12/11/2019

INSTALLATION DE SAMBA

Agostini Charles, Didier Joël, Marjolet Louis, Vicente Vaz

GROUPE 3

INSTALLATION DE SAMBA

Samba peut être qualifié d'équivalent à Active Directory hébergé sur systèmes UNIX. Il permet notamment de pouvoir mettre en place une solution annuaires comparable à AD sur des parcs informatiques basés exclusivement sous systèmes UNIX.

La suite de ce document est en anglais.

TABLE DES MATIERES

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

Assurez vous d'utiliser DEBIAN 10 pour suivre ce tutoriel.

INSTALLATION

1) During the installation of Debian (not "Graphical Install", just "Install"), set the following :

- Language : English (US)

- Country: France

- Locale: en_US.UTF-8

- Hostname: S-TCOM-SMB01

- Domain: isec-telecom.local

- Root Password: SMBprincipal4321!

- Real Name for the new user: S-TCOM-SMB01-ADM

- Username for the new user: s-tcom-smb01-adm

- Password: SMBprincipal4321!

* Partitioning

** Select "Guided - Use full disk"

** "All Files in One Partition"

** "Finish Partitioning and Write Changes to Disk"

** You can choose either a CLI environment or GUI, but in a production environment, you may choose the CLI**

- Select the 'root' user and type in the password (SMBprincipal4321!):

```
su root
```

- Add the user 's-tcom-smb01-adm' to the sudoers file :

```
sudo usermod -aG sudo s-tcom-smb01-adm
```

- Go back to the 's-tcom-smb01-adm' user account:

```
su s-tcom-smb01-adm
```

- Open the file /etc/apt/sources.list as sudo and comment all the lines starting by : "deb cdrom:[Debian GNU]", then save the file

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

- Install all the required packages by issuing this command:

```
sudo apt install python perl acl xattr python-crypto attr autoconf gdb
bind9utils bison build-essential debhelper dnsutils docbook-xml docbook-xsl
flex gdb libjansson-dev libacl1-dev libaio-dev libarchive-dev libattr1-dev
libblkid-dev libbsd-dev libcap-dev libcups2-dev libgnutls28-dev libgpgme-
dev libjson-perl libldap2-dev libncurses5-dev libpam0g-dev libparse-yapp-
perl libpopt-dev libreadline-dev nettle-dev perl-modules-5.28 pkg-config
python-all-dev python-dev python-dbg python-dev python-dnspython python3-
dnspython python-gpg python3-gpg python-markdown python3-markdown python3-
dev xsltproc zlib1g-dev liblmdb-dev lmdb-utils docbook-xsl cups git
libsasl2-dev libaio-dev libpam-dev valgrind autoconf ldap-utils krb5-user
samba attr winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config
libgssrpc4 libkadm5clnt-mit11 libkadm5srv-mit11 libkdb5-9 libldb1
libtalloc2 libtdb1 libtevent0 libwbclient0 python-ldb python-samba python-
talloc python-tdb samba-common samba-common-bin samba-dsdb-modules samba-
libs samba-vfs-modules tdb-tools krb5-doc ldb-tools smbldap-tools ufw -y
```

- You'll get a prompt asking if you want to "modify smb.conf to use WINS settings from DHCP". Select <No>. You won't get any more prompts afterwards.

CONFIGURING THE NETWORK INTERFACE, HOSTNAME

- Once all packages are installed, open /etc/NetworkManager/NetworkManager.conf and add "dns=none" in the [main] section.

- Then, restart NetworkManager:

```
sudo service network-manager restart
```

We'll now manually configure the main network interface.

- Identify the name of the interface you want to configure by issuing the "ip link show" command. In my case, my interface is called "ens33"

- Next, open /etc/network/interfaces and add the following lines :

==========

auto ens33

iface ens33 inet static

address 192.168.31.5/24

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

gateway 192.168.31.2

dns-nameservers 10.96.23.51 1.1.1.1

==========

Explanation: as my main interface is ens33, I'll set its IP address to 192.168.31.5, the gateway of the network to 192.168.31.2 and the DNS Servers to 10.96.23.51 (Private CESI DNS, when connected on CESI's local network) and 1.1.1.1 (Public Cloudflare DNS, when outside CESI)

- Now, modify the /etc/hosts file as follows:

127.0.0.1 localhost localhost.localdomain

192.168.31.5 S-TCOM-SMB01.isec-telecom.local S-TCOM-SMB01

- Edit the /etc/resolv.conf as follows:

==========

domain isec-telecom.local

search isec-telecom.local

nameserver 10.96.23.51

==========

- Now, reboot the server.

LET'S CONFIGURE SAMBA

- Remove /etc/samba/smb.conf:

```
rm /etc/samba/smb.conf
```

- Promote the DC (Realm: ISEC-TELECOM.LOCAL, NetBIOS Name: ITCOMDOM1, Password: SMBprincipal4321!) :

```
samba-tool domain provision –use-rfc2307 –server-role=dc –dns-
backend=SAMBA_INTERNAL –realm=ISEC-TELECOM.LOCAL –domain=ITCOMDOM1 –
adminpass=SMBprincipal4321!
```

If everything went well, you should see the following output:

Server Role: active directory domain controller

Hostname: S-TCOM-SMB01

NetBIOS Domain:ITCOMDOM1

DNS Domain: isec-telecom.local

- Now, remove krb5.conf:

```
rm /etc/krb5.conf
```

- Copy the new one generated:

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

- Edit the file and file in the required information. In my case, here is the content of the file once modified:

==========

[libdefaults]

default_realm = ISEC-TELECOM.LOCAL

dns_lookup_realm = true

dns_lookup_kdc = true

kdc_timesync = 1

ccache_type = 4

forwardable = true

proxiable = true

fcc-mit-ticketflags = true

[realms]

ISEC-TELECOM.LOCAL = {

kdc = S-TCOM-SMB01.isec-telecom.local

admin_server = S-TCOM-SMB01.infotrucs.lan

default_domain = isec-telecom.local

database_module = ldapconf

}

[domain_realm]

.isec-telecom.local = ISEC-TELECOM.LOCAL

isec-telecom.local = ISEC-TELECOM.LOCAL

==========

- You can now set all DNS-related entries to "192.168.31.3" in /etc/network/interfaces and /etc/resolv.conf

- Now, we'll configure Samba to make it start at boot time :

systemctl unmask samba-ad-dc

systemctl enable samba-ad-dc

sudo reboot now

- Now, we'll create the PTR record:

```
samba-tool dns zonecreate 192.168.31.5 31.168.192.in-addr.arpa -U
administrator
```

- We can try the Kerberos service:

kinit administrator

ADDING THE UNIDIRECTIONNAL TRUST RELATIONSHIP BETWEEN ISEC-GROUP.LOCAL AND ISEC-TELECOM.LOCAL

Now, we want to add an unidirectionnal trust relationship between these 2 domains so that only users from isec-group.local can access resources located in isec-telecom.local, but not the contrary.

If the NetBIOS Name for isec-group.local is IGRPDOM1, the username of the isec-group.local Domain Administrator is S-GRP-AD01-ADM, and its password is "ADprincipal4321!", then enter the following command on the Samba Server:

```
samba-tool domain trust create isec-group.local -UIGRPDOM1\\S-GRP-AD01-ADM%ADprincipal4321! --type=external --direction outgoing
```

Done! You can now start to edit the Samba DC configuration using RSAT Tools! Install a Windows 10 Computer, join it to the isec-telecom.local domain using the "administrator" user of the domaine and install the RSAT Tools. You'll then be able to edit AD objects like you would on your Windows AD DC!