CLOCKWORK COMPUTER

SAMBA AD DC WINDOWS 10

Implementación de un servidor Samba AD DC en Ubuntu Server y unión de un equipo Windows 10

En esta práctica, aprenderás a configurar un servidor Samba AD DC (Active Directory Domain Controller) en Ubuntu Server y a unir un equipo Windows 10 al dominio.

Objetivos:

- Configurar un servidor Ubuntu Server como controlador de dominio Samba AD.
- Unir un equipo Windows 10 al dominio Samba AD.
- Administrar usuarios y grupos en el dominio Samba AD.

Tareas:

1. **Preparación del servidor:**
    - Cambiar el nombre del servidor.
    - Configurar el archivo /etc/hosts.
    - Configurar la resolución de nombres con Samba como servidor DNS interno.
    - Instalar Samba y sus dependencias.
2. **Configuración de Samba AD DC:**
    - Crear un dominio Samba AD.
    - Configurar el servidor como controlador de dominio.
    - Sincronizar la hora con el servicio chrony.
3. **Verificación de Samba AD DC:**
    - Verificar los nombres de dominio y la resolución DNS.
    - Verificar los registros de servicio Kerberos y LDAP.
    - Autenticarse en el servidor Kerberos.
    - Conectarse al recurso compartido netlogon.
    - Cambiar la contraseña del usuario administrador.
    - Verificar el nivel de dominio de Windows AD DC.
4. **Administración de usuarios y grupos:**
    - Crear un nuevo usuario.
    - Listar los usuarios existentes.
    - Eliminar un usuario.
    - Listar los equipos unidos al dominio.
    - Eliminar un equipo del dominio.
    - Crear un nuevo grupo.
    - Listar los grupos existentes.
    - Listar los miembros de un grupo.
    - Agregar un usuario a un grupo.
    - Eliminar un usuario de un grupo.
5. **Unión de un equipo Windows 10 al dominio:**
    - Unir el equipo al dominio CLOCKWORK.LOCAL.
    - Verificar la unión al dominio.

Los comandos empleados en la práctica los encontraréis AQUÍ.

💻🔗 ¡Bienvenido a esta guía paso a paso para implementar un Controlador de Dominio Active Directory (AD DC) con Samba en Ubuntu Server y unir un equipo Windows 10 al dominio Samba AD DC! 🌟

En esta práctica aprenderemos a configurar un servidor Ubuntu como un Controlador de Dominio Active Directory utilizando Samba. Además, aprenderás cómo instalar y configurar NTPDATE para sincronizar el tiempo en el dominio, y cómo unir un equipo Windows 10 al dominio implementado en el AD DC de Samba.

¿Qué es Samba AD DC?

Samba es una implementación de software libre del protocolo SMB/CIFS que permite compartir archivos e impresoras entre sistemas operativos Windows y Linux. Un Controlador de Dominio Active Directory (AD DC) con Samba es una solución que proporciona funcionalidades de un dominio de Windows compatible con el protocolo Active Directory en sistemas Linux.

Pasos Detallados:

🛠️ **Instalación y Configuración de Samba AD DC:**

Configura tu servidor Ubuntu para actuar como un Controlador de Dominio Active Directory utilizando Samba.

🕒 **Instalación y Configuración de NTPDATE:**

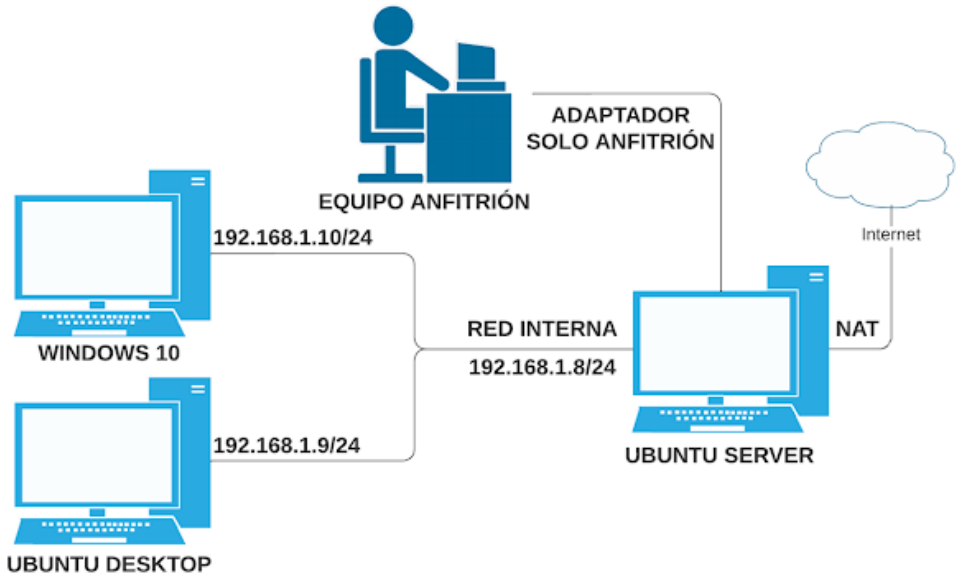
Instala y configura NTPDATE para sincronizar el tiempo en el dominio, garantizando una sincronización precisa entre los equipos del dominio.

💻 **Unión de un Equipo Windows 10 al Dominio Samba AD DC:**

Sigue los pasos para unir un equipo Windows 10 al dominio implementado en el AD DC de Samba, permitiendo la autenticación y gestión centralizada de usuarios y recursos.

Cada paso está explicado en detalle y acompañado de comandos específicos, diseñados para que cualquier usuario pueda seguir el proceso con facilidad.

La estructura de red empleada para la práctica es la siguiente.



Veamos en detalle qué es AD DC SAMBA.

Active Directory Domain Controller (AD DC) Samba es una implementación de código abierto del controlador de dominio de Microsoft Active Directory. Esta tecnología permite a los administradores de sistemas crear y gestionar dominios de red, así como proporcionar servicios de autenticación y autorización para usuarios, grupos y recursos en una red.

En términos más simples, un AD DC Samba es una herramienta que permite a las organizaciones crear y administrar un entorno de red seguro y centralizado. Proporciona funciones clave, como la gestión de cuentas de usuario, la autenticación de acceso a recursos de red y la configuración de políticas de seguridad.

Al implementar un AD DC Samba, las organizaciones pueden lograr los siguientes beneficios:

- **Centralización de la gestión de usuarios y recursos:** Todos los usuarios, grupos y recursos de red pueden ser gestionados desde un solo lugar, lo que facilita la administración y el mantenimiento.
- **Autenticación y autorización centralizadas:** Los usuarios pueden iniciar sesión en cualquier recurso de red utilizando las mismas credenciales de inicio de sesión, lo que simplifica el acceso y mejora la seguridad.
- **Implementación de políticas de seguridad:** Los administradores pueden establecer políticas de seguridad coherentes en toda la red, como contraseñas complejas, restricciones de acceso y auditorías de eventos.
- **Compatibilidad con aplicaciones y servicios de Microsoft:** Un AD DC Samba puede interoperar con sistemas Windows y proporcionar servicios de directorio compatibles con Microsoft Active Directory.

¡Sigue esta guía y configura tu servidor Ubuntu como un Controlador de Dominio Active Directory con Samba, y únete a un equipo Windows 10 al dominio para una gestión centralizada y segura de tus recursos de red! 🔒🌐

Preparación del servidor

1. Cambiar el nombre del servidor:

sudo hostnamectl set-hostname dc

Explicación:

- El comando hostnamectl se usa para configurar el nombre del servidor.
- El parámetro set-hostname establece el nombre del servidor a "dc".

2. Modificar el archivo hosts:

sudo nano /etc/hosts
192.168.1.8 dc.clockwork.local dc
Explicación:

- El archivo /etc/hosts mapea nombres de dominio a direcciones IP.
- Agregamos la línea 192.168.1.8 dc.clockwork.local dc para que el nombre de dominio dc.clockwork.local se resuelva a la dirección IP 192.168.1.8.

3. Verificar el FQDN:

hostname -f

Explicación:

- El comando hostname -f muestra el nombre de dominio completo (FQDN) del servidor.
- El FQDN debe ser dc.clockwork.local.

4. Verificar si el FQDN resuelve la dirección IP:

ping -c2 dc.clockwork.local

Explicación:

- El comando ping verifica si un host está activo.
- El parámetro -c2 envía dos paquetes ping.
- Si el comando responde con dos "Respuesta desde dc.clockwork.local", el FQDN se resuelve correctamente.

5. Desactivar el servicio systemd-resolved:

sudo systemctl disable --now systemd-resolved

Explicación:

- El servicio systemd-resolved administra la resolución de nombres de dominio.
- Lo desactivamos porque Samba AD DC necesita control total sobre la resolución de nombres.

6. Eliminar el enlace simbólico al archivo /etc/resolv.conf:

sudo unlink /etc/resolv.conf

Explicación:

- El archivo /etc/resolv.conf contiene la configuración de resolución de nombres.
- Eliminamos el enlace simbólico para poder configurar manualmente el archivo.

7. Crear el archivo /etc/resolv.conf:

sudo nano /etc/resolv.conf

Explicación:

- Creamos un nuevo archivo /etc/resolv.conf para configurar manualmente la resolución de nombres.

8. Agregar las siguientes líneas al archivo:

nameserver 192.168.1.8
nameserver 8.8.8.8
search clockwork.local
Explicación:

- Configuramos el servidor DNS principal como la dirección IP del servidor Samba AD DC (192.168.1.8).
- Añadimos el servidor DNS público de Google (8.8.8.8) como servidor DNS secundario.
- Configuramos el dominio de búsqueda como clockwork.local.

9. Hacer inmutable el archivo /etc/resolv.conf:

sudo chattr +i /etc/resolv.conf

Explicación:

- El comando chattr +i hace que el archivo sea inmutable, lo que significa que no se puede modificar accidentalmente.

Instalación de Samba

1. Actualizar el índice de paquetes:

sudo apt update

Explicación:

- El comando apt update actualiza la información de los paquetes disponibles.

2. Instalar Samba y sus dependencias:

sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony net-tools

CLOCKWORK.LOCAL
dc.clockwork.local
dc.clockwork.local
Explicación:

- El comando apt install instala Samba y todos los paquetes necesarios para su funcionamiento, incluyendo:
    - acl: Soporte para listas de control de acceso (ACL).
    - attr: Soporte para atributos extendidos de archivos.
    - samba: Implementación del protocolo SMB/CIFS.
    - samba-dsdb-modules: Módulos de la base de datos de Samba.
    - samba-vfs-modules: Módulos del sistema de archivos virtual de Samba.
    - smbclient: Cliente SMB para acceder a recursos compartidos.
    - winbind: Integración de Samba con Active Directory.
    - libpam-winbind: Módulo PAM para la autenticación con winbind.
    - libnss-winbind: Módulo NSS para la resolución de nombres con winbind.
    - libpam-krb5: Módulo PAM para la autenticación con Kerberos.
    - krb5-config: Configuraciones de Kerberos 5.
    - krb5-user: Soporte para usuarios de Kerberos 5.
    - dnsutils: Utilidades para la resolución de nombres.
    - chrony: Servidor de sincronización de tiempo.
    - net-tools: Utilidades de red.

3. Detención y deshabilitación de servicios innecesarios:

sudo systemctl disable --now smbd nmbd winbind

El comando detiene y deshabilita los servicios smbd, nmbd y winbind. Estos servicios no son necesarios para un servidor **Active Directory** de Samba, ya que:

- **smbd:** Es el demonio principal de Samba que proporciona el servicio de archivos e impresoras SMB/CIFS.
- **nmbd:** Es el demonio de nombres NetBIOS que facilita la resolución de nombres entre equipos Windows.
- **winbind:** Integra Samba con la API de Windows NT, lo que permite la autenticación de usuarios y grupos de Windows.

En un servidor **Active Directory**, la autenticación y el control de acceso se administran mediante Kerberos, por lo que no se necesitan winbind ni nmbd.

Explicación del comando:

- sudo: Otorga privilegios administrativos para ejecutar el comando.

- systemctl: Controla el sistema de inicio y gestión de servicios.
- disable: Deshabilita el inicio automático del servicio al arrancar el sistema.
- --now: Detiene el servicio inmediatamente si está en ejecución.
- smbd nmbd winbind: Especifica los nombres de los servicios a deshabilitar.

4. Habilitación del servicio Samba Active Directory:

sudo systemctl unmask samba-ad-dc
sudo systemctl enable samba-ad-dc

El servicio samba-ad-dc es el componente central de Samba para la funcionalidad de **Active Directory**. Se habilita con los siguientes comandos:

- sudo systemctl unmask samba-ad-dc: Elimina la máscara del servicio, que lo hace visible para el administrador de servicios.
- sudo systemctl enable samba-ad-dc: Habilita el inicio automático del servicio al arrancar el sistema.

5. Crear una copia de seguridad del archivo /etc/samba/smb.conf

sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig

Explicación:

El comando crea una copia de seguridad del archivo de configuración de Samba original /etc/samba/smb.conf.

Motivo:

Es importante realizar una copia de seguridad del archivo original antes de realizar cambios, ya que el proceso de aprovisionamiento de Samba Active Directory puede modificar la configuración. En caso de algún problema, se puede restaurar la configuración original.

Explicación del comando:

- sudo: Otorga privilegios administrativos para ejecutar el comando.
- mv: Mueve un archivo o directorio a otra ubicación.
- /etc/samba/smb.conf: Ruta del archivo de configuración original de Samba.
- /etc/samba/smb.conf.orig: Ruta de la copia de seguridad del archivo de configuración.

6. Configurar el dominio y el servidor de Samba AD:

sudo samba-tool domain provision

Realm: CLOCKWORK.LOCAL (Presiona Enter)
Domain: CLOCKWORK (Presiona Enter)
Server Role: dc (Presiona Enter)
DNS backend: SAMBA_INTERNAL (Presiona Enter)
DNS forwarder IP address: 8.8.8.8 (Presiona Enter)
Explicación:

- Responde a las preguntas del asistente samba-tool domain provision con la siguiente información:
    - **Realm:** El nombre de tu dominio (CLOCKWORK.LOCAL).
    - **Domain:** El nombre de tu dominio NetBIOS (CLOCKWORK).
    - **Server Role:** El rol del servidor (dc para controlador de dominio).
    - **DNS backend:** El backend DNS (SAMBA_INTERNAL para usar DNS interno de Samba).
    - **DNS forwarder IP address:** La dirección IP de un servidor DNS público (8.8.8.8 para Google DNS).

7. Crear una copia de seguridad del archivo de configuración predeterminado de Kerberos:

sudo mv /etc/krb5.conf /etc/krb5.conf.orig

Explicación:

- Hacemos una copia de seguridad del archivo de configuración de Kerberos original.

8. Reemplazar con el archivo generado por Samba:

sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf

Explicación:

- Copiamos el archivo de configuración de Kerberos generado por Samba a la ubicación correcta.

9. Iniciar el servicio Samba Active Directory:

sudo systemctl start samba-ad-dc

Explicación:

- Iniciamos el servicio Samba Active Directory.

10. Comprobar el estado del servicio:

sudo systemctl status samba-ad-dc

Explicación:

- Verificamos que el servicio Samba Active Directory esté funcionando correctamente.

Configuración de sincronización de tiempo

1. Cambiar permisos del directorio ntp_signd:

sudo chown root:_chrony /var/lib/samba/ntp_signd/

sudo chmod 750 /var/lib/samba/ntp_signd/

Explicación:

- Configuramos los permisos necesarios para la sincronización de tiempo con chrony.

2. Modificar el archivo de configuración de chrony:

sudo nano /etc/chrony/chrony.conf

Explicación:

- Abrimos el archivo de configuración de chrony para editarlo.

3. Agregar las siguientes líneas:

bindcmdaddress 192.168.1.8
allow 192.168.1.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
Explicación:

- Configuramos chrony como servidor NTP y definimos la ubicación del socket para la sincronización con Samba.

4. Reiniciar y verificar el servicio chronyd:

sudo systemctl restart chronyd

sudo systemctl status chronyd

Explicación:

- Reiniciamos el servicio chronyd y verificamos su estado.

Verificación de Samba Active Directory

1. Verificar nombres de dominio:

host -t A clockwork.local

host -t A dc.clockwork.local

Explicación:

- Verificamos que los nombres de dominio se resuelven correctamente.

2. Verificar registros de servicio Kerberos y LDAP:

host -t SRV _kerberos._udp.clockwork.local

host -t SRV _ldap._tcp.clockwork.local

Explicación:

- Verificamos que los registros de servicio Kerberos y LDAP apunten al servidor Samba AD DC.

3. Verificar recursos predeterminados:

smbclient -L clockwork.local -N

Explicación:

- Listamos los recursos compartidos disponibles en Samba Active Directory.

4. Autenticarse en Kerberos:

kinit administrator@CLOCKWORK.LOCAL
klist
Explicación:

- Nos autenticamos en el servidor Kerberos con el usuario administrador.
- El comando klist muestra los tickets de Kerberos obtenidos.

5. Conectarse al recurso compartido netlogon:

sudo smbclient //localhost/netlogon -U 'administrator'

Explicación:

- Nos conectamos al recurso compartido netlogon usando la cuenta de administrador.

6. Cambiar contraseña del usuario administrador:

sudo samba-tool user setpassword administrator

Explicación:

- Cambiamos la contraseña del usuario administrador por motivos de seguridad.

7. Verificar la integridad del archivo de configuración:

testparm

Explicación:

- Verificamos que el archivo de configuración de Samba no tenga errores.

8. Verificar el nivel de dominio de Windows AD DC:

sudo samba-tool domain level show

Explicación:

- Mostramos el nivel de dominio de Windows AD DC.

Administración de usuarios y grupos en Samba AD DC

Crear un usuario:

sudo samba-tool user create clockworker

Explicación:

- Creamos un nuevo usuario llamado clockworker.

Listar usuarios:

sudo samba-tool user list

Explicación:

- Mostramos una lista de todos los usuarios del dominio.

Eliminar un usuario:

samba-tool user delete <nombre_del_usuario>

Explicación:

- Eliminamos un usuario del dominio.

Listar equipos:

sudo samba-tool computer list

Explicación:

- Mostramos una lista de todos los equipos unidos al dominio.

Eliminar un equipo:

sudo samba-tool computer delete <nombre_del_equipo>

Explicación:

- Eliminamos un equipo del dominio.

Crear un grupo:

samba-tool group add <nombre_del_grupo>

Explicación:

- Creamos un nuevo grupo en el dominio.

Listar grupos:

sudo samba-tool group list

Explicación:

- Mostramos una lista de todos los grupos del dominio.

Listar miembros de un grupo:

sudo samba-tool group listmembers 'Domain Admins'

Explicación:

- Mostramos una lista de los miembros del grupo Domain Admins.

Agregar un miembro a un grupo:

sudo samba-tool group addmembers <nombre_del_grupo> <nombre_del_usuario>

Explicación:

- Agregamos un usuario a un grupo.

Eliminar un miembro de un grupo:

sudo samba-tool group removemembers <nombre_del_grupo> <nombre_del_usuario>

Explicación:

- Eliminamos un usuario de un grupo.

Unión de un equipo Windows 10 al dominio

1. En el equipo Windows 10:

- Abrir "Sistema" -> "Configuración avanzada del sistema" -> "Nombre del equipo, nombre de dominio y configuración de la red".
- Hacer clic en "Cambiar".
- Seleccionar "Unirse a un dominio".
- Introducir el nombre del dominio: CLOCKWORK.LOCAL.
- Hacer clic en "Siguiente".
- Introducir las credenciales de un usuario con permisos para unir equipos al dominio (por ejemplo, el administrator).
- Hacer clic en "Aceptar".
- Reiniciar el equipo.

2. Verificación de la unión al dominio:

- En el equipo Windows 10, abrir "Símbolo del sistema".
- Escribir el comando whoami /all.
- Verificar que el dominio se muestra en la información del usuario.