Cómo configurar un Controlador de Dominio y Directorio Activo GNU/Linux con Samba4

Samba es una suite libre que, desde 1992, ha proveído servicios de archivos e impresión a todo tipo de clientes SMB/CIFS, incluyendo muchas versiones de Microsoft Windows. Samba está disponible libremente bajo licencia GNU General Public License.

Para los fines de esta guía se asume que ya tienes experiencia manejando servidor y clientes en un entorno Windows. Así como también experiencia con GNU/Linux, ya que no me detendré a explicar como usar el editor vi o el comando sed y herramientas como iptables, Selinux y los initscripts del sistema.

En el futuro próximo Samba se convertirá en una alternativa fiable, económica y robusta, que de la mano con GNU/Linux, encontrará su nicho las PyMES, y posiblemente empresas más grandes, para que las mismas puedan montar su estructura informática con Controlador de Dominio, Directorio Activo y los demás servicios que se pueden configurar en Linux como Proxy, Servidor Web, Base de Datos, etc.

Es un placer para mí ver cómo ha llegado a esta etapa luego de varios años recorridos.

SOTWARE QUE UTILIZAREMOS

- Centos 6.3 virtualizado en VirtualBox
- Samba 4.0.0
- Bind
- NTP
- DHCP
- Kerberos
- Librerías de desarrollo (make, gcc, python, openssl, etc.)

Manos a la obra...

INSTALAR EL SISTEMA OPERATIVO

CentOS 6.3 minimal en VirtualBox con dos interfaces de red y todo lo demás por defecto

- eth0 como NAT para tomar conexión a Internet (10.0.2.0/24)
- eth1 Bridged a la LAN del Dominio (192.168.5.0/24)

Al finalizar la instalación y loguearnos por primera vez en el servidor cambiamos el hostname del mismo.

```
[root@localhost ~]# sed -i 's/HOSTNAME=localhost.local/HOSTNAME=sambapdc01.mydomain.local/g' /etc/sysconfig/network
[root@localhost ~]# reboot
```

Al regresar, deshabilitamos Selinux para evitar inconvenientes hasta nuevo aviso.

```
[root@sambapdc01 ~]# sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
```

Configurarmos la Interfaz de red para actualizar y descargar paquetes. Esta interfaz está NAT en la

configuración de la máquina virtual, pero editaremos el script ya que no nos interesa que el dhclient nos genere el fichero resolv.conf.

```
[root@sambapdc01 ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="static"
HWADDR="MACADDR"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
DEFROUTE="yes"
IPADDR="10.0.2.15"
NETMASK="255.255.255.0"
GATEWAY="10.0.2.2"
```

Configurar la interfaz de red para el Dominio y red local, quedando de la siguiente manera.

```
[root@sambapdc01 ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE="eth1"
BOOTPROTO="static"
HWADDR="MACADDR"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
USERCTL="no"
IPV6INIT="no"
PEERDNS="no"
DEFROUTE="no"
DNS1="127.0.0.1"
IPADDR=192.168.5.1"
NETMASK="255.255.255.0"
```

Editamos el fichero resolv.conf para resolver nombres de Internet.

```
[root@sambapdc01 ~]# vi /etc/resolv.conf
nameserver 10.0.2.2
nameserver 8.8.8.8

[root@sambapdc01 ~]# service network restart
```

ACTUALIZAR EL SISTEMA: Instalar dependencias, librerías de desarrollo y compilación, y otros servicios.

```
[root@sambapdc01 ~]# rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
[root@sambapdc01 ~]# rpm -i http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
[root@sambapdc01 ~]# yum update -y
[root@sambapdc01 ~]# yum install -y bash-completion nano wget screen
[root@sambapdc01 ~]# yum install -y dhcp bind bind-libs bind-utils bind-sdb make gcc rpm-build libtool autoconf openssl-devel libacl-devel libblkid-devel gnutls-devel readline-devel python-devel gdb pkgconfig gtkhtml2 setroubleshoot-server setroubleshoot-plugins policycoreutils-python libsemanage-python setools-libs-python setools-libs krb5-server krb5-libs krb5-workstation
[root@sambapdc01 ~]# reboot
```

DESCARGAR, INSTALAR SAMBA4

```
[root@sambapdc01 ~]# mkdir /usr/src/samba4
[root@sambapdc01 ~]# cd /usr/src/samba4
[root@sambapdc01 samba4]# wget http://samba.org/samba/ftp/stable/samba-4.0.0.tar.gz
[root@sambapdc01 samba4]# tar zxvf samba-4.0.0.tar.gz
[root@sambapdc01 samba4]# cd samba-4.0.0/
[root@sambapdc01 samba-4.0.0]# ./configure.developer
[root@sambapdc01 samba-4.0.0]# make
[root@sambapdc01 samba-4.0.0]# make install
```

Agregar la ruta de Samba4 al PATH

```
[root@sambapdc01 samba-4.0.0]# cd
[root@sambapdc01 ~]# nano .bash_profile
PATH=$PATH:$HOME/bin:/usr/local/samba/bin:/usr/local/samba/sbin
[root@sambapdc01 ~]# source .bashrc
```

Verificamos que se instaló correctamente.

```
[root@sambapdc01 ~]# samba -V
Version 4.0.0
```

HACER LA PROVISIÓN DEL DOMINIO CON SAMBA4

```
[root@sambapdc01 ~]# samba-tool domain provision --realm=mydomain.local --domain=MYDOMAIN --adminpass 'solucion.123' --server-role=dc --dns-backend=BIND9_DLZ
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.5.1
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=mydomain,DC=local
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=mydomain,DC=local
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              sambapdc01
NetBIOS Domain:        MYDOMAIN
DNS Domain:            mydomain.local
DOMAIN SID:            S-1-5-21-1013276544-984874934-2418686943
A phpLDAPadmin configuration file suitable for administering the Samba 4 LDAP server has been created in /usr/local/samba/private/phpldapadmin-config.php.
```

IMPRESCINDIBLE: INICIAMOS SAMBA PARA QUE EL MISMO CREE LA ESTRUCTURA DE ARCHIVOS Y CARPETAS NECESARIAS PARA SU FUNCIONAMIENTO. ESTO OCURREN AL INICIARLO POR PRIMERA VEZ.

```
[root@sambapdc01 ~]# samba -i -M single &
[root@sambapdc01 ~]# killall samba
```

CONFIGURAR DHCP

```
[root@sambapdc01 ~]# vi /etc/dhcp/dhcpd.conf
option domain-name "mydomain.local";
option domain-name-servers  192.168.5.1, 8.8.8.8;
option netbios-name-servers 192.168.5.1;
option ntp-servers 192.168.5.1;
authoritative;
subnet 192.168.5.0 netmask 255.255.255.0 {
        range 192.168.5.10 192.168.5.20;
        option broadcast-address 192.168.5.255;
        option routers 192.168.5.1;
}
```

CONFIGURAR DNS (BIND). Es importante perder todo el tiempo necesario para que este servicio esté a punto, ya que el funcionamiento de Samba4 depende totalmente del mismo.

```
[root@sambapdc01 ~]# service named start
[root@sambapdc01 ~]# named -v
BIND 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6_3.5
[root@sambapdc01 ~]# service named stop
```

Editar el fichero /etc/named.conf

Borramos todo el contenido del mismo solo dejando lo siguiente:

```
[root@sambapdc01 ~]# nano /etc/named.conf
options {
        allow-query { localhost; 192.168.5.1; };
        allow-transfer { localhost; 192.168.5.1; };
        allow-recursion { localhost; 192.168.5.1; };
        forwarders {10.0.2.2; 8.8.8.8;};
        tkey-gssapi-keytab "/usr/local/samba/private/dns.keytab";
};
include "/usr/local/samba/private/named.conf";
[root@sambapdc01 ~]# service named restart
```

Si nos devuelve un error en el comando anterior o dura mucho tiempo para iniciar, generamos los Keys (opcionalmente, si da error para iniciar por falta de las llaves).

```
[root@sambapdc01 ~]# rndc-confgen -a -r /dev/urandom
[root@sambapdc01 ~]# chmod 766 /etc/rndc.key
[root@sambapdc01 ~]# ln -s /usr/local/samba/private/dns.keytab /etc/krb5.keytab
```

Editar el fichero resolv.conf

```
[root@sambapdc01 ~]# nano /etc/resolv.conf
domain mydomain.local
nameserver 192.168.5.1
```

CONFIGURAR KERBEROS

Editamos el fichero de configuración dejando solo lo siguiente.

```
[root@sambapdc01 ~]# nano /etc/krb5.conf
[libdefaults]
        default_realm = MYDOMAIN.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

DESCARGAR, INSTALAR Y CONFIGURAR NTP (OPCIONAL)

Si no hay sincronización de tiempo entre servidor y clientes, muchos servicios no estarán disponibles para éstos últimos. Necesitamos una versión de NTP igual o superior a la 4.2.6. Lamentablemente la versión actual de CentOS no la provee, por lo que la descargaremos del sitio rpmfind.net.

```
[root@sambapdc01 ~]# wget ftp://rpmfind.net/linux/sourceforge/f/fu/fuduntu/yum/2012/STABLE/RPMS/ntp-4.2.6p3-0.1.rc10.fc14.i686.rpm
[root@sambapdc01 ~]# wget ftp://rpmfind.net/linux/sourceforge/f/fu/fuduntu/yum/2012/STABLE/RPMS/ntpdate-4.2.6p3-0.1.rc10.fc14.i686.rpm
[root@sambapdc01 ~]# rpm -i ntpdate-4.2.6p3-0.1.rc10.fc14.i686.rpm
[root@sambapdc01 ~]# rpm -i ntp-4.2.6p3-0.1.rc10.fc14.i686.rpm
```

En el final del fichero agregamos estas dos líneas.

```
[r oot@sambapdc01 ~]# nano /etc/ntp.conf
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
restrict default mssntp
```

Editamos las siguientes líneas, que ya existen, para que queden así:

```
server 127.127.1.1
fudge 127.127.1.1  stratum 12
```

Finalmente cambiamos los servidores públicos por estos, sin opciones adicionales:

```
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
```

Aplicamos los permisos necesarios para que los servicios tengan acceso a los ficheros de configuración y Selinux no nos de problemas si lo habilitamos luego y poder hacer las pruebas de lugar.

Agregamos la variable de entorno MYREALM

```
[root@sambapdc01 ~]# echo 'MYREALM="mydomain.local"' >> .bash_profile
[root@sambapdc01 ~]# echo 'export MYREALM' >> .bash_profile
```

Aplicar permisos y crear políticas de Selinux (por si lo habilitamos luego)

```
[root@sambapdc01 ~]# chgrp ntp /usr/local/samba/var/lib/ntp_signd/
[root@sambapdc01 ~]# chown named:named /usr/local/samba/private/dns.keytab
[root@sambapdc01 ~]# chown named:named /usr/local/samba/private/named.conf
[root@sambapdc01 ~]# chmod 644 /usr/local/samba/private/dns.keytab
[root@sambapdc01 ~]# chmod 644 /usr/local/samba/private/named.conf
[root@sambapdc01 ~]# chown named:named /usr/local/samba/private/dns
[root@sambapdc01 ~]# chmod g+r /usr/local/samba/private/dns.keytab
[root@sambapdc01 ~]# chmod 775 /usr/local/samba/private/dns
[root@sambapdc01 ~]# chcon -t named_conf_t /usr/local/samba/private/dns.keytab
[root@sambapdc01 ~]# chcon -t named_conf_t /usr/local/samba/private/named.conf
[root@sambapdc01 ~]# chcon -t named_var_run_t /usr/local/samba/private/dns
[root@sambapdc01 ~]# chcon -t named_var_run_t /usr/local/samba/private/dns/${MYREALM}.zone
[root@sambapdc01 ~]# semanage fcontext -a -t named_conf_t /usr/local/samba/private/dns.keytab
[root@sambapdc01 ~]# semanage fcontext -a -t named_conf_t /usr/local/samba/private/named.conf
[root@sambapdc01 ~]# semanage fcontext -a -t named_conf_t /usr/local/samba/private/named.conf.update
[root@sambapdc01 ~]# semanage fcontext -a -t named_var_run_t /usr/local/samba/private/dns
[root@sambapdc01 ~]# semanage fcontext -a -t named_var_run_t /usr/local/samba/private/dns/${MYREALM}.zone
[root@sambapdc01 ~]# semanage fcontext -a -t named_var_run_t /usr/local/samba/private/dns/${MYREALM}.zone.jnl
[root@sambapdc01 ~]# semanage fcontext -a -t ntpd_t /usr/local/samba/var/run/ntp_signd
[root@sambapdc01 ~]# chcon -u system_u -t ntpd_t /usr/local/samba/var/run/ntp_signd
[root@sambapdc01 ~]# chcon -u system_u -t ntpd_t /usr/local/samba/var/run/
[root@sambapdc01 ~]# chcon -t ntpd_t /usr/local/samba/var/run/ntp_signd/socket
```

Es posible que en los comandos chcon anteriores obtengamos una salida de error como esta:

```
chcon: can't apply partial context to unlabeled file `/usr/local/samba/var/run/ntp_signd'
```

Por lo que crearemos una política para que nos permita el acceso.

```
[root@sambapdc01 ~]# nano samba4.te
module samba4 1.0;

require {
   type ntpd_t;
   type usr_t;
   type initrc_t;
   class sock_file write;
   class unix_stream_socket connectto;
}
#============= ntpd_t ==============
allow ntpd_t usr_t:sock_file write;

#============= ntpd_t ==============
allow ntpd_t initrc_t:unix_stream_socket connectto;
```

La revisamos y cargamos.

```
[root@sambapdc01 ~]# checkmodule -M -m -o samba4.mod samba4.te
checkmodule:            loading policy configuration from samba4.te
checkmodule:            policy configuration loaded
checkmodule:            writing binary representation (version 10) to samba4.mod
[root@sambapdc01 ~]# semodule_package -o samba4.pp -m samba4.mod
[root@sambapdc01 ~]# semodule -i samba4.pp
```

REINICIAMOS EL SISTEMA

```
[root@sambapdc01 ~]# reboot
```

PROBAMOS TODO PARA VERIFICAR QUE ESTAMOS BIEN

```
[root@sambapdc01 ~]# samba -i -M single &
[root@sambapdc01 ~]# service named start
[root@sambapdc01 ~]# service ntpd start
[root@sambapdc01 ~]# service dhcpd start
```

Probando Samba4

```
[root@sambapdc01 ~]# smbclient -L localhost -U%
Domain=[MYDOMAIN] OS=[Unix] Server=[Samba 4.0.0]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.0.0)
Domain=[MYDOMAIN] OS=[Unix] Server=[Samba 4.0.0]

        Server               Comment
        ---------            -------
        Workgroup            Master
        ---------            -------

[root@sambapdc01 ~]# smbclient //localhost/netlogon -UAdministrator%'solucion.123' -c 'ls'
Domain=[MYDOMAIN] OS=[Unix] Server=[Samba 4.0.0]
  .                                   D        0  Tue Nov 13 05:57:23 2012
  ..                                  D        0  Tue Nov 13 05:58:17 2012

                52475 blocks of size 131072. 36544 blocks available
```

Podemos visualizar los usuarios y grupos:

```
[root@sambapdc0a1 ~]# wbinfo -u
Administrator
Guest
krbtgt
dns-sambapdc01

[root@sambapdc01 ~]# wbinfo -g
Enterprise Read-Only Domain Controllers
Domain Admins
Domain Users
Domain Guests
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Group Policy Creator Owners
Read-Only Domain Controllers
DnsUpdateProxy


[root@sambapdc01 ~]# samba-tool dns query 127.0.0.1 mydomain.local @ ALL
Password for [administrator@MYDOMAIN.LOCAL]:
  Name=, Records=4, Children=0
    NS: sambapdc01.mydomain.local. (flags=600000f0, serial=1, ttl=900)
    A: 192.168.5.1 (flags=600000f0, serial=1, ttl=900)
    A: 10.0.2.15 (flags=600000f0, serial=1, ttl=900)
    SOA: serial=5, refresh=900, retry=600, expire=86400, ns=sambapdc01.mydomain.local., email=hostmaster.mydomain.local. (flags=600000f0, serial=4,
ttl=3600)
  Name=_msdcs, Records=0, Children=0
  Name=_sites, Records=0, Children=1
  Name=_tcp, Records=0, Children=4
  Name=_udp, Records=0, Children=2
  Name=DomainDnsZones, Records=0, Children=2
  Name=ForestDnsZones, Records=0, Children=2
  Name=sambapdc01, Records=2, Children=0
    A: 192.168.5.1 (flags=f0, serial=1, ttl=900)
    A: 10.0.2.15 (flags=f0, serial=4, ttl=900)
```

Probando DNS (BIND)

```
[root@sambapdc01 ~]# host -t SRV _ldap._tcp.mydomain.local.
_ldap._tcp.mydomain.local has SRV record 0 100 389 sambapdc01.mydomain.local.

[root@sambapdc01 ~]# host -t SRV _kerberos._udp.mydomain.local.
_kerberos._udp.mydomain.local has SRV record 0 100 88 sambapdc01.mydomain.local.

[root@sambapdc01 ~]# host -t A sambapdc01.mydomain.local.
sambapdc01.mydomain.local has address 10.0.2.15
sambapdc01.mydomain.local has address 192.168.5.1
```

Probando el DNS Dinámico

```
[root@sambapdc01 ~]# samba_dnsupdate --verbose --all-names
IPs: ['fe80::a00:27ff:fe4d:34be%eth0', 'fe80::a00:27ff:fec8:cc01%eth1', '192.168.5.1', '10.0.2.15']
Calling nsupdate for A mydomain.local 192.168.5.1
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
mydomain.local.         900     IN      A       192.168.5.1

Calling nsupdate for A sambapdc01.mydomain.local 192.168.5.1
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
sambapdc01.mydomain.local. 900  IN      A       192.168.5.1
```

```
Calling nsupdate for A gc._msdcs.mydomain.local 192.168.5.1
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
gc._msdcs.mydomain.local. 900   IN      A       192.168.5.1

Calling nsupdate for CNAME f17b9ee0-af5a-4585-bd35-f7d0928dbeb6._msdcs.mydomain.local sambapdc01.mydomain.local
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
f17b9ee0-af5a-4585-bd35-f7d0928dbeb6._msdcs.mydomain.local. 900 IN CNAME sambapdc01.mydomain.local.

Calling nsupdate for SRV _kpasswd._tcp.mydomain.local sambapdc01.mydomain.local 464
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kpasswd._tcp.mydomain.local. 900 IN    SRV     0 100 464 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kpasswd._udp.mydomain.local sambapdc01.mydomain.local 464
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kpasswd._udp.mydomain.local. 900 IN    SRV     0 100 464 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kerberos._tcp.mydomain.local sambapdc01.mydomain.local 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.mydomain.local. 900 IN   SRV     0 100 88 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kerberos._tcp.dc._msdcs.mydomain.local sambapdc01.mydomain.local 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.dc._msdcs.mydomain.local. 900 IN SRV 0 100 88 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kerberos._tcp.default-first-site-name._sites.mydomain.local sambapdc01.mydomain.local 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.default-first-site-name._sites.mydomain.local. 900 IN SRV 0 100 88 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kerberos._tcp.default-first-site-name._sites.dc._msdcs.mydomain.local sambapdc01.mydomain.local 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.default-first-site-name._sites.dc._msdcs.mydomain.local. 900 IN SRV 0 100 88 sambapdc01.mydomain.local.

Calling nsupdate for SRV _kerberos._udp.mydomain.local sambapdc01.mydomain.local 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._udp.mydomain.local. 900 IN   SRV     0 100 88 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.mydomain.local. 900  IN      SRV     0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.dc._msdcs.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
```

```
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.dc._msdcs.mydomain.local. 900 IN SRV 0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.gc._msdcs.mydomain.local sambapdc01.mydomain.local 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.gc._msdcs.mydomain.local. 900 IN SRV 0 100 3268 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.pdc._msdcs.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.pdc._msdcs.mydomain.local. 900 IN SRV 0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.mydomain.local. 900 IN SRV 0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.dc._msdcs.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.dc._msdcs.mydomain.local. 900 IN SRV 0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.gc._msdcs.mydomain.local sambapdc01.mydomain.local 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.gc._msdcs.mydomain.local. 900 IN SRV 0 100 3268 sambapdc01.mydomain.local.

Calling nsupdate for SRV _ldap._tcp.cda1bb16-ac5e-4c47-b520-144ae8e0193c.domains._msdcs.mydomain.local sambapdc01.mydomain.local 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.cda1bb16-ac5e-4c47-b520-144ae8e0193c.domains._msdcs.mydomain.local. 900 IN SRV 0 100 389 sambapdc01.mydomain.local.

Calling nsupdate for SRV _gc._tcp.mydomain.local sambapdc01.mydomain.local 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_gc._tcp.mydomain.local. 900    IN      SRV     0 100 3268 sambapdc01.mydomain.local.

Calling nsupdate for SRV _gc._tcp.default-first-site-name._sites.mydomain.local sambapdc01.mydomain.local 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_gc._tcp.default-first-site-name._sites.mydomain.local. 900 IN SRV 0 100 3268 sambapdc01.mydomain.local.

Calling nsupdate for A mydomain.local 10.0.2.15
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
mydomain.local.         900     IN      A       10.0.2.15

Calling nsupdate for A sambapdc01.mydomain.local 10.0.2.15
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
sambapdc01.mydomain.local. 900  IN      A       10.0.2.15
```

```
Calling nsupdate for A gc._msdcs.mydomain.local 10.0.2.15
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
gc._msdcs.mydomain.local. 900   IN      A       10.0.2.15
```

Probando Kerberos

```
[root@sambapdc01 ~]# kinit administrator@MYDOMAIN.LOCAL
Password for administrator@MYDOMAIN.LOCAL:
Warning: Your password will expire in 41 days on Tue Jan  5 00:01:50 2013

[root@sambapdc01 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@MYDOMAIN.LOCAL

Valid starting     Expires            Service principal
11/20/12 01:31:04  11/20/12 11:31:04  krbtgt/MYDOMAIN.LOCAL@MYDOMAIN.LOCAL
        renew until 11/21/12 01:31:00
```

CREAR EL SCRIPT PARA EL DAEMON DE SAMBA4

```
[root@sambapdc01 ~]# nano /etc/rc.d/init.d/samba4
 #! /bin/bash
 #
 # samba4       Bring up/down samba4 service
 #
 # chkconfig: - 90 10
 # description: Activates/Deactivates all samba4 interfaces configured to \
 #              start at boot time.
 #
 ### BEGIN INIT INFO
 # Provides:
 # Should-Start:
 # Short-Description: Bring up/down samba4
 # Description: Bring up/down samba4
 ### END INIT INFO
 # Source function library.
 . /etc/init.d/functions

 if [ -f /etc/sysconfig/samba4 ]; then
         . /etc/sysconfig/samba4
 fi

 CWD=$(pwd)
 prog="samba4"

 start() {
     # Attach irda device
     echo -n $"Starting $prog: "
         /usr/local/samba/sbin/samba
         sleep 2
         if ps ax | grep -v "grep" | grep -q /samba/sbin/samba ; then success $"samba4 startup"; else failure $"samba4 startup"; fi
     echo
 }
 stop() {
     # Stop service.
     echo -n $"Shutting down $prog: "
         killall samba
         sleep 2
         if ps ax | grep -v "grep" | grep -q /samba/sbin/samba ; then failure $"samba4 shutdown"; else success $"samba4 shutdown"; fi
     echo
 }
 status() {
         /usr/local/samba/sbin/samba --show-build
 }

 # See how we were called.
```

```
case "$1" in
start)
        start
    ;;
stop)
        stop
    ;;
status)
        status irattach
        ;;
restart|reload)
        stop
        start
        ;;
*)
    echo $"Usage: $0 {start|stop|restart|status}"
    exit 1
esac

exit 0
```

Le damos los permisos necesarios

```
[root@sambapdc01 ~]# chmod 755 /etc/init.d/samba4
```

ACTIVAMOS LOS SERVICIOS PARA QUE INICIEN EN EL ARRANQUE DEL SISTEMA

```
[root@sambapdc01 ~]# chkconfig samba4 --level 345 on
[root@sambapdc01 ~]# chkconfig dhcpd --level 345 on
[root@sambapdc01 ~]# chkconfig named --level 345 on
[root@sambapdc01 ~]# chkconfig ntpd --level 345 on
```

CONFIGURAR EL SERVIDOR PARA COMPARTIR CONEXIÓN A INTERNET. Esta parte es opcional, pero muy importante, sobre todo si luego queremos configurar un proxy como Squid para filtrar el contenido de navegación en la red local y mantener un cache de los datos de navegación de los usuarios.

```
[root@sambapdc01 ~]# iptables -F
[root@sambapdc01 ~]# iptables -P INPUT ACCEPT
[root@sambapdc01 ~]# iptables -P FORWARD ACCEPT
[root@sambapdc01 ~]# iptables -P OUTPUT ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -p icmp -j ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -i lo -j ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -i eth0 -j ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -i eth1 -j ACCEPT
[root@sambapdc01 ~]# iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
[root@sambapdc01 ~]# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
[root@sambapdc01 ~]# iptables -A FORWARD -p icmp -j ACCEPT
[root@sambapdc01 ~]# iptables -A FORWARD -i lo -j ACCEPT
[root@sambapdc01 ~]# iptables -A FORWARD -i eth0 -j ACCEPT
[root@sambapdc01 ~]# iptables -A FORWARD -i eth1 -j ACCEPT
[root@sambapdc01 ~]# iptables -A FORWARD -j REJECT --reject-with icmp-host-prohibited
[root@sambapdc01 ~]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@sambapdc01 ~]# service iptables save
[root@sambapdc01 ~]# service iptables restart
[root@sambapdc01 ~]# sed -i 's/net.ipv4.ip_forward = 0/net.ipv4.ip_forward = 1/g' /etc/sysctl.conf
[root@sambapdc01 ~]# sysctl -w
```

REINICIAMOS EL SISTEMA

```
[root@sambapdc01 ~]# init 6
```

COMPROBAR DESDE UN HOST DEL DOMINIO QUE EL SERVIDOR ESTA FUNCIONANDO

```
[root@rainbow ~]# nmap 192.168.5.1
Starting Nmap 5.51 ( http://nmap.org ) at 2012-11-25 16:16 AST
Nmap scan report for 192.168.5.1
Host is up (0.0055s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
111/tcp  open  rpcbind
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
636/tcp  open  ldapssl
1024/tcp open  kdm
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 08:00:27:70:DD:A9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

AUNQUE FALTAN ALGUNAS CONFIGURACIONES ADICIONALES PARA SU CORRECTO FUNCIONAMIENTO, YA NUESTRO CONTROLADOR DE DOMINIO ESTA LISTO PARA USARSE, POR LO QUE PODEMOS AGREGAR AL DOMINIO CLIENTES WINDOWS EN LA MISMA FORMA TRADICIONAL CON SERVIDORES WINDOWS.

CONFIGURAR UNA CARPETA COMPARTIDA

El proceso de provisión creó el archivo de configuración de Samba4 ubicado en /usr/local/samba/etc/smb.conf el cual no tiene recursos compartidos configurados. Así que agregaremos un recurso compartido a modo de prueba.

```
[root@sambapdc01 ~]# mkdir /root/Shared
[root@sambapdc01 ~]# nano /usr/local/samba/etc/smb.conf
[Shared]
    path = /root/Shared
    comment = Root's shared folder
    read only = yes
```

En las versiones anteriores de Samba4 es necesario reiniciar el servicio para que los compartidos se hagan visibles.

AGREGAR IMPRESORAS COMPARTIDAS

Podemos compartir las impresoras conectadas al servidor usando CUPS, y ya que Samba4 se comunica con CUPS vía sockets, no es necesario hacer configuración o dar permisos mas que escuchar la directiva del socket de CUPS.

```
[root@sambapdc01 ~]# mkdir /usr/local/samba/var/spool
[root@sambapdc01 ~]# chmod 1777 /usr/local/samba/var/spool
```

Editamos el fichero de configuración de Samba4 y agregamos lo siguiente.

```
[root@sambapdc01 ~]# /usr/local/samba/etc/smb.conf
[printers]
   path = /usr/local/samba/var/spool
   comment = All Printers
   browseable = Yes
   read only = No
   printable = Yes
```

Por conveniencia los clientes Windows pueden consultar el servidor que sirve las impresoras en busca de controladores. Para habilitar esta funcionalidad en Samba4 debemos crear el compartido especial print$.

```
[root@sambapdc01 ~]# mkdir -p /usr/local/samba/var/print/{COLOR,IA64,W32ALPHA,W32MIPS,W32PPC,W32X86,WIN40,x64}
[root@sambapdc01 ~]# nano /usr/local/samba/etc/smb.conf:
[print$]
   path = /usr/local/samba/var/print
   comment = Point and Print Printer Drivers
   read only = No
```

Nota: No es necesario reiniciar el daemon de Samba4

AGREGAR MAS USUARIOS AL ACTIVE DIRECTORY DE SAMBA4. Al contrario que en versiones anteriores, Samba4 no requiere un usuario local por cada usuario que creamos en Samba.

```
[root@sambapdc01 ~]# samba-tool user add fraterneo
New Password:
Retype Password:
User 'fraterneo' created successfully
```

Lo verificamos viendo su SID

```
[root@sambapdc01 ~]# wbinfo --name-to-sid fraterneo
S-1-5-21-4036476082-4153129556-3089177936-1005 SID_USER (1)
```

CONFIGURANDO ROAMING PROFILES

```
[root@sambapdc01 ~]# mkdir /usr/local/samba/var/profiles
```

Editamos el fichero de configuracion de Samba4 y agregamos lo siguiente.

```
[root@sambapdc01 ~]# nano /usr/local/samba/etc/smb.conf
[profiles]
    path = /usr/local/samba/var/profiles
    read only = No
```

En Windows usando RSAT vamos a Active Directory Users and Computers, seleccionamos todos lo usuarios, clic al botón derecho del mouse y abrimos Properties. Luego en la pestaña Profile, colocamos la siguiente ruta tal como está.

```
\\sambapdc01.mydomain.local\profiles\%USERNAME%
```

También hay que darle los permisos desde Windows a la carpeta profiles. Entramos como usuario administrator y aplicamos los permisos para que todos los usuarios puedan crear su profile en la forma típica como se hace en un servidor Windows.

PROBANDO SINCRONIZACION DEL TIEMPO. Desde un cliente Windows probamos que nuestro servidor esté sincronizando el tiempo.

```
C:\>w32tm /resync /rediscover
Enviando comando Resync a local computer...
El comando se ha completado correctamente.
```

Más recursos, herramientas y fuentes:
Samba4 Howto
Directorio Activo en Linux
Configuration of NTP for Samba4
Windows Support Tools
Windows Administration Tools Pack
Group Policy Management Console
Group Policy Central

Cómo configurar un Controlador de Dominio y Directorio Activo GNU/Linux con Samba4 by Claudio Concepción Certad is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License.