Documentation gérez les postes de travail d'une entreprise

Procédure rédigée par : Vassenet-Guihot Romain

Version	Date	Auteur(s)	Commentaire
1.0	13/06/19	Romain Vassenet-Guihot	Initialisation du document
1.1	24/06/19	Romain Vassenet-Guihot	Modification professionnel du document

I - Présentation générale du scénario :

Les postes de travail de l'entreprise sont gérés par Active Directory. L'entreprise dispose d'un site distant qui n'accueille que trois personnes. Etant donnée la petite taille de ce site, jusqu'à présent les trois postes de travail de ce site étaient gérés à part sans Active Directory, mais les employés se plaignent de ne pas pouvoir accéder à tous les services de l'entreprise.

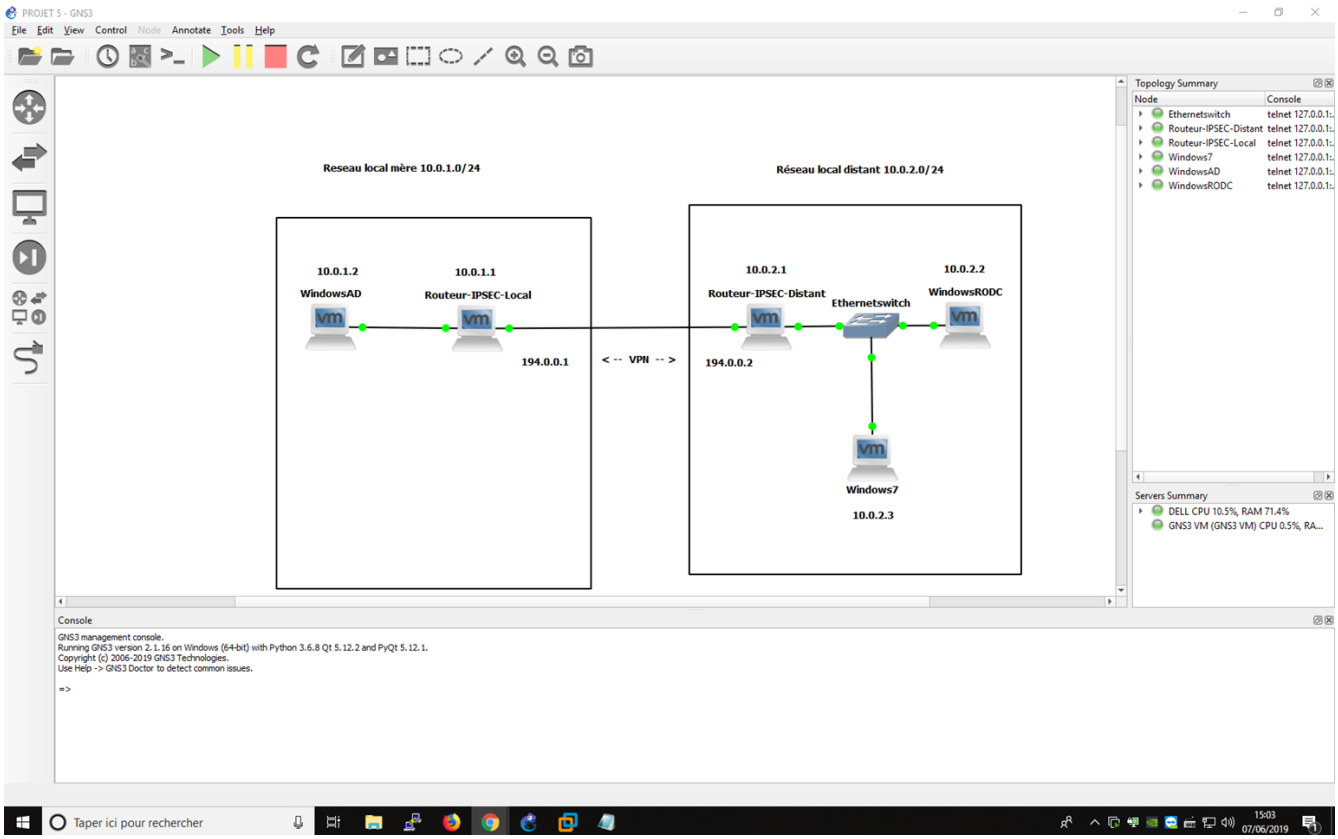
L'objectif est de pouvoir aussi gérer ces postes distants via l'AD. Pour cela il faudra créer une connexion VPN entre les deux sites pour intégrer les postes de travail du site distant dans le réseau local "mère". Il faudra donc installer un RODC sur le site distant et veiller à ce que la synchronisation avec le DC de la maison "mère" ne perturbe pas trop le réseau pendant les heures de bureau. Enfin, il faudra créer des comptes AD et appliquer toutes les GPO adaptées aux trois employés du site distant, Alice Dupont (commercial), Philippe Martin (commercial) et Christophe Henri (service technique).

II - Virtualisation GNS3 du réseau de l'entreprise :

Afin de simuler ce scénario, nous allons virtualiser notre architecture réseau grâce à GNS3.

Sur le réseau local "mère" de plan d'adressage 10.0.1.0/24, nous utiliserons un Windows Server 2019 pour l'Active Directory ainsi qu'un Linux de distribution Debian 9 pour notre Routeur VPN.

Sur le réseau Distant de plan d'adressage 10.0.2.0/24, nous utiliserons également un Windows Server 2019 pour le RODC ainsi qu'un Linux de distribution Debian 9 pour notre Routeur VPN. Pour simuler un poste de travail sur le site distant, nous utiliserons un Windows 7.



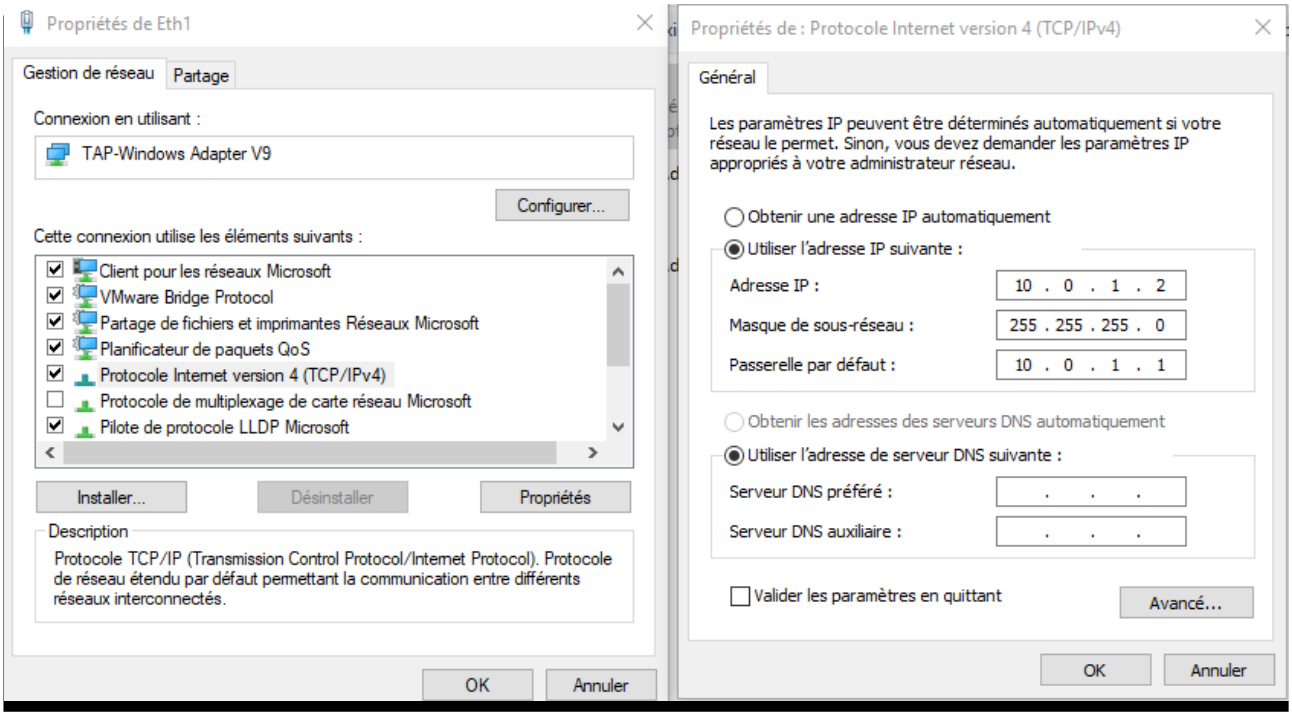
Architecture Réseau GNS3 – Projet 5

(Zoom nécessaire pour mieux visualiser)

III - Installation Standard Active Directory :

Une fois l'installation de notre Windows Server 2019 faite, il faudra configurer sa carte réseau Ethernet afin de respecter notre plan d'adressage réseau et la topologie générale.

Pour configurer la carte réseau, il faudra faire simplement Windows + R, puis rechercher le programme suivant : npca.cpl. Avec un clic droit sur la carte réseau, dans propriétés, puis avec un double click sur Protocol Internet Version 4, nous avons la possibilité de configurer manuellement la carte réseau. (Ces configurations réseaux seront obligatoire sur l'ensemble des machine Windows installées pour cette démonstration)



Configuration réseau IPV4 de la carte Ethernet Active Directory

Il nous faut ensuite vérifier que notre Windows Server 2019 Ping correctement le Routeur VPN afin de vérifier que leur plan d'adressage est bien sur le même réseau et qu'il n'y a pas d'erreur.

Après quoi nous devons installer le service AD DS pour active Directory en ajoutant des rôles et des fonctionnalités, service AD DS, puis accepter l'installation par défault. Une fois l'installation terminée, il faudra promouvoir en tant que contrôleur de domaine.

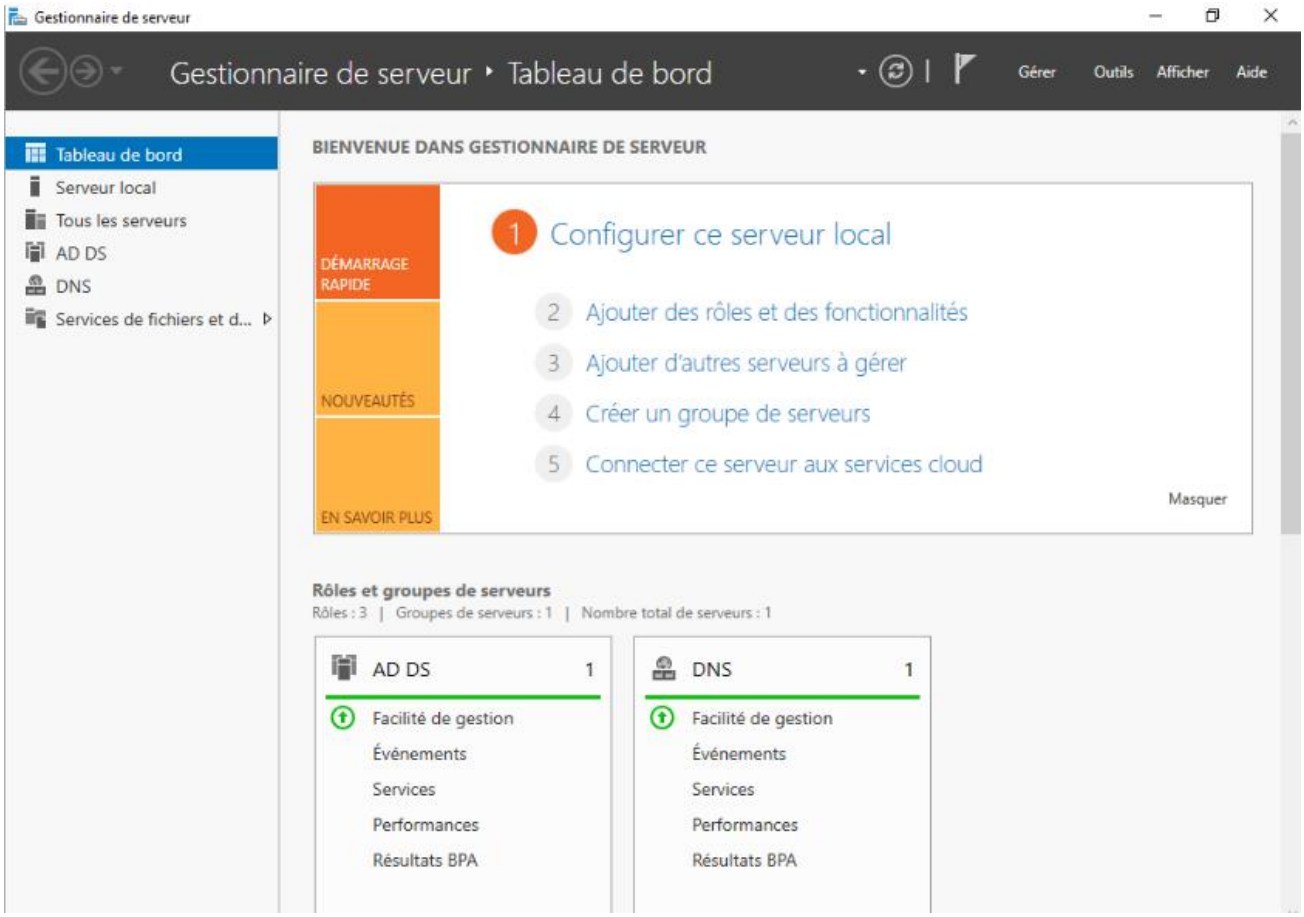
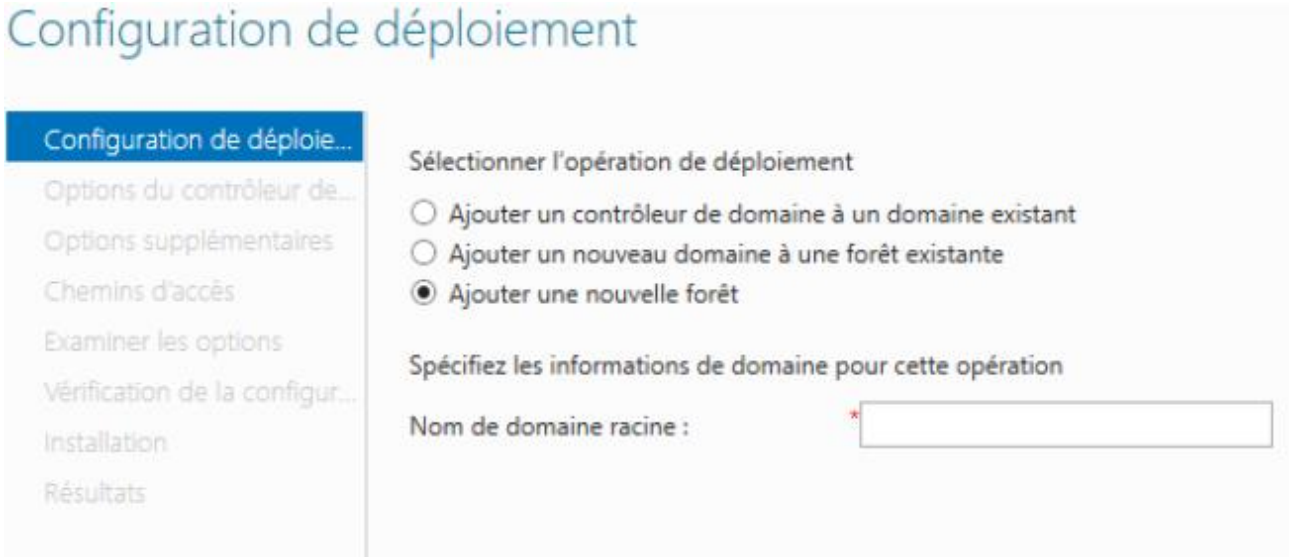


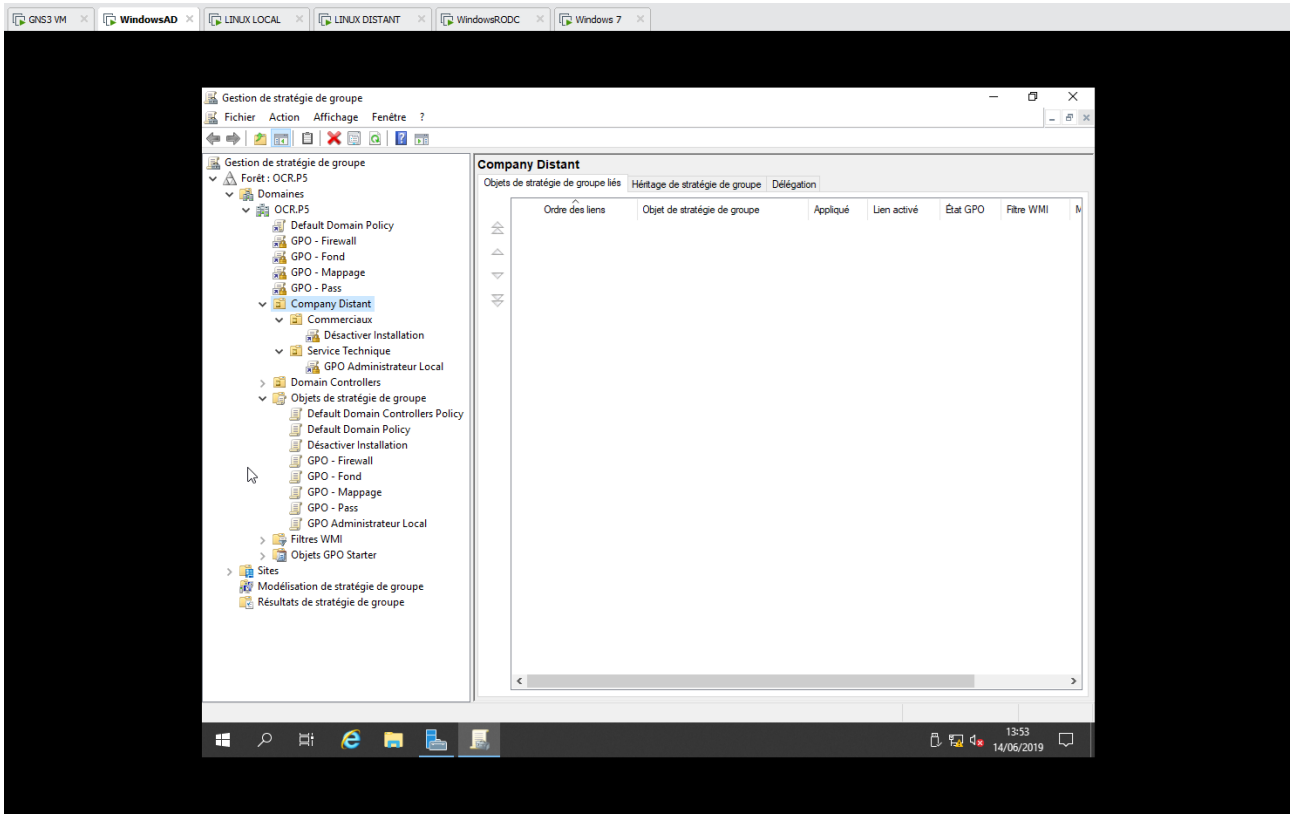
Tableau de bord Active Directory, Ajouter des rôles et des fonctionnalités



Promouvoir en tant que contrôleur de domaine AD

Notre domaine sera nommé OCR.P5.

Afin de mieux organiser notre domaine, nous allons créer également des unités organisationnelles à partir de l'outil Utilisateurs et ordinateurs Active Directory. Puis à partir de notre domaine, ici « OCR.P5 » nous allons créer notre unité « Company Distant »



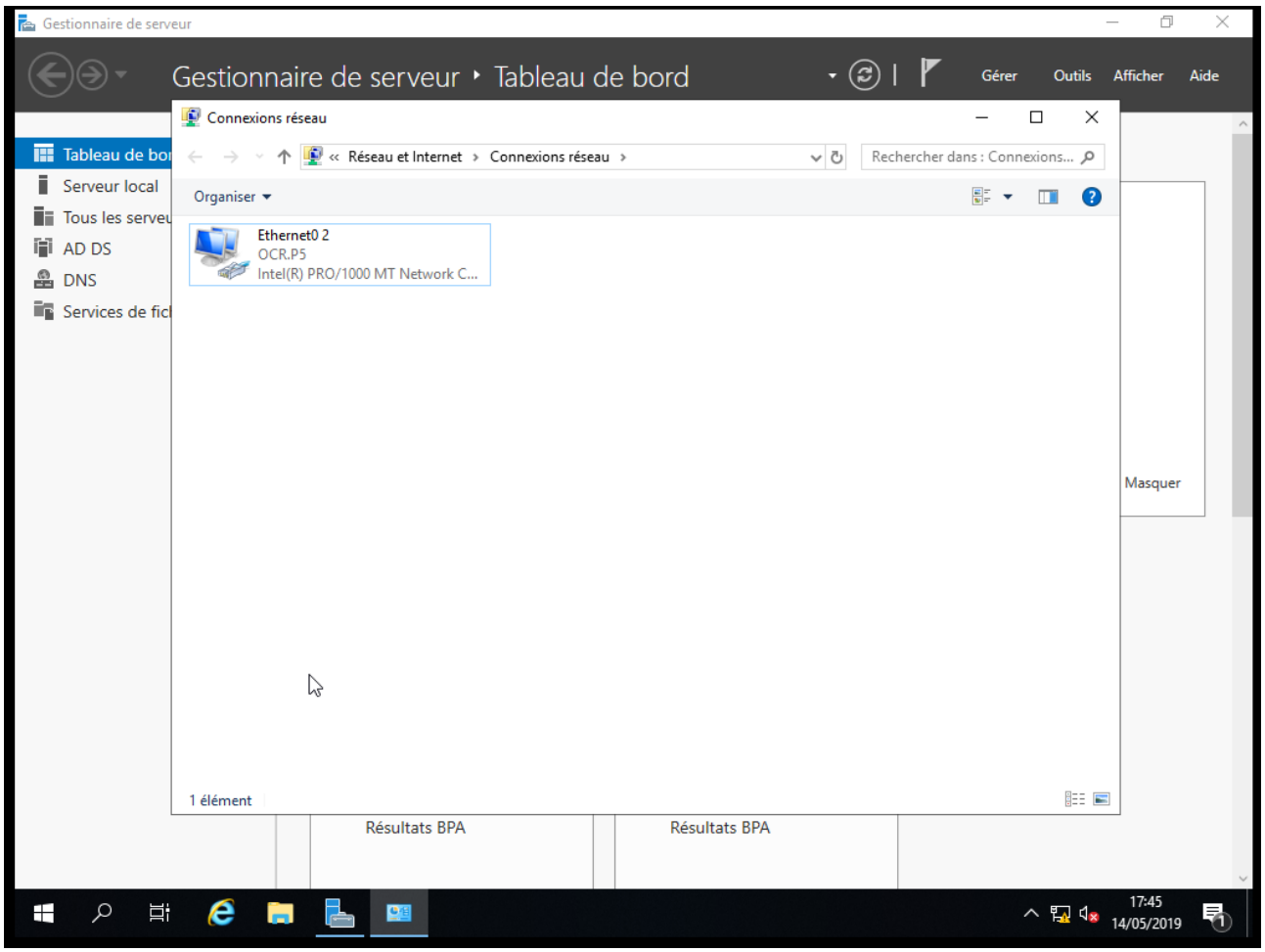
Gestion de stratégie de groupe Active Directory - GPO

Nous pouvons apercevoir également des GPO dans la capture d'écran, que nous verrons lors de l'Installation Management Active Directory dans la partie VI.

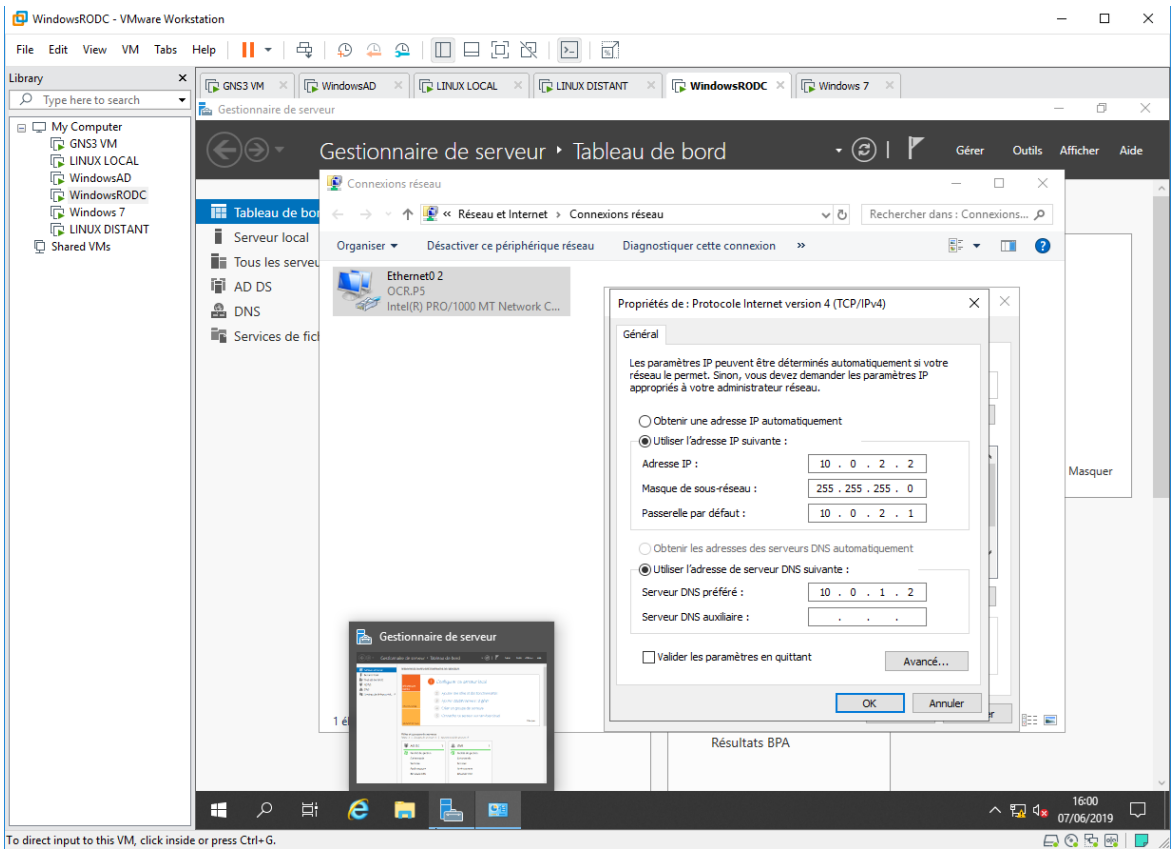
IV - Installation RODC :

Afin d'installer sur le site distant le RODC sur notre Serveur Windows 2019 ayant pour IP 10.0.2.2, nous devons de nouveau installer le service AD DS en ajoutant des rôles et fonctionnalités puis le promouvoir en tant que contrôleur de domaine.

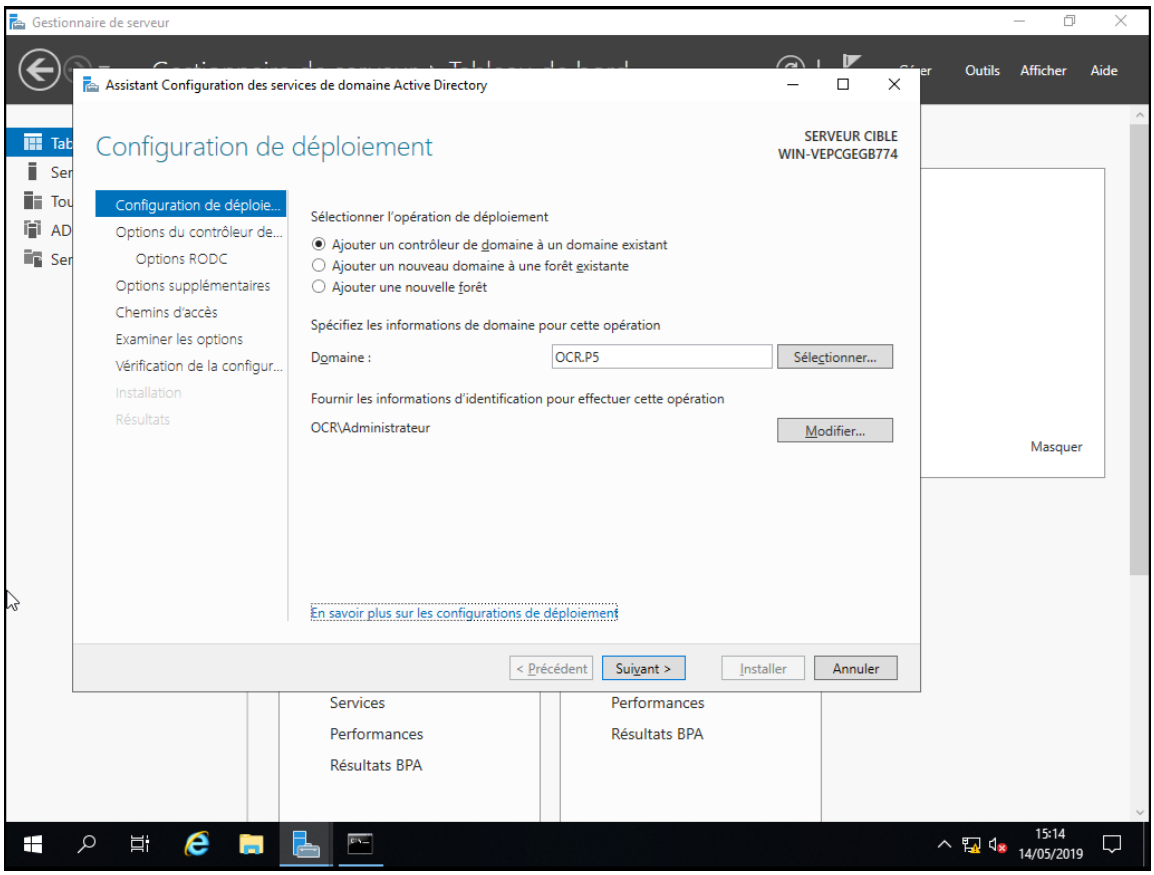
Il faudra également penser à ajouter le contrôleur de domaine au domaine existant OCR.P5 puis définir les options du contrôleur de domaine en RODC, lecture seule



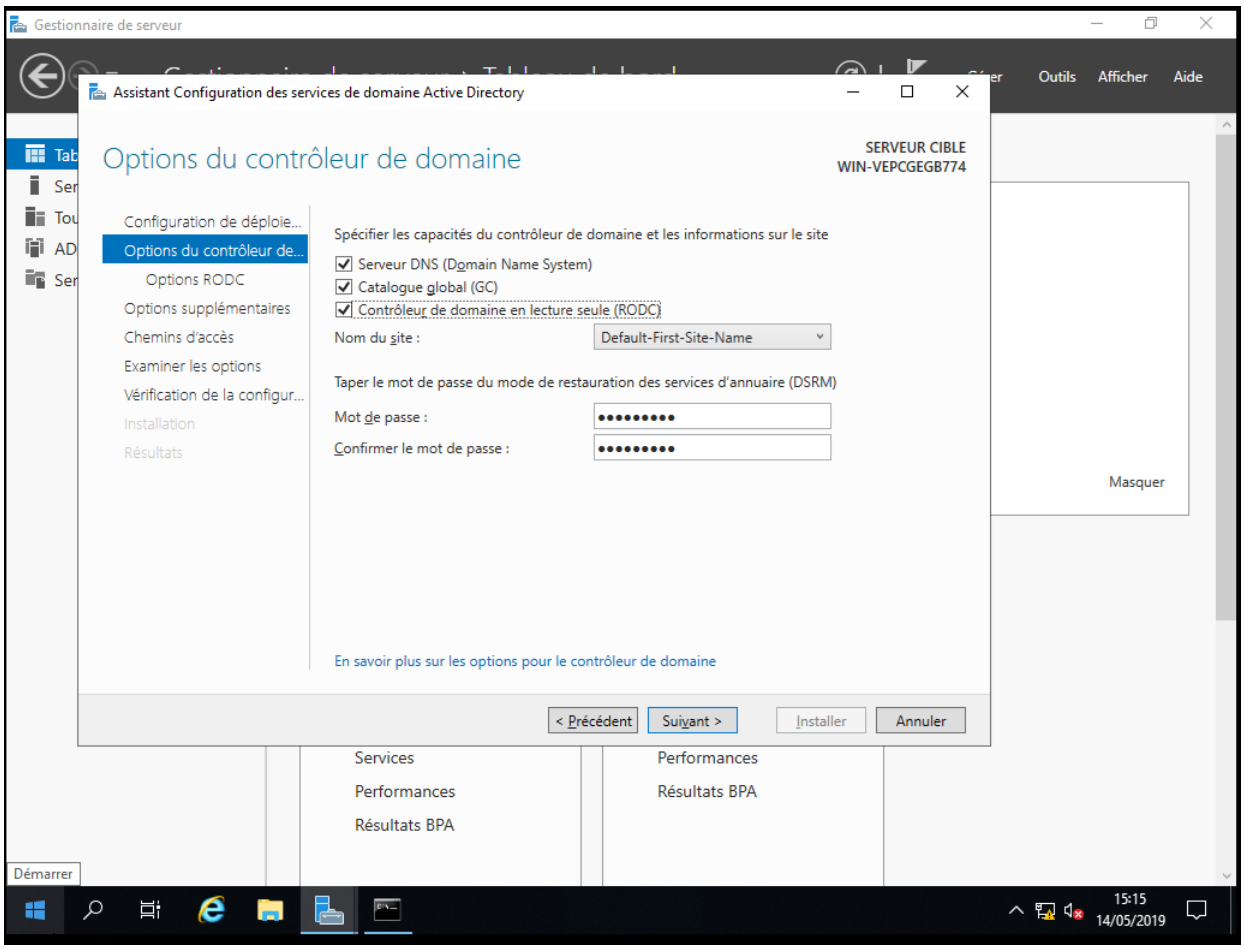
Carte Réseau Ethernet RODC – [ncpa.cpl via exécuter (Windows + R)]



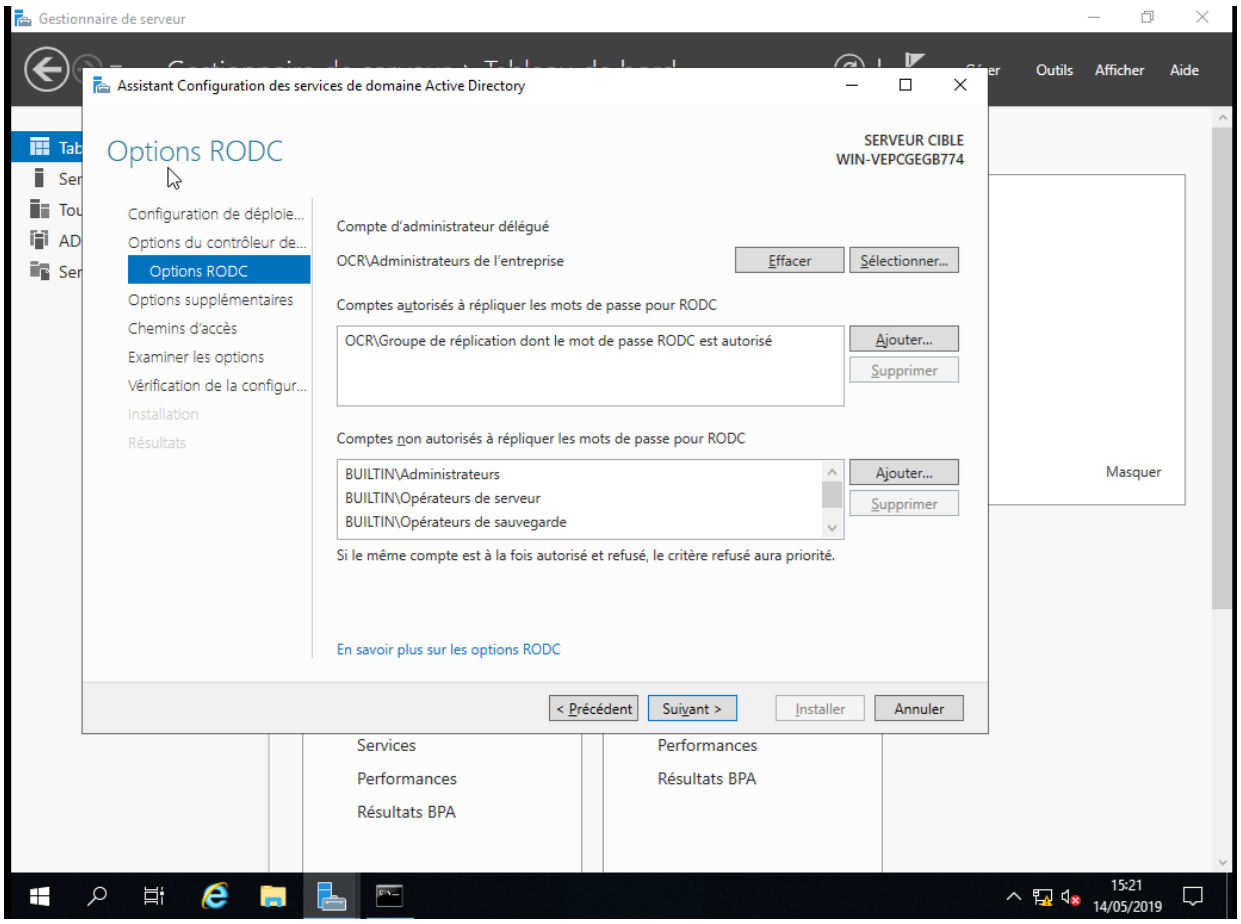
Configuration réseau IPV4 de la carte Ethernet RODC



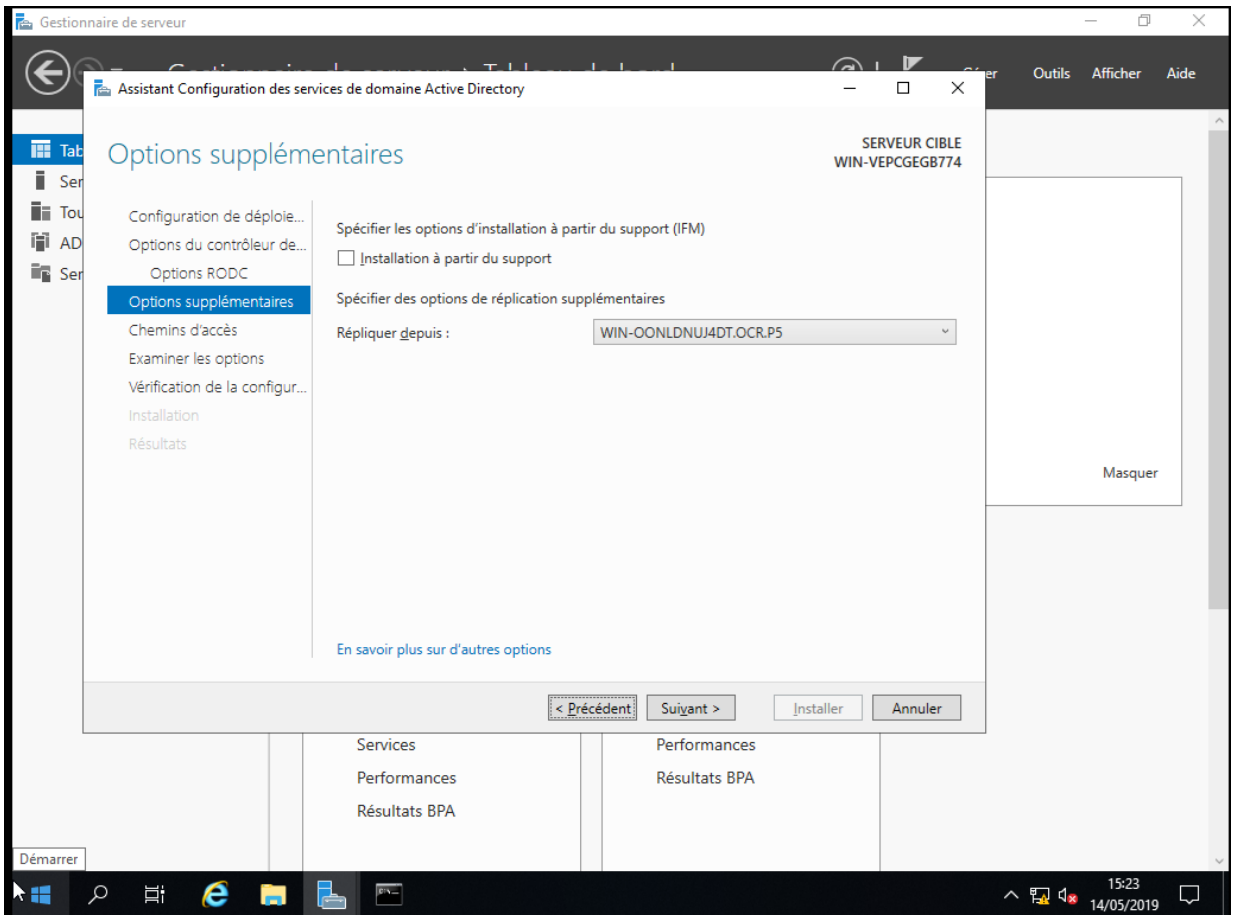
Promouvoir contrôleur de domaine en tant que RODC – L'ajouter à un domaine existant



Configuration contrôleur en tant que lecture seule - RODC



Configuration RODC - Réplication de mot de passe



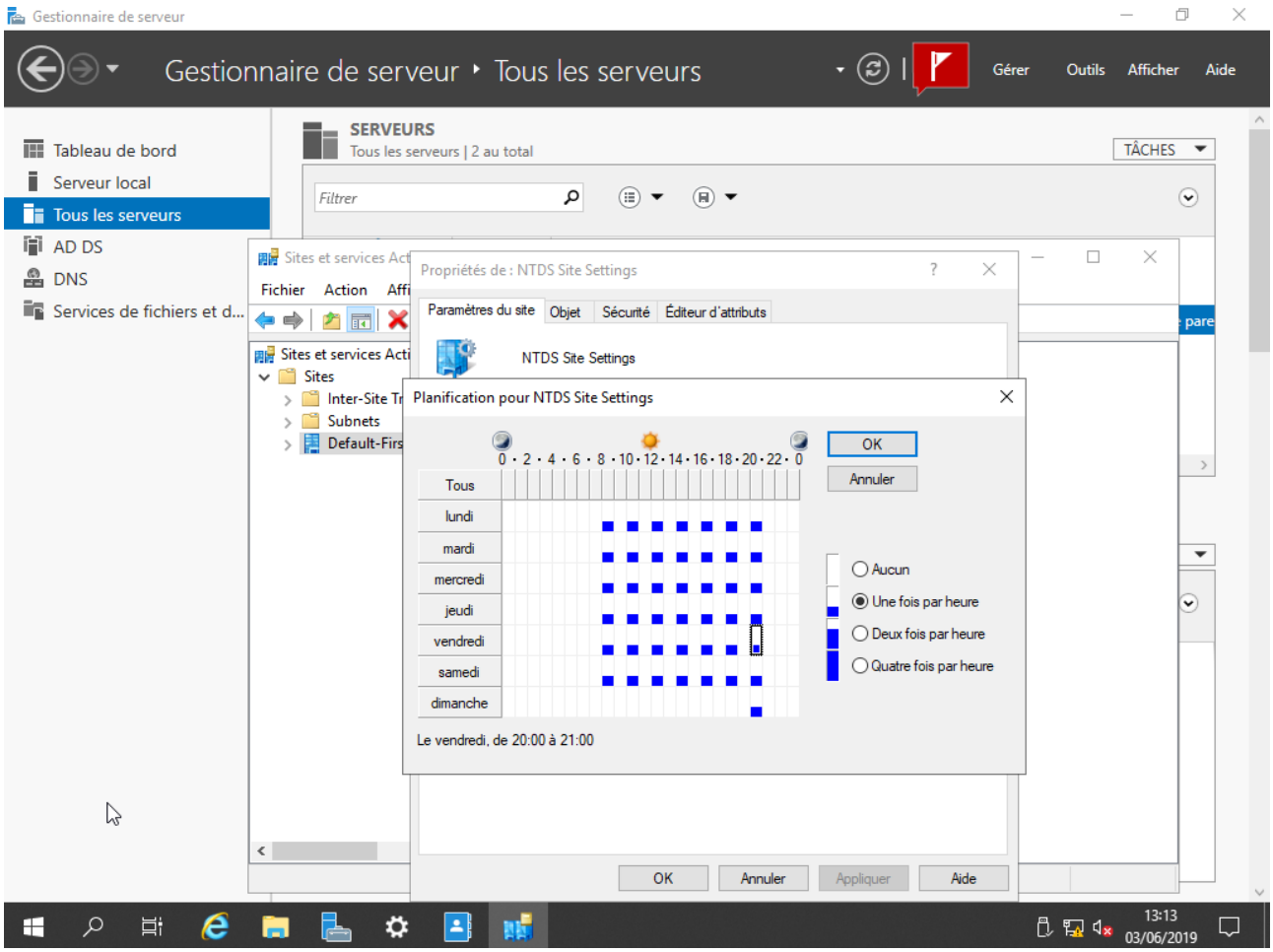
Configuration RODC - Réplication depuis AD

Après quoi la configuration est automatique, si l'on souhaite installer sur une partition pour plus de sécurité on peut également configurer cela dans l'étape d'après mais, par défaut cela sera dans le sysvol.

Nous devons également programmer la planification de la réplication de l'AD vers le RODC sur des plages horaires précises.

Afin de réduire le trafic durant les heures de bureau nous veillerons à réduire un maximum la réplication.

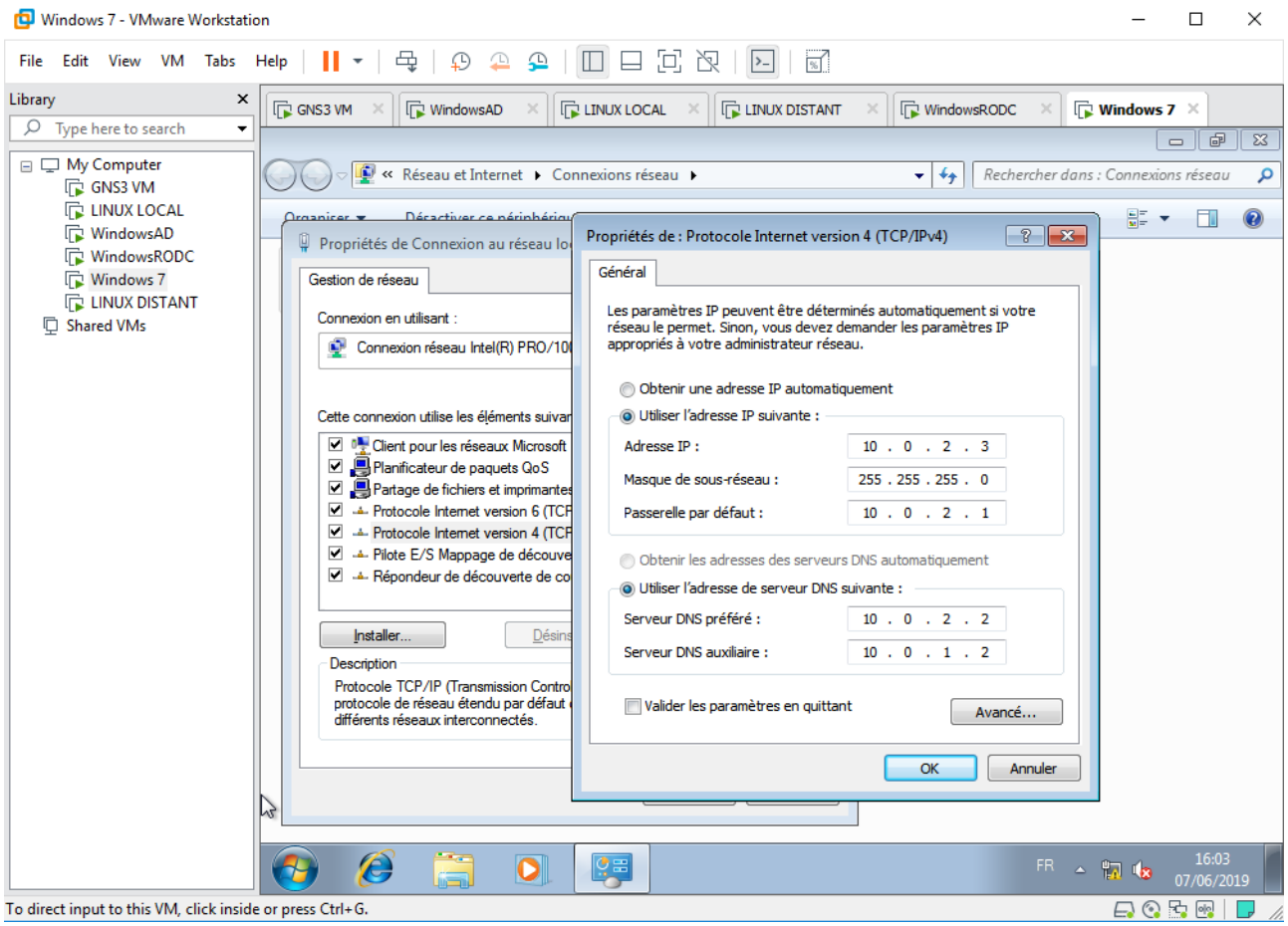
Pour cela il faudra utiliser l'outil site et service active directory et modifier la planification.



Planification Hebdomadaire de réplication AD vers RODC

V - Installation du poste Client :

Afin de simuler l'un des postes des employés, il faudra installer windows 7 et configurer sa carte réseau en définissant les DNS pour que la machine discuter obligatoirement avec le RODC. Les DNS de la carte réseau sont indispensables pour communiquer avec un serveur Windows Active Directory ou RODC.



Configuration réseau IPV4 de la carte Ethernet Windows 7

VI - Configuration Tunnel VPN IPSEC :

Afin de configurer le Tunnel VPN IPSEC nous devons configurer les adressages réseaux sur les machines linux locale et distante afin de respecter notre topologie.

Il nous faut également configurer les paquets indispensables pour l'utilisation du client strongswan pour créer notre tunnel VPN IPSEC.

```
apt update && apt upgrade –y

apt install strongswan –y
```

Il nous faut également configurer nos deux Machines Linux en mode routeur. Pour cela on modifie notre fichier sysctl.conf :

Fichier de configuration routage : nano/etc/sysctl.conf

```
net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

Fichier de configuration réseau linux local : nano/etc/network/interfaces

```
auto ens32

iface ens32 inet static

address 194.0.0.1

netmask 255.255.255.0

option-routeur 194.0.0.2


auto ens33

iface ens33 inet static

address 10.0.1.1

netmask 255.255.255.0

option-routeur 194.0.0.1
```

Fichier de configuration réseau Linux Distant : nano/etc/network/interfaces

```
auto ens32

iface ens32 inet static

address 194.0.0.2

netmask 255.255.255.0

option-routeur 194.0.0.1


auto ens33

iface ens33 inet static

address 10.0.2.1
```

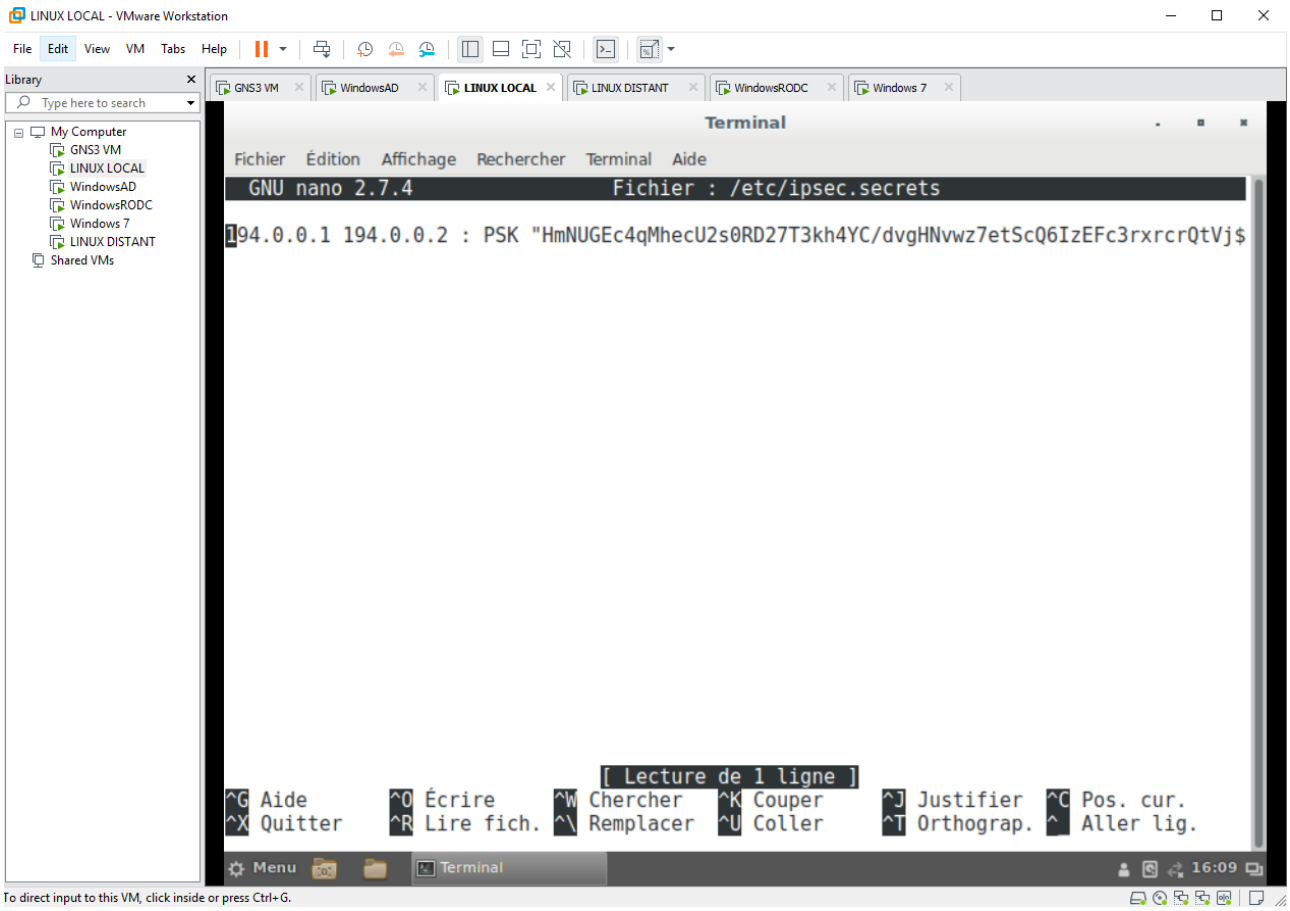
```
netmask 255.255.255.0

option-routeur 194.0.0.2
```

Pour créer un tunnel VPN, les deux sites doivent pouvoir s'échanger une clé en base64 afin de sécuriséer les échanges.

Pour générer une clé nous allons utiliser la commande suivant sur la machine locale.

```
openssl rand -base64 64
```

Il nous faudra ensuite ajouter la configuration de cette clé partagée sur les deux Routeur VPN en renseignant dans le fichier de configuration suivant le format : IP WAN LOCAL IP WAN DISTANT CLE DE SECURITE



Fichier de configuration sur routeur Linux Local /etc/ipsec.secrets - Partage clé base64 entre les reseaux sortant de nos deux routeurs.

Après quoi il nous reste plus qu'à créer notre fichier de configuration du VPN pour que notre réseau local mère communique correctement avec le réseau local distant :

Rappel : Réseau Local mère en 10.0.1.0/24 & Réseau Local Distant en 10.0.2.0/24

Fichier de configuration VPN Linux local : nano/etc/ipsec.conf

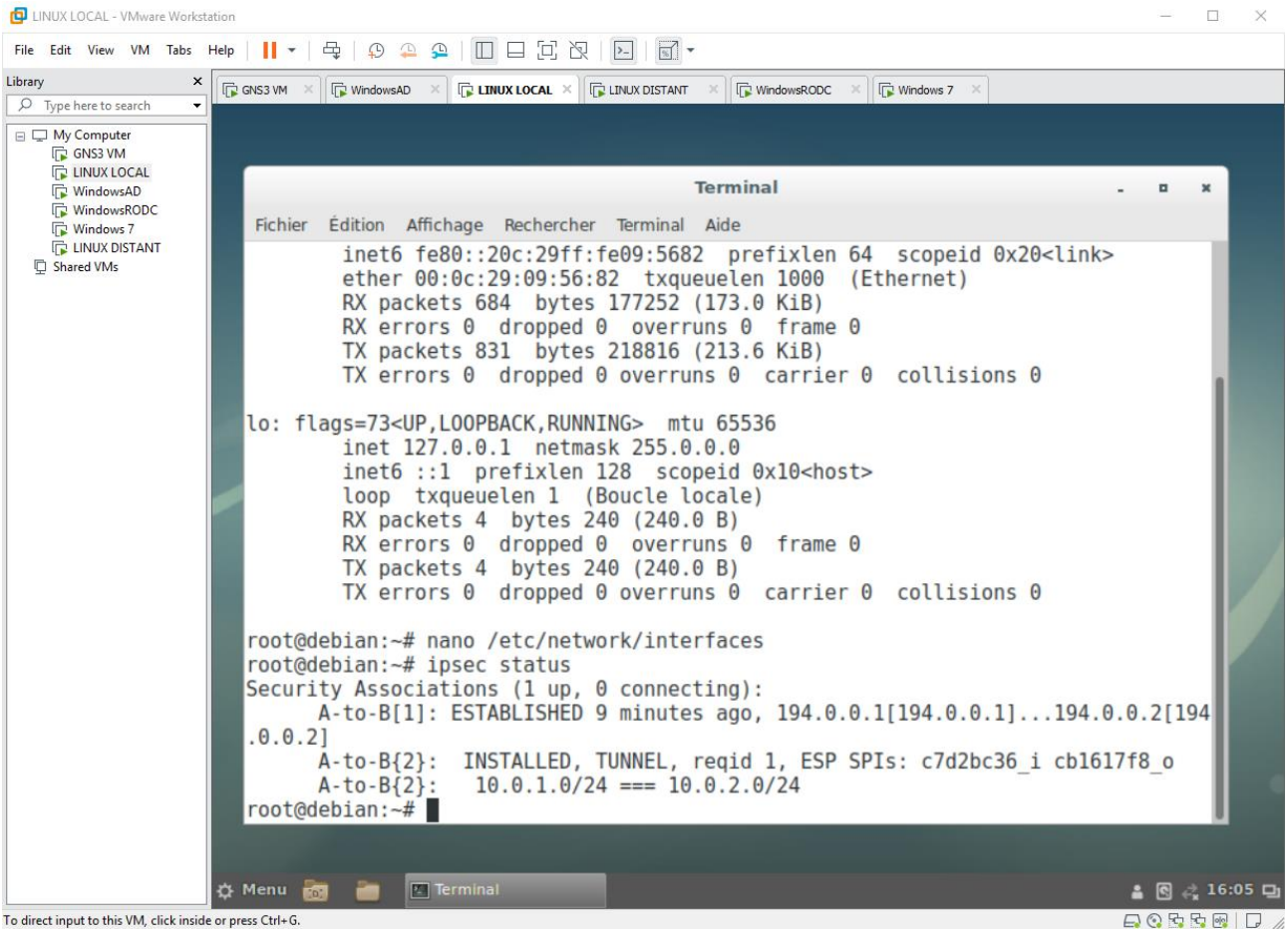
```
# basic configuration
config setup
        charondebug= « all »
        uniqueids=yes
        strictcrlpolicy=no

# connection to A o B
conn A-to-B
    authby=secret
    left=%defaultroute
    leftid=194.0.0.1
    leftsubnet=10.0.1.1/24
    right=194.0.0.2
    rightsubnet=10.0.2.1/24
    ike=aes256-sha2_256-modp1024 !
    esp=aes256-sha2_256 !
    keyingtries=0
    ikelifetime=1h
    lifetime=8h
    dpddelay=30
    dpdtimeout=120
    dpdaction=restart
    auto=start
```

Fichier de configuration VPN Linux distant : nano/etc/ipsec.conf

```
# basic configuration
config setup
        charondebug= « all »
        uniqueids=yes
        strictcrlpolicy=no

# connection to B o A
conn B-to-A
    authby=secret
    left=%defaultroute
    leftid=194.0.0.2
    leftsubnet=10.0.2.1/24
    right=194.0.0.1
    rightsubnet=10.0.1.1/24
    ike=aes256-sha2_256-modp1024 !
    esp=aes256-sha2_256 !
```

```
keyingtries=0
ikelifetime=1h
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=restart
auto=start
```

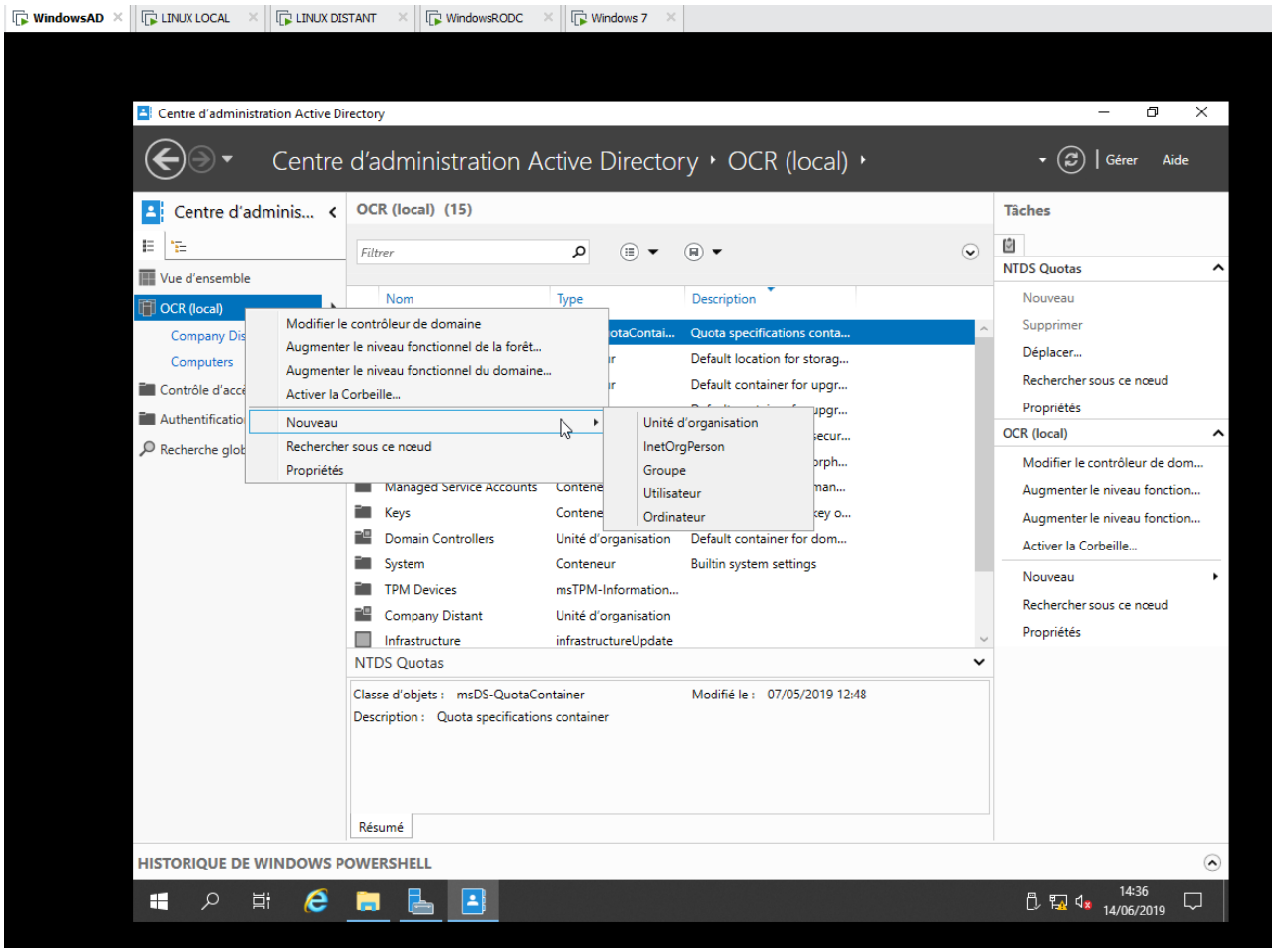
Afin de vérifier la connectivité du VPN on fait la commande suivante : ipsec status



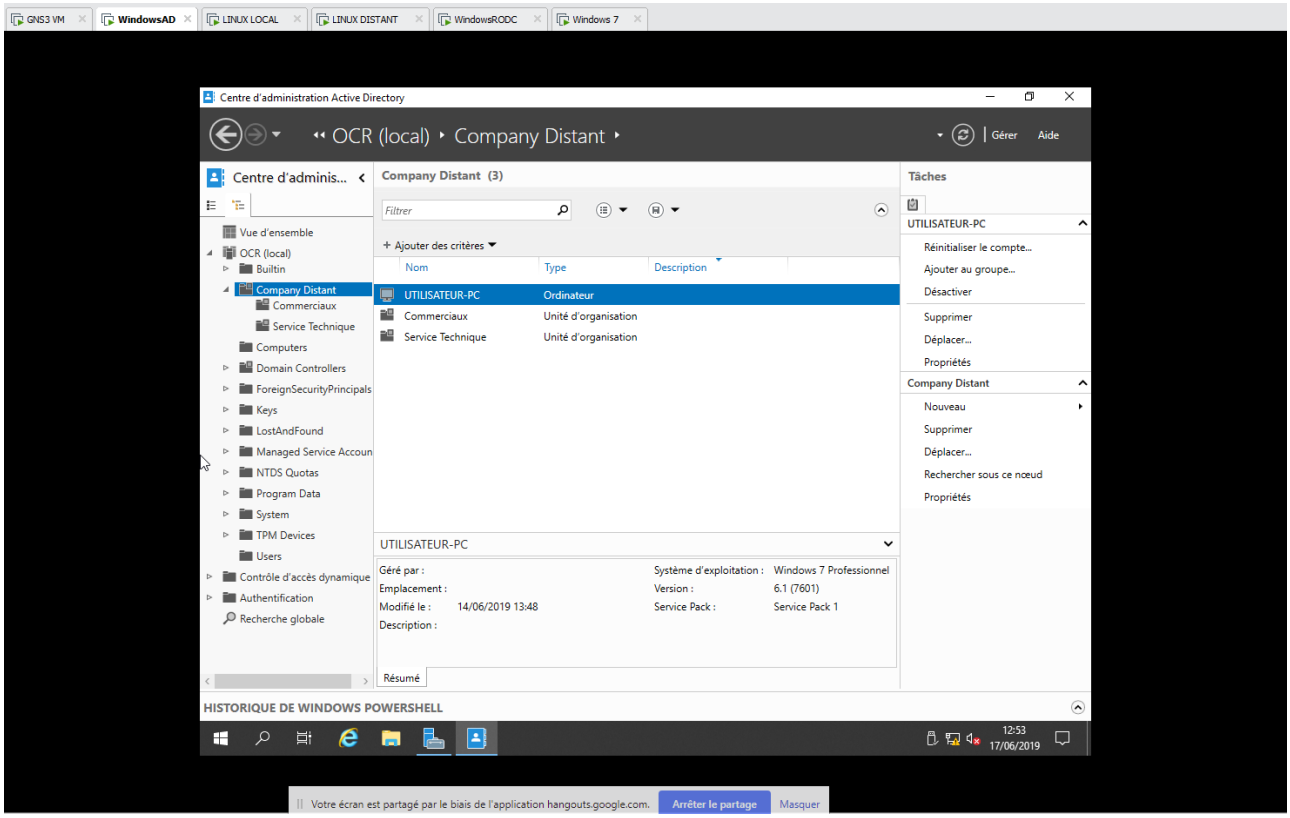
Terminal Routeur Linux Local - ipsec status – Tunnel VPN actif entre nos deux réseaux, local & distant

VII - Configuration UO & GPO :

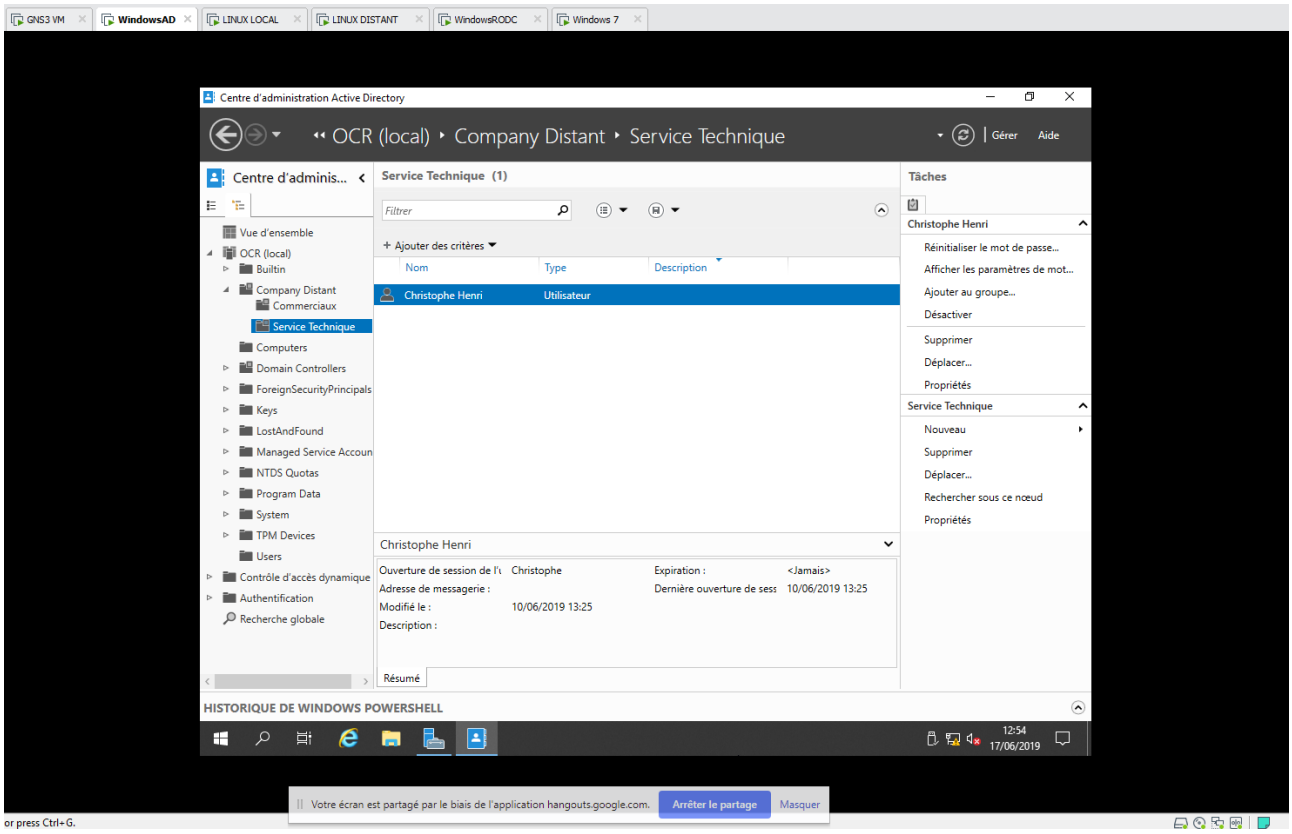
Afin de hiérarchiser de façon claire et précise une entreprise sous active directory nous avons besoin de connaitre les effectifs humains, les différents métiers, et également les entreprises externes qui auront également besoin de se connecter aux services de l'entreprise sous le même domaine.



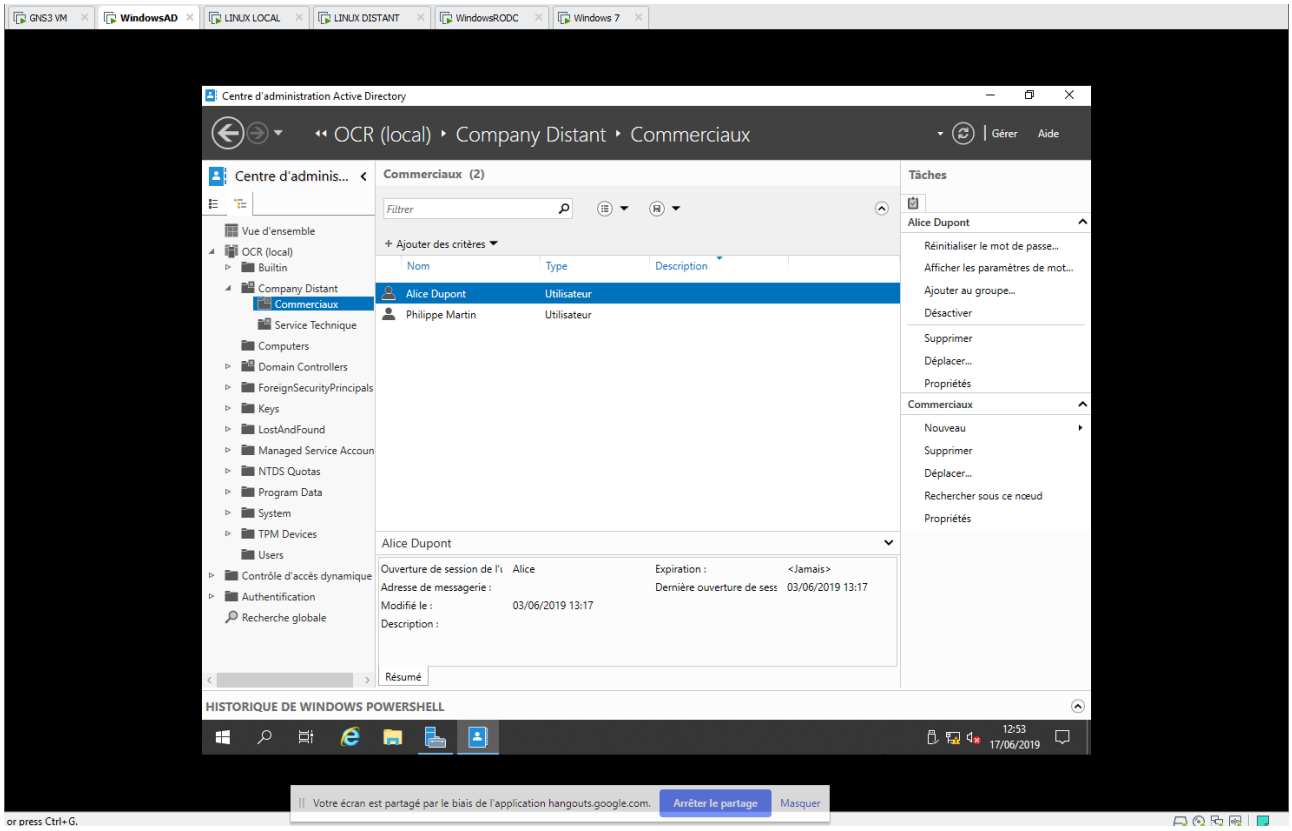
Centre d'administration pour créer des unités organisationnelles via Active Directory



Classification en UO de mon entreprise fictive par département via mon AD



UO Utilisateur de mon departement Service Technique - AD

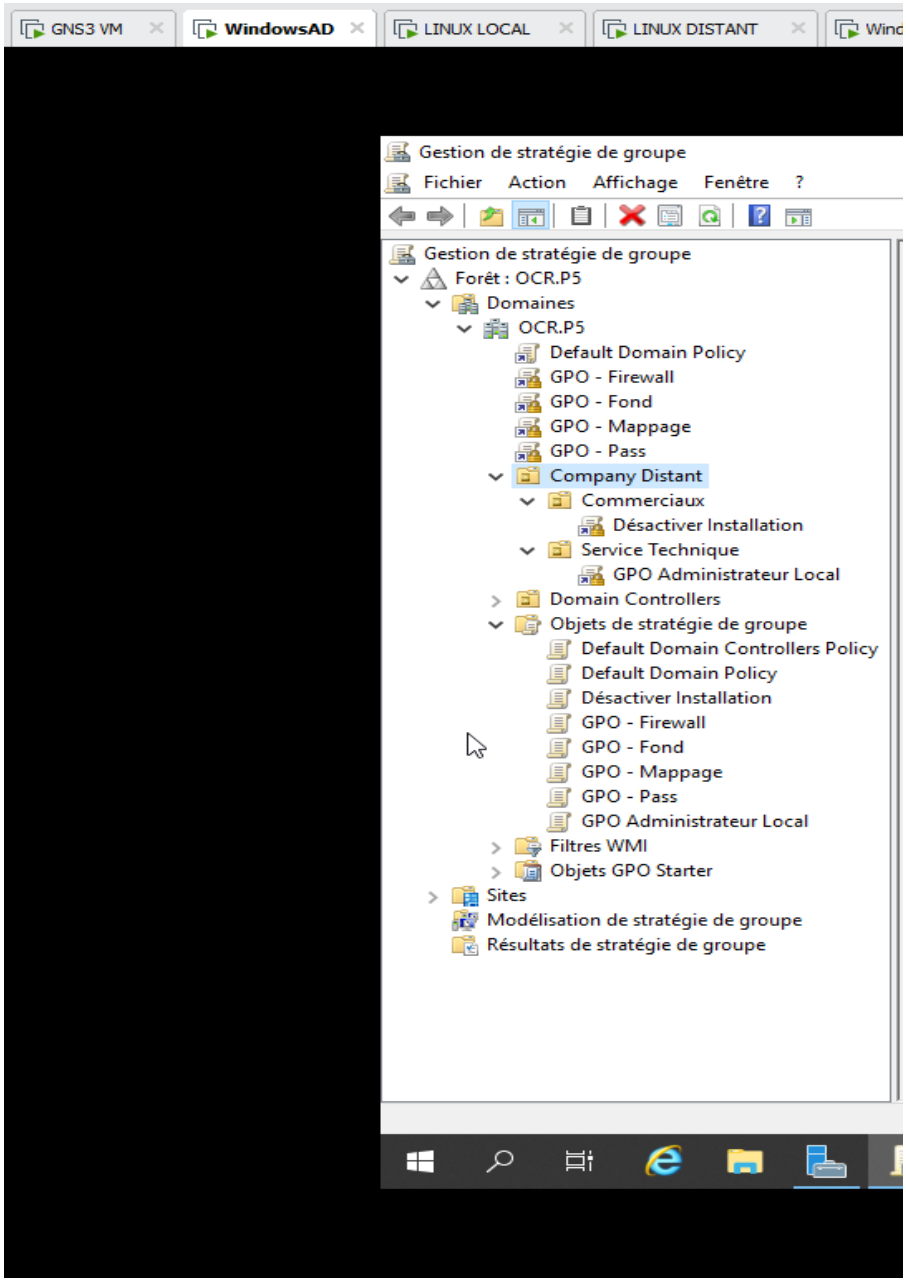


UO Utilisateur de mon departement Commercial - AD

Parmi les différents rôles d'un Active Directory se trouve le rôle de gestion du parc. Active Directory permet de gérer l'ensemble des machines et utilisateurs du système d'information, et pour cela utilise les "stratégies de groupe".

Concrètement, les GPO sont un ensemble de règles/actions qui s'appliquent à un ensemble bien défini d'objets. Une GPO permet de faire beaucoup de choses telles que modifier la complexité des mots de passes, le pare-feu, le fond écran au démarrage de la session, des taches planifiées, des mappages réseaux et bien d'autres encore.

Ce GPO sont automatiquement crées dans Objets de stratégie de groupe mais ces dernières peuvent être liées dans l'arborescence de notre entreprise sous active directory.



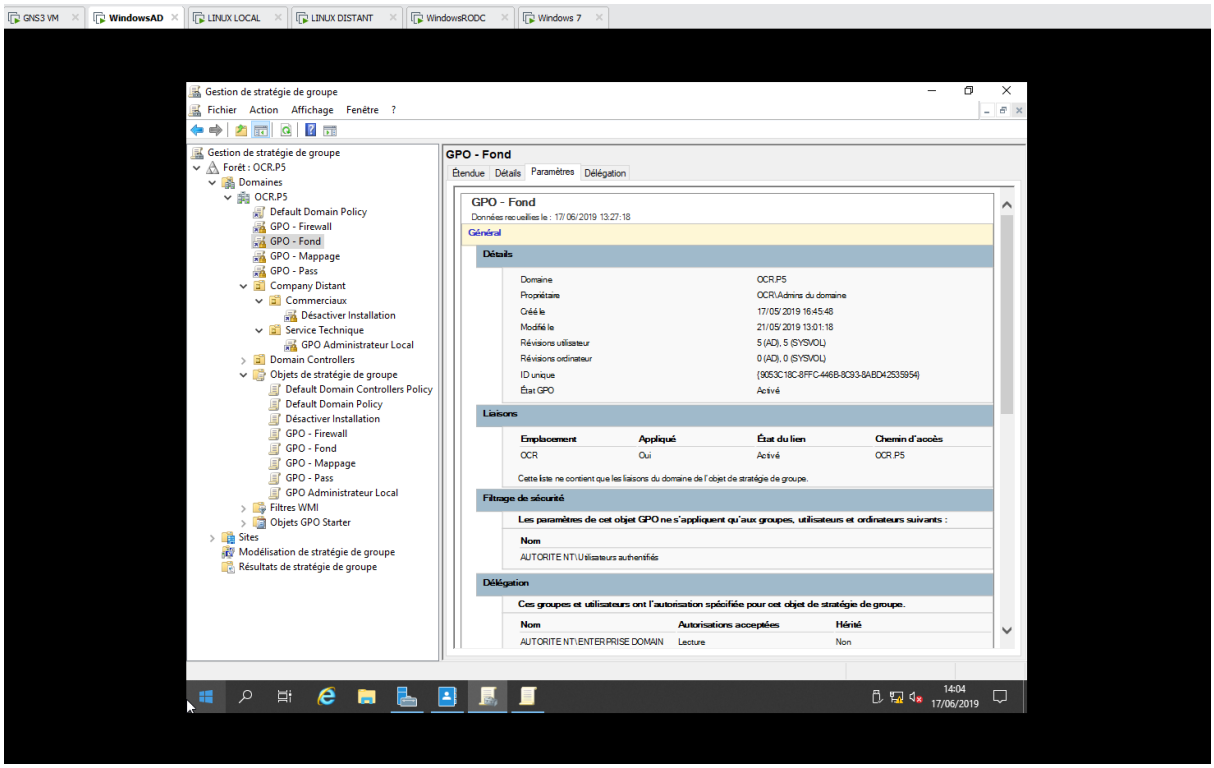
Arborescence des stratégies de groupe - AD

Avec un click droit puis créer un GPO à ce domaine et le lié ici, nous avons la possibilité de « hiérarchiser » nos règles aux groupes définies lors de la création de nos unités organisationnelles.

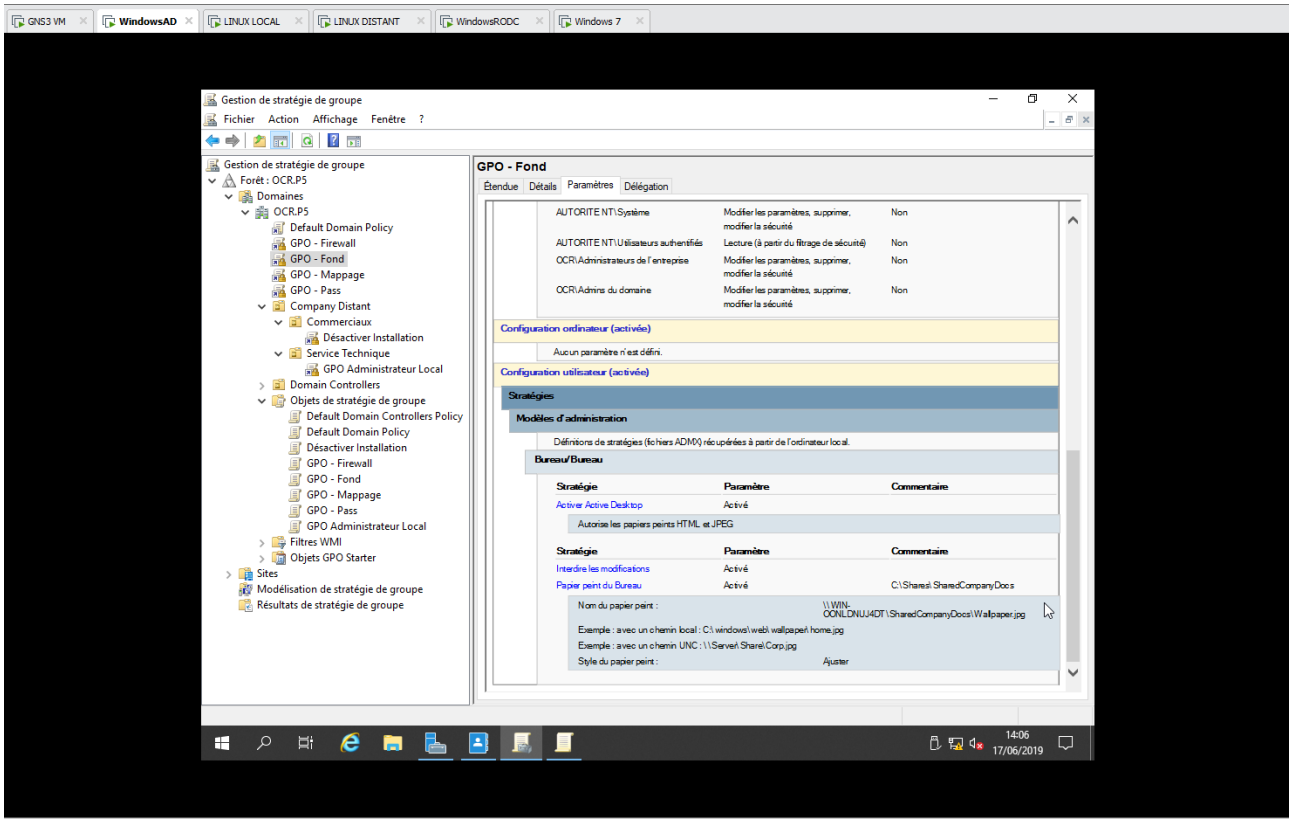
Il faut également bien penser à les activer avec un click droit sur la GPO ciblée pour les activer.

Voici quelques exemples de GPO configurés et activés avec le détail de l'arborescence de l'installation :

GPO Fond Ecran Entreprise :

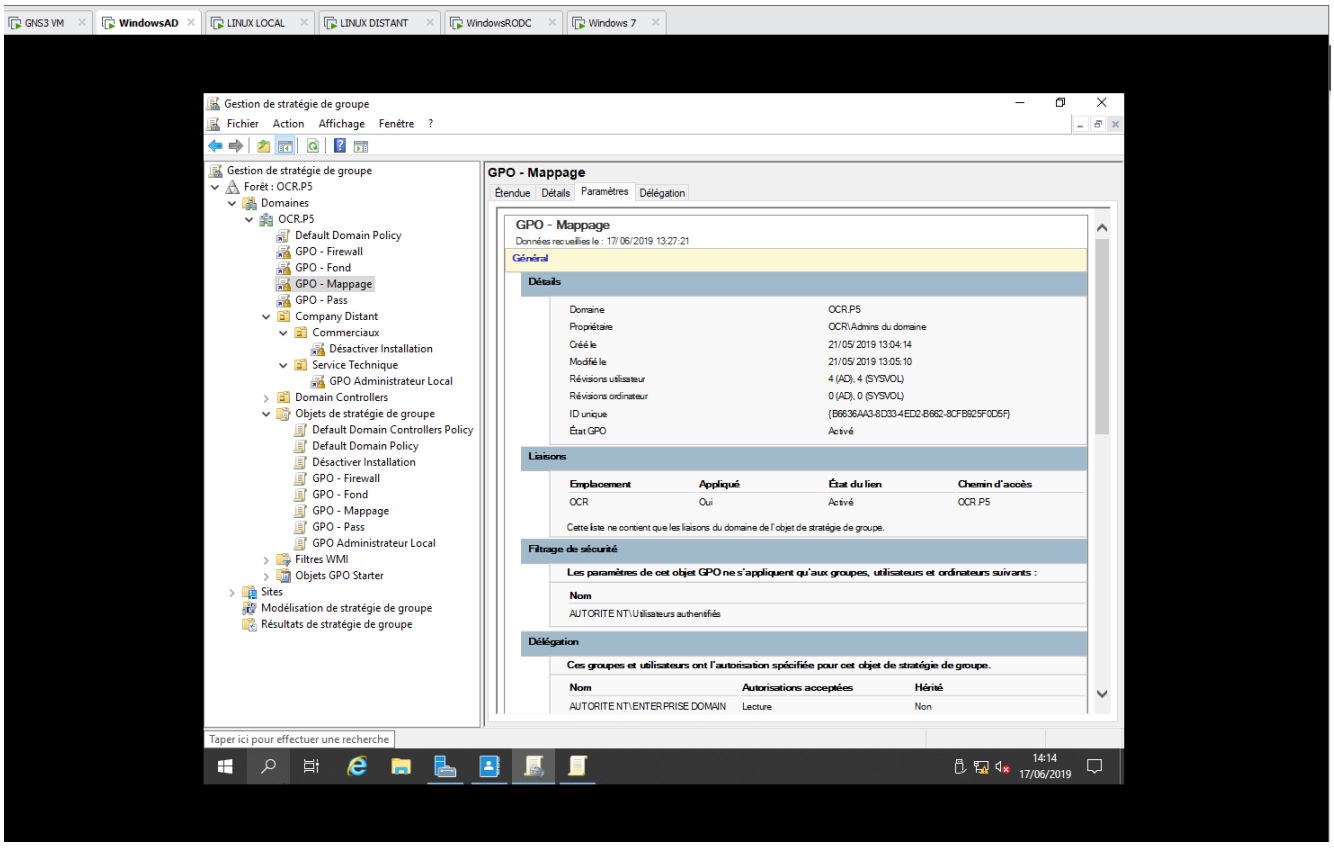


Arborescence détaillé GPO fond 'écran - AD

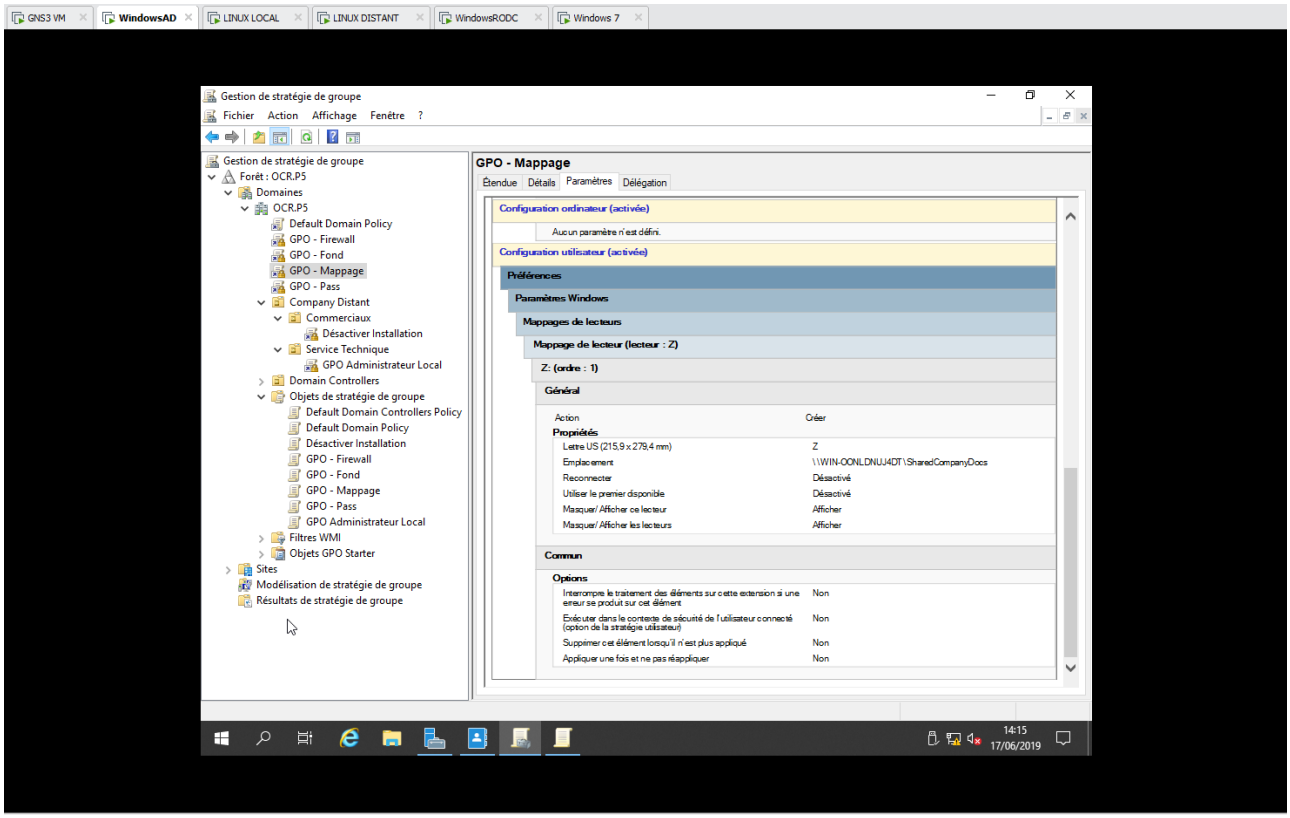


Arborescence détaillé n°2 GPO fond 'écran - AD

GPO Mappage Réseau :

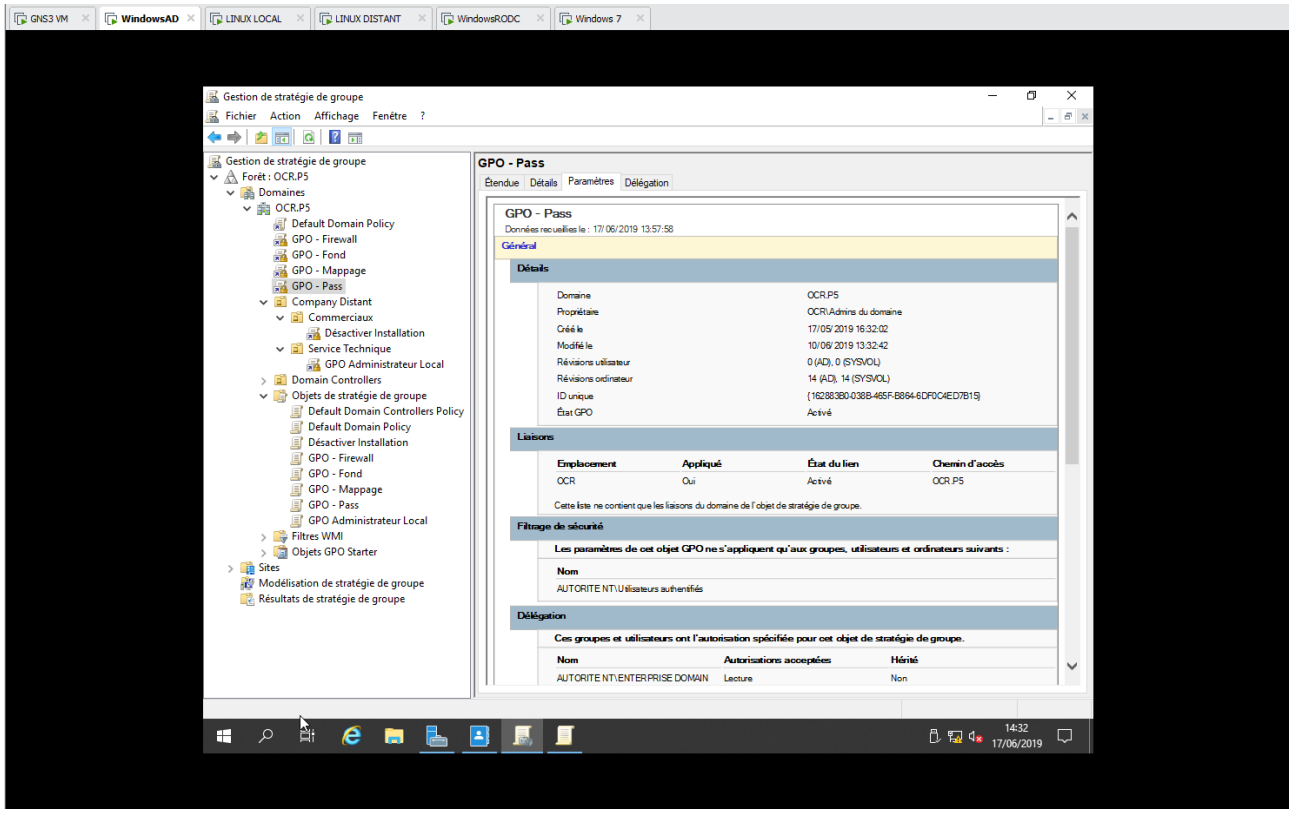


Arborescence détaillé GPO Mappage Réseau - AD

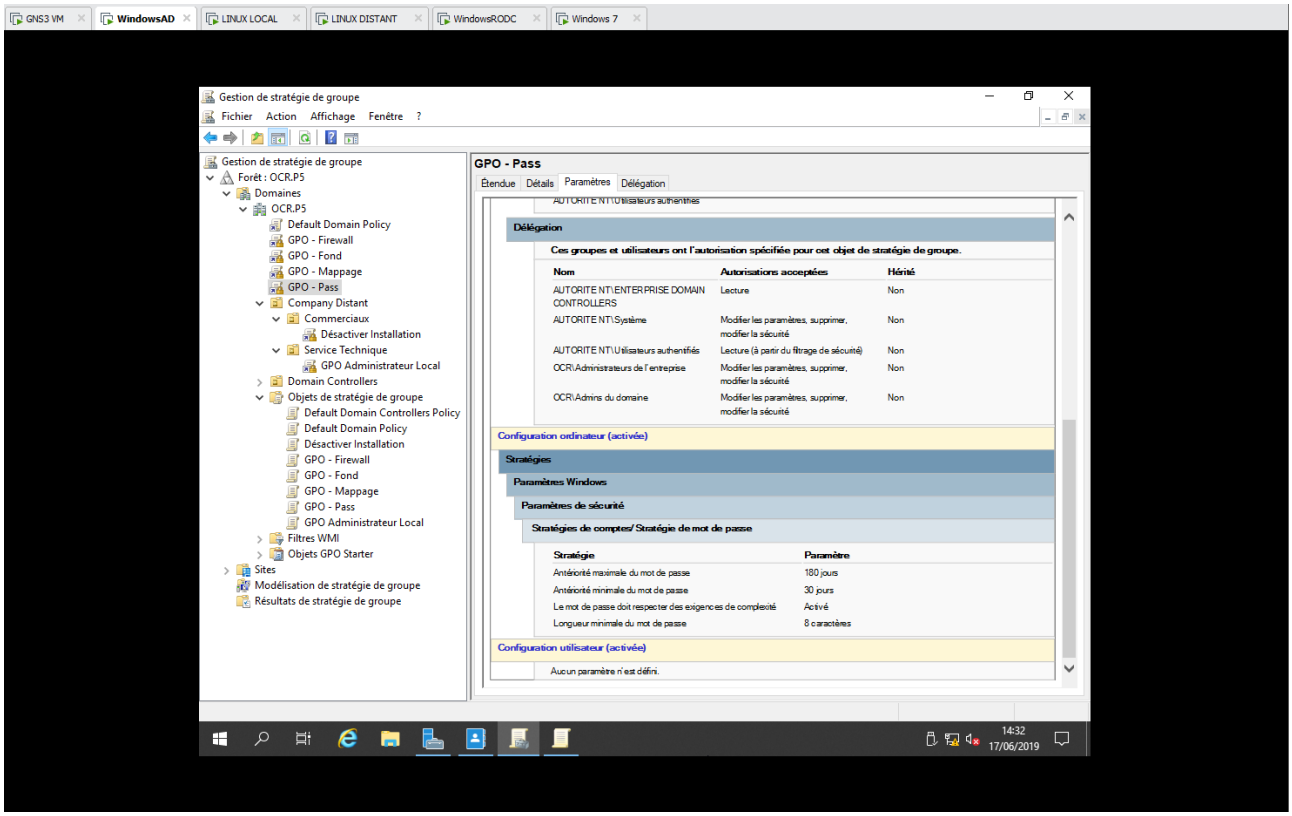


Arborescence détaillé GPO Mappage Réseau n°2 - AD

GPO Complexité Mot de Passe :

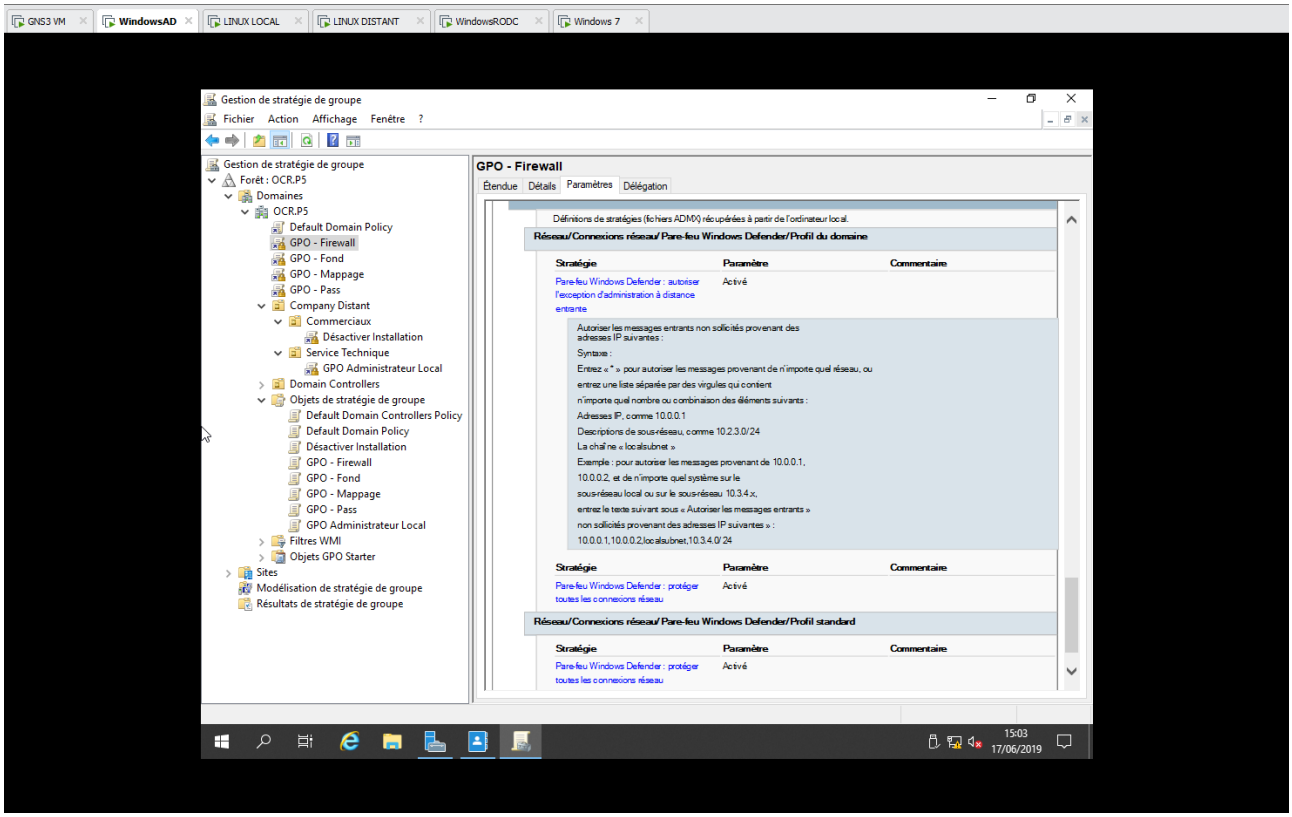


Arborescence détaillé GPO Complexité Mot de Passe - AD



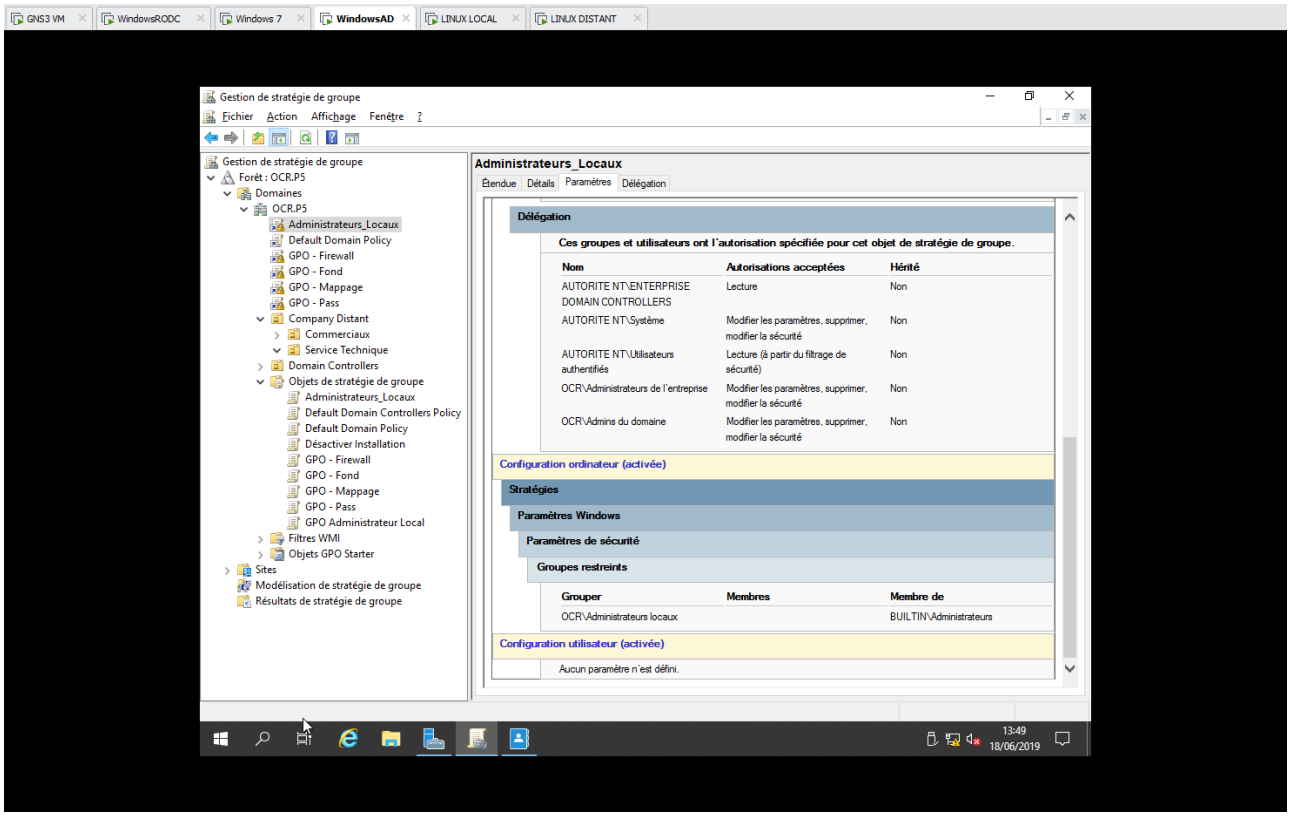
Arborescence détaillé GPO Complexité Mot de Passe n°2 - AD

GPO Firewall :



Arborescence détaillé GPO Firewall - AD

GPO Administrateur Local :

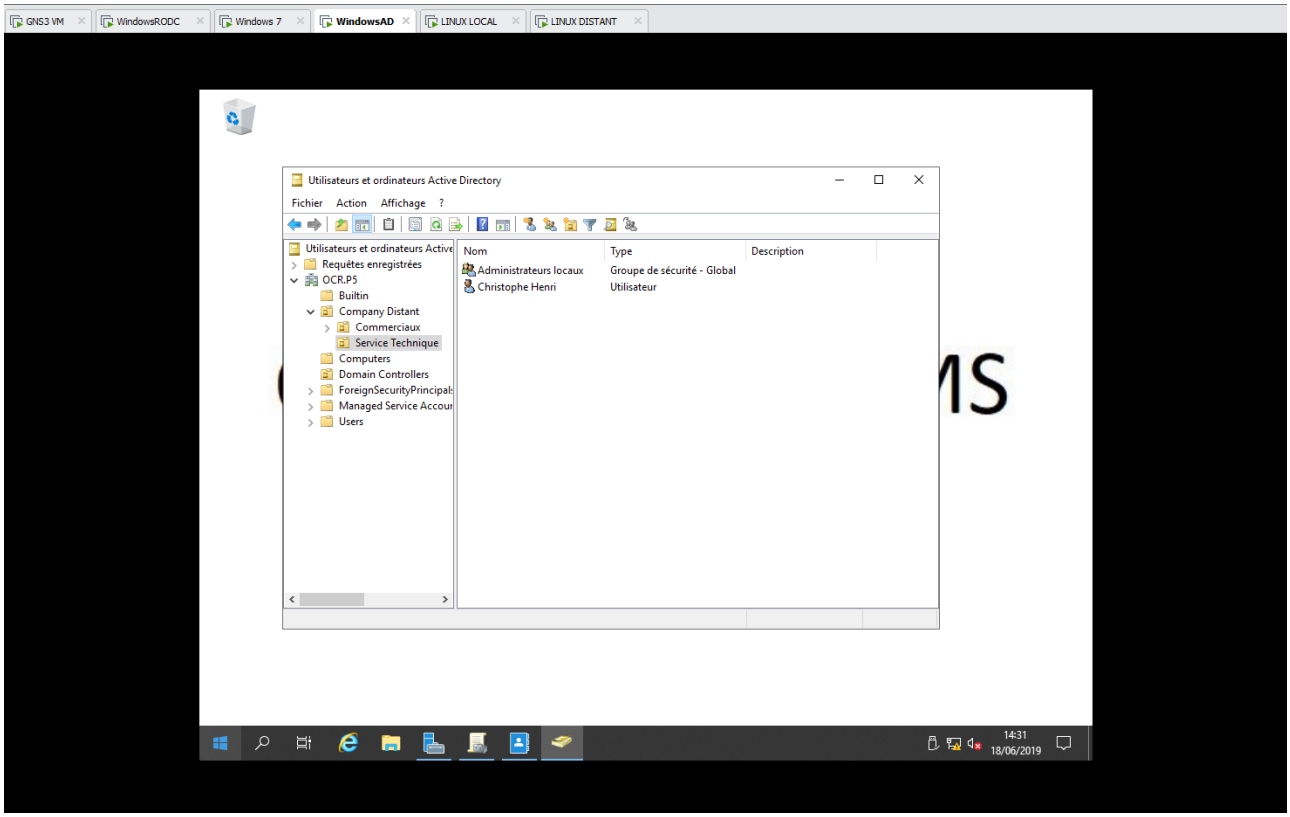


Arborescence détaillé GPO Administrateur Local - AD

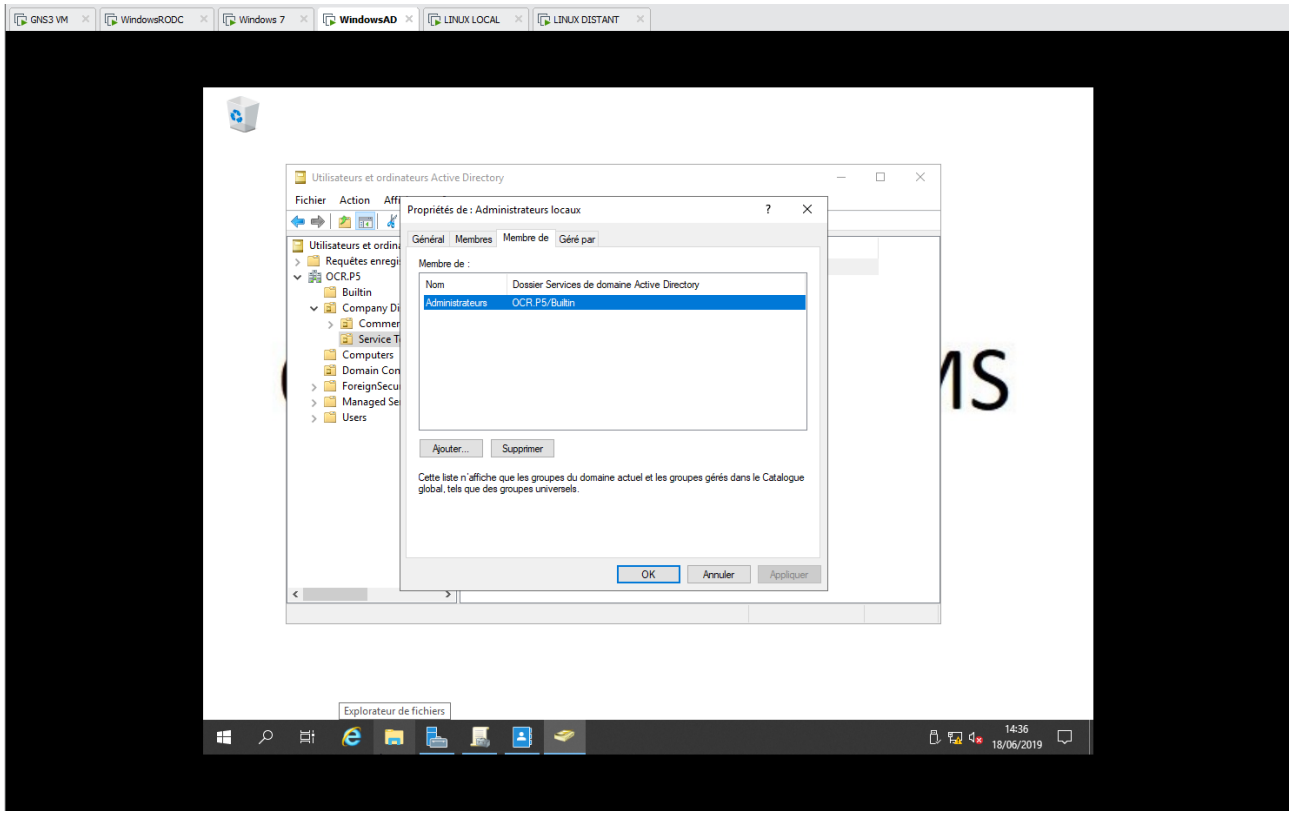
Afin de rendre administrateur local notre employé Christophe Henri du service Technique nous allons créer un nouveau groupe et ajouter Christophe Henri en tant que membre du groupe créer.

Ce groupe Administrateur local fera partie sera membre de « administrateurs »

Ainsi tous les nouveaux membres ajoutés à notre groupe administrateur local aura la capacité d'être sans aucun restriction de privilèges sur son ordinateur à condition bien sûr d'avoir classifier notre GPO correspondante.

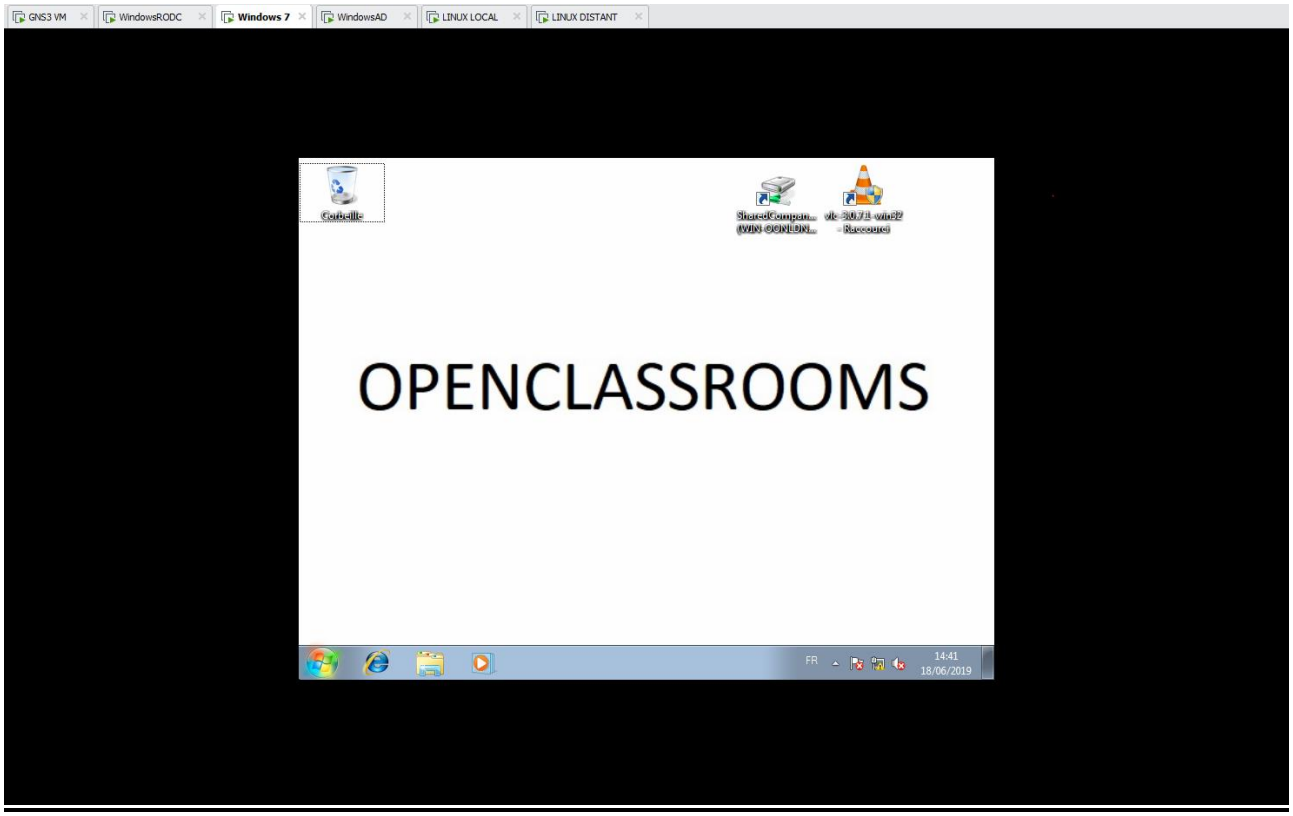


Configuration Nouveau Groupe Administrateurs locaux



Configuration Nouveau Groupe Administrateurs locaux suite – Le groupe est membre de Administrateurs & Christophe est membre du groupe administrateur locaux

Démarrage session client avec règles GPO



Démarrage sous la session client via le poste Windows 7 du groupe distant.

Afin d’afficher les GPO : Dans une invite de commande : gpresult /R (Attention : cela n’affichera les GPO que pour, l’utilisateur et non pour l’ordinateur)

Afin d’afficher les GPO pour l’ordinateur : Dans une fenêtre de recherche Windows +R : rsop.msc

Afin de forcer la synchronisation de GPO sur l’ordinateur client : gpupdate /force (un redémarrage de la session sera demandé)