Limitacions d'accés

UF2 - Instal·lació i adminstració de serveis de transferència de fitxers

Creació d'usuaris i grups

Els usuaris es poden classificar en:

- Usuaris anònims
- Usuaris locals del sistema
- Usuaris propis del servei FTP anomenats usuaris virtuals

Usuaris anònims

L'accés anònim permet que qualsevol client pugui accedir a l'àrea pública del servidor FTP.

Es fa amb un usuari "anonymus".

Té permisos especials, se li pot restringir l'accés de lectura i el de publicar.

Usuaris locals

Permet accedir al servei FTP als usuaris del SO.

Per permetre'ls l'accés al servei FTP hem d'activar la directiva

local_enable

Per permetre'ls pujar documents caldrà més directives.

Usuaris locals

L'accés es pot permetre o restringir segons es desitgi.

Els usuaris locals accedeixen al home que és el directori de publicació.

Tenen dret a navegar per tot el sistema de fitxers, però sels pot engabiar (chroot).

Usuaris Virtuals

Són usuaris identificats que no són usuaris del sistema.

Usuaris propis de FTP.

Cal portar la seva gestió amb els fitxers d'usuaris i contrasenyes.

En un servidor vsftpd s'anomenen **virtual users**.

Usuaris Virtuals

L'avantatge d'aquest model és que permet accés identificat sense necessitat de comptes d'usuari en el sistema.

L'inconvenient és que s'ha de dur una gestió d'usuaris paral· lela a la del sistema.

Usuaris Virtuals

El que busquem és permetre l'accés a contingut que ha de ser accessible a usuaris no validats en el sistema, però que no es vol fer públic a tothom.

Usuaris Virtuals

Procés per generar usuaris virtuals al servidor vsftpd:

1. Crear la base de dades d'usuaris virtuals.
2. Crear/editar el fitxer de PAM per usar la base de dades.
3. Generar el directori de publicació de l'usuari virtual i crear l'usuari.
4. Generar el fitxer de configuració per permetre l'ús d'usuaris virtuals.

Configuració de l'accés anònim

Habitualment els usuaris anònims tenen accés a un directori de publicació on poden fer descàrregues però no pujar documents.

Es crea automàticament un usuari anomenat **ftp** (usuari del sistema que representarà als usuaris anònims)

Configuració de l'accés anònim

Els elements que cal configurar relacionats amb l'accés anònim són:

1. Determinar si es permet l'accés a usuaris anònims
2. Determinar si se'ls concedeix el dret a pujar documents.
3. concedir-los o no el dret a crear directoris en el servidor.
4. Determinar l'usuari, grup i màscara amb la que poden pujar els documents
5. Engabiar (chroot) o no l'usuari en el seu accés al sistema de fitxers
6. Establir si cal demanar contrasenya als usuaris anònims
7. Generar una llista de contrasenyes no acceptades pel sistema
8. Establir permisos a fitxers i directoris des dels quals es permet descarregar i pujar documents.

Configuració de l'accés anònim

Es crea un usuari **ftp** (representant)

ftp no té dret a realitzar sessions interactives amb el sistema

el seu directori serà /srv/ftp (pot variar)

dins hi sol haver un directori **pub** amb la documentació d'accés públic.

```
root@server:/# grep "ftp" /etc/passwd
ftp:x:116:127:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
root@server:/#
```

Limitacions d’accés

1. Rendiment
2. Mode de transferència
3. Seguretat
4. Mode del servei: autònom o xinetd
5. Gesetió de logs
6. Bàners globals i missatges de directori

Rendiment

- **accept_timeout** (60): estableix el timeout per establir connexions segures
- **anon_max_rate** (0): taxa màxima de transferència. En bytes per segon (0= il· limitat)
- **connect_timeout** (60): temps màxim per respondre una connexió tipus PORT
- **data_connection_timeout** (300): nombre màxim de segons d'inactivitat en una sessió de transferència.
- **delay_failed_login** (1): nombre de segons de la pausa abans d'indicar un error d'inici de sessió
- **delay_successful_login** (0): nombre de segons de pausa abans de permetre una connexió correcta.

Rendiment

- **idle_session_timeout** (300): màxim de segons que una sessió pot estar inactiva.
- **local_max_rate** (0): taxa màxima de transferència per un usuari local.
- **max_clients** (0): nombre màxim de client connectats concurrentment.
- **max_login_fails** (3): màxim d'intents d'inici fallits. Després es tanca sessió.
- **max_per_ip** (0): màxim de clients simultànis des de la mateixa IP.
- **one_process_model** (YES): activa el model *one process per connection* (proporciona més velocitat de processament de les peticions client.

Mode d'accés

Els servidors FTP permeten treballar en ASCII i en binari.

Per defecte binari. ASCII fa un ús més intensiu dels recursos.

- **ascii_upload_enable** (YES): permet pujar documents en mode ASCII
- **ascii_download_enable** (YES): permet descàrregues ASCII
- **async_abor_enable** (NO): si s'activa, permet a clients antics cancel·lar descàrregues a mig fer. Sinó els clients es bloquejen.

Seguretat

- **pasv_min_port** (0): minim port permès per connexions tipus PASV
- **pasv_max_port** (0): port màxim permès per connexions tipus PASV
- **pasv_enable** (YES): permet connexions passives
- **port_enable** (YES): si és NO, no permet la transferència de dades en mode actiu.
- **tcp_wrappers** (NO): permet establir regles de connexió en funció dels noms d'amfitrions o adreces.
- **Ls_recurse_enable** (NO): per defecte desactivat. Poder fer llistats recursius amb l'ordre -R
- **local_unmask** (077): valor per defecte de la màscara de permisos per elements publicats per usuaris locals.

Seguretat

- **dirlist_enable** (YES): especifica si es concedeix el permís de fer llistats
- **download_enable** (YES): permet o no descàrrega de continguts
- **hide_ids** (NO): permet ocultar info d'usuari i grup en els llistats de directoris. Es mostra sempre FTP.
- **hide_file** (none): permet indicar patrons de noms de fiter exclosos dels llistats.
- **pam_service_name** (vsftpd): nom del servei PAM que s'utilitza.
- **ftp_username** (ftp): nom de l'usuari real del sistema que s'utilitzarà per connexions anònimes.

Mode de servei

El servidor pot funcionar en mode autònom o dins del superservei de xarxa xinetd.

Es poden executar diverses instàncies del servidor per atendre diferents seus virtuals.

- **listen** (YES): directiva que indica al servidor que ha de funcionar en mode autònom
- **listen_adress** (adreça IP): indica per quina adreça IP escolta el servidor.

Mode de servei - xinetd

- **disable** (no): indica el servei que ha de ser escoltat per el xinetd
- **socket_type** (stream): utilitza TCP
- **wait** (no): un sol thread o multithread (si s'executa una sola instància o vàries)
- **user** (root): el servei s'executa en nom de l'usuari root
- **server** (/usr/local/sbin/vsftpd): nom de l'executable del servidor
- **per_source** (5): màxim de 5 connexions simultànies des d'un mateix client
- **instances** (200): permet un màxim de 200 clients simultànis
- **no_access** (192.168.1.3): denega l'accés a clients amb aquesta IP
- **log_on_sucess** (+=PID HOST DURATION): format dels logs per connexions
- **log_on_failure** (+=HOST): format de logs per connexions fallides

Logs

cal indicar si cal generar els logs de les connexions clients o no.

cal establir el fomrat de missatges.

- **xferlog_enable** (YES/NO): cal generar logs de les connexions realitzades.
- **xferlog_file** (/var/log/vsftpd.log): ubicació i nom del fitxer de logs
- **xferlog_std_format** (YES/NO): format de missatges estàndard.

Bànners i missatges

Se sol mostrar un missatge de benvinguda als usuaris.

Es poden afegir fitxers .message on el contingut es mostrarà automàticament en forma de capçalera quan l'usuari accedeixi al directori.