12/11/2019

Procédures d'installations

Joel Agostini Charles, Didier Joël, Marjolet Louis, Vicente VazGROUPE 3

GROUPE 3

PROCEDURES D'INSTALLATIONS

TABLE DES MATIERES

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

INSTALLATION DE S-GRP-AD01

Lancez le script **ScriptInstall_S-GRP-AD01.ps1** sur **S-GRP-AD01** et suivez les instructions**.**

(https://github.com/joeldidier/ActiveDirectory-Monitoring-CESI-Project/blob/master/scripts/S-GRP-AD01/ScriptInstall_S-GRP-AD01.ps1**)**

Le code du script est très commenté et très explicite, mais il serait assez long de tout reformuler.

Le script configure tout :

- Le Réseau
- Le serveur DHCP
- L'installation de la forêt AD
- L'ajout d'utilisateurs, de groupes et d'OU dans l'AD
- La création des partages réseau
- L'installation de l'imprimante PDFCreator, son partage, ainsi que le téléchargement de 7-Zip, utilisé ultérieurement avec la GPO

LE SCRIPT NE CONFIGURE PAS LES GPO ! ELLES DOIVENT ÊTRE AJOUTEES MANUELLEMENT PAR LA SUITE !

INSTALLATION DE S-GRP-AD02

S-GRP-AD02 est le contrôleur de domaine secondaire, ou replica. Il stocke une copie de l'annuaire du domaine isec-group.local et fait office de contrôleur de domaine de secours.

Il exécute également un service DHCP.

L'installation est très courte et ne nécessite aucune interface graphique. On fera tout avec PowerShell.

Au choix donc : exécutez le script **ScriptInstall_S-GRP-AD02.ps1**, ou entrez les commandes suivantes manuellement (commandes tirées du script).

(https://github.com/joeldidier/ActiveDirectory-Monitoring-CESI-Project/blob/master/scripts/S-GRP-AD02/ScriptInstall_S-GRP-AD02.ps1**)**

RESEAU

Partant du principe que le serveur possède une seule interface réseau, on récupère son unique numéro :

```
$AdapterIndex = (Get-NetAdapter).ifIndex
```

On assigne une nouvelle IP manuellement :

```
New-NetIPAddress -InterfaceIndex $AdapterIndex -IPAddress "192.168.31.4" -
DefaultGateway "192.168.31.2" -PrefixLength "24"
```

On spécifie des serveurs DNS :

```
$DNS1 = "192.168.31.3"
$DNS2 = "192.168.31.4"
$dnsList = $DNS1,$DNS2
Set-DnsClientServerAddress -InterfaceIndex $AdapterIndex -ServerAddresses
("$DNS1","$DNS2")
```

Et on autorise le ping IPv4 et IPv6 vers le serveur :

```
New-NetFirewallRule -DisplayName "Allow inbound ICMPv4" -Direction Inbound -
Protocol ICMPv4 -IcmpType 8 -Action Allow
New-NetFirewallRule -DisplayName "Allow inbound ICMPv6" -Direction Inbound -
Protocol ICMPv6 -IcmpType 8 -Action Allow
```

SERVICE DHCP

On installe le service DHCP :

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

On rajoute la plage d'IP à distribuer :

```
Add-DhcpServerV4Scope -Name "ISEC Users Group" -StartRange "192.168.31.21" -
EndRange "192.168.31.253" -SubnetMask "255.255.255.0"
```

Et on indique les DNS à préciser aux clients :

```
Set-DhcpServerV4OptionValue -DnsServer $dnsList -Router "192.168.31.2" -Force -
PassThru
```

INSTALLATION DU CONTROLEUR DE DOMAINE

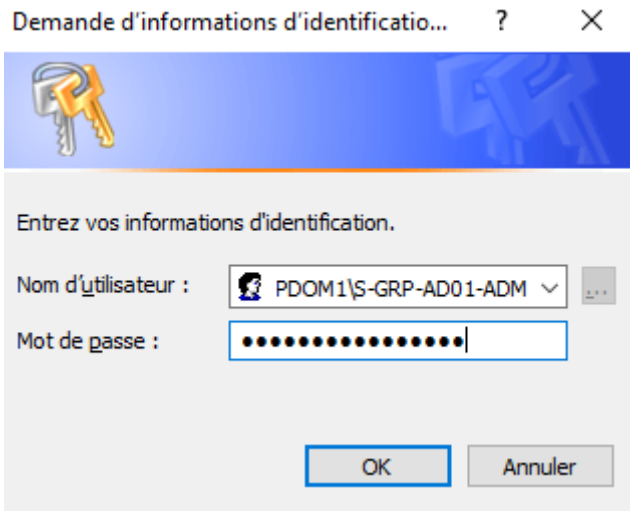
On va d'abord installer le rôle ADDS :

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Et enfin, on ajoute le contrôleur de domaine à la forêt existante de isec-group.local. Il faudra rentrer, dans la fenêtre qui sera apparue, le compte Administrateur du domaine isec-group.local (IGRPDOM1\S-GRP-AD01-ADM) et son mot de passe associé.

```
Install-ADDSDomainController -CreateDnsDelegation:$false -DatabasePath
'C:\Windows\NTDS' -DomainName "$DomainName" -InstallDns:$true -LogPath
'C:\Windows\NTDS' -NoGlobalCatalog:$false -SiteName 'Default-First-Site-Name' -
```

```
SysvolPath 'C:\Windows\SYSVOL' -NoRebootOnCompletion:$true -Force:$true -Credential
(Get-Credential)
```



Il est à présent possible de redémarrer le serveur pour que tout soit entièrement opérationnel.

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

INSTALLATION DE S-TCOM-SMB01

Nous partirons du principe que le serveur exécute Debian 10 (Buster).

Voici quelques paramètres à spécifier lors de l'installation :

- 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!

Pour ce qui est du partitionnement :

- Sélectionnez « Guided - Use full disk »
- Puis : "All Files in One Partition"
- Enfin : "Finish Partitioning and Write Changes to Disk"

Une fois Debian démarré :

1) Passez en root (su root)
2) Ouvrez le fichier **/etc/apt/sources.list** et commentez les lignes commençant par « deb cdrom:[Debian GNU]… »
3) Installez tous les paquets requis avec cette commande :

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

- S'il vous est demandé si vous voulez modifier le fichier smb.conf, sélectionnez « Non ».

4) Ouvrez **/etc/NetworkManager/NetworkManager.conf** , rajoutez **dns=none** dans la section [main], puis redémarrez le service réseau :

sudo service network-manager restart

5) Ouvrez **/etc/network/interfaces** puis rajouter ces lignes (remplacez ens33 par le nom de votre interface réseau):

```
auto ens33
iface ens33 inet static
        address 192.168.31.5/24
        gateway 192.168.31.2
dns-nameservers 10.96.23.51 1.1.1.1
```

6) Modifiez **/etc/hosts** et assurez vous que son contenu soit :

```
domain isec-telecom.local
search isec-telecom.local
nameserver 10.96.23.51
```

Redémarrez le serveur.

7) Une fois le serveur redémarré, supprimez **/etc/samba/smb.conf** :

rm /etc/samba/smb.conf

8) Générez un nouveau fichier de configuration :

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

On notera les paramètres suivants :

realm=ISEC-TELECOM.LOCAL

domain=ITCOMDOM1

adminpass=SMBprincipal4321!

Si tout ce passe bien, voici ce qui devrait s'afficher à l'écran :

Server Role:	**active directory domain controller**
Hostname:	**S-TCOM-SMB01**
NetBIOS Domain:	**ITCOMDOM1**
DNS Domain:	**isec-telecom.local**

9) Vidons **/etc/krb5.conf** de son contenu, et assurons nous qu'il ne contienne que les lignes suivantes:

```
[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
```

10) Configurons Samba4 pour qu'il se lance au démarrage du serveur :

```
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
```

Redémarrons le serveur.

11) Une fois le serveur redémarré, rajoutons un enregistrement PTR pour notre DC Samba (le mot de passe correspond à **adminpass** vu précédemment):

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

12) Testez l'authentification Kerberos avec l'utilisateur administrator :

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël

kinit administrator

Si tout est OK, Kerberos devrait informer de la date d'expiration du mot de passe.

13) Nous allons terminer par rajouter une relation d'approbation unidirectionnelle, donnant le droit aux membres de isec-group.local d'accéder aux ressources de isec-telecom.local (mais pas l'inverse).

    Si le nom NetBIOS du domaine **isec-group.local** est **IGRPDOM1**, l'administrateur du domaine **isec-group.local** est **S-GRP-AD01-ADM** et que son mot de passe est **ADprincipal4321!**
    Alors il faut entrer la commande suivante :

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

Il est alors possible, via les outils RSAT, de se connecter au serveur Samba et de commencer l'ajout d'utilisateurs, de groupes, d'OU ou encore de GPO !

L'ensemble des fichiers de configuration « définitifs » sont visibles ici :
https://github.com/joeldidier/ActiveDirectory-Monitoring-CESI-Project/tree/master/configuration_files/S-TCOM-SMB01

Agostini Charles
Didier Joël
Marjolet Louis
Didier Joël