Documentación Técnica Completa de Servicios

Este documento contiene la documentación técnica organizada, clara y explicativa de los siguientes servicios:

1. **Servidor FTP (vsftpd)**
2. **Servidor RADIUS (FreeRADIUS)**
3. **Servidor de Correo (Postfix + Dovecot)**

Cada sección explica el propósito de cada comando, la razón técnica detrás de cada ajuste y la lógica del flujo de configuración.

---

1. Documentación Técnica — Servidor FTP (vsftpd)

Un servidor FTP (File Transfer Protocol) es un servicio que permite la transferencia estructurada y segura de archivos entre equipos dentro de una red. En un entorno empresarial, la implementación de un servidor FTP es fundamental cuando se requiere almacenar, compartir o distribuir archivos de manera centralizada entre diferentes departamentos o usuarios.
El servidor vsftpd, conocido por su estabilidad y alto nivel de seguridad, es ideal para organizaciones que necesitan un mecanismo confiable para manejar documentos internos, respaldos, desarrollos o distribuciones de software.
Las implementación dentro de DITECA usa este servicio gracias a que ofrece:

- Acceso controlado por usuarios locales, garantizando seguridad.
- Transferencias rápidas y estables incluso con grandes volúmenes de datos.
- Modo pasivo, que facilita la conectividad detrás de firewalls.
- Facilidad de administración, lo que reduce costos operativos.

1.1 Instalación y actualización del sistema

```
sudo apt update && sudo apt upgrade -y
```

Actualiza la lista de paquetes y aplica actualizaciones de seguridad.

```
sudo apt install vsftpd -y
```

Instala el servidor FTP "Very Secure FTP Daemon".

```
systemctl status vsftpd
sudo systemctl enable --now vsftpd
```

Verifica si el servicio está activo y lo habilita para que inicie automáticamente.

1.2 Configuración del archivo /etc/vsftpd.conf

Se edita el archivo principal de configuración:

```
sudo nano /etc/vsftpd.conf
```

Ajustes principales: - **listen=YES** → Indica que vsftpd escucha en IPv4. - **listen_ipv6=NO** → Desactiva IPv6 para evitar conflicto. - **anonymous_enable=NO** → Deshabilita accesos anónimos. - **local_enable=YES** → Permite usuarios locales. - **write_enable=YES** → Permite subir archivos. -

local_umask=022 → Establece permisos por defecto. - **ftpd_banner=...** → Mensaje de bienvenida opcional.

Activación del modo pasivo

```
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=40100
pasv_address=(IP DEL SERVIDOR)
```

Permiten conexiones PASV y definen el rango de puertos a usar.

1.3 Reinicio del servicio

```
sudo systemctl restart vsftpd
systemctl status vsftpd
```

Aplica cambios y verifica el estado.

1.4 Creación de usuario FTP

```
sudo adduser ftpuser
```

Crea un usuario dedicado para FTP.

Creación de carpetas y permisos:

```
sudo mkdir -p /home/ftpuser/ftp
sudo chown ftpuser:ftpuser /home/ftpuser/ftp
```

Garantiza acceso seguro al usuario.

1.5 Configuración del Firewall (UFW)

```
sudo ufw enable
sudo ufw allow 21/tcp
sudo ufw allow 20/tcp
sudo ufw allow 40000:40100/tcp
sudo ufw reload
```

Abre puertos requeridos para FTP activo y pasivo.

1.6 Comando de verificación

```
ss -tlnp | grep :21
```

Muestra si el servicio está escuchando en el puerto 21.

1.7 Troubleshoot avanzado

Incluye comandos para garantizar permisos y estructura del servicio.

```
sudo grep -q '^allow_writeable_chroot=' /etc/vsftpd.conf || echo
'allow_writeable_chroot=YES' | sudo tee -a /etc/vsftpd.conf
sudo mkdir -p /var/run/vsftpd
sudo touch
/var/run/vsftpd/empty
sudo chown root:root /var/run/vsftpd /var/run/vsftpd/empty
sudo chmod 755 /var/run/vsftpd /var/run/vsftpd/empty
sudo apt install -y dos2unix
sudo dos2unix /etc/vsftpd.conf
sudo systemctl daemon-reload
sudo systemctl restart vsftpd
```

Corrigen errores comunes como: - directorios inexistentes - permisos incorrectos - incompatibilidad de formato de archivo

---

2. Documentación Técnica — Servidor RADIUS (FreeRADIUS)

2.1 Instalación de dependencias

```
sudo apt-get install tasksel
sudo tasksel
```

Permite instalar servicios adicionales (Apache, etc.) si son requeridos.

```
sudo apt-get install freeradius
```

Instala FreeRADIUS.

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación centralizada utilizado para validar usuarios y dispositivos que intentan acceder a una red o servicio. En entornos empresariales, FreeRADIUS es uno de los servidores más utilizados gracias a su robustez, escalabilidad y compatibilidad con routers, switches y puntos de acceso Wi-Fi empresariales.

Dentro de DITECA implementaremos RADIUS, siendo una parte clave porque permite:

- Controlar quién accede a la red, evitando conexiones no autorizadas.
- Unificar la autenticación desde un servidor central.
- Aumentar la seguridad en redes Wi-Fi, especialmente en empresas con múltiples empleados.
- Registrar intentos de acceso, permitiendo auditorías y trazabilidad.

Con RADIUS, las organizaciones pueden implementar seguridad empresarial como WPA2/WPA3-Enterprise, garantizando que cada usuario posea credenciales únicas y seguras.

2.2 Configuración de usuarios

Edición del archivo de usuarios:

```
sudo nano /etc/freeradius
```

Se agregan líneas con estructura:

```
usuario Cleartext-Password :=
"contraseña" Reply-Message = "mensaje
opcional"
```

Define usuarios válidos para autenticación.

2.3 Configuración de clientes

Archivo:

```
sudo nano /etc/freeradius/3.0/clients.conf
```

Entrada típica:

```
client 192.168.1.1 {
    secret =
    SRug2021
    shortname = FreeRadius-UG
}
```

Indica: - **IP del dispositivo** que usará Radius (AP o router) - **secret** → clave compartida - **shortname** → identificador

---

2.4 Iniciar y reiniciar servicio

```
sudo service freeradius start
sudo service freeradius
restart
```

Activa el servidor.

2.5 Prueba de autenticación

Comando:

```
sudo radtest usuario contraseña IPcliente 1812 secreto
```

Ejemplo:

```
sudo radtest yeinel TngoSueno45 192.168.1.1 1812 SRug2021
```

Debe devolver 3 líneas “Access-Accept”.

2.6 Configuración del AP

- Se ingresa al gateway (ej: 192.168.1.1)
- Ajustes → WiFi → Seguridad empresarial WPA2
- Parámetros:
- **WPA2 + AES**
- **IP del servidor RADIUS**: IP del equipo Ubuntu
- **Puerto**: 1812
- **Contraseña radius**: SRug2021

---

3. Documentación Técnica — Servidor de Correo (Postfix + Dovecot)

Un servidor de correo permite a una empresa manejar internamente el envío, recepción y almacenamiento de correos electrónicos utilizando un dominio corporativo propio (ejemplo: usuario@midominio.local). Postfix se encarga del envío y distribución de correos (SMTP), mientras que Dovecot gestiona la recepción y acceso a los buzones mediante IMAP o POP3.
Implementaremos un servidor de correo empresarial, el cual nos ofrece múltiples ventajas tales como:

- Control total sobre la mensajería corporativa.
- Mayor seguridad y privacidad al no depender de plataformas externas.
- Personalización del dominio, lo que fortalece la identidad empresarial.
- Posibilidad de integrar filtros, backups y políticas internas.
- Acceso seguro mediante TLS y autenticación centralizada.

Un servidor de correo interno es esencial para empresas que requieren comunicaciones confiables, privadas y con control administrativo completo.

3.1 Actualización del sistema

```
sudo apt update && sudo apt upgrade -y
```

Mantiene el sistema preparado para instalación.

3.2 Instalación de Postfix y Dovecot

```
sudo apt install postfix dovecot-core dovecot-imapd dovecot-pop3d -y
```

Incluye soporte SMTP (Postfix) y POP3/IMAP (Dovecot).

Configuración inicial: - Tipo: *Internet Site* - Nombre: *mail.midominio.local*

3.3 Archivo /etc/mailname

```
sudo nano /etc/mailname
```

Define el dominio del servidor.

3.4 Certificados TLS

```
sudo openssl req -new -x509 -days 3650 -nodes -out ...
```

Crea un certificado autofirmado para cifrar conexiones.

Permisos:

```
sudo chmod 600 /etc/ssl/private/mail.key.pem
```

Seguridad máxima para la clave privada.

3.5 Configuración principal de Postfix

Archivo:

```
sudo nano /etc/postfix/main.cf
```

Parámetros clave: - **myhostname**, **myorigin**, **mydestination** → Identidad del servidor. - **home_mailbox = Maildir/** → Usa formato moderno Maildir. - **TLS** habilitado mediante:

```
smtpd_tls_cert_file=...
smtpd_tls_key_file=...
smtpd_use_tls=yes
```

Habilitación del puerto 587

```
sudo nano /etc/postfix/master.cf
```

Se habilita "submission" para clientes autenticados.

3.6 Crear usuario de correo

```
sudo adduser prueba
```

Usuario almacenará su buzón en /home/prueba/Maildir.

3.7 Configuración de Dovecot

Maildir

```
mail_location = maildir:~/Maildir
```

Autenticación

```
disable_plaintext_auth = yes
auth_mechanisms = plain login
```

Integración Postfix ↔ Dovecot

Socket de autenticación:

```
unix_listener /var/spool/postfix/private/auth {
  mode = 0660
  user = postfix
  group = postfix
}
```

Certificados

Dovecot usa los mismos certificados para IMAP/POP3.

3.8 Pruebas

Envío

```
swaks --to prueba@mail.midominio.local ...
```

Ver recepción

```
ls -l /home/prueba/Maildir/new
```

Pruebas TLS

```
openssl s_client -connect localhost:993
```

3.9 Integración con Thunderbird

Incluye puertos, métodos de autenticación y configuración manual.
