Configuración Automática de Servidores con Ansible

Este documento describe el uso de Ansible para la automatización de la configuración de un servidor DNS, un servidor FTP y la creación de usuarios y certificados en un entorno Debian.

Resumen

El archivo de Ansible tiene los siguientes objetivos:

1. Configurar un servidor DNS (`Bind9`) con autoridad sobre el dominio `sistema.sol`.
2. Crear usuarios con directorios y archivos predeterminados.
3. Configurar e instalar un servidor FTP seguro (`vsftpd`), incluyendo conexiones anónimas y autenticadas.
4. Generar claves y certificados SSL para asegurar las comunicaciones.
5. Reiniciar y validar los servicios configurados.

Estructura de Tareas

Configuración del Servidor DNS

- **Actualizar lista de paquetes**: Se asegura de que la lista de paquetes esté actualizada antes de instalar `Bind9`.

```
- name: Actualizar lista de paquetes
  ansible.builtin.package:
    update_cache: true
```

- **Instalación de Bind9**: Se instalan los paquetes necesarios para el servicio DNS.

```
- name: Instalar Bind9
  ansible.builtin.package:
    name:
      - bind9
      - bind9-utils
      - bind9-doc
```

- **Copia de archivos de configuración**: Se copian archivos personalizados para configurar las zonas DNS y los archivos de opciones.

```
- name: Configurar Bind9 conf
  ansible.builtin.copy:
    src: ../dns/named.conf.local
    dest: /etc/bind
```

- **Reinicio**: Se reinicia el servicio `bind9` para aplicar los cambios.

```
- name: Reiniciar servicio Bind9
  systemd:
    name: bind9
    enabled: true
    state: restarted
```

Configuración de Usuarios y Directorios

- **Creación de usuarios**: Se crean usuarios con sus respectivos directorios y contraseñas cifradas.

```
- name: Crear usuario "luis"
  ansible.builtin.user:
    name: luis
    shell: /bin/bash
    create_home: yes
    password: "<hash>"
```

- **Copia de archivos**: Se copian los archivos de usuario a sus respectivos directorios para facilitar el acceso a información preconfigurada.

```
- name: Copiar los archivos "luis1.txt" y "luis2.txt"
  ansible.builtin.copy:
    src: ../usuarios/luis/
    dest: /home/luis
```

Configuración del Servidor FTP Seguro

- **Instalación de vsftpd**: Se instala el paquete `vsftpd` para el servicio FTP.

```
- name: Instalar vsftpd
  ansible.builtin.package:
    name:
      - vsftpd
```

- **Archivo de configuración**: Se copia un archivo personalizado `vsftpd.conf` con las configuraciones necesarias para el servidor.

```
- name: Copiar archivo vsftpd.conf
  ansible.builtin.copy:
    src: ../vsftpd/vsftpd.conf
    dest: /etc/
```

- **Certificados SSL**: Se generan claves y certificados autofirmados para asegurar las conexiones.

```
- name: Generar clave privada
  command:
    cmd: openssl genrsa -out /etc/ssl/private/sri.key 2048
```

- **Configuración de usuarios no enjaulados**: Se define una lista de usuarios que no estarán restringidos a su directorio `home`.

```
- name: Lista de usuarios no enjaulados
  ansible.builtin.copy:
    src: ../vsftpd/vsftpd.chroot_list
    dest: /etc/
```

- **Reinicio del servicio**: Se reinicia el servicio `vsftpd` para aplicar los cambios.

```
- name: Reiniciar servicio
  systemd:
    name: vsftpd
    enabled: true
    state: restarted
```

Configuración de un Servidor DNS y Prueba de Resolución

Este documento explica los pasos para configurar un servidor DNS maestro en un entorno basado en Debian. Se incluye la configuración de zonas directas e inversas, así como la validación de su funcionamiento.

Requisitos Previos

1. **Red configurada en el rango 192.168.X.0/24.**
2. **Acceso a una máquina virtual Debian llamada tierra para actuar como servidor DNS.**
3. **Las otras máquinas virtuales (mercurio, venus, marte) configuradas con sus respectivas direcciones IP y nombres de dominio.**

Pasos para Configurar el Servidor DNS

1. **Preparar el Sistema**

```
Instalar el paquete bind9 en Debian:
sudo apt update
sudo apt install bind9
```

2. **Archivos de Configuración**

```
Crear el archivo de configuración de la zona directa
(/var/lib/bind/db.sistema.sol):
```

```
$ORIGIN sistema.sol.
$TTL    86400
@   IN  SOA  tierra.sistema.sol. root.sistema.sol. (
            1     ; Serial
        604800     ; Refresh
        86400     ; Retry
        2419200     ; Expire
        86400 )   ; Negative Cache TTL
;
@       IN  NS    tierra.sistema.sol.
tierra  IN  A     192.168.56.103
mercurio IN  A    192.168.56.101
venus   IN  A     192.168.56.102
marte   IN  A     192.168.56.104
ftp     IN  CNAME tierra
```

```
Crear el archivo de configuración de la zona inversa (/var/lib/bind/db.192.168.56):
```

```
$ORIGIN 56.168.192.in-addr.arpa.
$TTL    86400
@   IN  SOA  tierra.sistema.sol. root.sistema.sol. (
            1     ; Serial
        604800     ; Refresh
        86400     ; Retry
        2419200     ; Expire
        86400 )   ; Negative Cache TTL
;
@       IN  NS    tierra.sistema.sol.
101     IN  PTR   mercurio.sistema.sol.
102     IN  PTR   venus.sistema.sol.
103     IN  PTR   tierra.sistema.sol.
```

```
104     IN  PTR   marte.sistema.sol.
```

3. **Actualizar el Archivo de Configuración Principal** Modificar /etc/bind/named.conf.local para incluir las zonas:

```
zone "sistema.sol" {
    type master;
    file "/var/lib/bind/db.sistema.sol";
};
```

```
zone "56.168.192.in-addr.arpa" {
    type master;
    file "/var/lib/bind/db.192.168.56";
};
```

4. **Configuración Adicional** Editar /etc/bind/named.conf.options para agregar un reenviador:

```
options {
    directory "/var/cache/bind";
    forwarders {
        1.1.1.1;
    };
    dnssec-validation no;
    listen-on-v6 { any; };
};
```

5. **Reiniciar el Servicio DNS** Verificar y reiniciar el servicio:

```
sudo named-checkconf
sudo named-checkzone sistema.sol /var/lib/bind/db.sistema.sol
sudo named-checkzone 56.168.192.in-addr.arpa /var/lib/bind/db.192.168.56
sudo systemctl restart bind9
```

Prueba del Servidor DNS

1. **En las máquinas clientes, configurar /etc/resolv.conf para usar tierra como servidor DNS:**

```
nameserver 192.168.56.103
search sistema.sol
```

2. **Probar la resolución directa:**

```
dig @192.168.56.103 tierra.sistema.sol
```

3. **Probar la resolución inversa:**

```
dig -x 192.168.56.103 @192.168.56.103
```

Configuración de vsftpd.conf

Este archivo README explica las configuraciones del archivo `vsftpd.conf` que es usado para configurar el servidor **vsftpd** (Very Secure FTP Daemon), un servidor FTP ligero y seguro.

1. Archivo vsftpd.conf

Este archivo contiene una configuración personalizada y avanzada para un servidor FTP en el dominio `sistema.sol`.

Principales configuraciones:

1. Modo de operación del servidor:

- `listen=YES`: Configura el servidor como independiente (standalone) y lo habilita para conexiones IPv4.
- `listen_ipv6=NO`: No habilita soporte para IPv6 en esta configuración.

2. Mensajes personalizados:

- `ftpd_banner="--- Welcome to the FTP server of 'sistema.sol' ---"`: Mensaje de bienvenida al conectarse.
- `dirmessage_enable=YES`: Activa mensajes personalizados en directorios (archivos `.message`).

3. Permitir usuarios anónimos y configuraciones:

- `anonymous_enable=YES`: Permite acceso anónimo.
- `anon_upload_enable=NO`: No permite a usuarios anónimos subir archivos.
- `anon_other_write_enable=NO`: No permite a usuarios anónimos realizar modificaciones (el acceso es solo de lectura).

4. Control de usuarios locales:

- `local_enable=YES`: Permite el acceso a usuarios locales.
- `write_enable=YES`: Permite a los usuarios locales subir y modificar archivos.

- `chroot_local_user=YES`: Enjaula a los usuarios locales en sus directorios personales.
- `chroot_list_enable=YES`: Excluye de la restricción a usuarios listados en `/etc/vsftpd.chroot_list`.

5. Restricciones de ancho de banda y conexiones:

- `local_max_rate=5242880`: Límite de velocidad para usuarios locales (5 MB/s).
- `anon_max_rate=2097152`: Límite de velocidad para usuarios anónimos (2 MB/s).
- `max_clients=15`: Máximo de 15 clientes conectados simultáneamente.

6. Tiempo de espera:

- `idle_session_timeout=720`: Cierra la sesión tras 720 segundos de inactividad.

7. Configuración de seguridad (FTPS):

- `ssl_enable=YES`: Habilita FTPS (FTP con SSL/TLS).
- `force_local_data_ssl=YES` y `force_local_logins_ssl=YES`: Obliga a que todas las conexiones locales sean cifradas.
- `rsa_cert_file` y `rsa_private_key_file`: Especifica los certificados SSL utilizados.

Configuración de vsftpd

Comprobación del servidor creado

Paso 1: Configuración inicial en FileZilla, ingresando el servidor, nombre de usuario y puerto.

[Paso 1] | *../images/vstfpdinfo/1.png*

Paso 2: Confirmación del certificado del servidor, verificando la autenticidad y aceptándolo.

[Paso 2] | *../images/vstfpdinfo/2.png*

Paso 3: Transferencia exitosa de un archivo desde el servidor remoto al cliente local.

[Paso 3] | *../images/vstfpdinfo/3.png*

Paso 4: Conexión al servidor FTP con credenciales específicas.

[Paso 4] | *../images/vstfpdinfo/4.png*

Paso 5: Uso de la terminal para conectarse al servidor FTP como usuario `luis` y listar los archivos disponibles.

[Paso 5] | *../images/vstfpdinfo/5.png*

Paso 6: Conexión al servidor FTP como usuario `maria`, navegando entre directorios y listando carpetas.

[Paso 6] | *../images/vstfpdinfo/6.png*

Paso 7: Conexión al servidor FTP en modo anónimo, mostrando acceso limitado a los directorios públicos.

[Paso 7] | *../images/vstfpdinfo/7.png*

2. Uso y propósito de los archivos:

- **vsftpd.conf**: Archivo personalizado para un entorno productivo en el servidor de `sistema.sol`.
- **vsftpd.conf.bak**: Archivo de respaldo con configuraciones predeterminadas, útiles para entender las opciones básicas y como referencia para crear una configuración propia.

3. Cómo usar estos archivos:

1. Configurar `vsftpd.conf`:

1. Copiar el archivo en `/etc/vsftpd.conf`.
2. Ajustar las rutas de los certificados (`rsa_cert_file` y `rsa_private_key_file`) si difieren en tu sistema.
3. Crear o editar `/etc/vsftpd.chroot_list` para definir usuarios excluidos del enjaulamiento.

2. Revertir a `vsftpd.conf.bak`:

1. Usar este archivo como plantilla básica para restaurar una configuración mínima.
2. Renombrarlo como `vsftpd.conf` y adaptarlo según sea necesario.
3. Recomendaciones de seguridad:
    - Usar FTPS siempre que sea posible (`ssl_enable=YES`).
    - Limitar el acceso anónimo a solo lectura o deshabilitarlo por completo.
    - Usar listas de control (`chroot_list_enable=YES`) para definir excepciones de acceso.

3. Comandos útiles:

Iniciar/Detener/Restaurar el servicio:

```
sudo systemctl start vsftpd
sudo systemctl stop vsftpd
sudo systemctl restart vsftpd
```

Verificar estado del servicio:

```
sudo systemctl status vsftpd
```

Probar la conexión FTP:

```
ftp localhost
```

Ejercicio 2.2

1. Verificar si pftp está instalado

Comando para verificar si está instalado:

```
which pftp
```

- Si el comando muestra una ruta como `/usr/bin/pftp`, significa que está instalado.
- Si no está instalado, el comando no devolverá ningún resultado.

Instalar pftp si no está instalado:

En sistemas basados en Debian/Ubuntu:

```
sudo apt update
sudo apt install ftp
```

2. Configurar el archivo `~/.netrc` para conexiones automáticas

1. **Crear o editar el archivo `~/.netrc`:**

   ```
   nano ~/.netrc
   ```

2. **Agregar la configuración de un servidor FTP:**

   ```
   Escribe en el archivo la siguiente estructura para cada servidor al que quieras
   conectarte:
   ```

   ```
   machine <nombre_del_servidor>
   login <usuario>
   password <contraseña>
   ```

3. **Guardar y salir del archivo:**
   - En **nano**, presiona:
   - `Ctrl + O` para guardar los cambios.
   - Luego, presiona `Enter` para confirmar.
   - Finalmente, `Ctrl + X` para salir.
4. **Asegurar que el archivo tiene permisos restringidos (seguridad):**

   ```
   Ejecuta el siguiente comando para garantizar que solo el propietario pueda acceder
   al archivo:
   ```

   ```
   chmod 600 ~/.netrc
   ```

3. Probar la conexión automática

Después de configurar el archivo `~/.netrc`, puedes conectarte automáticamente al servidor sin ingresar credenciales manualmente.

Usar pftp:

```
pftp tierra.sistema.sol
```

Ejericio 2.3

1. Establecer conexión anónima al servidor `ftp.cica.es` desde `tierra.sistema.sol`

Usa el comando `ftp` para conectarte de forma anónima:

```
ftp ftp.cica.es
```

2. Examinar el directorio actual en el servidor

Después de conectarte al servidor, utiliza el siguiente comando para ver el directorio actual:

```
pwd
```

3. Examinar el directorio actual en el cliente

Para ver el directorio actual del cliente (tu máquina local) mientras estás conectado al servidor FTP, usa:

```
!pwd
```

4. Listar los archivos en el servidor

Para ver los archivos y carpetas en el directorio actual del servidor FTP, utiliza:

```
ls
```

5. Listar los archivos en el cliente

Para listar los archivos en el directorio actual de tu máquina local (cliente) mientras estás conectado al servidor FTP, usa:

```
!ls
```

6. Descargar `/pub/check` del servidor al cliente

Usa el comando `get` para descargar un archivo desde el servidor FTP a tu máquina local:

```
cd /pub
get check
```

7. Crear el directorio imágenes en el cliente dentro de pruebasFTP

Para crear un directorio en el cliente:

1. Sal de la sesión FTP temporalmente con `!`:

```
!mkdir -p pruebasFTP/imágenes
```

2. Confirma que se creó el directorio usando:

```
!ls pruebasFTP
```

8. Subir el archivo datos1.txt al servidor

Asegúrate de que el archivo `datos1.txt` exista en el cliente. Luego, usa el comando `put` para subirlo al servidor:

```
put datos1.txt
```

9. Cerrar la conexión

Para salir de la sesión FTP, usa:

```
bye
```

Uso de Cliente Gráfico para FTP

Paso 1: Abrir FileZilla

Comando para instalar FileZilla en sistemas basados en Debian/Ubuntu. Usa el comando `sudo apt install filezilla`.

Paso 2: Interfaz inicial de FileZilla

Al abrir FileZilla, verás la interfaz inicial donde podrás configurar los parámetros para conectar a un servidor FTP.

[Paso 2] | *../images/gráfico/2.png*

Paso 3: Configuración de un nuevo sitio FTP

Para configurar un nuevo sitio FTP en FileZilla, ingresa el host (`ftp.rediris.es`), selecciona el tipo de cifrado y habilita el acceso anónimo si es necesario.

[Paso 3] | *../images/gráfico/3.png*

Paso 4: Advertencia sobre conexión insegura

Al conectar al servidor, FileZilla mostrará una advertencia sobre el uso de FTP sin cifrado (inseguro). Si es necesario, puedes aceptar y continuar con la conexión.

[Paso 4] | *../images/gráfico/4.png*

Paso 5: Estado de la conexión al servidor

El estado de la conexión al servidor FTP se verifica y se muestra que la conexión ha sido exitosa.

[Paso 5] | *../images/gráfico/5.png*

Paso 6: Transferencia de archivos desde el cliente

En este paso, se transfiere un archivo (`welcome.msg`) desde el servidor FTP a tu cliente local.

[Paso 6] | *../images/gráfico/6.png*

Paso 7: Exploración de los archivos en el cliente

Después de la transferencia, el archivo (`welcome.msg`) aparece en tu sistema local y se puede abrir en un editor de texto.

[Paso 7] | *../images/gráfico/7.png*

Paso 8: Navegación en los directorios del cliente y servidor

Aquí puedes ver la vista comparativa de los directorios locales y remotos en FileZilla, destacando la transferencia completada.

[Paso 8] | *../images/gráfico/8.png*

Paso 9: Servicios reiniciados en el sistema

En esta imagen, se muestran los servicios que se reinician después de la instalación o actualización del software.

[Paso 9] | *../images/gráfico/9.png*

Paso 10: Resultado final

El proceso finaliza con éxito, mostrando que FileZilla está configurado y listo para gestionar conexiones FTP.

[Paso 10] | *../images/gráfico/10.png*

Preguntas

a. ¿Qué modo ha usado el cliente (activo o pasivo) al descargar el listado de archivos del servidor?

FileZilla, por defecto, utiliza el **modo pasivo** para las conexiones FTP. En este modo, el cliente inicia la conexión tanto para los comandos como para la transferencia de datos, lo cual es útil cuando hay cortafuegos o routers NAT en el camino.

b. ¿Cuál es la IP del servidor de ftp.rediris.es?

La IP del servidor `ftp.rediris.es` es **130.206.13.2**.

c. ¿De los 6 dígitos que aparecen en el mensaje 227 "Entering Passive Mode (...) qué significan los 2 últimos números?

En el mensaje **227 Entering Passive Mode (192,0,2,1,104,31)**, los dos últimos números **104** y **31** representan el puerto remoto para la conexión de datos pasiva. Estos números corresponden al puerto **(104 * 256 + 31 = 26719)**, que es el puerto utilizado para la transferencia de datos en modo pasivo.