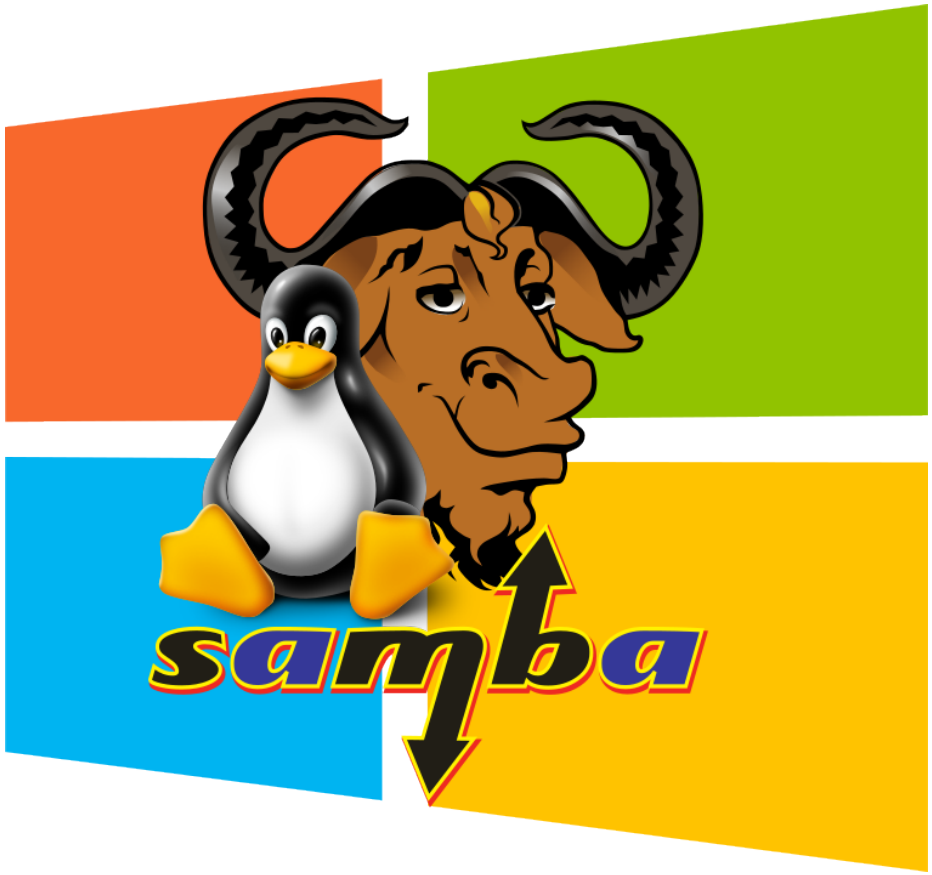

Implementación de un Active Directory Domain Controller en GNU/Linux con Samba 4

¿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 2011-2013 Santiago
- Grupo Popular (2012)
- Instructor en FCLD (2014)
- Editor en SambaWiki (2023)
- Cybersecurity Master UAPA (2024...)

Nivel...

☑ AVANZADO

INTERMEDIO

BÁSICO

Contenido

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

¿Qué es Active Directory?

- Es un servicio de directorios (organización de usuarios, equipos, y otros recursos de red) basado en LDAP y SMB para redes Windows.
- El protocolo SMB (Server Message Block) es un protocolo de comunicación cliente-servidor que se utiliza para el acceso compartido a archivos, directorios, impresoras, puertos serie y otros recursos de una red. También proporciona un mecanismo de comunicación entre procesos (IPC) autenticado.
- 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).
- En la actualidad es más robusto gracias a los Roles and 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

Alternativas

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

A pesar de éstas alternativas, un controlador de dominio Active Directory es un trabajo mejor realizado por un servidor de Microsoft Windows.

Requerimientos de hardware

Hardware	Mínimo	Servidor Infraestructura
CPU	Intel Celeron 1.50 GHz	Core i5, 3.20 GHz
RAM	4 GB	8 GB
Disco	300 GB	500 GB / 1 TB

Requerimientos de software

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

¿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.
- Functional Level 2016 dispobible desde Samba 4.19
- Soporte para Authentication Silos y Authentication Policies para Samba 4.20

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 (sincronización del tiempo)
- DHCP (asignación automática confiuración de red y actualización dinámica del DNS)
- Kerberos (autenticación transparente)
- SSSD (permite tratar usuarios y grupos locales como si fueran del dominio)
- 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

Infraestructura

- **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.

La distro...

☑ Almalinux

☑ Fedora

☑ Ubuntu

SELinux

- **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

Apparmor

Apparmor permite crear los perfiles para procesos y/o aplicaciones específicas de forma interactiva:

```
root@sambapdc01:~# /usr/local/bin/dhcp-dyndns.sh &
root@sambapdc01:~# aa-genprof /usr/local/bin/dhcp-dyndns.sh
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /usr/local/bin/dhcp-dyndns.sh.
Setting /usr/local/bin/dhcp-dyndns.sh to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /usr/local/bin/dhcp-dyndns.sh

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.
```

Firewall

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

Puertos activos

Service	Port	Protocol
DNS *	53	tcp/udp
Kerberos	88	tcp/udp
ntp **	123	udp
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Name Service	137	udp
NetBIOS Datagram	138	udp
NetBIOS Session	139	tcp
LDAP	389	tcp/udp
SMB over TCP	445	tcp
Kerberos kpasswd	464	tcp/udp
LDAPS ***	636	tcp
Global Catalog	3268	tcp
Global Catalog SSL ***	3269	tcp
Dynamic RPC Ports ****	49152-65535	tcp

https://wiki.samba.org/index.php/Samba_AD_DC_Port_Usage

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/sssd/sssd.conf`

Preparación del servidor

- **Instalación de software requerido, dependencias y librerías de desarrollo/compilación**

```
# dnf install -y rsync-daemon cockpit acpid rpcgen mlocate bash-completion nmap nano wget
git dhcp-server python3-dns make gcc rpm-build libtool autoconf openssl-devel libacl-devel
libblkid-devel gnutls-devel readline-devel platform-python-devel gdb pkgconfig
setroubleshoot-server setroubleshoot-plugins policycoreutils-python-utils python3-
libsemanage python3-cryptography python3-pyasn1 python3-ply python3-setools setools krb5-
server krb5-workstation popt-devel libxml2-devel libattr-devel keyutils-libs-devel cyrus-
sasl-devel libidn2-devel libsepol-devel openldap-clients perl perl-ExtUtils-MakeMaker perl-
Parse-Yapp perl-Test attr zlib-devel libaio-devel cups-devel libxslt docbook-style-xsl
openldap-devel pam-devel lmdb-devel gpgme-devel libarchive-devel python3-markdown libtasn1-
tools systemd-devel dbus-devel perl-JSON flex flex-devel jansson-devel bison sssd-ldap sssd-
krb5 gutenprint foomatic cups libcap-devel libuv-devel libnghttp2-devel
```

Preparación del servidor

- **Instalación de Samba 4**

```
# ./configure.developer --bindir=/bin/ --sbindir=/sbin/ --sysconfdir=/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 --sysconfdir=/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
```

Preparación del servidor

- **Configuración Bind (DNS)**

```
# rndc-confgen -a -c /etc/named/rndc.key

# nano /etc/named/named.conf
    ...
    ...
    include "/var/lib/samba/bind-dns/named.conf";
    include "/etc/named/rndc.key";
```

Preparación del servidor

- **Configuración de Kerberos**

```
# nano /etc/krb5.conf
     [libdefaults]
     default_realm = FCLD.LOCAL

     [realms]
      FCLD.LOCAL = {
       kdc = sambapdc01.fcld.local
       admin_server = sambapdc01.fcld.local
       default_domain = fcld.local
      }

     [domain_realm]
      .fcld.local = FCLD.LOCAL
      fcld.local = FCLD.LOCAL
      sambapdc01 = FCLD.LOCAL
```

Preparación del servidor

- **Configuración de NTP**

```
# nano /etc/ntp.conf
     #Samba NTP socket folder
     ntpsigndsocket  /var/lib/samba/var/lib/ntp_signd/
     server 10.42.0.1 iburst prefer
     ...
     ...
```

- **Configuración de DHCP**

```
# nano /etc/dhcp/dhcpd.conf
     option domain-name "fcld.local";
     option domain-name-servers  10.42.0.1, 94.140.14.15, 94.140.15.16;
     option netbios-name-servers 10.42.0.1;
     option ntp-servers 10.42.0.1;
     include "/etc/named/rndc.key";
     ...
     ...
```

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_dnsupdate`

Comandos

```
samba-tool domain provision \
--use-rfc2307 \
--realm=FCLD.LOCAL \
--domain=fcld \
--adminpass 'Solucion.123' \
--server-role=dc \
--option="ad dc functional level = 2016" \
--function-level=2016 \
--dns-backend=BIND9_DLZ
```

Agregar atributos RFC2307 a usuarios y grupos en el directorio LDAP.

Establece el nombre Kerberos del realm (todo en mayúsculas).

Establece el nombre del Dominio (todo en minúsculas).

Establece el password del usuario Administrator del dominio.

Establece el rol del sistema (dc=domain controller).

Establece la opción en el fichero smb.conf.

Establece el functional level del dominio.

Establece el backend del DNS (Bind 9 con soporte DLZ).

Servidor secundario

- **Configurar**
  - DNS para que apunte al primario
  - Kerberos para que apunte al primario
  - Bind será un servidor DNS adicional
  - DHCP failover/load balancing
  - SSSD y NTP configuraciones similares primario
  - Firewall, SELinux/Apparmor configuraciones similares
  - SysVol replication (ver guía en SambaWiki)

- **Unirse al dominio**
  - samba-tool domain join *fcld.local DC --dns-backend=BIND9_DLZ -U Administrator*

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.
- Desde el cambio a Entra ID, Azure AD Connect está descontinuado.

Nuestro lab (escenario)

- **Servidor Primario**

Sistema Operativo	:	Almalinux 9.2 x86_64 boot
Realm (NetBIOS)	:	FCLD.LOCAL
Domain	:	flcd
FQDN	:	sambapdc01.fcld.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	:	flcd
FQDN	:	sambapdc02.fcld.local.
Interfaz enp1s0	:	10.42.0.3/24 (LAN)

Nuestro lab (escenario)

- **Cliente Windows**

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

- **Cliente Linux**

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

Recursos web

- http://almalinux.org/
- https://ubuntu.com/server/docs
- http://www.samba.org/
- 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://www.firstattribute.com/en/news/azure-ad-connect/
- https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

Comentarios, preguntas y sugerencias...

¿...?

Contacto