2.5:/usuarios /mnt nfs _netdev,rw,auto 0 0
```

  - **_netdev**: no retrasa el mount si el servidor no está disponible (evita que se produzca)

- NFS se basa en https://ca.wikipedia.org/wiki/Remote_Procedure_Call
- `rpcinfo`

- Redhat deja Centos, alternativas:
  - https://rockylinux.org/
  - http://linkat.xtec.cat/portal/index.php
  - centos 7, 4 años
  - centos 8, a final de año

DHCP

- DOC: Material Practicas LPIC-2/LPIC-202/1-Domain Name Server/Laboratorio DHCP.pdf
- DOC: (pag 165)
- `yum -y install dhcp`
- **/etc/dhcp/dhcp.conf**

```
authoritative;
default-lease-time 86400;
max-lease-time 86400;
ddns-updates on; # actualizar zonas de DNS
ddns-update-style interim;
shared-network miredlocal {
 subnet 192.168.2.0 netmask 255.255.255.0 {
 option routers 192.168.2.1;
 option subnet-mask 255.255.255.0;
 option broadcast-address 192.168.2.255;
 option domain-name "curso.esp";
 option domain-name-servers 192.168.2.150, 80.58.0.33;
 option netbios-name-servers 192.168.2.1;
 range 192.168.2.50 192.168.2.90;
 }
 host m253 {
  option host-name "m253.mi-red-local.com";
  hardware ethernet 00:50:BF:27:1C:1C;
  fixed-address 192.168.2.253;
  }
 host m254 {
  option host-name "m254.mi-red-local.com";
  hardware ethernet 00:01:03:DC:67:23;
  fixed-address 192.168.2.254;
  }
}
```

- DDNS: Dinamic DNS. Actualizar el DNS de manera automática al repartir IPs por DHCP
- opciones:
  - authoritative: Cuando hay dos servidores dhcp en la red el que tenga este parámetro es el que va a servir a la red y cuando este servidor este caído servirá a la red el otro servidor.
  - not authoritative: La función de este parámetro es justo la contraria del anterior. Es

decir: la configuración del servidor de DHCP no es concluyente y los clientes mal configurados que sean detectados por el servidor, seguirán con su configuración intacta.

- ddns-updates: Activa la actualización DNS mediante los valores asignados por DHCP.
- ddns-update-style: Define el método de actualización automática de las DNS. Los valores pueden ser ad-hoc, interim y none.
- default-lease-time: Especifica la cantidad de tiempo, en segundos, que será mantenida una asignación de direcciones, siempre y cuando el cliente no haya especificado algo concreto.
- ignore allow / client-updates: Permite la actualización de las asignaciones (allow)

de un cliente a requerimiento de este, o bien las asignaciones se actualizan cuando el servidor así lo requiera (ignore).

- max-lease-time: Especifica la cantidad máxima de tiempo, en segundos, que será mantenida una asignación de direcciones. No está sujeta a esta especificación la asignación dinámica BOOTP.
- netmask: Define la mascara de red de la Subred
- one-lease-per-client: Cuando la opción se iguala a on y un cliente solicita una

asignación de dirección (DHCPREQUEST), el servidor libera de forma automática cualquier otra asignación asociada a dicho cliente. Con esto se supone que si el cliente solicita una nueva asignación es porque ha olvidado que tuviera alguna, luego tiene un sólo interfaz de red. No dándose esta situación entre los clientes no es muy aconsejable el uso de esta opción.

- option broadcast-address: Define la dirección de broadcast de la Red.
- option domain-name-servers: Define el nombre de los servidores DNS.
- option nis-servers: Define la lista de servidores NIS (Sun Network Information Server) disponibles. Los servidores se listan en orden de preferencia. Para establecer el nombre del dominio NIS, se usará option nis-domain <nombre>.
- option routers: Define el router , gateway o pasarela de enlace listadas en orden de preferencia.
- option subnet-mask : Definición de la máscara de subred general.
- range ip-menor ip-mayor: En una declaración de subred, este parámetro define el rango de direcciones que serán asignadas. Pueden darse dos instrucciones range seguidas del modo:
  - range 192.168.0.11 192.168.0.100;
  - range 192.168.0.125 192.168.0.210;
- server-identifier: Identifica la máquina donde se aloja el servidor de DHCP. Su uso

se aplica cuando la máquina en cuestión tiene varias direcciones asignadas en un mismo interfaz de red.

- shared-network: Declaración de Subred compartida.
- subnet: Declaración de Subred.
- **/var/lib/dhcpd/dhcpd.leases**
- cliente
- `dhclient <interfaz>`
- `dhclient -r <interfaz>`:liberar IP
- DHCP relay:Las comunicaciones DHCP se realizan por broadcast y los mensajes broadcast no pasan a través de lo routers. Por consiguiente, tanto las peticiones DHCP, como las respuestas de los servidores no producen ninguna acción fuera de la red local. La solución mas fácil consiste evidentemente en poner un servidor DHCP en cada segmento de red donde sean necesarios. Sin embargo, si se desea utilizar solo un servidor para varias redes, existe una solución, que son los agentes de DHCP relay.

DDNS

- DOC: Material Practicas LPIC-2/LPIC-202/1-Domain Name Server/Laboratorio DNS.pdf (pag.13)
  - añadir zonas en dhcpd.conf
  - añadir **allow-update** en el named.conf
  - al recibir una solicitud DHCP, actualiza unos ficheros .jnl que es donde mantiene la configuración

necesaria para el DNS

PAM

- DOC: Material Practicas LPIC-2/LPIC-202/6-Network Client Management/Modulos de autenticacion con conexion (PAM)/Presentacion PAM.pdf
- mucha atención con los cambios. Los cambios se aplican directamente!
- **/etc/pam.d/**
- estructura de la línea:
    - tipo:
        - auth (autenticación): Autentica al usuario mediante un método y le proporciona los privilegios.
        - account (verificación): Comprueba si el usuario tiene permiso para utilizar el servicio o si el servicio esta permitido (control horario, por ejemplo).
        - password (actualización): Actualiza el mecanismo de autenticación.
        - session (sesión): Acciones que deben ejecutarse antes y/o después del acceso del usuario.
    - control: como actua PAM ante un fallo: ignorar, terminar ejecución, etc…
        - palabras (simple o histórica):
            - requisite: Se envía fallo sin ejecutar otros módulos.
            - required: Se enviará fallo, ejecutando previamente los otros módulos.
            - sufficient: Se enviará correcto si no existe fallo previo.
            - optional: Su respuesta solo se usa si no existe otro módulo de este servicio y tipo.
        - acciones (manera nueva):
            - [valor1=accion1 valor2=accion2]
    - camino al módulo:
        - si empieza por / es path absoluto
        - si no, bajo **/lib/security**
    - argumentos

FTP

- DOC: (pag 271)
- Material Practicas LPIC-2/LPIC-202/3-File Sharing/4-FTP/Laboratorio servidor FTP vfsftpd.pdf
- Material Practicas LPIC-2/LPIC-202/3-File Sharing/4-FTP/Labotatorio securizar FTP con

OpenSSL.pdf

- TPC/21: comandos
- TPC/20: transmisión de datos
- modo activo
    - el servidor establece el puerto en la máquina de destino (cliente). Problemas con firewalls
- modo pasivo
    - ? → https://ccnadesdecero.es/diferencias-ftp-modo-activo-pasivo/

Laboratorio: instalación

- vsftpd (orientado a seguridad)
    - jail
    - **/etc/vsftpd/vsftpd.conf**

```
anonymous_enable=NO
allowascii_upload_enable=YES
ascii_download_enable=YES
chroot_local_user=YES
```

```
chroot_list_enable=YES
allow_writeable_chroot=YES
chroot_list_file=/etc/vsftpd/chroot_list # excluidos del chroot
ls_recurse_enable=YES
listen=YES
Listen_ipv6=NO
```

- `adduser -s /sbin/nologin gerente`
- `passwd gerente` → no estará enjaulado ya que lo hemos añadido a **chroot_list**
- `passwd vagrant`

Laboratorio: securizar con TLS

- DOC: Material Practicas LPIC-2/LPIC-202/3-File Sharing/4-FTP/Labotatorio securizar FTP con OpenSSL.pdf

- `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem -sha256`

- /etc/vsftpd/vsftp.conf

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem

#Habilitamos el uso de SSL
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

# Las siguientes directrices establecen la preferencia de TLSv1 sobre
SSLv2 y SSLv3
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH # especial filezilla
require_ssl_reuse=NO # especial filezilla
force_local_data_ssl=YES
force_local_logins_ssl=YES
force_anon_data_ssl=YES
force_anon_logins_ssl=YES
```

- https://clouding.io/hc/es/articles/360015466560-A%C3%B1adir-SSL-Let-s-Encrypt-en-vsFTPd
- chequea y da información del certificado: `openssl s_client -connect 192.168.2.5:21 -starttls ftp -CApath /etc/ssl/private`