



# Implementación de un Active Directory Domain Controller en GNU/Linux con Samba 4

# ¿Quién es fraterneo?

- Hijo, esposo, padre...
- Entusiasta y divulgador de GNU/Linux y el FLOSS (2006)
- Blogger (2007)
- Informático egresado de la UASD (2008)
- Editor en Muy Linux (2010-2011)
- Charlista/conferencista (2012)
- Coordinador del FLISOL 2012 Santiago
- Grupo Popular (2012)
- Instructor en FCLD (2014)
- Editor en SambaWiki (2023)

☒ AVANZADO

INTERMEDIO

BÁSICO

# Contenido

- ¿Qué es Active Directory?
- Términos relacionados
- Requerimientos de hardware
- Requerimientos de software
- Alternativas
- ¿Qué es Samba?
- Soporte AD en Samba 4
- Infraestructura
- Componentes adicionales
- SELinux y Firewall
- Preparación del servidor
- Comandos #
- Ficheros de configuración
- Administración
- Azure AD Connect
- Nuestro lab (escenario)
- Recursos Web
- Comentarios y preguntas
- Contacto

# ¿Qué es Active Directory?

- Es un servicio de directorios (organización de usuarios, equipos, y otros recursos de red) basado en LDAP para redes Windows.
- Fue una mejora considerable con respecto a Windows NT.
- Disponible desde Windows 2000/2003 Server.
- Ofrece seguridad de Dominio, Forests, etc.
- Muy flexible gracias a Group Policy y otras funcionalidades (roles, features).

# Términos relacionados

- **Realm** (Ámbito de actuación)
- **Schema** (Esquema)
- **KDC** (Key Distribution Server)
- **FSMO** (Flexible Single Master Operations)
- **DC** (Domain Controller, Domain Component)
- **OU** (Organizational Unit)
- **GPO** (Group Policy)

# Términos relacionados

- **Functional Levels:**
  - Domain functional levels:
    - MS Windows 2008 R2
  - Forest functional levels
    - MS Windows 2008 R2
  - Schema
    - MS Windows 2012 R2

# Requerimientos de hardware

## Hardware

CPU

RAM

Disco

## Mínimo

Quad-core, 2.83 GHz

4 GB

500 GB

## Recomendado

Core i7, 3.20 GHz

8 GB

1 TB



# Requerimientos de software

- Distribución GNU/Linux
  - RHEL: Almalinux 9 boot (Rocky Linux, CentOS Stream)
  - Fedora
  - Debian (Ubuntu y otros derivados)
- Samba 4
- Bind 9 (con soporte DLZ)
- DHCP
- NTP
- Kerberos
- SSSD

# Alternativas

- **Samba 4**
- OpenLDAP
- ApacheDS
- FreeIPA
- 389 Directory Server
- OpenDJ
- jumpcloud

# ¿Qué es Samba?

- Implementación del protocolo SMB (CIFS).
- Desarrollado por Andrew Tridgell en 1992.
- Escrito en C, C++ y Python.
- Multiplataforma (Unix, Linux, Solaris, BSD, OS X Server).
- Libre bajo licencia GNU Lesser GPLv3.
- Problemas de seguridad en 3.6.3.
- Microsoft contribuyó código fuente del protocolo SMB3 (luego de sentencia de Comisión Europea).

# Soporte AD desde Samba 4.0

- Puede actuar como PDC o hacer join en un Windows AD existente como DC o RODC.
- Uso de Group Policy, Roaming Profiles, Print Server, Shared Folders, etc.
- Fácil de administrar desde Windows con RSAT o Webmin, SWAT (descontinuado), PowerShell.
- Los clientes Windows se unen de forma transparente.
- Unir clientes GNU/Linux (Likewise Open, winbind, realm, samba domain join) con fines administrativos y de autenticación.

# Infraestructura

- **DNS Backend:**
  - SAMBA\_INTERNAL : Servidor de nombres interno.
  - BIND\_FLATFILE : DNS en ficheros texto plano (descontinuado).
  - **BIND9\_DLZ** : **DNS en bases de datos (LDB).**
  - NONE : Sin DNS (No recomendado).

# Infraestructura

- NTP o Chrony (sincronización del tiempo)
- DHCP (asignación automática configuración de red y actualización dinámica del DNS)
- Kerberos (autenticación transparente)
- Heimdal KDC distribución de tokens
- LDAP como backend AD
- Seguridad:
  - Firewall (iptables o firewalld)
  - SELinux, Apparmor (requieren mucho tiempo de troubleshooting), TCP Wrappers, directivas en el fichero smb.conf

- **Servidor Secundario:**
  - Replicación de Active Directory, Bind y SysVol
  - DHCP failover
  - Kerberos, NTP y SSSD
  - Print Server (CUPS)
  - File Server (SMB/CIFS, NFS, FTP, SFTP, etc.)

# Componentes adicionales

- Proxy Cache Squid, en modo Intercepción o con Autenticación LDAP
- LTSP (Linux Terminal Server)
- Servidor RIS (PXE, WDS)
- Otros servicios disponibles en GNU/Linux
  - Apache (web)
  - Bacula (backup)
  - Postfix, Dovecot (mail)
  - Etc, etc.



- **Modos de operación**
  - Enforcing (se hacen cumplir las políticas de seguridad)
  - **Permissive (emite mensajes cuando se infringe una política)**
  - Disabled (deshabilitado)
- **Fichero de configuración**
  - `/etc/selinux/config`

# Firewall

- **Firewalld**
  - `firewall-cmd`
- **iptables**
  - `systemctl disable firewalld.service`
  - `systemctl mask firewalld.service`
  - `dnf install -y iptables-utils iptables-services`

# Preparación del servidor

- **Instalación de Samba 4**

```
# ./configure.developer --bindir=/bin/ --sbindir=/sbin/ --sysconffdir=/etc/samba/ --  
prefix=/var/lib/samba/ --mandir=/usr/share/man/
```

- **Instalación de Bind 9**

```
# groupadd -g 2500 named  
# useradd -c "Bind 9" -g named -u 2500 -d /var/named -s /sbin/nologin named  
# ./configure --sysconffdir=/etc/named --localstatedir=/var/named --with-gssapi=yes
```

- **Instalación de NTP 4**

```
# groupadd -g 8700 ntp &&  
# useradd -c "NTP 4" -d /var/lib/ntp -u 8700 -g ntp -s /sbin/nologin ntp  
# ./configure --enable-ntp-signd
```

# Comandos #

- **Crear un Dominio o unirse a uno existente**
  - `samba-tool domain provision --interactive`
  - `samba-tool domain join options`
- **Administración de usuarios y contraseñas**
  - `kinit <administrator>@<realm>`
  - `klist`
  - `kpasswd`
  - `wbinfo`
  - `samba-tool user setpassword usuario`
- **Consulta DNS y otros**
  - `smbclient`
  - `host`, `nslookup`, `dig`, `samba_dnupdate`

# Ficheros de configuración

- **Samba**
  - `/etc/samba/smb.conf`
- **Bind**
  - `/etc/named/named.conf`
  - `/var/lib/samba/private/named.conf`
- **Kerberos**
  - `/etc/krb5.conf`

# Ficheros de configuración

- **DHCP**
  - `/etc/dhcp/dhcpd.conf`
- **NTP**
  - `/etc/ntp.conf`
- **SSSD**
  - `/etc/sss/sssd.conf`

# Administración

- **MS Windows Remote Server Administration Tools (RSAT)**
  - Instalar en un cliente Windows
  - Iniciar sesión DOMAIN\administrator
- **Webmin**
  - Interfaz web
  - Disponible en los repositorios
- **Cockpit (cockpit-samba-ad-dc)**
  - Presentado en sambaXP 2021
  - Fedora (copr), Debian/Ubuntu
- **CLI (samba-tool, wbinfo, kinit, net)**
  - Disponibles nativamente

# Azure AD Connect

- Sincronizar usuarios, grupos, equipos, GPO, etc.
- Configurar un ambiente híbrido integrando nuestro Active Directory on-premises con Azure Active Directory, aplicaciones de Microsoft 365 y otras.
- NO es una herramienta de migración o backup.
- Reemplazó a DirSync y Azure AD Sync.



# Nuestro lab (escenario)

- **Servidor Primario**

Sistema Operativo	:	Almalinux 9.2 x86_64 boot
Realm (NetBIOS)	:	FCLD.LOCAL
Domain	:	fld
FQDN	:	sambapdc01.fld.local.
Interfaz enp1s0	:	192.168.122.15/24 (WAN)
Interfaz enp2s0	:	10.42.0.1/24 (LAN)

# Nuestro lab (escenario)

- **Servidor Secundario**

Sistema Operativo	:	Almalinux 9.2 x86_64 boot
Realm (NetBIOS)	:	FCLD.LOCAL
Domain	:	fldc
FQDN	:	sambapdc02.fldc.local.
Interfaz enp1s0	:	10.42.0.3/24 (LAN)

# Nuestro lab (escenario)

- **Cliente Windows**

Sistema Operativo	:	MS Windows 10 con RSAT
FQDN	:	windows10.fcid.local.
Interfaz de red	:	10.42.0.10 (LAN)

- **Cliente Linux**

Sistema Operativo	:	Ubuntu 22.02
FQDN	:	ubuntu.fcid.local.
Interfaz de red	:	10.42.0.11 (LAN)

# Recursos web

- <http://almalinux.org/>
- <http://www.samba.org/>
- [https://wiki.samba.org/index.php/Main\\_Page](https://wiki.samba.org/index.php/Main_Page)
- <https://www.isc.org/downloads/bind/>
- <http://bind-dlz.sourceforge.net/>
- <http://www.ntp.org/>
- <http://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>
- <https://www.microsoft.com/en-us/download/details.aspx?id=45520>
- [https://wiki.samba.org/index.php/Azure\\_AD\\_Sync](https://wiki.samba.org/index.php/Azure_AD_Sync)
- <https://www.firstattribute.com/en/news/azure-ad-connect/>

# Comentarios, preguntas y sugerencias...

¿...?

# Contacto

