

COMMANDES TP

DUT R&T 2EME ANNEE

LE GRUIEC Clément

V2.2

Table des matières

1 – Modèle OSI et TCP/IP + protocoles connus :	2
2 - Commande de base d'un routeur CISCO :	3
3 - Commande de base switch Hp/Cisco :	3
4 – Commandes OS :	4
a) Commande de base LINUX:	4
b) Répertoire et fichier utiles LINUX :	5
c) Commande de base WINDOWS :	5
5 - Mise en place utile :	6
a) Vlan :	6
b) Port espion :	6
c) Telnet :	7
e) NAT/PAT :	7
6 – Routage dynamique :	8
a) RIP :	8
b) OSPFv2 :	8
c) BGP :	9
c.1) eBGP :	9
c.2) iBGP :	9
d) MPLS :	9
7 - Installation de services :	10
a) Apache :	10
b) NIS et NFS :	13
b.1) NIS	13
b.2) NFS	14
c) DHCP :	16
d) Active directory Windows (WIN SERV 2012):	18
d.1) SERVEUR	18
d.2) Clients:	36

1 – Modèle OSI et TCP/IP + protocoles connus :

Modèle :

OSI	TCP/IP
7 – APPLICATION (données) : Programme qui a besoin du réseau. Exemple : navigateur internet, logiciel de messagerie. Protocoles : http, FTP, SSH, VoIP...	APPLICATION
6 – PRESENTATION (données) : Formatage des données, chiffrement. Exemple : HTML, ASCII, Unicode, MIME...	
5 – SESSION (données) : En charge du dialogue (établir/maintenir une connexion) entre les machines.	
4 – TRANSPORT (segments) : Identification des ports, segmentations, combinaison des msg, type de cnx. Exemple : routeur Protocoles : TCP, UDP, SCTP...	TRANSPORT
3 – RESEAU (paquets) : Routage des paquets, définir le trajet @ip src et dst / @mac src et dst. Exemple : routeur Protocoles : IP, ARP, ICMP	INTERNET
2 – LIAISONS DE DONNEES (trames) : Adresses mac, détection des erreurs. Exemple : carte réseau, switch Protocoles : Ethernet, Wi-fi, Bluetooth	ACCES AU RESEAU
1 – PHYSIQUE (bits) : Signal électrique, support de transmission. Exemple : câble, hub Support : ADSL, USB, coaxial...	

Protocoles Connus :

Couche	Protocole	N° de port	Couche	Protocole	N° de port
3	IP	4	7	HTTP	80
4	UDP	17	7	HTTPS	443
4	TCP	6	7	SNMP	161 & 162
3	ICMP	1	7	FTP	20 & 21
3	BOOTP	67 & 68	7	SMTP	25
5	DNS	53	7	IMAP4	143
7	TELNET	23	7	POP3	110
7	SSH	22			

2 - Commande de base d'un routeur CISCO :

COMMANDE AVEC PROMPT	UTILISATION
> enable	Passage en mode privilégié
#show running-config	Visualisation de la config en cours
#show startup-config	Visualisation de la config de démarrage
#show ip route	Visualisation de la table de routage ipv4
#show ipv6 route	Visualisation de la table de routage ipv6
#show ip interface (<interface>)	Visualisation de l'état détaillé des interfaces (ipv4)
#show ipv6 interface (<interface>)	Visualisation de l'état détaillé des interfaces (ipv6)
#show ip interface brief (<interface>)	Visualisation de l'état en bref des interfaces (ipv4)
#show ipv6 interface brief (<interface>)	Visualisation de l'état en bref des interfaces (ipv6)
#show arp	Visualisation de la table ARP
#clear arp-cache	vider cache arp
#conf t	Passage en mode config générale
(config)#hostname <nouveau-nom>	Renommer le routeur
(config)#ip routing	Activation du routage ipv4
(config)#ipv6 unicast-routing	Activation du routage ipv6
(config)#ip route <@dest> <mask_pointé> <gw>	Mise en place d'une route statique (ipv4)
(config)#ipv6 route <@dest>/<maskCIDR> <gw>	Mise en place d'une route statique (ipv6)
(config)#ip route 0.0.0.0 0.0.0.0 0.0.0.0 <gw>	Mise en place d'une route par défaut (ipv4)
(config)#ipv6 route ::/0 <gw>	Mise en place d'une route par défaut (ipv6)
(config)#int <nom_interface>	Passage en mode config d'une interface
(config-if)#ip address <@ip> <mask_pointé>	Config de l'adresse ip de l'interface (ip4)
(config-if)#ipv6 address <@ip>/<mask_CIDR>	Config de l'adresse ip de l'interface (ip6)
(config-if)#no shut	Activation de l'interface
#copy flash:vierge2600.cfg startup-config	Chargement d'une config standard (Resto backup)
#reload	Redémarrage routeur

3 - Commande de base switch Hp/Cisco :

COMMANDE AVEC PROMPT	UTILISATION
#erase startup-config	Remettre à l'état d'usine
#reload	Redémarrer
#conf t	Passage en mode config générale
#show startup-config	Visualisation de la config de démarrage
(config)#hostname <nouveau-nom>	Renommer le routeur

4 – Commandes OS :

a) Commande de base LINUX:

COMMANDE	UTILISATION
man <commande>	Infos sur la commande
cd <chemin>	Se déplacer
mv <source> <dest>	Déplacer un fichier
cp <source> <dest>	Copier un fichier
mv <source> <source>/<nouveau nom>	Renommer un fichier
pwd	Connaître le répertoire où on est
touch <nom.extension>	Créer un fichier
ls	Lister un répertoire
mkdir	Créer un répertoire
rmdir	Supprimer un répertoire vide
rm	Supprimer (répertoire, fichier...)
rm -r	Supprimer récursivement /!\
chmod	Modifier les droits
chown	Modifier propriétaire et groupe propriétaire
chgrp	Modifier groupe propriétaire
ps	voir les processus
grep	chercher (à utiliser avec un pipe)
ifconfig <int> <ip>/<mask>	configurer l'@ip d'une interface
route add -net <ip> netmask <mask> gw <gw>	Ajouter une route statique
route add default gw <gw>	Ajouter une route par défaut
netstat -rn	afficher la table de routage
netstat -ant	voir les ports tcp (actif ou non)
/etc/init.d/<nom> <start,stop, restart>	Allumer éteindre redémarrer un service
mount	Monter un volume
umount	Démonter un volume
df	voir les ponts de montage en cours
useradd	créer un utilisateur
userdel	supprimer un utilisateur
groupadd	créer un groupe
groupdel	supprimer un group
more	afficher le contenu d'un fichier
tail -x	afficher les x dernière ligne d'un fichier
arp -an	afficher la table ARP

ping6 -l <int> <@>	Ping en ipv6
ping6 -l <int> ff02 ::1	Voir tous les hôtes actifs du lien
ip -6 addr show (<int>)	Paramètre ipv6
netstat -6rn	Table de routage ipv6
route -A inet6 add <@>/<maskCIDR> gw <@gw>	Ajouté une route statique en ipv6
ip -6 addr add <@>/<maskCIDR> dev <int>	Mettre une ipv6 sur une interface

b) Répertoire et fichier utiles LINUX :

répertoire	UTILISATION
/etc/network/interface	Config à froid des interfaces
/etc/init.d/	Répertoire contenant les services
/etc/passwd	fichier contenant les users
/etc/shadow	mdp et infos sur les users
/etc/group	liste des groupes
/etc/fstab	liste les montages disponibles (monte au boot)
/etc/mtab	Liste les points actuellement montés
/etc/resolv.conf	association d'un domaine à une ip
/etc/hosts.conf	ordre de résolution de noms
/etc/nsswitch.conf	ordre de traduction
/proc/sys/net/ipv4/ip_forward	Activer/désactiver le routage (1/0)
/var/log/	répertoire contenant les logs

c) Commande de base WINDOWS :

COMMANDE	UTILISATION
dir	Lister un répertoire
cd <chemin>	Se déplacer
ipconfig	Affiche la conf des interfaces
Netstat -rn	Table de routage
Copy <src> <dest>	Copier un fichier
Erase <fichier>	Supprimer un fichier
Help	Aide
Mkdir	Créer un répertoire
Md	Créer un répertoire
rmdir	Supprimer un répertoire
rd	Supprimer un répertoire
Shutdown	Arrêt de la machine
Time	Affiche l'heure système
Ver	Version de Windows

5 - Mise en place utile :

a) Vlan :

Sur le switch :

COMMANDE AVEC PROMPT	commentaire
#conf t	
(config)#Vlan <numeroVlan>	Creation d'un Vlan
(Vlan-<n°vlan>)# tagged <n°port>	tagger 1 ports
(Vlan-<n°vlan>)# tagged <n°port1>,<n°port2>...	tagger certain ports
(Vlan-<n°vlan>)# tagged <n°port1>-<n°portn>...	tagger une plage de port
(Vlan-<n°vlan>)# untagged <n°port>	untagger 1 ports
(Vlan-<n°vlan>)# untagged <n°port1>,<n°port2>	untagger certain ports
(Vlan-<n°vlan>)#untagged <n°port1>-<n°portn>	untagger une plage de port
(Vlan-<n°vlan>)#name <nom>	Nommage d'un vlan
#sh vlan	voir les vlans

Sur le routeur :

COMMANDE AVEC PROMPT	commentaire
(config)#int <interface>.<n°interface> ex : int fa0/0.10	création d'une sous-interface et passage en mode conf de cette interface
(config-subif)# encapsulation dot1q <n°vlan>	Activation du 802.1q
(config-if)#ip address <@ip> <mask_pointé>	Config de l'adresse ip de l'interface
(config-if)#no shut	Activation de la sous-interface

b) Port espion :

HP Procurve :

COMMANDE AVEC PROMPT	commentaire
(config)# mirror-port <id-port>	On config le port de sortie
(config)# interface ethernet <port/s> monitor	On config le/s port/s à espionner
#show monitor	Config du port monitoring

Cisco :

COMMANDE AVEC PROMPT	Commentaire
(config)# monitor session 1 destination interface <id-port>	On config le port de sortie
(config)# monitor session 1 source interface <id-port> <mode>	On config le/s port/s à espionner <Mode> : rien, ou « both », « rx », « tx »
#show monitor	Affichage de la config du port monitoring

c) Telnet :

COMMANDE AVEC PROMPT	commentaire
(config)#line vty 0 4	permet 5 session simultanée
(config-line)#password bonjour	config un mdp
(config-line)#login	configure l'invite

e) NAT/PAT :

COMMANDE AVEC PROMPT	commentaire
(config)#int <nom_int>	Passage en mode config de l'interface
(config-if)#ip nat inside	On déclare comme interface interne
(config-if)#ip nat outside	On déclare comme interface externe

Dynamique :

COMMANDE AVEC PROMPT	commentaire
(config)#access-list 1 permit 192.168.0.0 0.0.255.255	liste 1 des machines autorisées à être traduite (=accès wan)
(config)#access-list 1 deny host <@ip>	Interdire une machine
(config)#ip nat inside source list 1 interface <int_entrée wan> overload	comment s'effectue la traduction

Statique :

COMMANDE AVEC PROMPT	commentaire
(config)#ip nat inside source static <protocol_c4> <@ip_in> <port_in> <@port_out> <port_out>	règle de traduction statique avec port
(config)#ip nat inside source static <@ip_in> <@ip_out>	règle de traduction statique sans port

Test et dépannage :

COMMANDE AVEC PROMPT	commentaire
#sh ip nat statistics	Info sur le nat actuellement en place
#clear ip nat translation *	supprimer la table de traduction en cache
#sh ip nat translations verbose	voir les récentes utilisation du nat

6 – Routage dynamique :

a) RIP :

COMMANDE AVEC PROMPT	Commentaire
(config)#router rip	Active la fct rip et passe en config du rip
(config-router)#version 2	Active le rip en version 2
(config-router)#network <@remise direct>	Parle RIP sur l'interface et inclus le res dans les annonces. (=déclaration d'un réseau)
(config-router)#redistribute connected	Inclus tous les réseaux en remise direct dans les annonces
(config-router)#passive-interface <nom-int>	Ne pas parler rip sur l'interface
(config-router)#no auto-summary	Permet de ne pas fusionner les réseaux en fct des classe A, B, C
#sh ip protocols	Permet d'observer les infos sur les protocoles de routage
#sh ip rip database	Visualiser la base rip (utile dépannage)

b) OSPFv2 :

COMMANDE AVEC PROMPT	Commentaire
(config)#router ospf <n° d'instance>	Créer une nouvelle instance OSPF
(config-router)#router-id <ID>	(Optionnel) Conf du router ID (id=une IP)
#show ip ospf <n° d'instance>	Visualisation des info OSPF sur l'instance
(config-router)#network <@ip> <mask inversé> area <n° de zone>	Configurez les interfaces sur lesquelles OSPF sera activé
config-router)# redistribute connected	Redistribution des routes connectées
(config-router)#passive-interface <int>	On mute les interfaces qui n'ont pas besoin ospf
#show ip ospf neighbor	Voir les voisins OSPF
#show ip ospf database	Voir la BDD OSPF
#sh ip rip database	Visualiser la base rip (utile dépannage)
(config-if)#ip ospf priority <priority>	Mettre la priorité manuellement
(config-if)#ip ospf hello-interval <interval>	Changer l'intervalle des messages Hello
(config-if)#ip ospf dead-interval <interval>	Changer l'intervalle du time-out
(config-router)#clear ip ospf process	Restart le process ospf

c) BGP :

remarque : le routage dans les AS doit être opérationnel.

<https://www.networklab.fr/bgp-configuration-basique/>

c.1) eBGP :

(e pour extérieur)

COMMANDE AVEC PROMPT	Commentaire
(config)#int l<n°>	Créer une interface loopback (virtuelle)
(config)#router bgp <n°AS>	On active bgp en spécifiant <u>notre</u> n° d'AS
(config-router)#neighbor <ip_dist> remote-as <n° D'AS dist>	Puis on ajoute une relation de voisinage
#show ip bgp summary	Voir l'état des relations
(config-router)#network @ip_res mask <mask>	Include des reseau dans le bgp

c.2) iBGP :

COMMANDE AVEC PROMPT	Commentaire
(config)#int l<n°>	Créer une interface loopback (virtuelle)
(config)#router bgp <n°AS>	On active bgp en spécifiant <u>notre</u> n° d'AS
(config-router)#neighbor <ip_dist> remote-as <n° D'AS dist>	Puis on ajoute une relation de voisinage (Même as entre voisin en ibgp)
#show ip bgp summary	Voir l'état des relations
(config-router)#neighbor <@ipdist> update-source loopback <n° loopback>	Changer la source des messages (quand on reçoit de l'interface phys au lieu de la vertu)
(config-router)#neighbor @ipvoisi next-hop-self	Changer le Next-Hop par son IP quand il va redistribuer des routes

d) MPLS :

remarque : le routage dans les AS doit être opérationnel.

COMMANDE AVEC PROMPT	Commentaire
(config)#int l<n°>	Créer une interface loopback (virtuelle)
(config)#ip cef	Activation CEF (accélération du routage)
#sh ip ip cef <prefix> detail	Voir detail commutation pour ce préfix
(config-if)#mpls ip	Activation de LDP
#sh mpls ldp bindings <prefix> 24 detail	Info sur les infos sur les labels, les voisins
#sh mpls forwarding-table	Visualiser la table de commutation
VPN (prendre une interface, pas de conf @ip !):	
(config-if)#xconnect <@loopback d'en face> <n°du chemin virtuelle> encapsulation mpls	Montage d'un tunnel entre les deux routeurs

7 - Installation de services :

a) Apache :

- **/var/www/** = Répertoire racine des docs du serveur web
- **/etc/apache2/** = Répertoire contenant les fichiers de configuration.
 - ➔ 'apache2.conf' pour la config générale du serv
 - ➔ 'sites-available/default' pour la config de l'accès aux différentes page du site par défaut

Dans default :

```
<VirtualHost *:80>
```

```
    ServerAdmin webmaster@localhost
```

```
    DocumentRoot /var/www
```

```
    <Directory />
```

```
        Options FollowSymLinks
```

```
        AllowOverride None
```

```
    </Directory>
```

```
    <Directory /var/www/>
```

```
        Options Indexes FollowSymLinks MultiViews
```

```
        AllowOverride None
```

```
        Order allow,deny
```

```
        allow from all
```

```
        DirectoryIndex premier.htm // page par défaut quand on va dans le dossier
```

```
    </Directory>
```

```
    ...
```

- **/etc/init.d/apache2 restart** pour redémarrer Apache
- **/var/log/apache2/access.log** pour checker les logs concernant les entrées sur le site

- rendre privé :

```
<Directory /var/www/resPrivé>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from all
    allow from 10.3.1.0/255.255.255.0 // n'autorise que ce réseau
    DirectoryIndex resPrive.htm // page par défaut quand on va dans le dossier
</Directory>
```

- Mettre un mdp sur une page :

On créer un fichier mdp avec un utilisateur

```
root@S3:/etc/apache2# htpasswd -c .mdp clement
```

New password:

Re-type new password:

Adding password for user clement

On ajoute un second utilisateur

```
root@S3:/etc/apache2# htpasswd .mdp alan
```

New password:

Re-type new password:

Adding password for user alan

On change le default.conf

```
<Directory /var/www/prive/>
Options Indexes FollowSymLinks MultiViews
AllowOverride all
Order allow,deny
allow from all
DirectoryIndex prive.htm
</Directory>
```

On met le fichier .htaccess dans le dossier prive aussi :

AuthUserFile /etc/apache2/.mdp

AuthGroupFile /dev/null

AuthName "Accès privé"

AuthType Basic

<limit GET>

require valid-user

</limit>

- Héberger du multi site :

root@S3:/#mkdir -p /home/www/sn.gtr

root@S3:/home/www/s3.gtr# a2ensite sn.gtr.conf

root@S3:/home/www/s3.gtr# service apache2 reload

on ajoute dans default :

<Directory /home/*/public_html>

AllowOverride AuthConfig

Options Indexes SymLinksIfOwnerMatch IncludesNoExec

Order deny,allow

</Directory>

b) NIS et NFS :

b.1) NIS

On créer un répertoire dans /home/ dans lequel on va mettre les home directory des users...

Changement de nom du domaine NIS :

root@S6:/home/group2p6# **ypdomainname <nom_de_domaine>** (à chaud)

Éditer : '/etc/defaultdomain' pour une config à froid.

Compilation et création BDD :

root@S6:/home/group2p6# **cd /var/yp**

root@S6:/var/yp# **make**

make[1]: Entering directory '/var/yp//<domaine>'

Updating passwd.byname...

failed to send 'clear' to local ypserv: RPC: Program not registeredmake[1]: Leaving directory '/var/yp/<domaine>'

root@S6:/var/yp# **ls**

binding Makefile nicknames tempo6

Répertoire avec les infos NIS :

root@S6:/var/yp/<domaine># **ls**

Dans le fichier etc/yp.conf qui gère la config d'accès à nis (pour chaque machine):

domain <nom_de_domaine> server <@ipServ>

(remarque : Si le serv est aussi client mettre ip 127.0.0.1 pour lui)

Configurer /etc/nsswitch.conf qui permet de pouvoir utiliser des données NIS :

passwd: **files nis**

group: **files nis**

shadow: **files nis**

gshadow: **files nis**

(remarque : mettre files nis sinon les user locaux n'auront plus accès en cas de bug réseau)

Pour configurer le serveur NIS. Nous avons suivi ces étapes :

- 1) définir le nom de domaine à chaud et/ou à froid
- 2) Compilation de la BDD (make dans /var/yp)
- 3) Vérifier la création de la BDD dans /var/yp qui portera le nom de domaines
- 4) configurer le fichier /etc/yp.conf (domain,server et non serveUr)..
- 5) Dans le fichier /etc/nsswitch.conf pour configurer la lecture des mdp et groupes.
- 6) Dans /etc/default/nis pour définir les clients et serveur (true ou false)
- 7) redémarrer les services rpcbind et NIS

Pour configurer le client NIS. Nous avons suivi ces étapes :

- 1) définir le nom de domaine à chaud et/ou à froid
- 4) configurer le fichier /etc/yp.conf (domain,server et non serveUr)..
- 5) Dans le fichier /etc/nsswitch.conf pour configurer la lecture des mdp et groupes.
- 6) Dans /etc/default/nis pour définir les clients et serveur (true ou false)
- 7) redémarrer les services rpcbind et NIS

ypcat permet de visualiser les fichier dans **:/var/yp/<domaine>**

b.2) NFS

Dans le fichier /etc/exports :

/home/<domaine>/ @ip1(rw,sync,no_subtree_check) @ip2(rw,sync,no_subtree_check)

On redémarre le service nfs :

root@S6:/etc/init.d# service **nfs-kernel-server** restart

root@S6:/etc/init.d# service **rpcbind** restart

Monter un dossier nfs sur un client :

mkdir /home/group2p6

mount -t nfs 10.6.2.1:/home/group2p6 /group2p6/

(mount -t nfs <@ipserv>:<chemin source> <chemin des dest>)

(Remarque : mettre le point de montage dans mtab pour le mount au boot)

Connexion avec l'interface graphique :

gedit /etc/lightdm/lightdm.conf

mettre greeter-show-manual-login=true

Redémarrer complètement la machine. (Redémarrer lightdm ne suffit pas)

Sécurité :

On peut autoriser des réseaux ou des adresses spécifiques en modifiant le fichier

/etc/ypserv.securenets.

/home/group2p6/

10.6.2.2(rw,sync,no_subtree_check) 10.6.1.3(rw,sync,no_subtree_check,no_root_squash)

Par default c'est root_squash pour empêcher d'être root partout.

c) DHCP :

- **/var/lib/dhcp/dhcpd.leases** contient les machines associées à des ip encore valide ou non
- **/etc/dhcp/dhcpd.conf** contient la config du serv DHCP
- **#/usr/sbin/dhcpd -d -f** Lancement du serv en mode debug

-Lancement du client en manuel :

#dhclient -v eth0

-arrêt du client en manuel :

#dhclient -r eth0

- Lancement du dhcp en mode service :

root@S3:~# service isc-dhcp-server start

(Remarque : vérifier les logs pour voir si pas de pb au démarrage)

Pour config le client à froid en dhcp (/etc/network/interface) :

auto eth0

allow-hotplug eth0

iface eth0 inet dhcp

Exemple de conf dhcp (dhcpd.conf) :

```
subnet 192.168.3.0 netmask 255.255.255.192{  
    #option routers 192.168.3.62 ;  
    #option subnet-mask 255.255.255.192 ;  
    #option broadcast-address 192.168.3.63 ;  
    #range dynamic-bootp 192.168.3.30 192.168.3.40 ;  
    #default-lease-time 60 ; #max-lease-time 60 ;  
    #option domain-name-servers 82.12.13.14;
```

}//On bloque l'attribution sur un réseau en mettant tout en commentaire

```
subnet 192.168.103.0 netmask 255.255.255.192{  
    option routers 192.168.103.62 ;  
    option subnet-mask 255.255.255.192 ;  
    option broadcast-address 192.168.103.63 ;  
    range dynamic-bootp 192.168.103.30 192.168.103.40 ;  
    default-lease-time 60 ; max-lease-time 60 ;  
    option domain-name-servers 82.12.13.14; //DNS  
    host dn{ //attribuer une adresse de manière constante et automatique  
        hardware ethernet 00:23:ae:74:64:50;  
        fixed-address 192.168.103.30;  
    }  
}
```

On mets le routeur en mode relai :

Cisco :

```
Router(config)#int e1
```

```
Router(config-if)#ip helper-address <int>
```

(remarque : l'interface est celle qui reçoit la trame de broadcast)

Linux :

Service isc-dhcp-relay

d) Active directory Windows (WIN SERV 2012):

Source :

<https://www.supinfo.com/articles/single/4500-mise-place-active-directory-windows-server-2012>

<https://www.windows8facile.fr/windows-server-2012-installer-active-directory-dns-dhcp/>

<https://www.cbouba.fr/cles-de-licences-generiques-microsoft-pour-installation/>

https://wikileaks.org/ciav7p1/cms/page_46628880.html

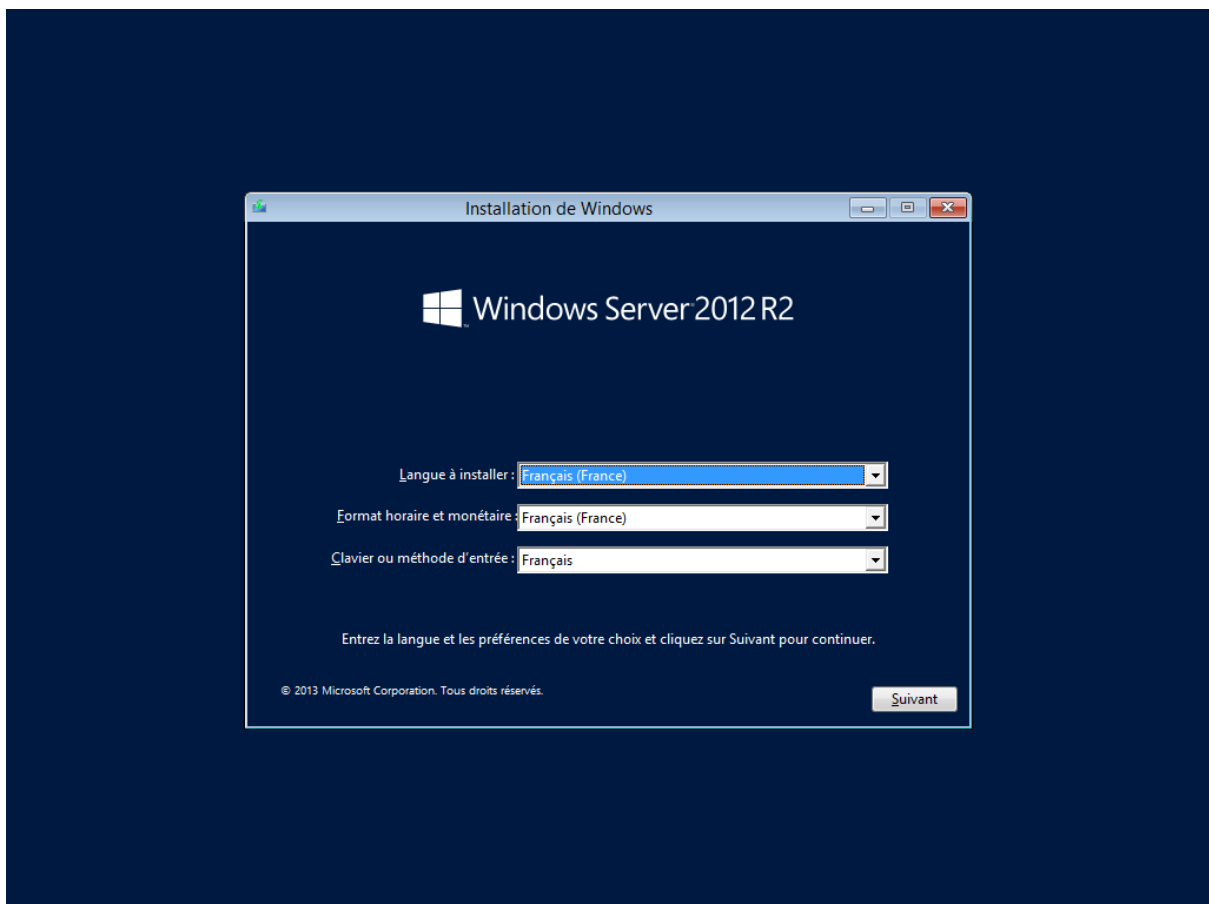
<https://windows.developpez.com/actu/81214/Gestion-simple-des-droits-pour-un-serveur-de-fichiers-dans-un-domaine-Active-Directory-un-billet-de-blog-de-benjamin-f/>

d.1) SERVEUR

Installation de Windows Server

Afin de mettre en place Active Directory, nous allons tout d'abord installer le système d'exploitation « Windows Server 2012 R2 ».

L'installation de celui-ci est très classique et ressemble à celle de Windows 8.



Configuration

Nous allons maintenant configurer notre serveur.

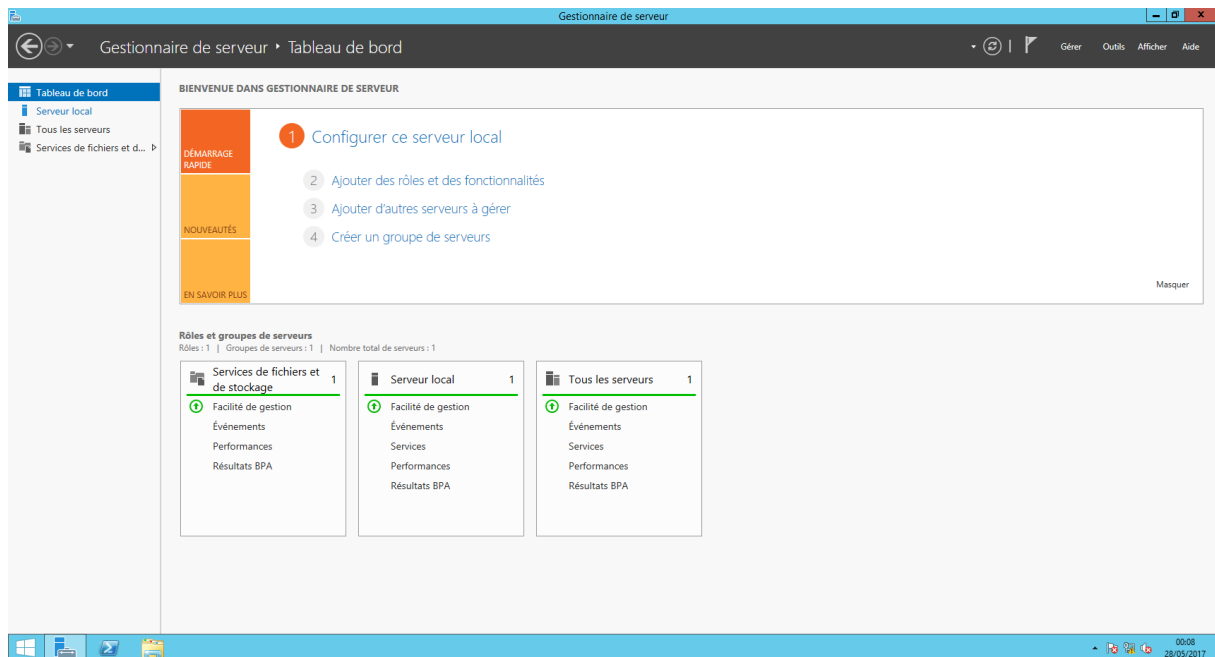
Veuillez-vous référer au tableau ci-dessous pour avoir la même configuration que moi.

Nom serveur	DC
Adresse Ip	192.168.52.10
Masque sous réseaux	255.255.255.0
Passerelle	-
Plage réseau	192.168.1.0/24

Hostname

Pour modifier le nom d'hôte du serveur, vous devrez ouvrir le « Gestionnaire de serveur ».

Après avoir ouvert le « Gestionnaire de serveur », vous obtenez ceci à l'écran :



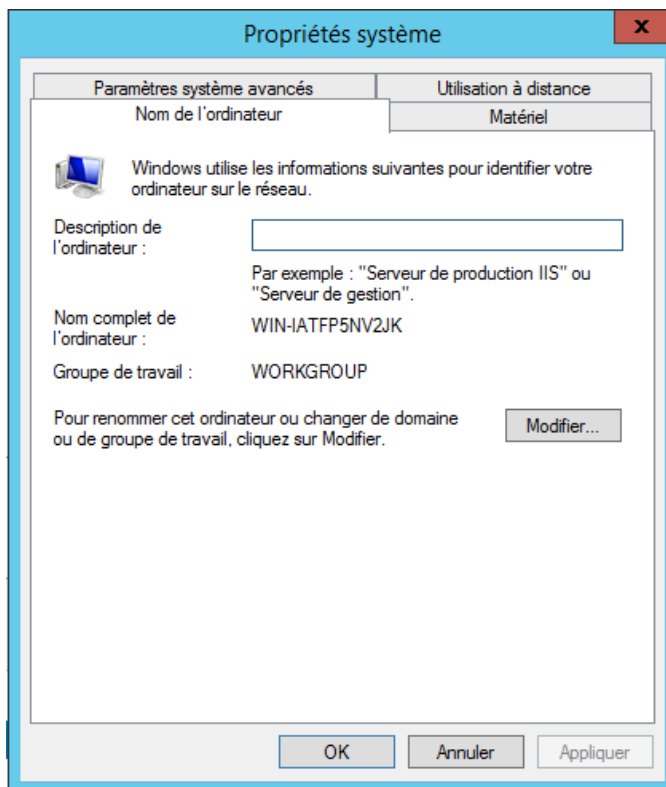
Ensuite, il faudra cliquer sur « Serveur local » (Voir le menu à gauche).

Après avoir cliqué sur « Serveur local », vous obtenez les propriétés de votre serveur, à savoir :

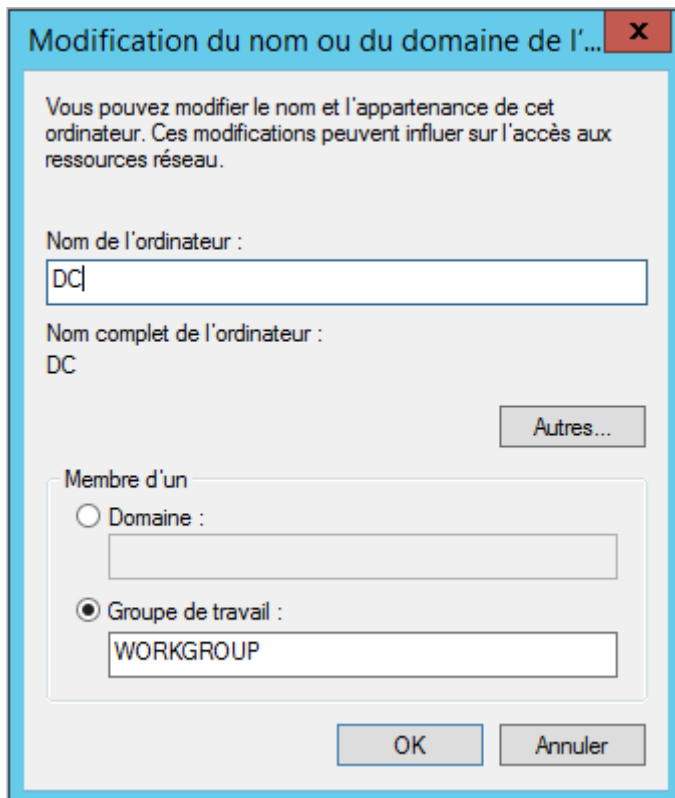
- Le nom d'hôte de votre serveur
- Le statut du pare-feu
- Le statut de la gestion à distance
- Les informations de vos cartes Ethernet

Le nom actuel de votre serveur est WIN-..... (Suivi de chiffres et de lettres).

Cliquez sur le nom actuel de votre serveur, vous obtenez ceci à l'écran :



Pour renommer votre serveur, cliquez sur le bouton « Modifier... »



Une fois renommé, cliquez sur « OK ».

Un message vous demandant de redémarrer votre serveur va s'afficher, cliquer sur « OK », puis fermer.

Cliquez sur « Redémarrer maintenant ».

Après le redémarrage de votre serveur, vous pourrez constater que le nom d'hôte à changer.

Réseau

Nous allons maintenant configurer notre carte réseau.

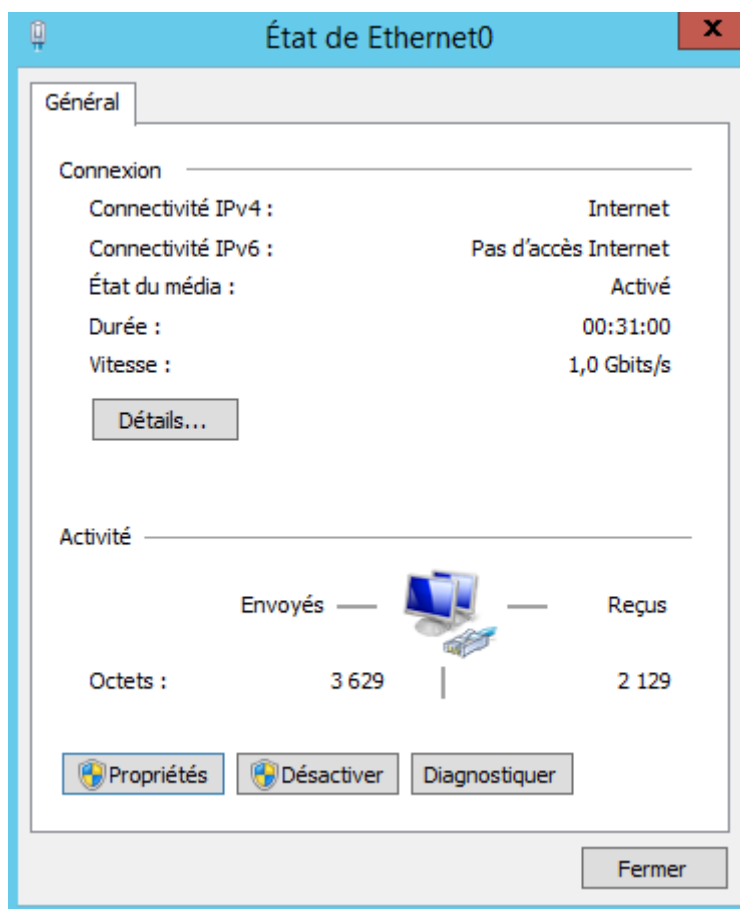
Pour ce faire, vous devrez ouvrir le « Gestionnaire de serveur ».

Ensuite, cliquez sur « Serveur local » (Voir le menu à gauche).

En face du nombre de votre carte réseau dans mon cas « Ethernet0 », cliquez sur « **Adresse IPv4 attribuée par DHCP...** ».

Cliquez, ensuite sur la carte réseau que vous souhaitez configurer.

Vous obtenez ceci à l'écran :



Pour attribuer une adresse fixe à votre serveur, cliquez sur « **Propriétés** », puis « **Protocole Internet version 4** ».

Vous pouvez maintenant renseigner les champs suivants :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) [X]

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 52 . 10

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

NB : Ce serveur sera aussi le Serveur DNS donc nous mettons l'adresse 127.0.0.1 qui correspond à lui-même (Localhost).

Cliquez sur « OK » quand vous avez terminé.

Votre serveur dispose maintenant d'une adresse IP fixe.

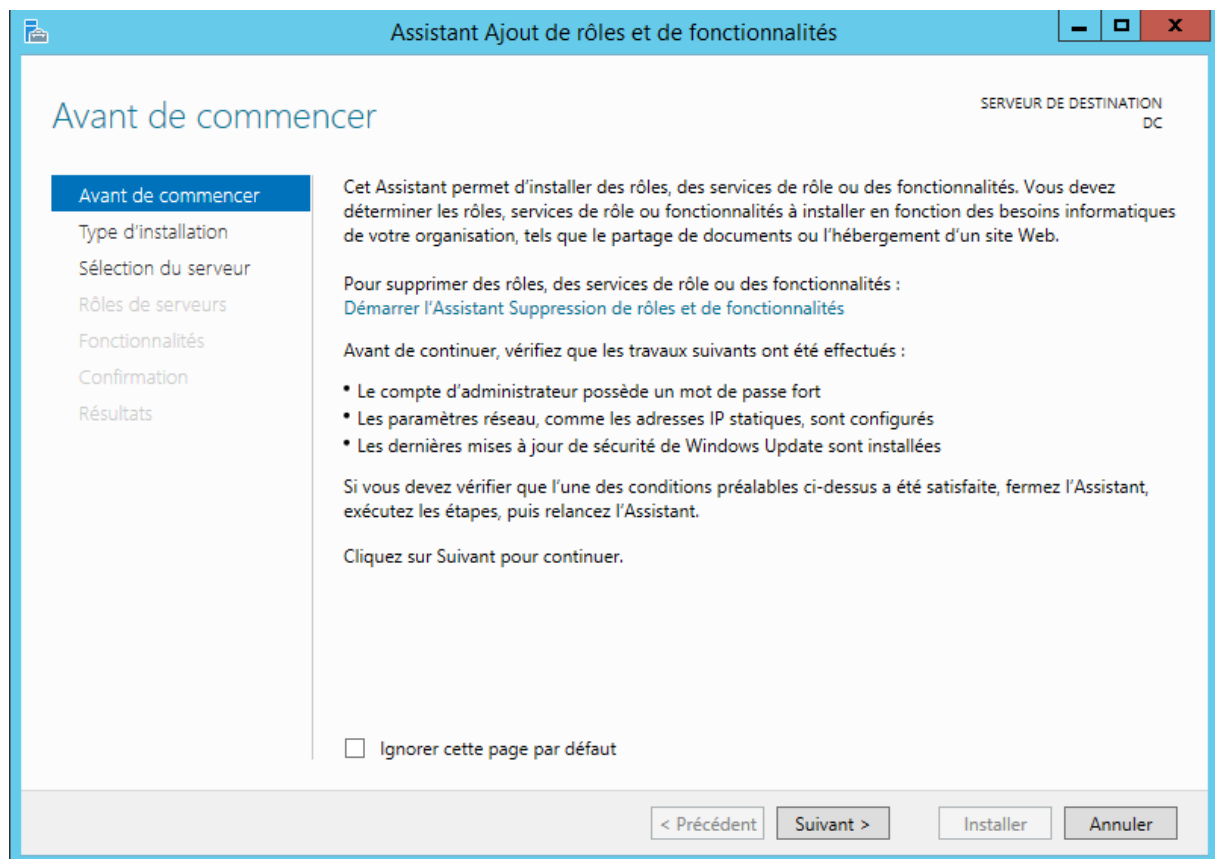
Installation « Active Directory Domain Services »

Nous allons maintenant procéder à l'installation d'Active Directory.

Pour ce faire, dans le Gestionnaire de serveur cliquez sur « **Gérer** » (en haut à droite).

Ensuite, cliquez sur « **Ajouter des rôles et des fonctionnalités** ».

Vous obtenez ceci :



Cliquez sur « Suivant », laissez cocher ce qui est par défaut : Installation basée sur un rôle ou une fonctionnalité, puis cliquez sur « Suivant ».

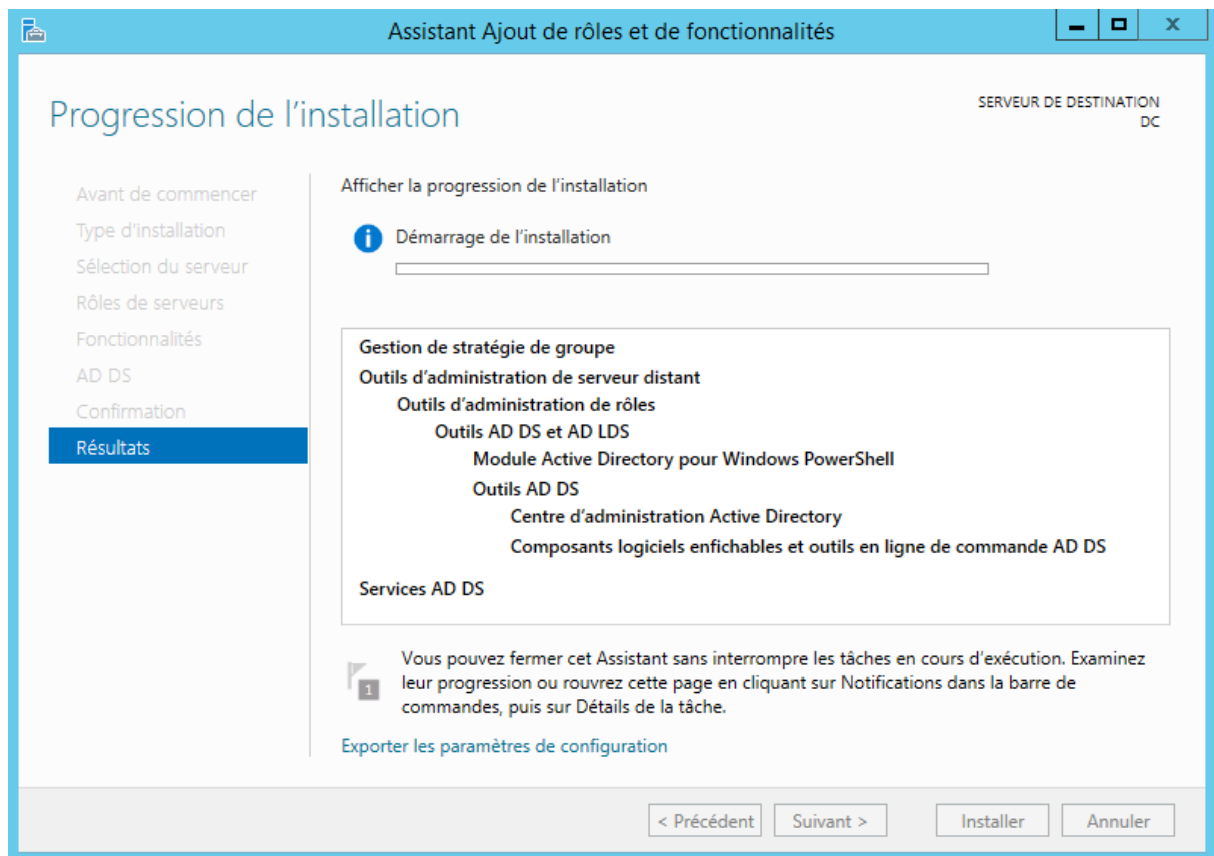
Ensuite, cliquez à nouveau sur « Suivant ».

Maintenant, cocher le rôle « Services AD DS », puis cliquer sur « Ajouter des fonctionnalités ».

Cliquez ensuite sur « Suivant » (3 fois).

Cliquez maintenant sur « Installer ».

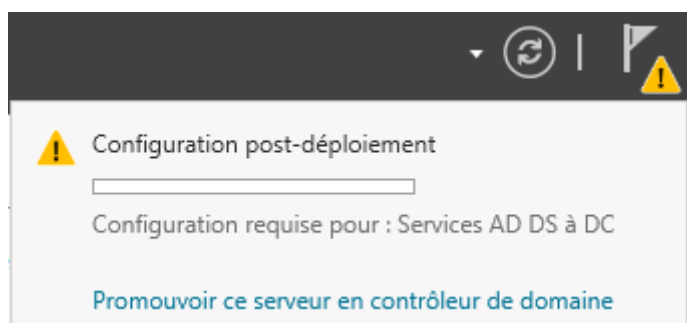
Vous obtenez ceci :



Une fois le jaune rempli.

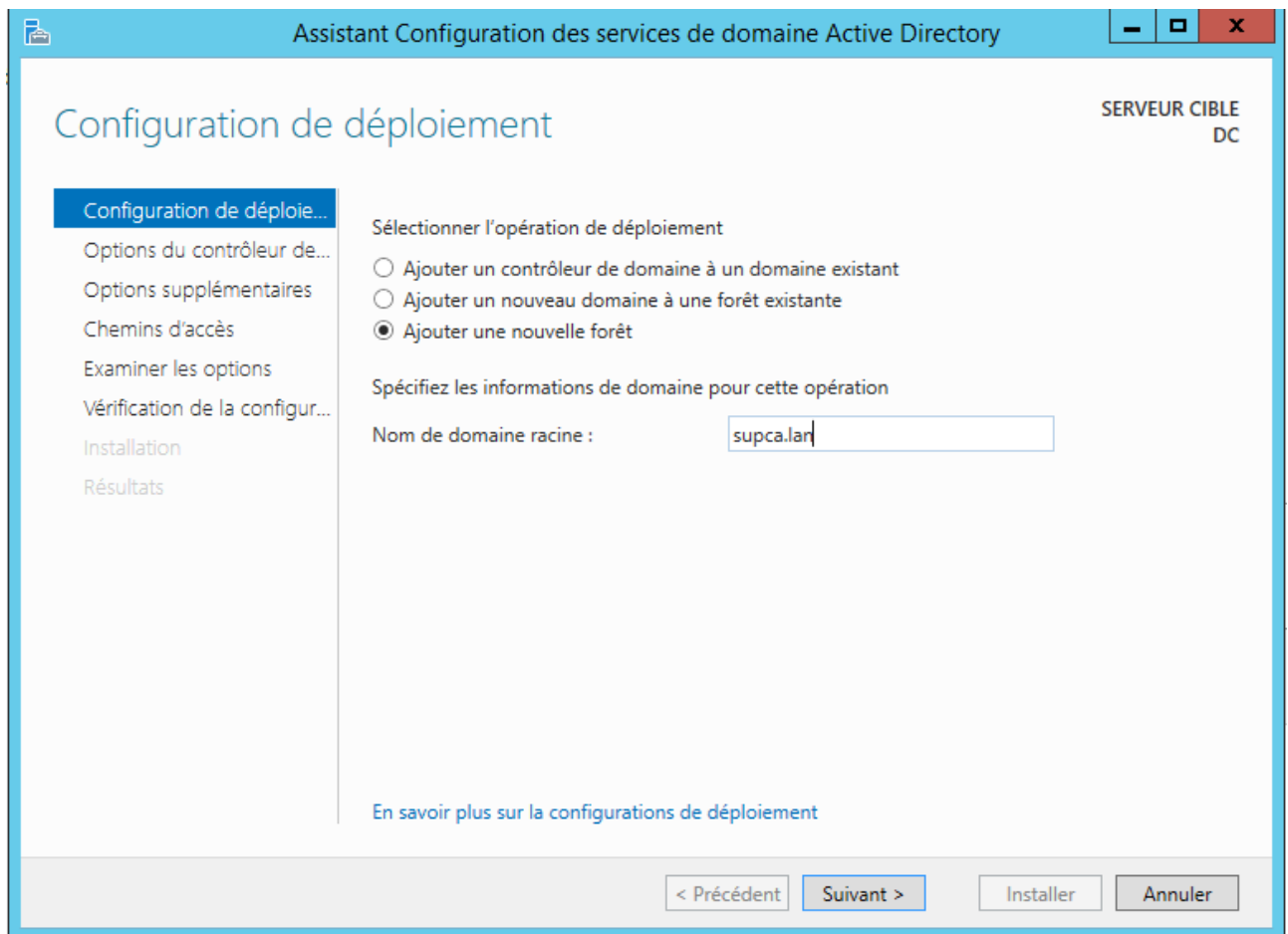
Cliquez sur « Fermer ».

Maintenant, nous allons promouvoir ce serveur en contrôleur de domaine.



Cliquer sur le drapeau avec le panneau jaune, puis sur « Promouvoir ce serveur en contrôleur de domaine ».

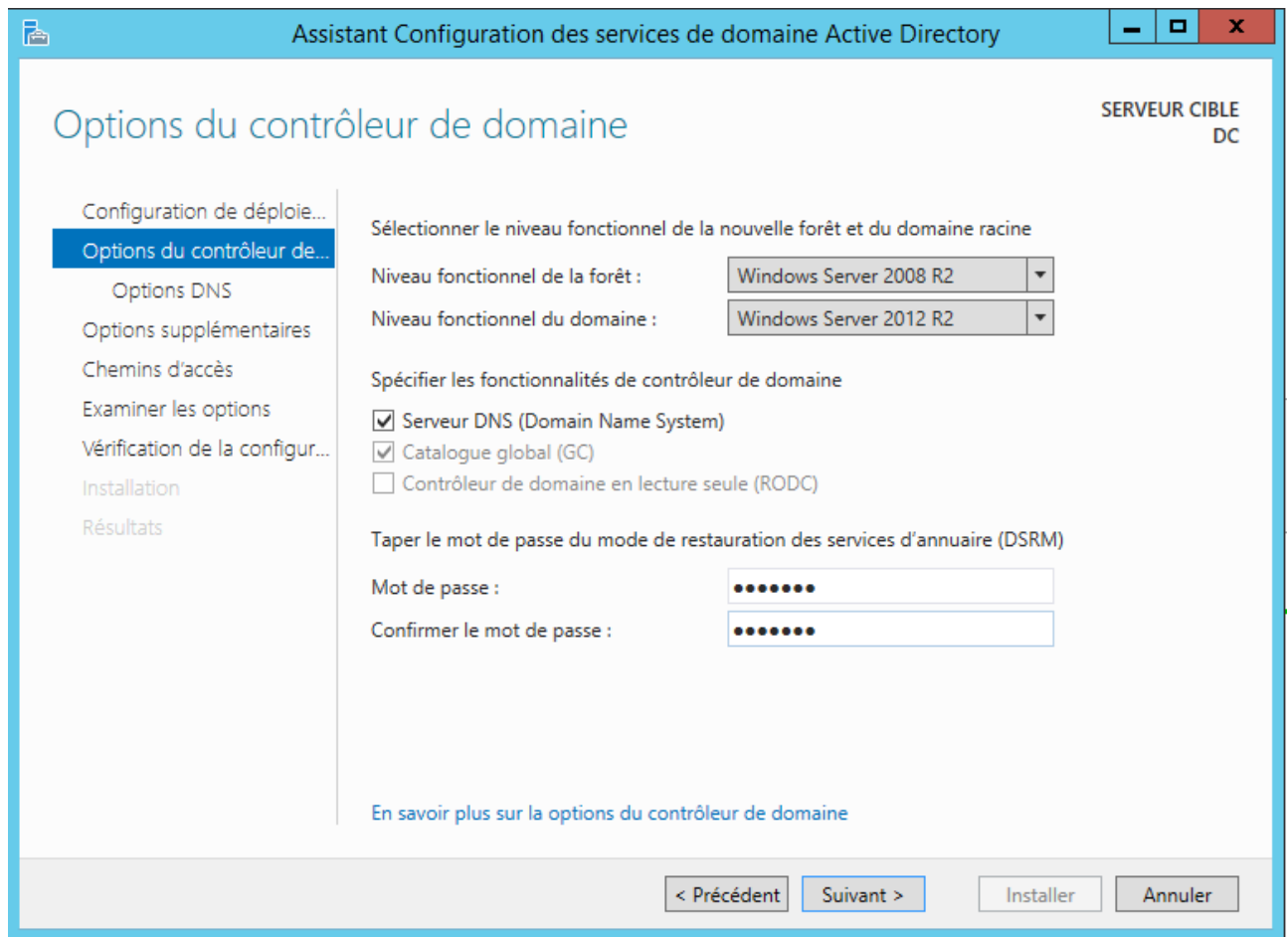
Vous obtenez ceci :



Cliquer sur Ajouter une nouvelle forêt, et renseigner le nom de votre domaine.

Dans mon cas « supca.lan ».

Pour poursuivre, cliquez sur « Suivant ».



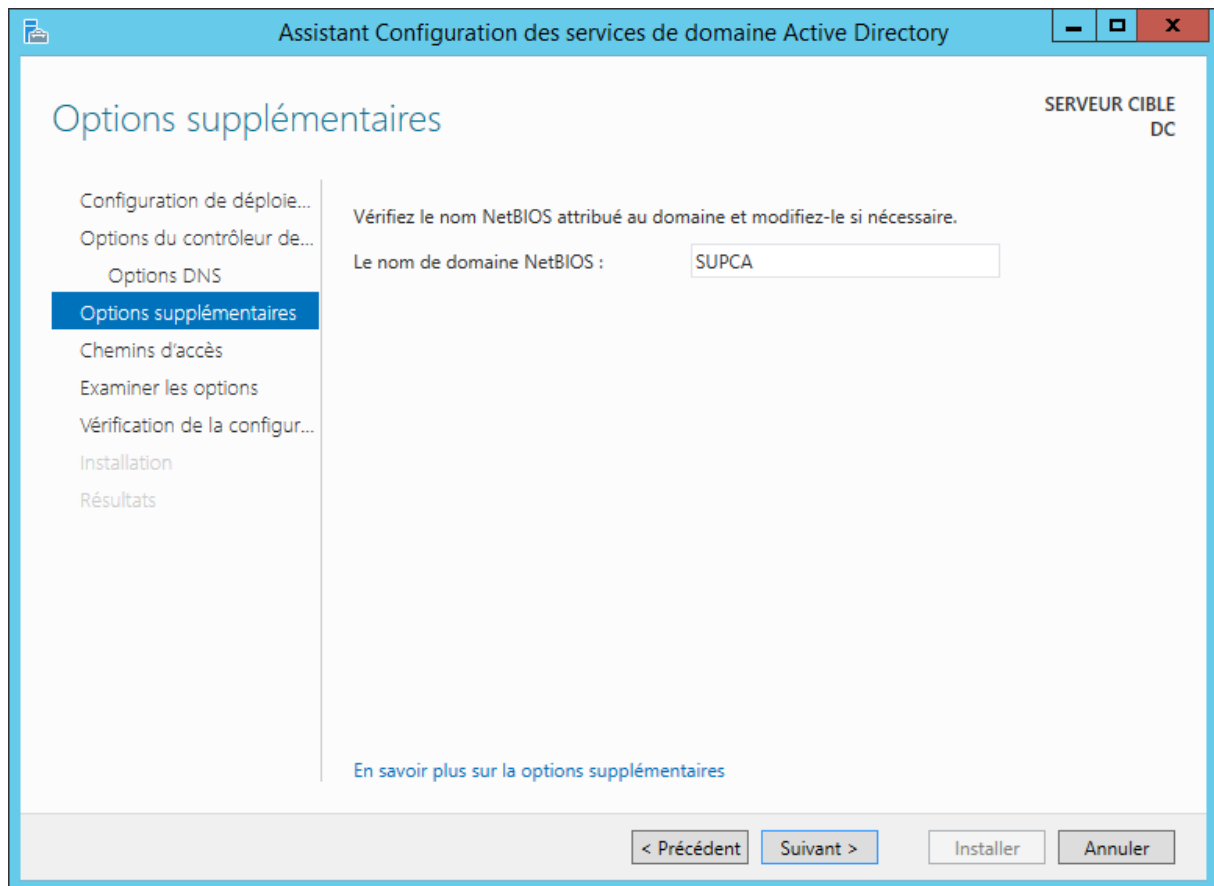
NB : Si dans votre architecture vous disposez d'un serveur antérieur à Windows 2012.

Je vous recommande de mettre en niveau fonctionnel de la forêt le nom de l'OS antérieur de votre infrastructure.

Cliquez sur « Suivant » pour poursuivre.

Une erreur apparaît sur l'écran suivant. Ce message survient, car aucun serveur DNS n'est installé sur la machine. Cliquez simplement sur « Suivant » pour le créer.

Ensuite, indiquer un nom NetBIOS au domaine.



Cliquez sur « Suivant ».

Laisser les valeurs de l'écran suivant par défaut (NTDS et SYSVOL).

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :	C:\Windows\NTDS	...
Dossier des fichiers journaux :	C:\Windows\NTDS	...
Dossier SYSVOL :	C:\Windows\SYSVOL	...

Puis cliquez sur « Suivant ».

L'installation est prête et un récapitulatif est affiché pour vérifier la configuration.

Cliquez sur « Suivant ».

Une vérification système est effectuée, cliquez sur « Installer ».

Le serveur va ensuite redémarrer automatiquement.

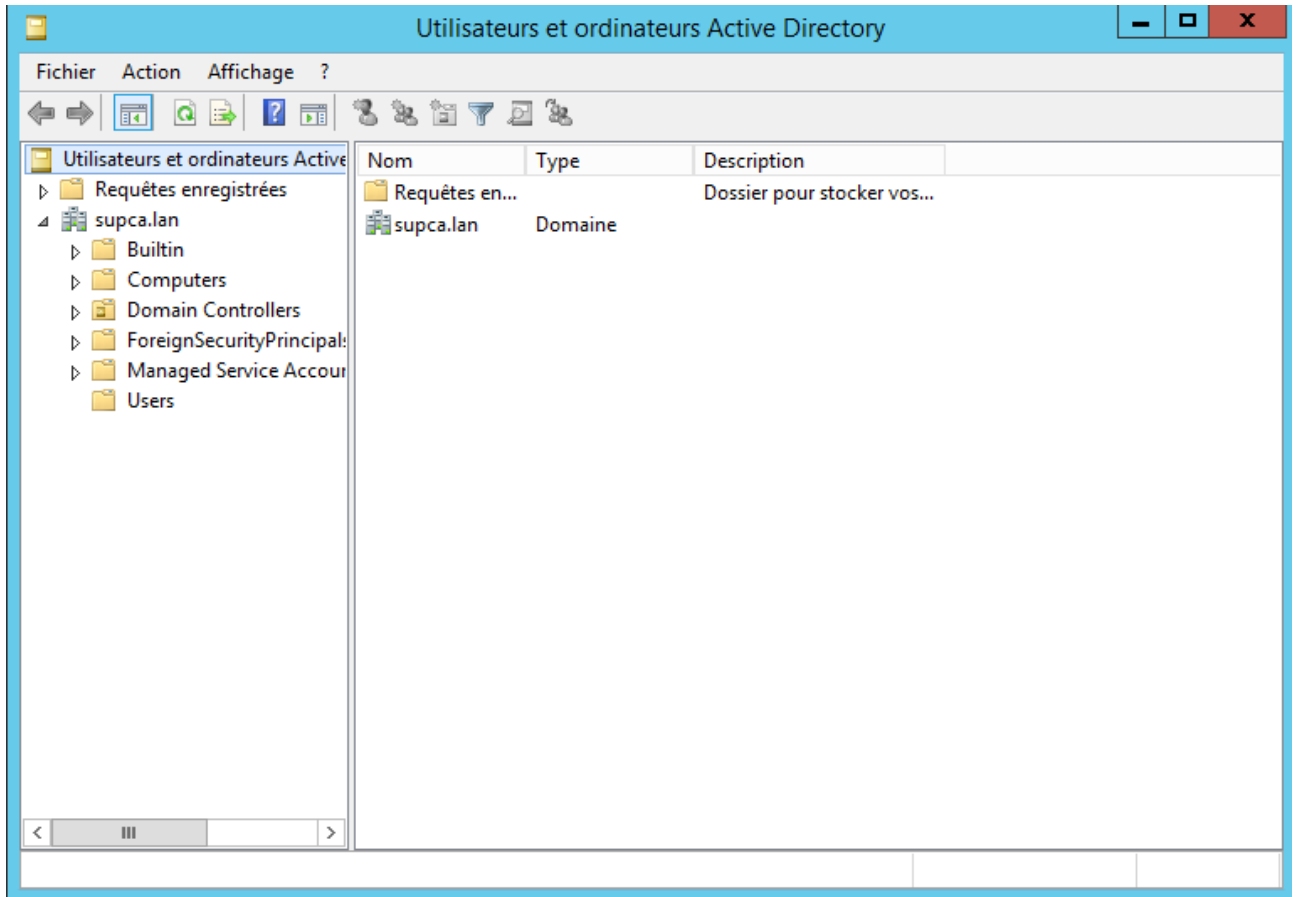
Le login se fait maintenant avec votre compte et mot de passe du domaine.

Votre contrôleur de domaine est maintenant prêt.

Gestion des utilisateurs

Nous allons maintenant créer des utilisateurs.

Pour ce faire cliquer dans le menu sur : Outils > Utilisateurs et ordinateurs Active Directory.



Cliquez sur le nom de votre domaine.

Puis cliquez dans le menu sur Action > Nouveau > Utilisateur.

Renseignez les champs :

- Prénom
- Nom
- Nom d'ouverture de session

Même dans les petites entreprises, cela peut devenir très vite complexe par la multiplication des droits donnés à différents utilisateurs sur un même dossier.

Encore plus quand il faut donner des droits différents à ces même utilisateurs dans les sous-dossiers.

Les besoins de base envers un dossier sont eux assez simples :

- Y faire ce que l'on veut : Lire, modifier, ajouter, et supprimer des fichiers.
- Lire les fichiers d'un dossier, sans pouvoir les modifier
(rien n'empêche de copier le fichier sur le bureau pour le modifier en local, mais celui-ci ne pourra pas remplacer le fichier existant dans le dossier racine.)
- Ne pas y avoir accès.

La méthode que je vais vous présenter se base sur les points suivants :

- Pas de sous-partage.
- Pas de gestion des droits dans les sous-dossiers.
- Tous les dossiers sont gérés sur la racine du partage.
- Un groupe de Domaine Locale avec des droits en lecture sur le dossier racine.
- Un groupe de Domaine Locale avec des droits en écriture sur le dossier racine.
- Activer ABE.

Ainsi, une fois en place, il n'y aura plus à toucher au droits définis sur les dossiers créés.

Si un utilisateur ou un groupe défini d'utilisateurs doit avoir un accès à un dossier, il n'y aura qu'à le mettre dans le groupe adéquate depuis Active directory.

Les utilisateurs ne verront que les dossiers racine auxquels ils au minimum un droit de lecture.

La méthode dans la pratique

Énoncé de l'exercice

2 utilisateurs, "user1" et "user2" auront accès à un partage "TEST" sur lequel se trouvera les dossiers racines.

Le partage sera effectué sur un serveur de fichier Windows 2012r2 appelé SRV-FIC2.

- User1 pourra lire et écrire dans le dossier "Dossier1" et lire les fichiers du dossier "Dossier2".
- User2 pourra lire et écrire dans le dossier "Dossier2" mais n'aura aucun droit sur le dossier "Dossier1".
- Pour une meilleure lisibilité, nous utiliseront ABE pour que user2 ne voit que le dossier sur lequel il a des droits.

Les groupes

Chaque groupe portera le même nom que le dossier pour l'identifier facilement, plus une lettre qui nous indiquera s'il s'agit du groupe de lecture ou du groupe d'écriture.

Dans AD, j'utilise une nouvelle O.U appelée Groupes_GDL pour Groupes de Domaine Locale.
On crée dedans les groupes Dossier1_R, Dossier1_W, Dossier2_R, et Dossier2_W.

Pour suivre la méthode AGDLP, ces groupes seront des groupes de Domaine Local.

⚠ Vous pourrez par la suite créer des groupes globaux qui réuniront les utilisateurs d'un même service.

Par exemple Commerciaux, direction, RH, secrétaires,

Ensuite il faudra mettre les groupes globaux des services dans les groupes de domaine Local auxquels ils ont des droits.

Pour les besoins de l'exercice, on va mettre directement les utilisateurs dans les groupes de domaine local.

Donc selon l'énoncé:

➡ L'utilisateur User1 qui a des droits en écriture sur dossier 1 et en lecture sur dossier2 ira dans les groupes Dossier1_W et dossier2_R

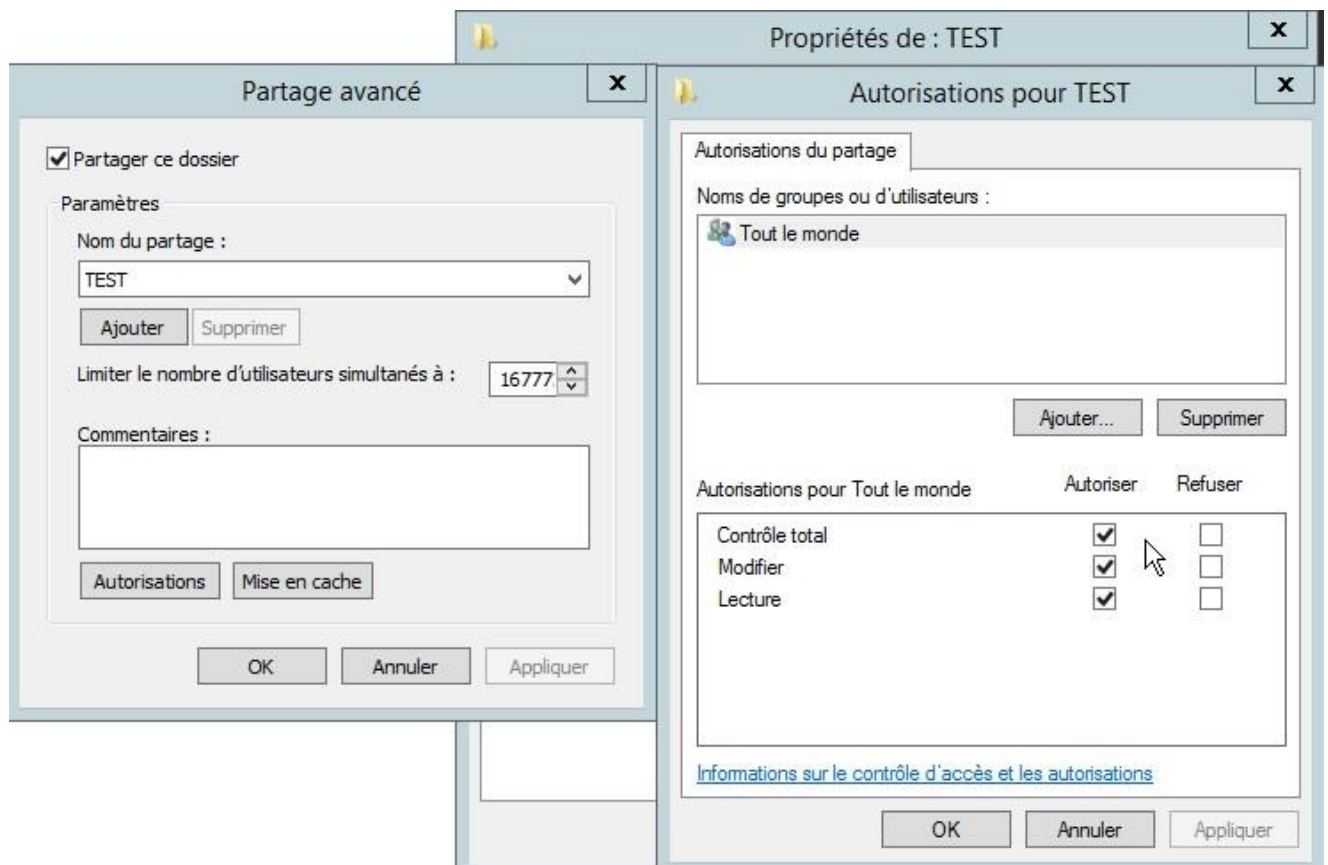
➡ L'utilisateur User2, qui a des droits en écriture sur le dossier2 mais aucun droit sur dossier 1 n'ira que dans le groupe dossier2_W.

Le partage

Sur le serveur de fichier, attachez un nouveau disque NTFS nommé DATA.

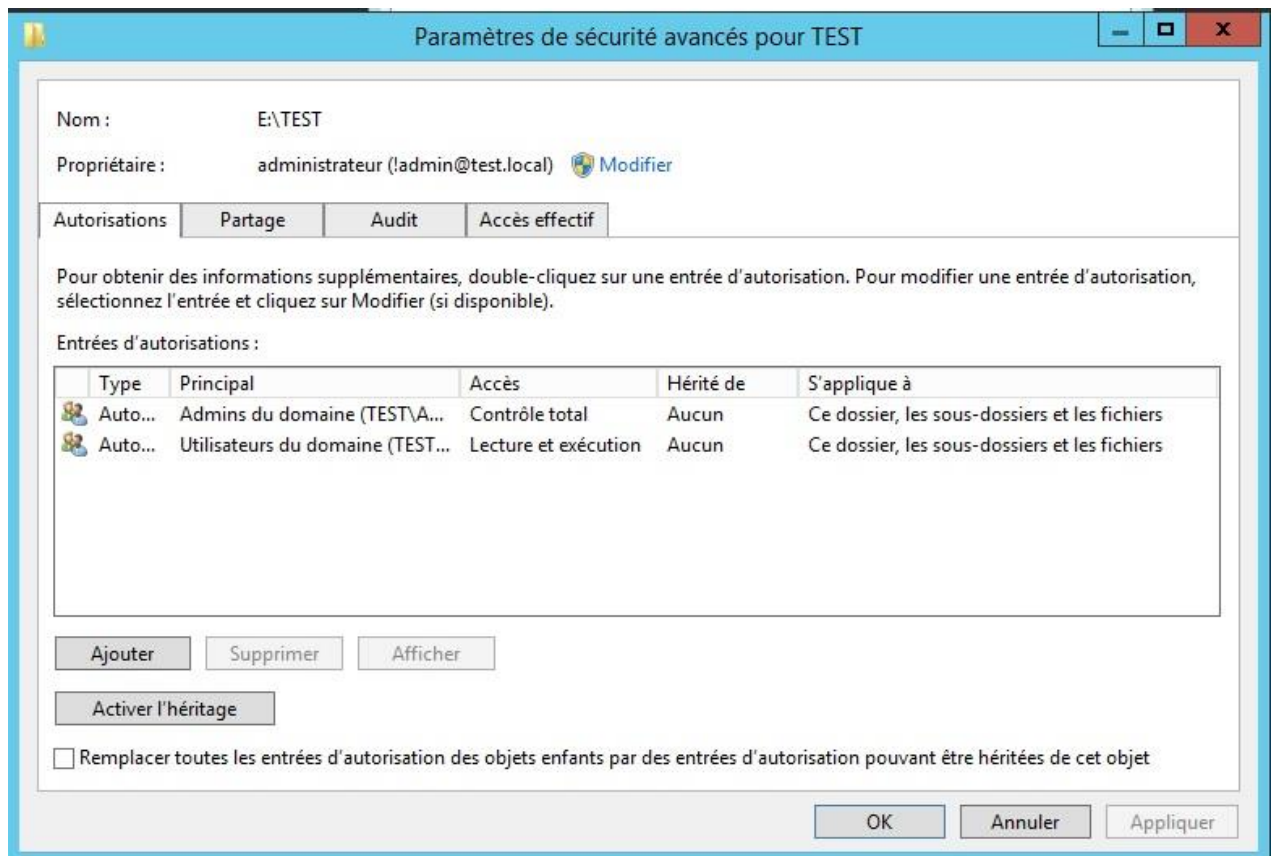
Sur le disque DATA, créer un nouveau dossier "TEST".

Utilisez le mode de partage avancé pour donner des droits de partage en contrôle total au groupe "tout le monde".



Nous allons gérer les droits via NTFS:

- Allez dans les propriétés/onglet sécurité/bouton avancé.
- Désactivez l'héritage, et supprimez toutes les autorisations héritées de l'objet.
- Ajoutez admins du domaine en contrôle total (CT).
- Ajoutez utilisateurs du domaine que vous laissez en lecture (valeur par défaut)



Les dossiers

Une fois le partage effectué, on va pouvoir créer les dossiers gérés, auxquels on définira les droits d'accès via NTFS.

On crée les dossiers "dossier1" et "dossier2".

La première chose est de désactiver l'héritage.

Donc clic droit sur le dossier/propriétés/avancer/modifier les autorisations, et on désactive l'héritage.

⚠ Soit on réinjecte les droits déjà présents, soit on part sur une base vierge.

Cela ne changera pas grand-chose ici.

- On supprime les autorisations héritées (*pour cet exemple, on va repartir sur une base vierge*).
- On ajoute le groupe "admins du domaine" en contrôle total.
- On ajoute le groupe "Dossier1_R", et on lui laisse ces droits de base en "Default value".
- On ajoute Dossier1_W auquel on rajoute "modification" aux droits de base, la droite écriture va se mettre automatiquement.

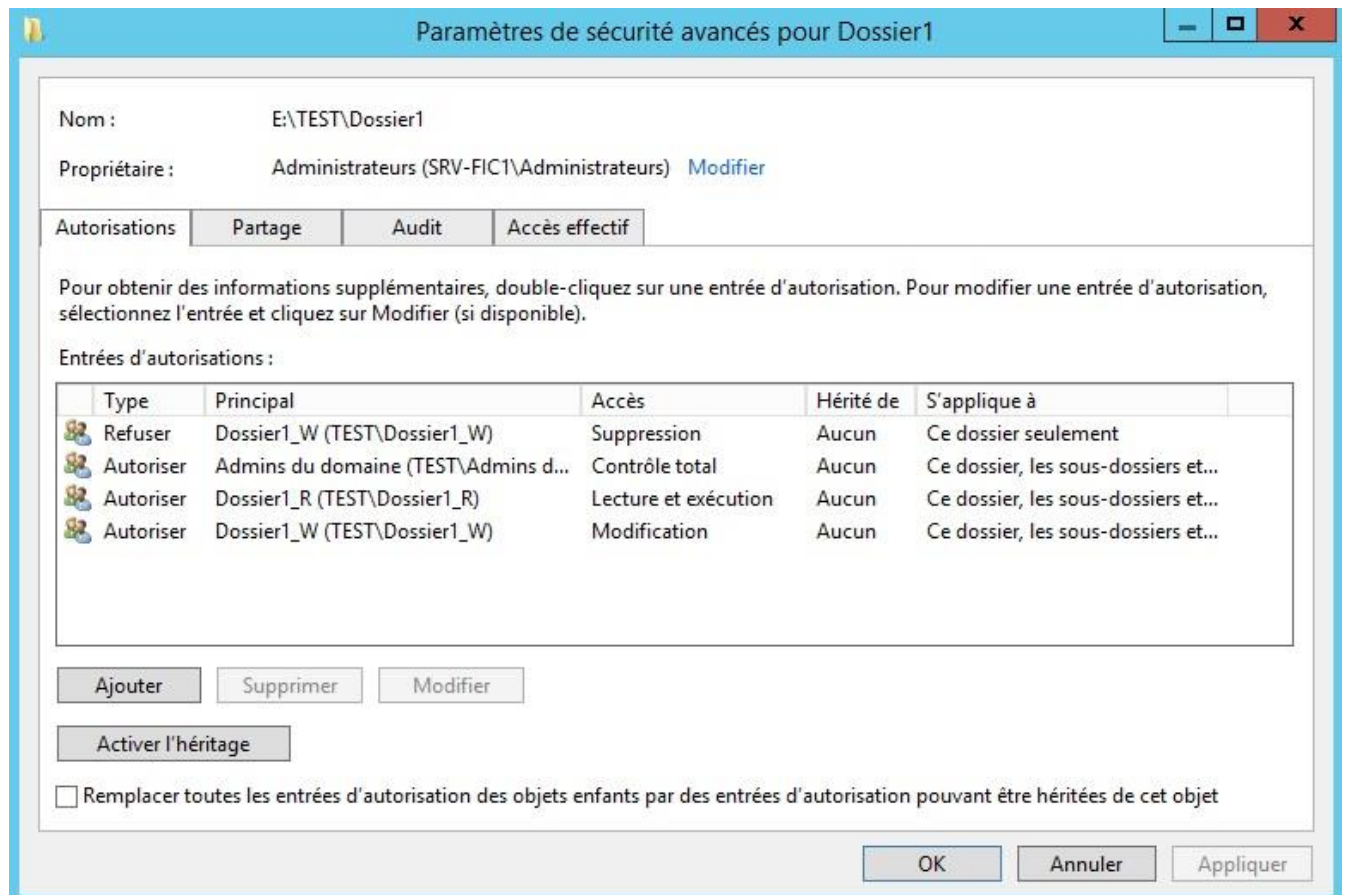
Pour éviter toute catastrophe, on va maintenant rajouter un refus pour le groupe en écriture

Dans les autorisations avancées, on rajoute le groupe "Dossier1_W".

On spécifie un "REFUS" sur "ce dossier seulement" pour l'attribut "suppression".

⚠ Attention, bien spécifier "Ce dossier seulement" car les refus l'emportent toujours sur les autorisations.

Pour vérification, vous devez vous retrouver avec ces droits :



On fait maintenant la même chose pour le dossier "Dossier2", en lui configurant ses groupes de la même façon.

On récapitule

On doit donc avoir :

- 2 utilisateurs : User1 et User2
- 4 groupes de domaine Locale : Dossier1_R, Dossier1_W, Dossier2_r, et Dossier2_W
- User1 est dans Dossier1_W et Dossier2_R
- User2 est dans Dossier2_W
- Un dossier TEST partagé en "CT" pour le groupe "tout le monde" avec des droits NTFS de base en lecture pour les utilisateurs du domaine.
- Les dossiers racine "Dossier1" et "Dossier2" sur lesquels ont défini les droits sur les groupes respectifs

Connexions de test

On se connecte en User1, on doit pouvoir :

- Lire et écrire dans le dossier Dossier1
- Lire ce qu'il y a dans le dossier Dossier2

En se connectant en User2, on ne peut que lire et écrire dans le dossier "Dossier2"

ABE

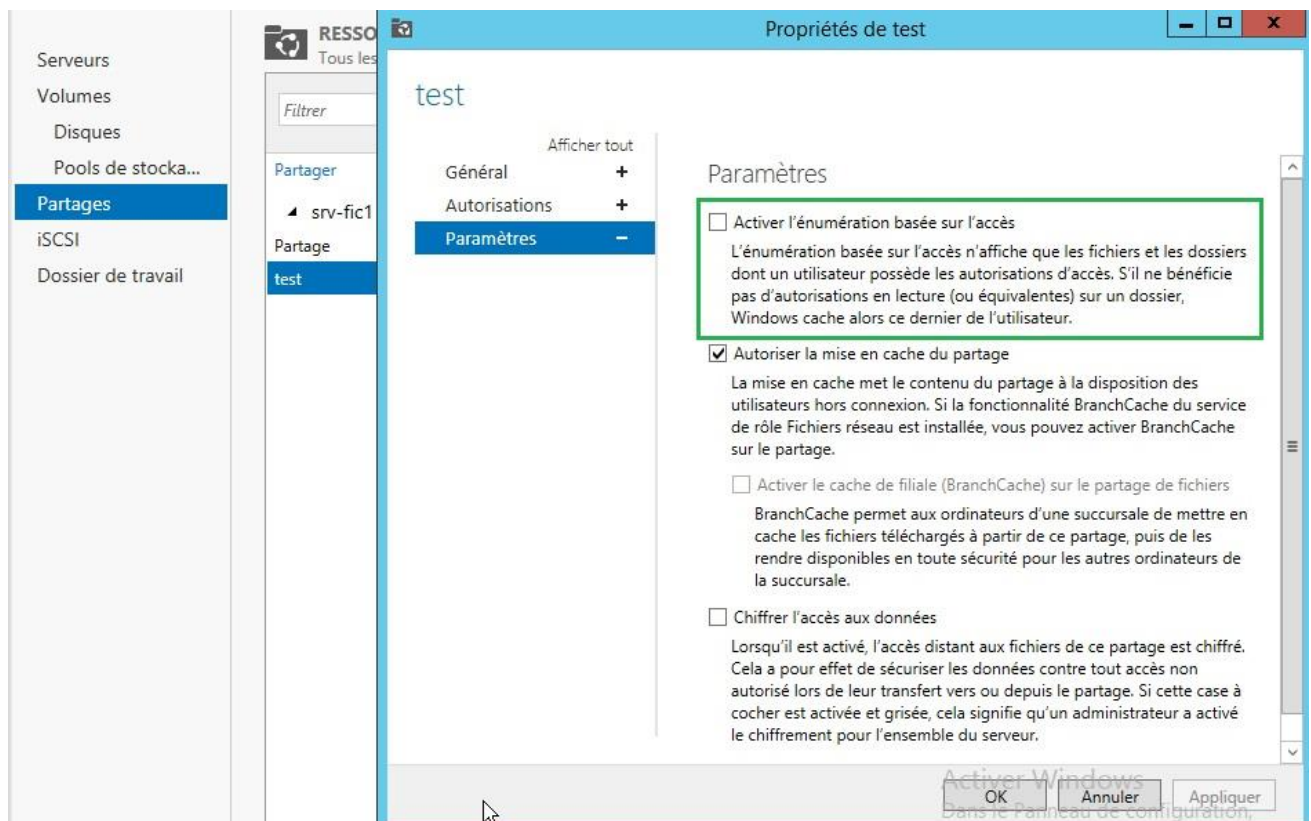
Il faut aller sur le serveur de fichier pour activer Access Based Enumeration.

Connectez-vous dans le gestionnaire de serveur, et allez dans le menu de gauche "Services de fichiers et de stockage".

Ensuite allez dans "Partages".

Vous y trouverez la liste de tous les partages référencés sur le serveur.

Sélectionnez le partage "TEST", et allez dans les propriétés puis "paramètres".



Maintenant, les utilisateurs ne verront plus que les dossiers auxquels ils ont le droit.

Recherches associées

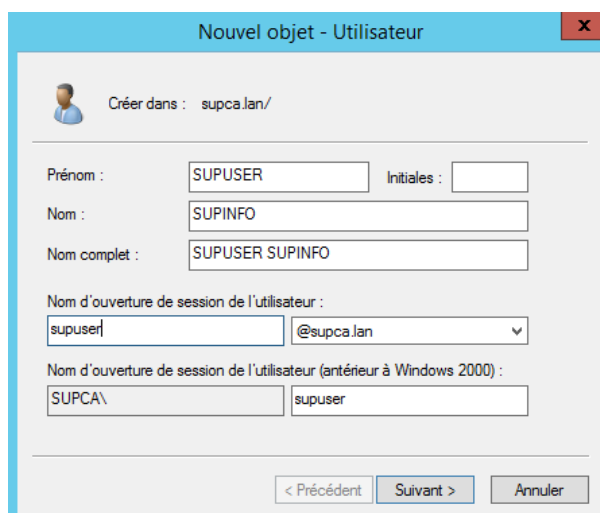
Pour commencer à aller plus loin, vous pouvez faire des recherches concernant les termes suivants :

- Droits NTFS
- Active directory
- AGDLP
- ABE (Access-based Enumeration)

Conclusion

C'est la méthode que j'utilise actuellement en 3 partages montés en lecteurs réseaux.

L'effort d'administration est faible, ce qui me permet de traiter les demandes d'accès rapidement avec un faible risque d'erreur.



Puis cliquez sur « Suivant ».

Renseignez le mot de passe que vous souhaitez attribuer à cet utilisateur et cliquez sur « Suivant », puis sur « Terminer ».

Votre utilisateur est maintenant créé.

d.2) Clients:

Pour intégrer une machine à votre domaine, il faut au préalable :

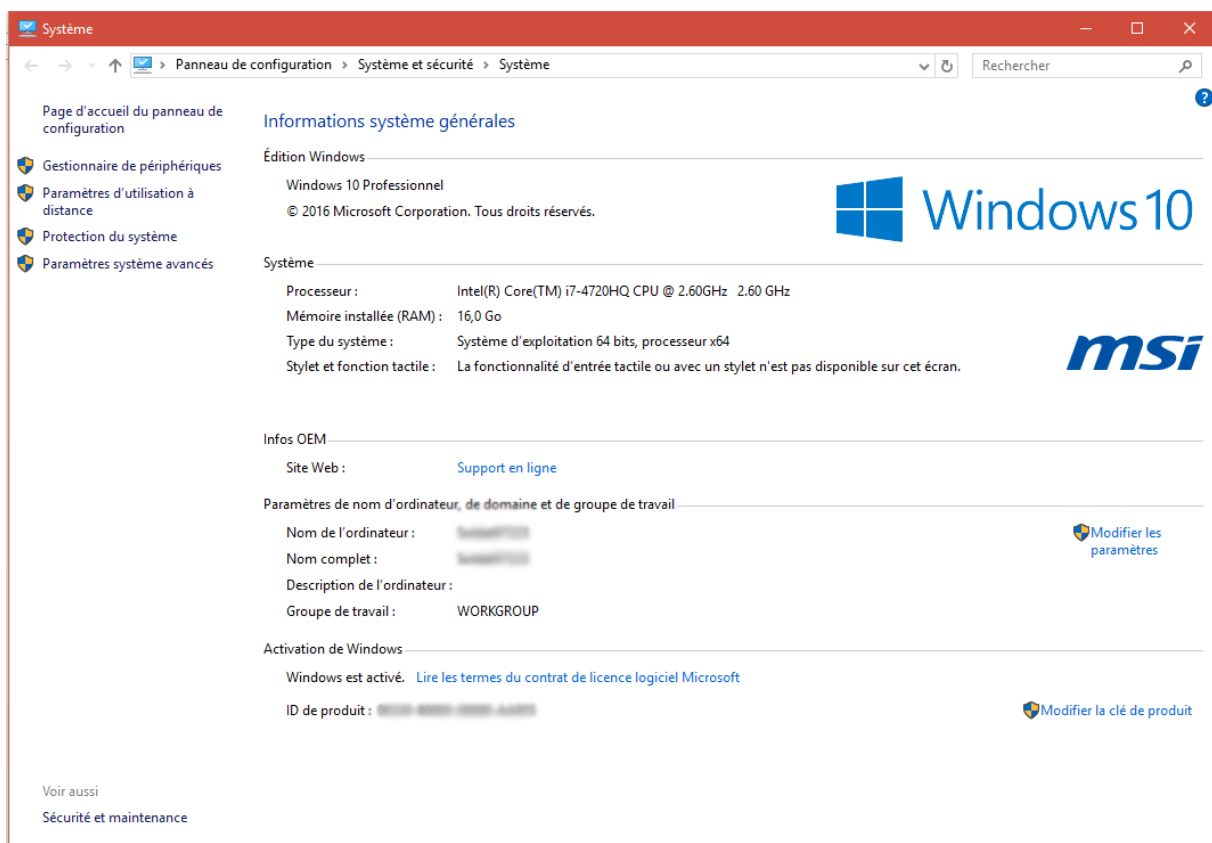
- Changer le nom d'hôte de votre Ordinateur (Pas obligatoire, mais conseiller)
- Faire un ping pour vérifier que vous arrivez à joindre votre contrôleur de domaine.

Pour changer le nom d'hôte de votre ordinateur :

Si vous avez un Windows 8.1 / 10

1. Effectuez un clic droit sur le logo Windows (en bas à gauche sur la barre des tâches)
2. Cliquez sur « Système »

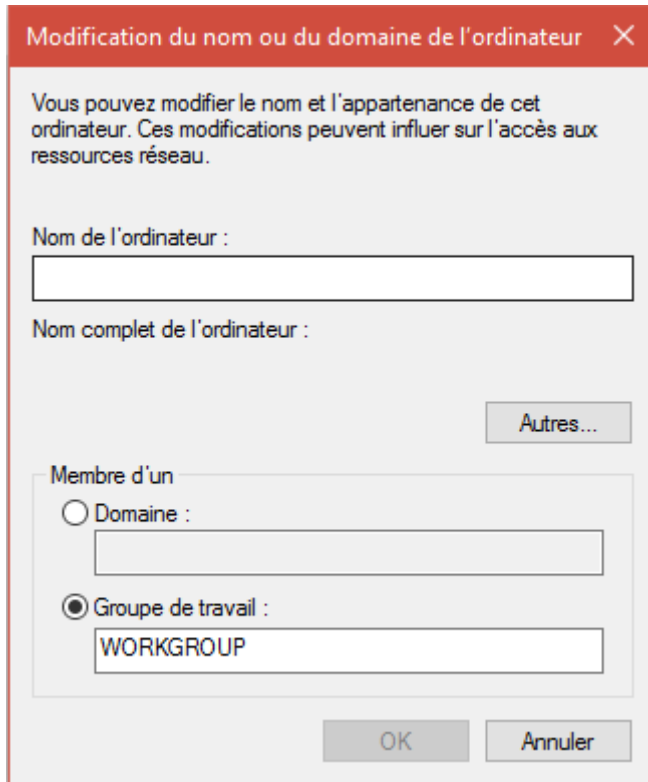
On obtient ceci :



Ensuite, cliquez sur « Modifier les paramètres ».

Une fenêtre s'ouvre, cliquez sur « Modifier ».

On obtient ceci à l'écran :



Pour changer le nom hôte de votre machine, remplissez les champs «Nom de l'ordinateur».

Exemple : PC-COMPTA

Cochez « Domaine » au lieu de groupe de travail et remplissez le champ par le nom de votre domaine dans mon cas : SUPCA.lan.

Cliquez sur « OK » pour valider.

Il vous faudra redémarrer votre ordinateur par la suite.

Après le redémarrage, votre ordinateur sera lié au domaine, il vous suffira de vous connecter avec votre nom d'utilisateur.

Dans notre cas : SUPCA\supuser

Auteur : LE GRUIEC Clément

Mail : clement@legruiec.fr

Tel : 06.33.28.26.48