TP Serveur Active Directory

Valentin Benard

16 09 2024

ID de la machine : 2325303
Nom de la machine : serveur-2012-vb

PARTIE QUESTIONS

Depuis quelle version de Windows Server, existe A.D. ?
Active Directory a été présenté en 1999 et introduit la première fois avec Windows 2000 Server Edition.

Source : Wikipédia.

Qu'est ce qu'un contrôleur de domaine ?
Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification de sécurité au sein d'un domaine de réseau informatique. Il s'agit d'un serveur réseau chargé d'autoriser l'accès de l'hôte aux ressources du domaine.

Source : Wikipédia.

Quels sont les protocoles utilisés par l'annuaire Active Directory ?
Active Directory est un service d'annuaire de Microsoft qui utilise **LDAP** comme protocole pour interroger et modifier les informations de l'annuaire, offrant une structure plus riche et des services intégrés pour la gestion des ressources informatiques.

LDAP (Lightweight *Directory* Access Protocol) est un *protocole* ouvert et multiplateforme *utilisé* pour l'authentification des services d'*annuaire*.

Source : digital-solutions.konicaminolta.fr, Varonis.com

Quels sont les méthodes d'authentification possibles Active Directory ?
NTLM et Kerberos sont des protocoles d'authentification utilisés au sein de l'environnement Microsoft Active Directory.

Source : france.devoteam.com

Active Directory introduit les notions de domaine, forêt, arborescence. Définissez ces termes

Domaine : Un domaine constitue la base d'Active Directory, chaque domaine peut avoir des domaines enfants qui comportent eux même ses propres utilisateurs, groupes et ressources.

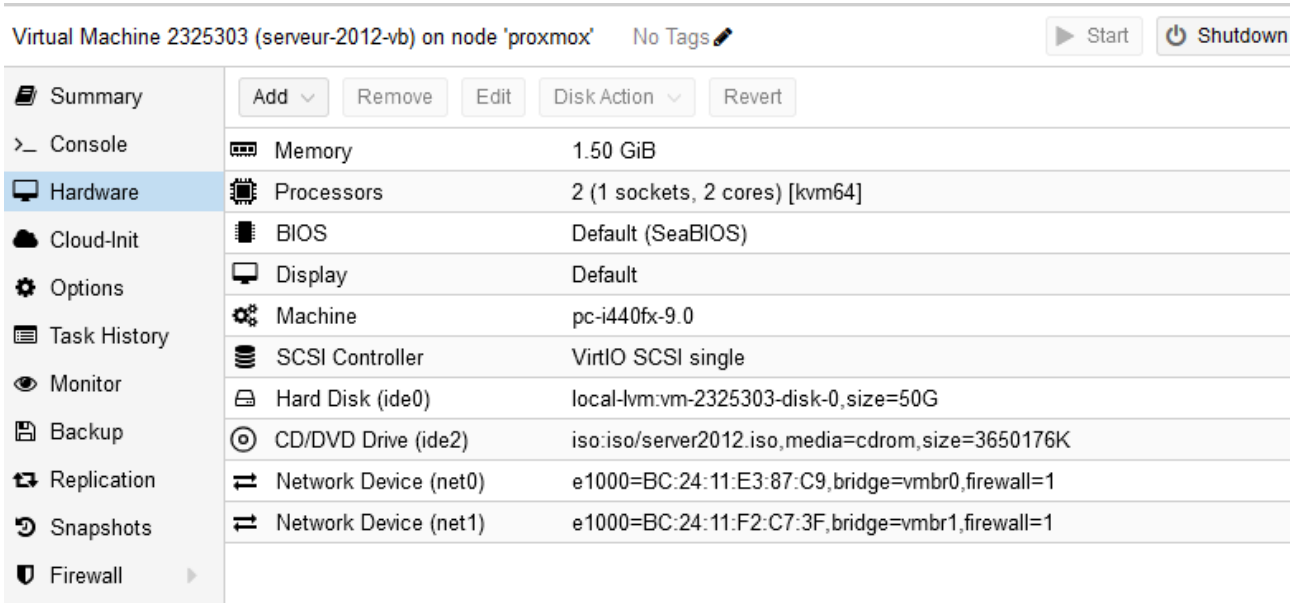
Arbre : Un arbre est un regroupement hiérarchique de plusieurs domaines.

Forêt : Une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

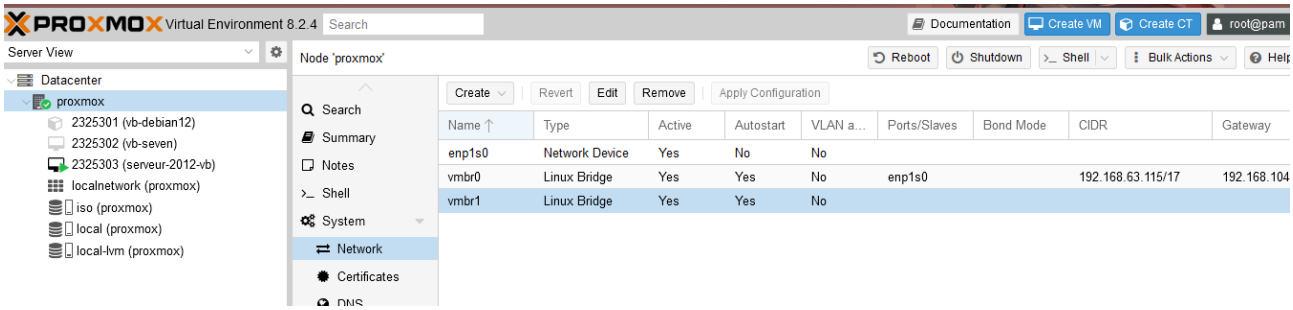
Arborescence : Une arborescence est la façon dont est structué les domaines, sous domaines et arbres au sein d'une structure Active Directory.

TP

La machine virtuelle Windows Server est créée sur notre serveur Proxmox précédemment configuré avec l'iso « serveur2012 », la configuration est la suivante :



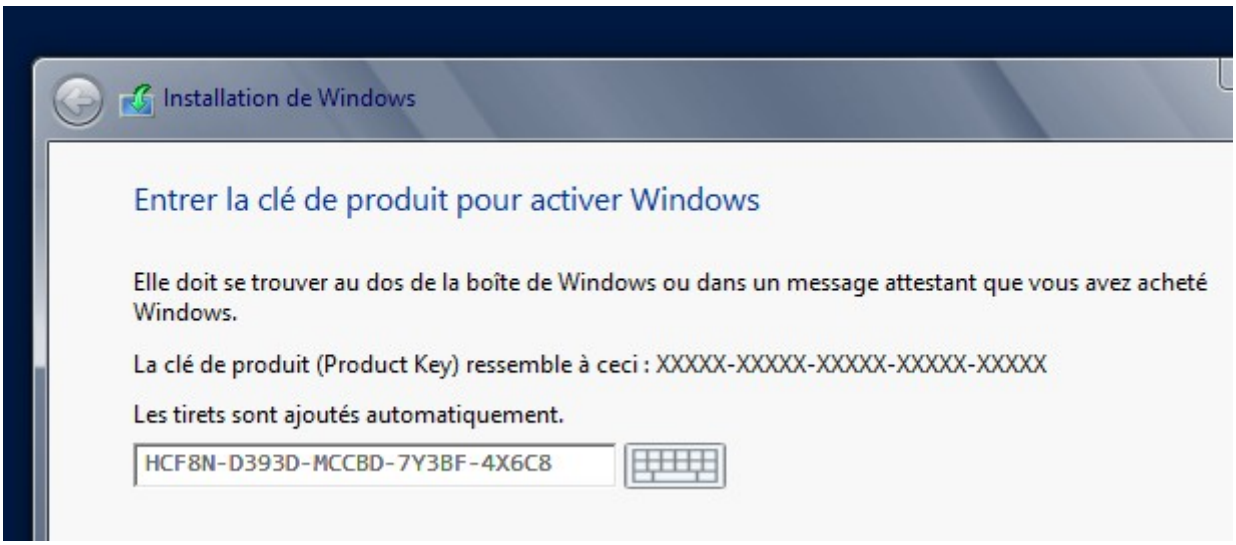
Une deuxième carte réseau a dû être ajoutée au serveur Proxmox (vmbr1), sa configuration est vide selon les instructions :



NOTE : La carte vmbr0 a été supprimée conformément aux instructions.

Dans l'installation de Windows Server, la clé suivante est renseignée :

HCF8N-D393D-MCCBD-7Y3BF-4X6C8

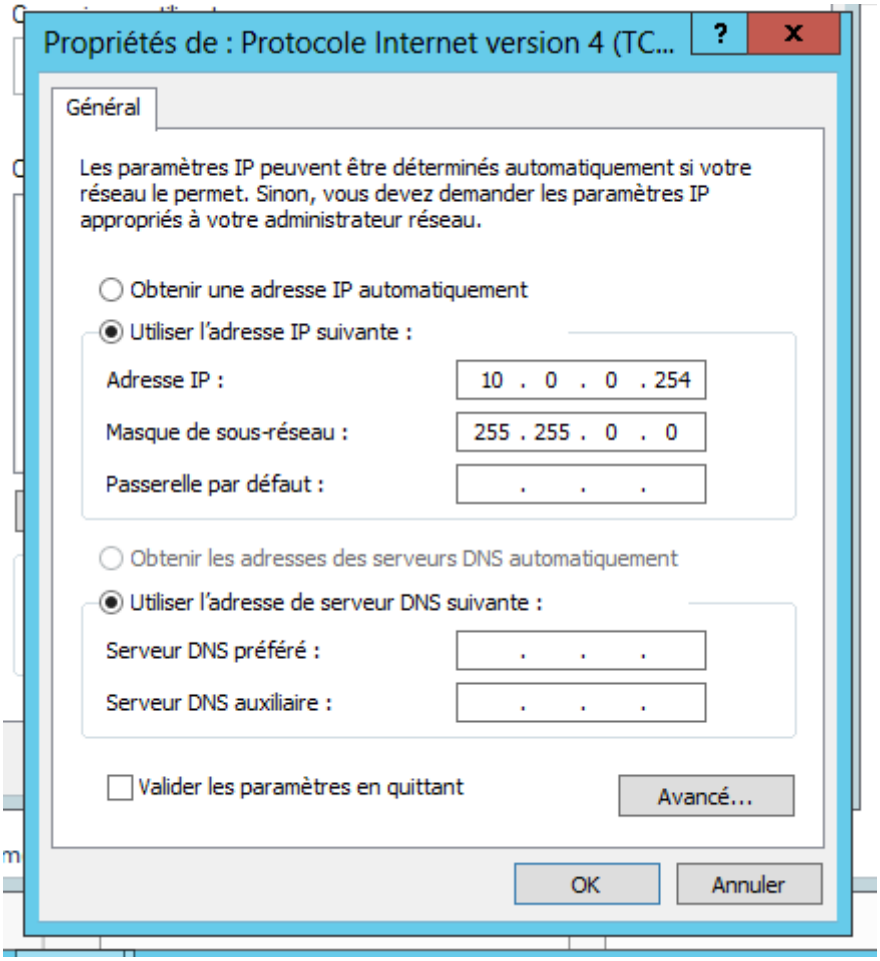


L'installation est en suite lancée.

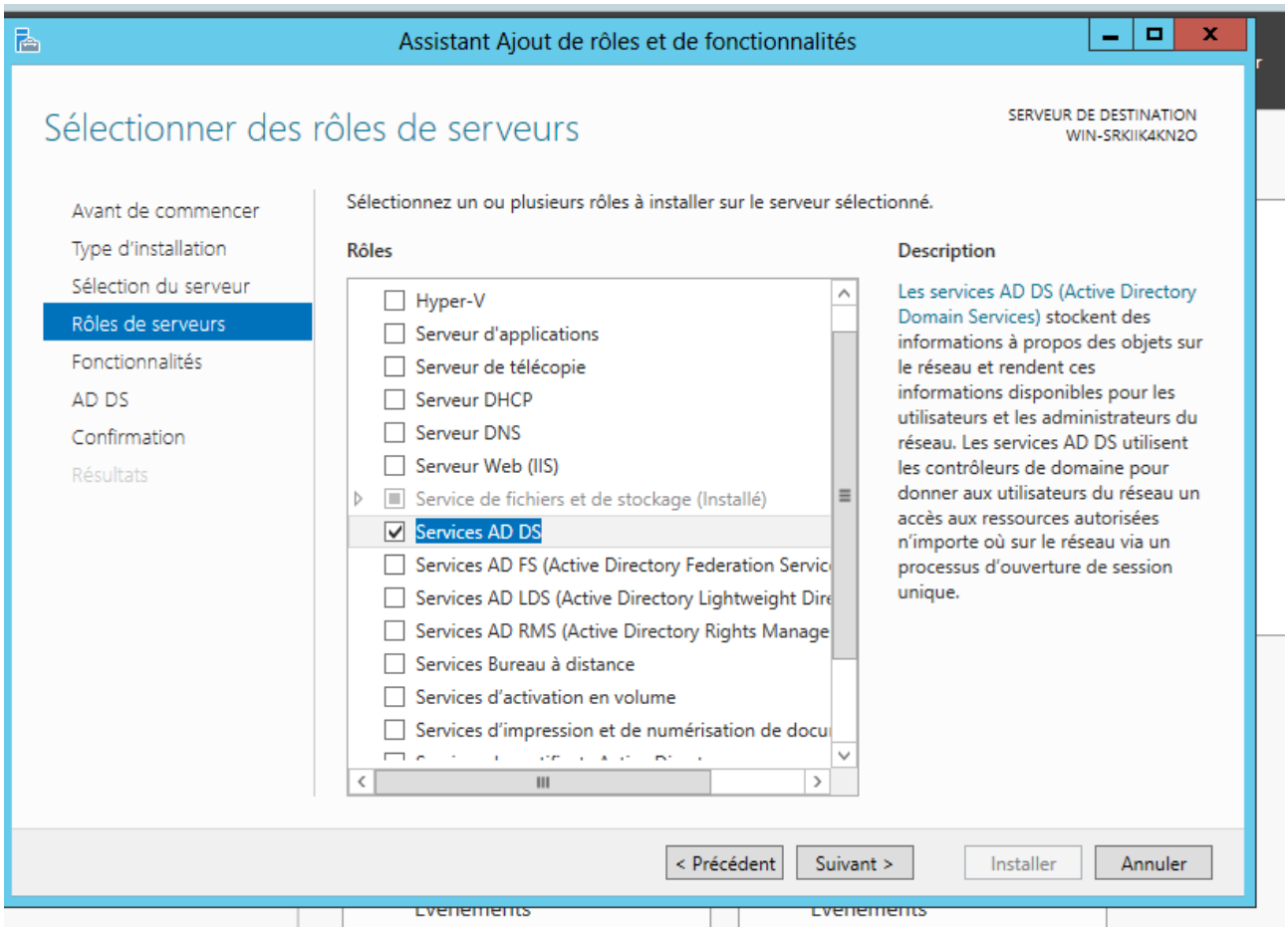
Le mot de passe du compte **Administrateur** est défini sur **eleve$1**.

Configuration des cartes réseau du serveur :

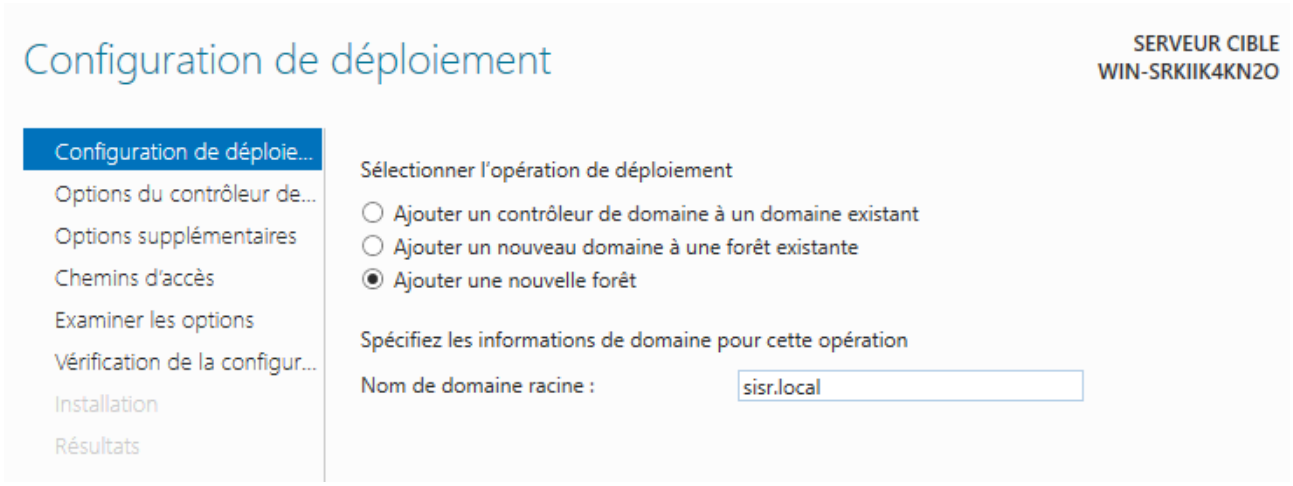
Carte **vmbr1** :

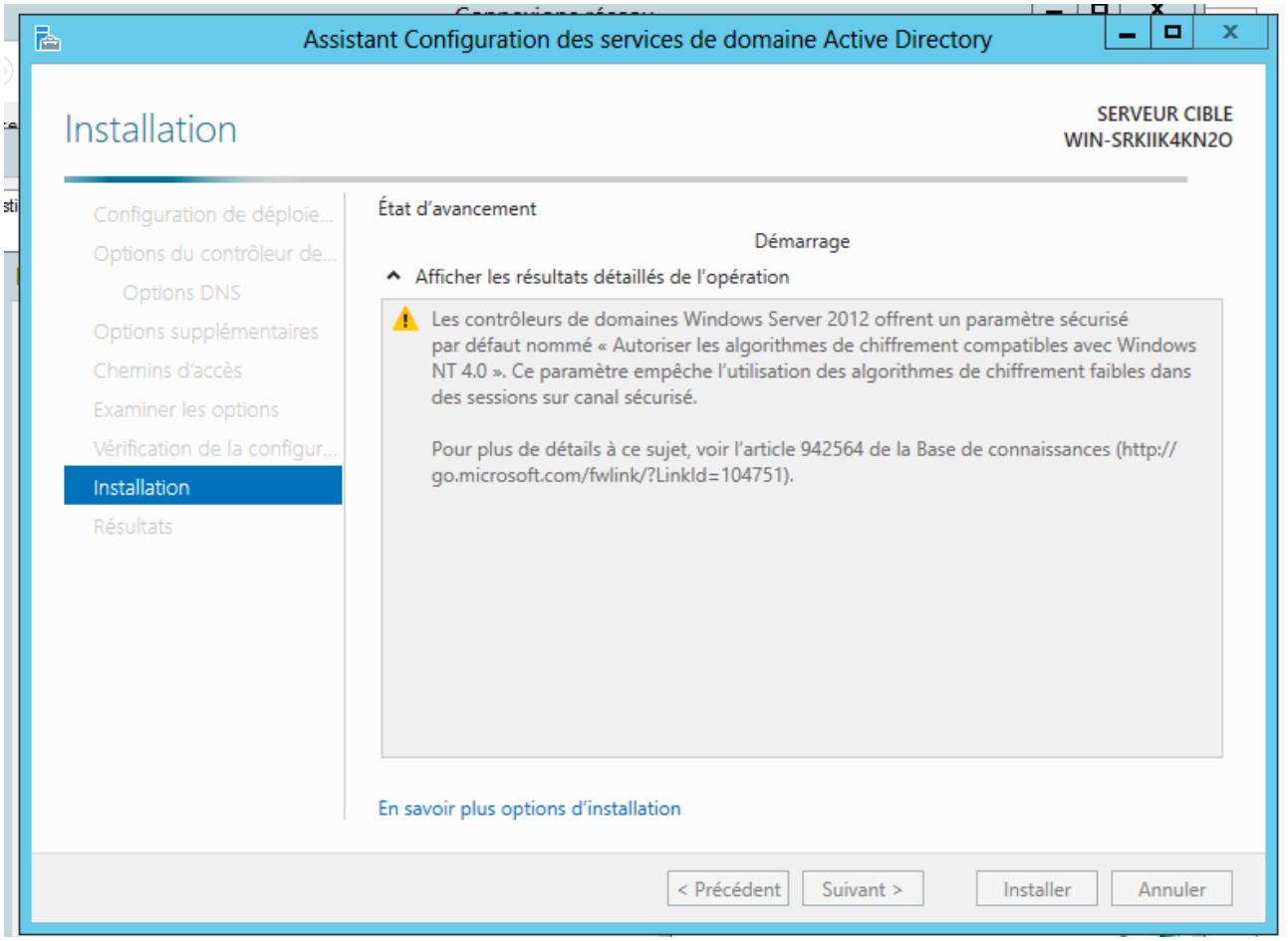


Par la suite, la fonctionnalité Active Directory (Domain Services) est installé :



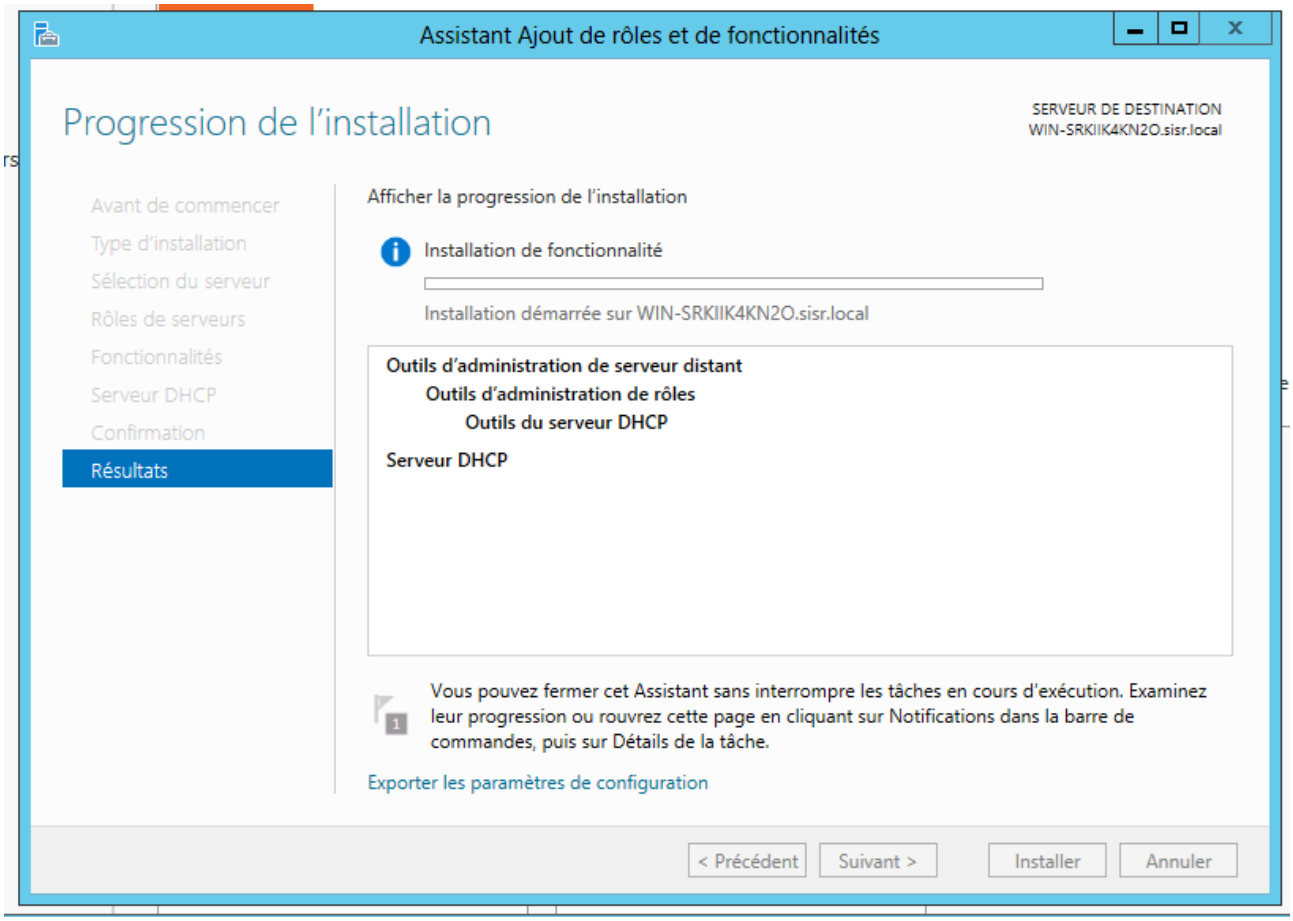
Ajout d'un nouveau domaine sisr.local





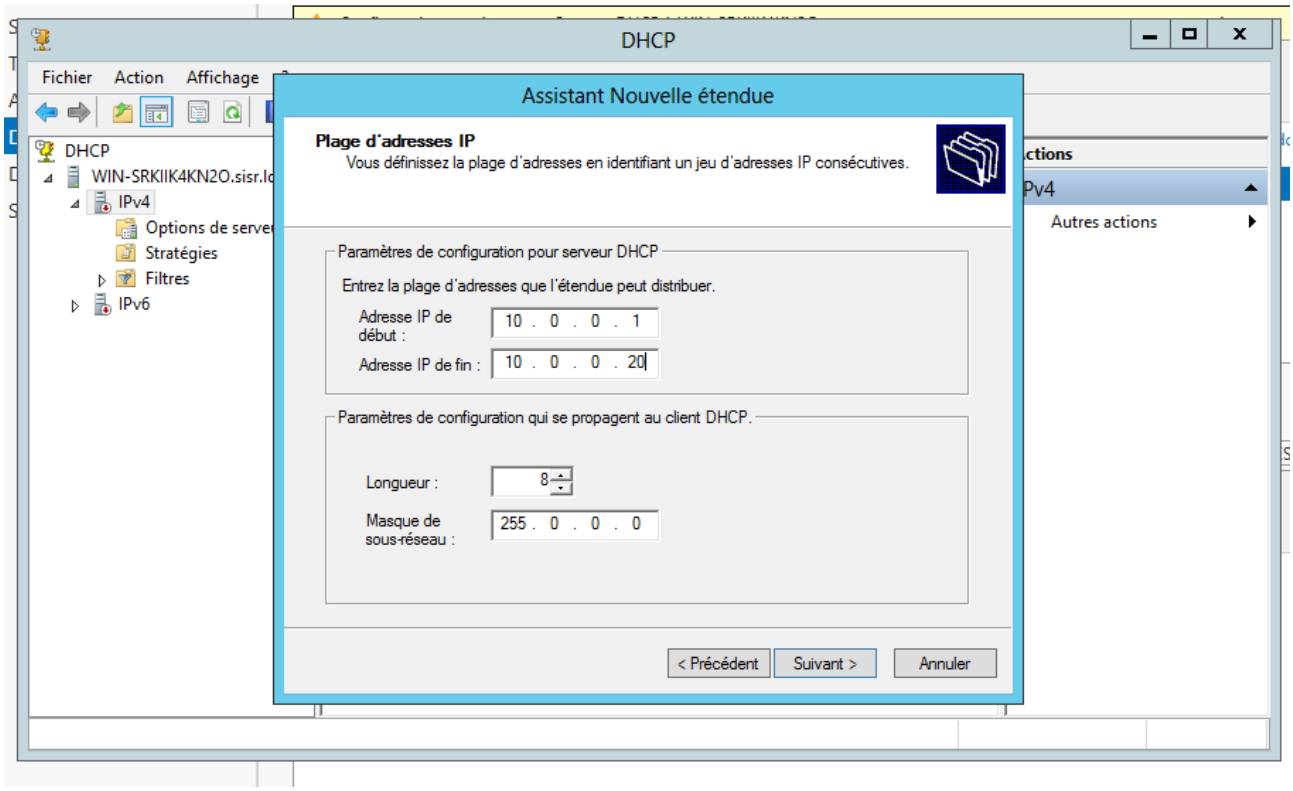
Configuration du serveur DHCP :

L'installation du service est lancé dans Windows Server 2012 :

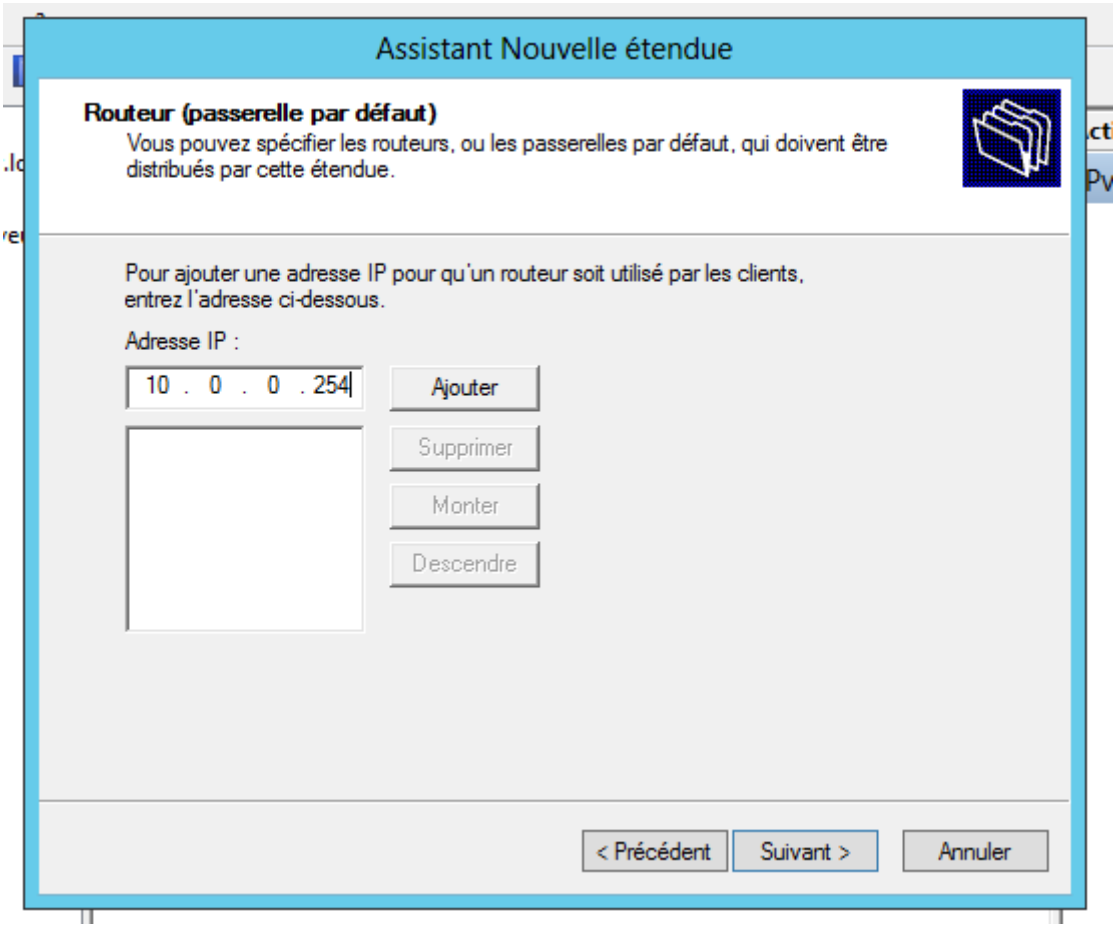


Configuration du serveur DHCP

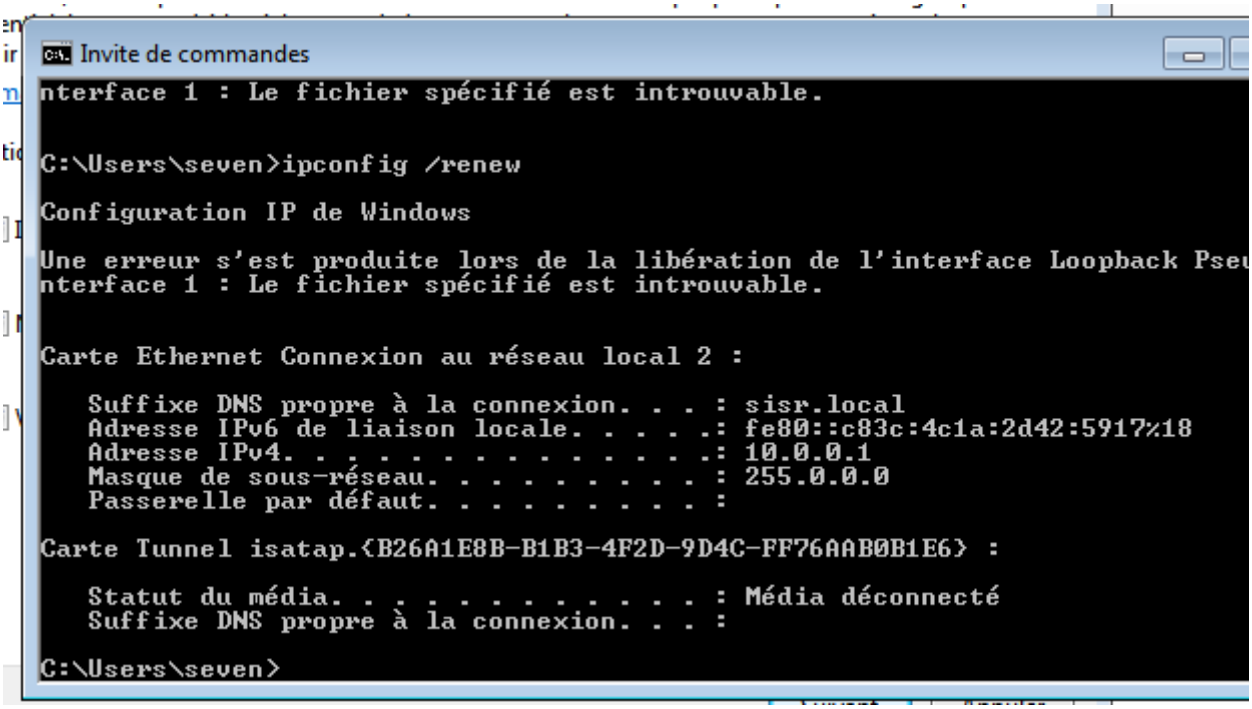
Configuration de la plage d'IP selon les instructions 10.0.0.1 – 10.0.0.20



Configuration de l’adresse du routeur (IP du serveur Windows 2012)



Résultat sur la machine client Seven (DHCP) :



QUESTIONS

Qu'est ce qu'une unité organisationnelle (U.O.) ?

Une Unité Organisationnelle est l'unité qui regroupe les éléments tel que les utilisateurs ordinateurs etc.

Quelle est la différence entre une U.O. et un groupe (dans quels cas utilise-t-on l'un et l'autre) ?

Une UO sert à organiser la structure d'Active Directory, de déléguer l'administration à différents niveaux, appliquer des politiques de groupe à des unités organisationnelles spécifiques.

Un groupe sert à gérer les droits d'accès, distribuer des ressources ou des logiciels, et regrouper des objets ayant des caractéristiques communes (par exemple, tous les administrateurs.)

Une **UO** est comme une bibliothèque avec des rayons, chaque rayon (UO) regroupe des livres (objets) sur un sujet spécifique, un **groupe** est comme une liste de lecture, une liste peut contenir des livres de différents rayons, mais ils ont tous un point commun (par exemple, tous les livres de science fiction).

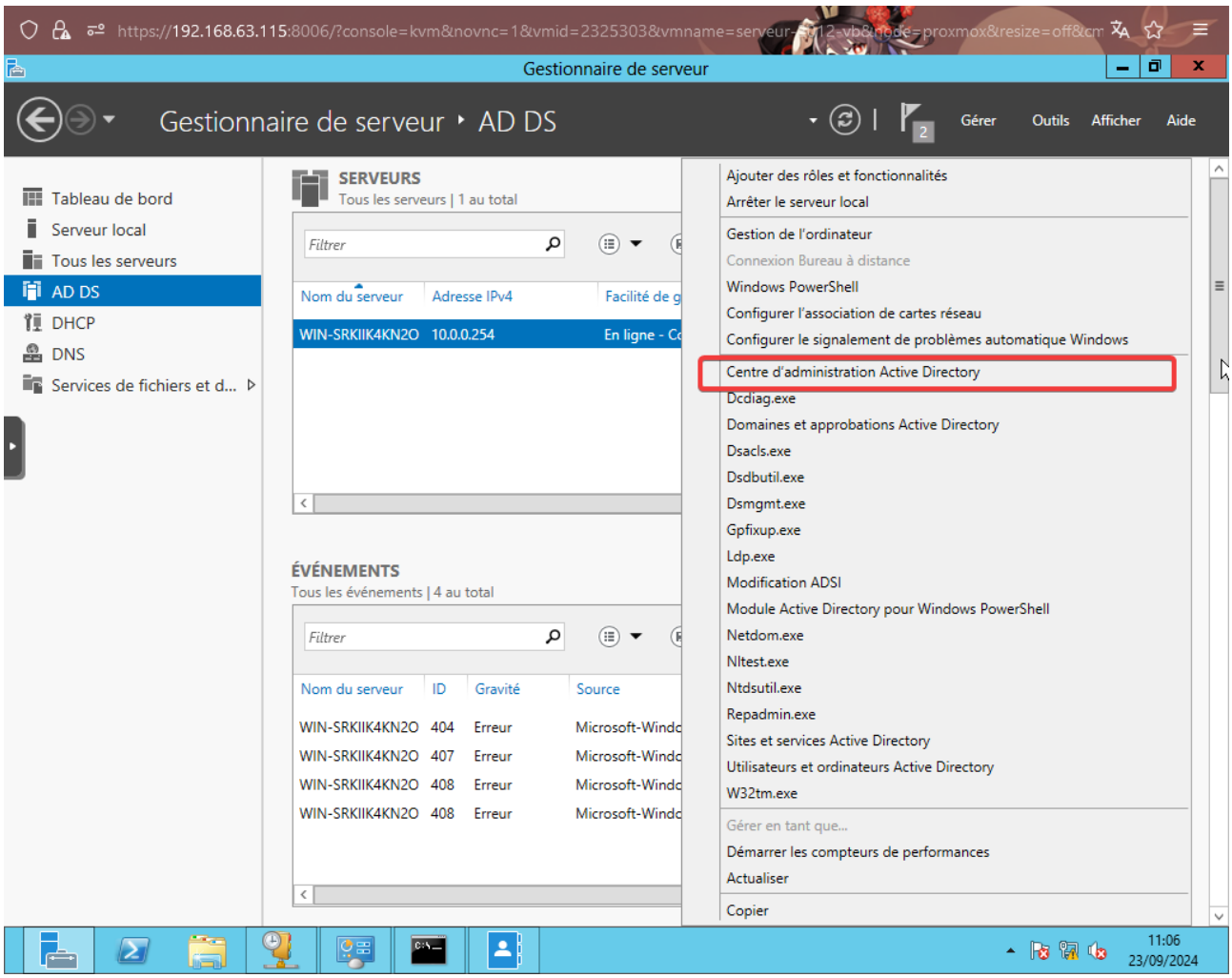
Exemple concret :

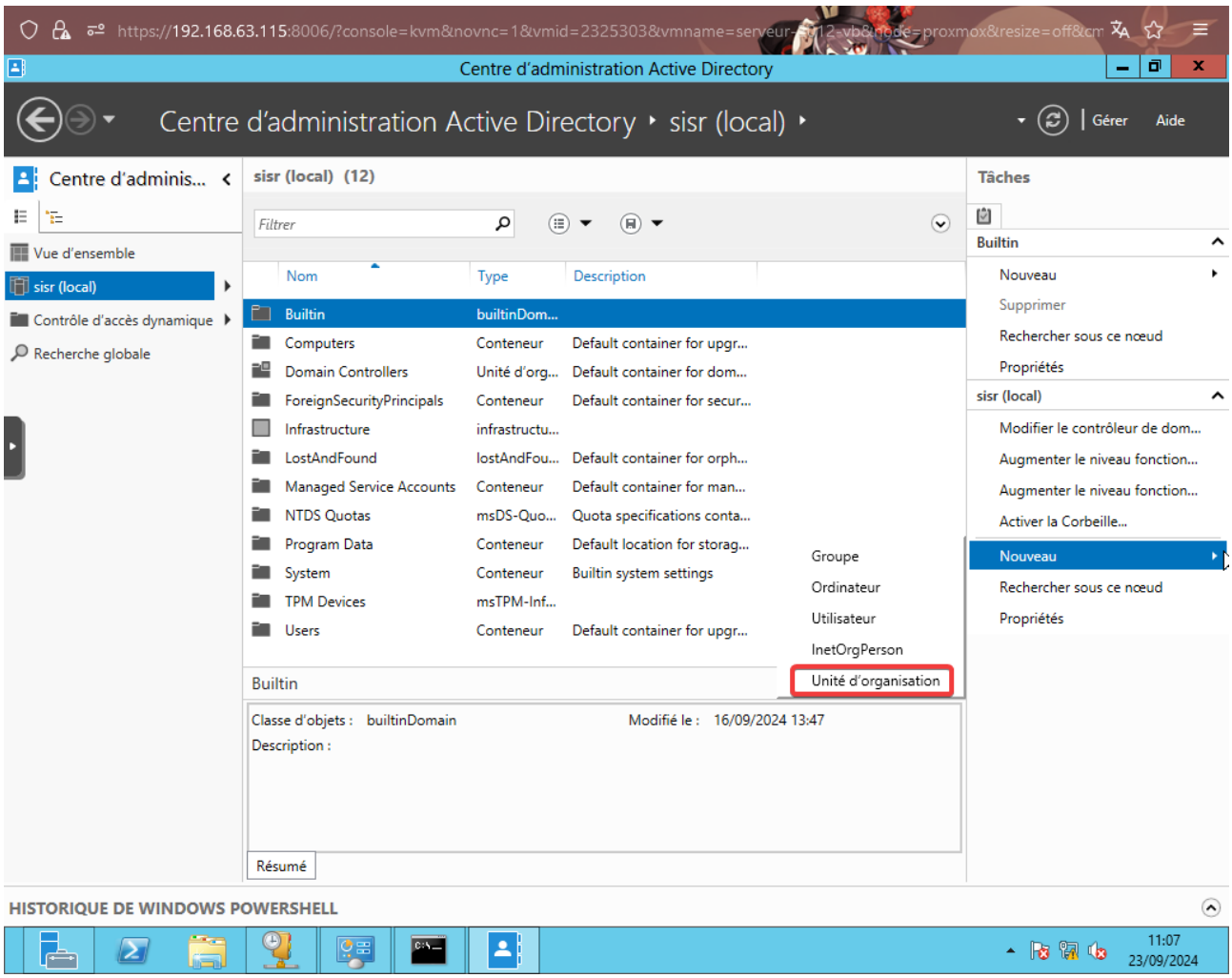
Dans une entreprise, on peut créer une UO « Département Commercial » et un groupe « Commercial avec droits administrateurs ».

L'**UO** servirait à organiser les utilisateurs et les ordinateurs du département commercial

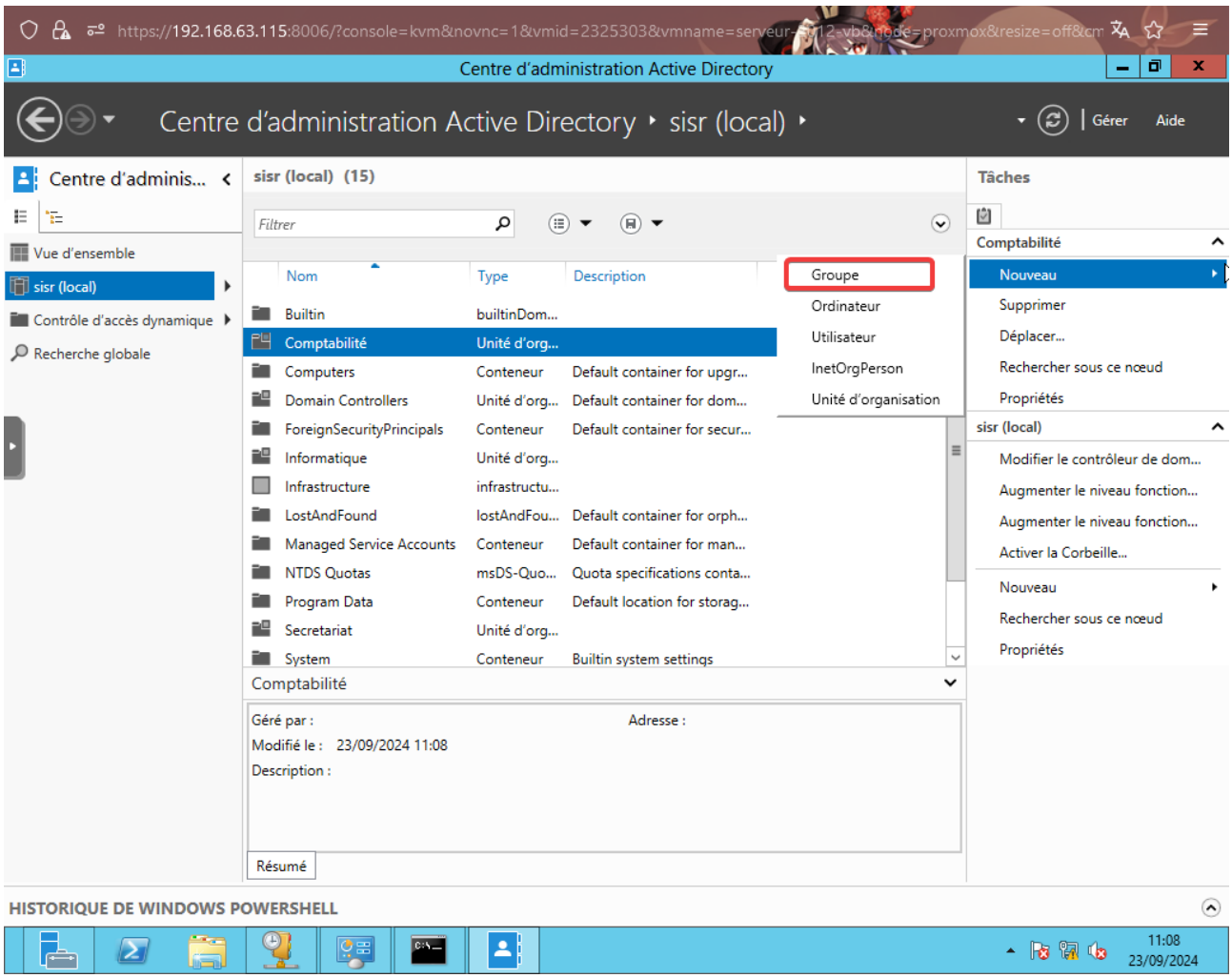
Le **groupe** servirait à attribuer des droits d'administration sur certains serveurs uniquement aux commerciaux ayant besoin de ces droits.

Création d'unités organisationnelles


https://192.168.63.115:8006/?console=kvm&novnc=1&vmid=2325303&vmname=serveur-2012-vb&node=proxmox&resize=off&cr
Gestionnaire de serveur
Gestionnaire de serveur ‣ AD DS
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DHCP
DNS
Services de fichiers et d...
SERVEURS
Tous les serveurs | 1 au total
Filtrer
Nom du serveur
Adresse IPv4
Facilité de g
WIN-SRKIIK4KN2O
10.0.0.254
En ligne - C
ÉVÉNEMENTS
Tous les événements | 4 au total
Filtrer
Nom du serveur
ID
Gravité
Source
WIN-SRKIIK4KN2O 404 Erreur Microsoft-Windc
WIN-SRKIIK4KN2O 407 Erreur Microsoft-Windc
WIN-SRKIIK4KN2O 408 Erreur Microsoft-Windc
WIN-SRKIIK4KN2O 408 Erreur Microsoft-Windc
Ajouter des rôles et fonctionnalités
Arrêter le serveur local
Gestion de l'ordinateur
Connexion Bureau à distance
Windows PowerShell
Configurer l'association de cartes réseau
Configurer le signalement de problèmes automatique Windows
Centre d'administration Active Directory
Dcdiag.exe
Domaines et approbations Active Directory
Dsacls.exe
Dsdbutil.exe
Dsmgmt.exe
Gpfixup.exe
Ldp.exe
Modification ADSI
Module Active Directory pour Windows PowerShell
Netdom.exe
Nltest.exe
Ntdsutil.exe
Repadmin.exe
Sites et services Active Directory
Utilisateurs et ordinateurs Active Directory
W32tm.exe
Gérer en tant que...
Démarrer les compteurs de performances
Actualiser
Copier
11:06
23/09/2024

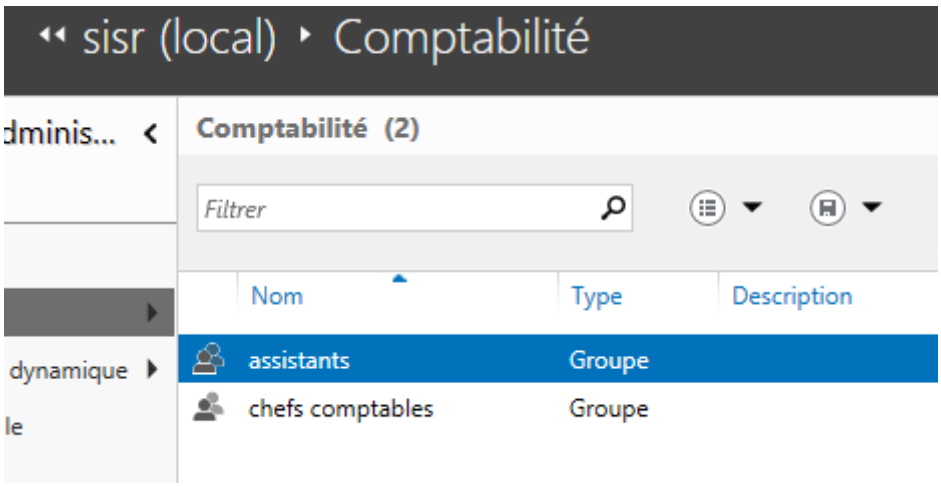


Les trois UO sont créées (Comptabilité, Secretariat, Informatique), les groupes sont en suite créées :



- Dans l'U.O. Comptabilité, création du groupe **assistants** et le groupe **chefs comptables**.
- Dans l'U.O. Secrétariat, création du groupe **accueil** et su groupe **assistantes de direction.**
- Dans l'U.O. Informatique, création du groupe **développeurs** et du groupe **techniciens réseau.**

Résultat pour l'UO comptabilité:



Création des utilisateurs :

Instructions :

Utilisateurs :

Chaque utilisateur devra pouvoir se connecter par le login suivant :
Première lettre du prénom, nom complet, par exemple Sam Secrét devra taper :
ssecret

Le mot de passe sera **Azerty77**

Les utilisateurs ne pourront pas changer de mot de passe.

– Sam Secrét et Will Tariat seront ajoutés à l'U.O Secrétariat et dans le groupe Accueil.

– Julie Assist et Rose Directi seront ajoutés à l'U.O Secrétariat et dans le groupe Assistantes de direction.

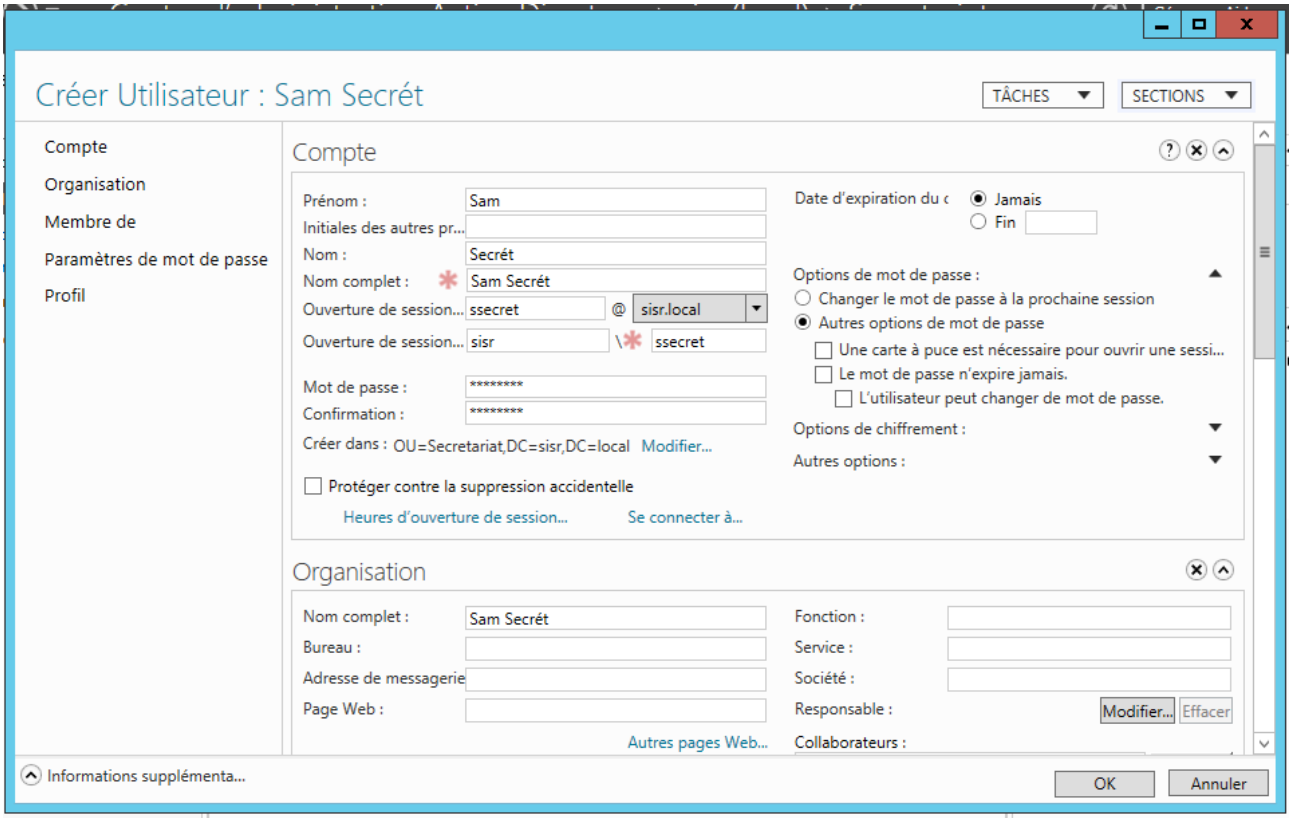
– Jean Develo et Joseph Peur seront ajoutés à l'U.O Informatique et dans le groupe Développeurs.

– Lucien Tec et Arthur Nicien seront ajoutés à l'U.O Informatique et dans le groupe Techniciens réseau.

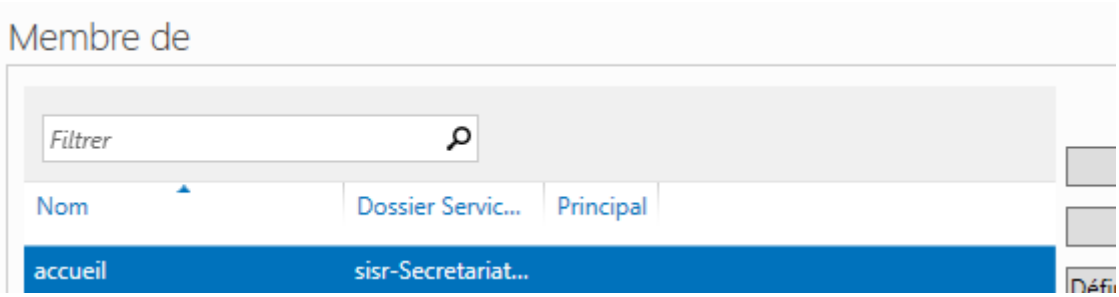
– Yves Comp et François Table seront ajoutés à l'U.O Comptabilité et dans le groupe chefs comptables.

– Mathieu Assis et Fabien Tant seront ajoutés à l'U.O Comptabilité et dans le groupe assistants.

Le nom prénom, l'username et le mot de passe est défini, il est également paramétré que l'utilisateur ne peut pas changer son mot de passe.

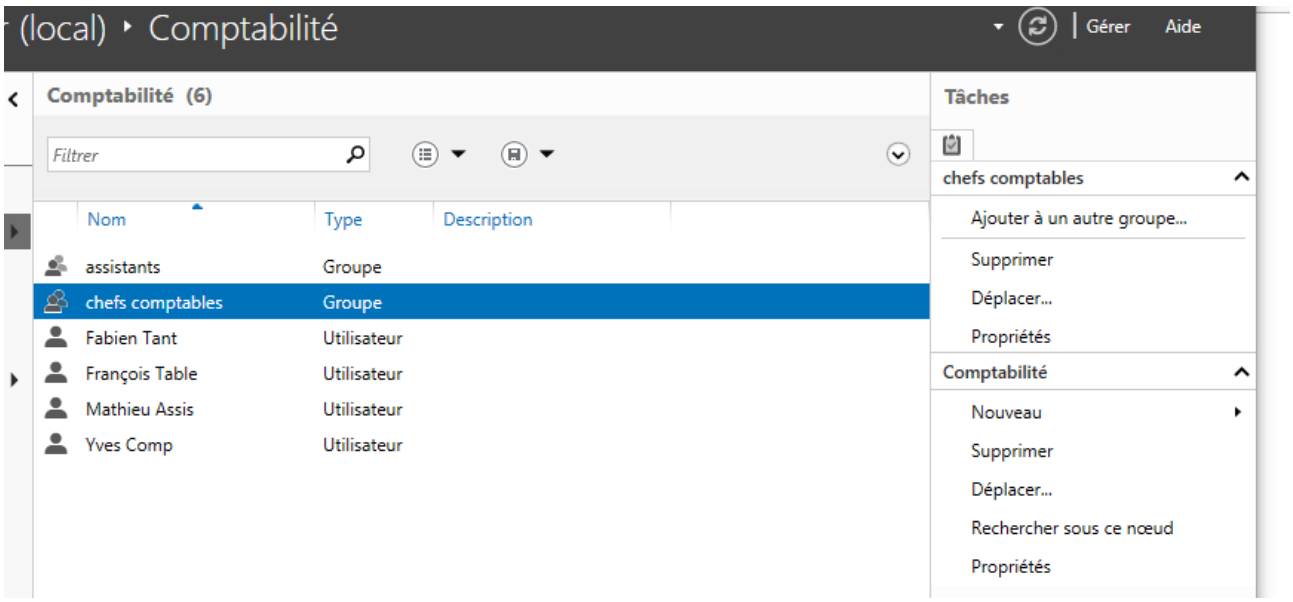


Il est ajouté à son groupe respectif.

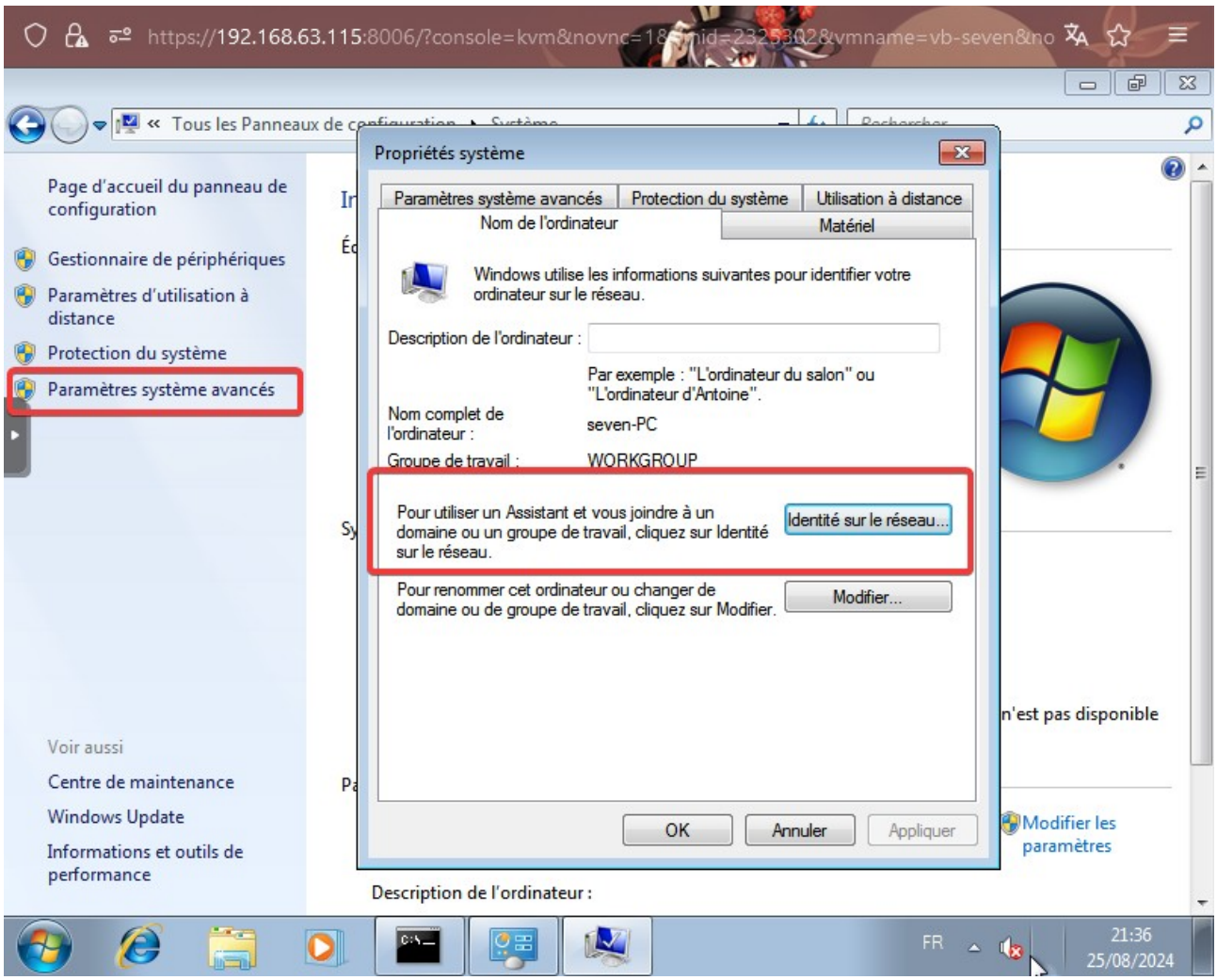


Les mêmes étapes sont répétées pour les 11 autres utilisateurs.

Résultat pour l'UO Comptabilité :



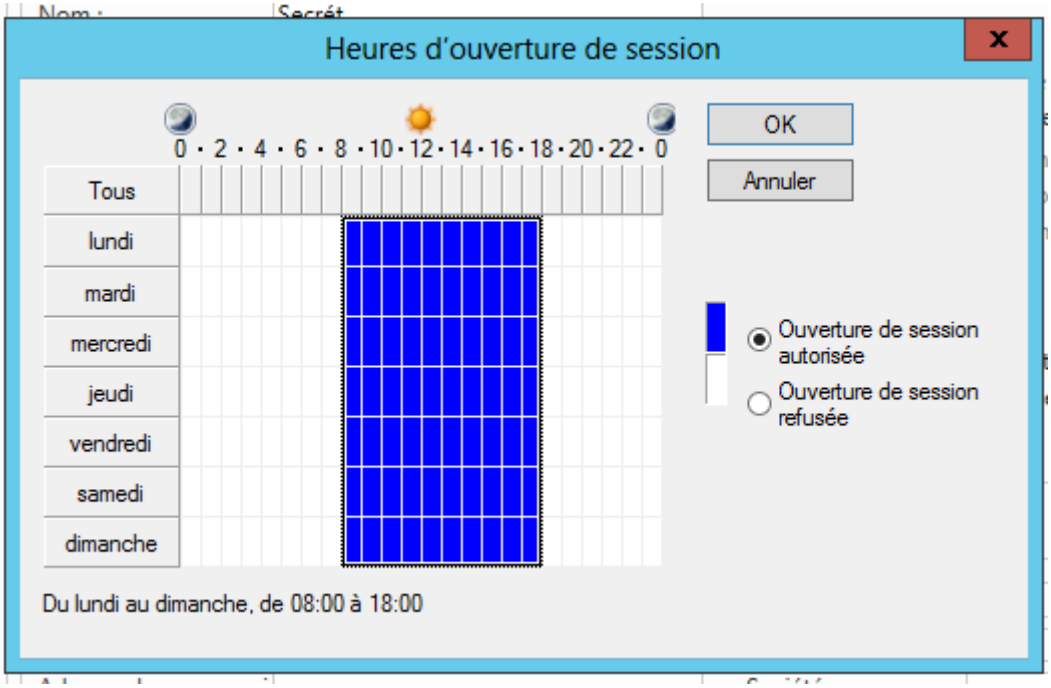
Intégration d’un client dans le domaines



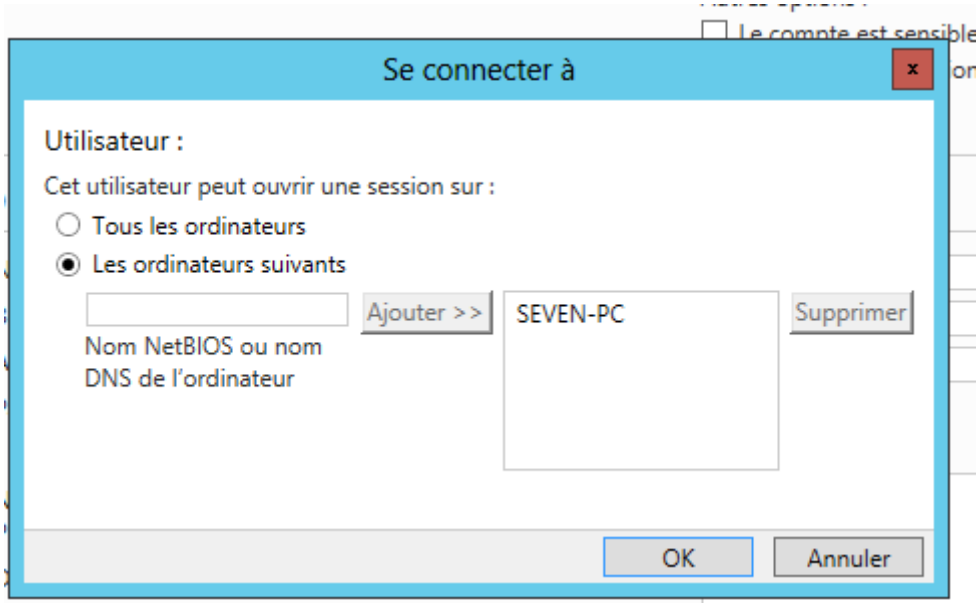
Résultat :

Mot de passe : Azerty77

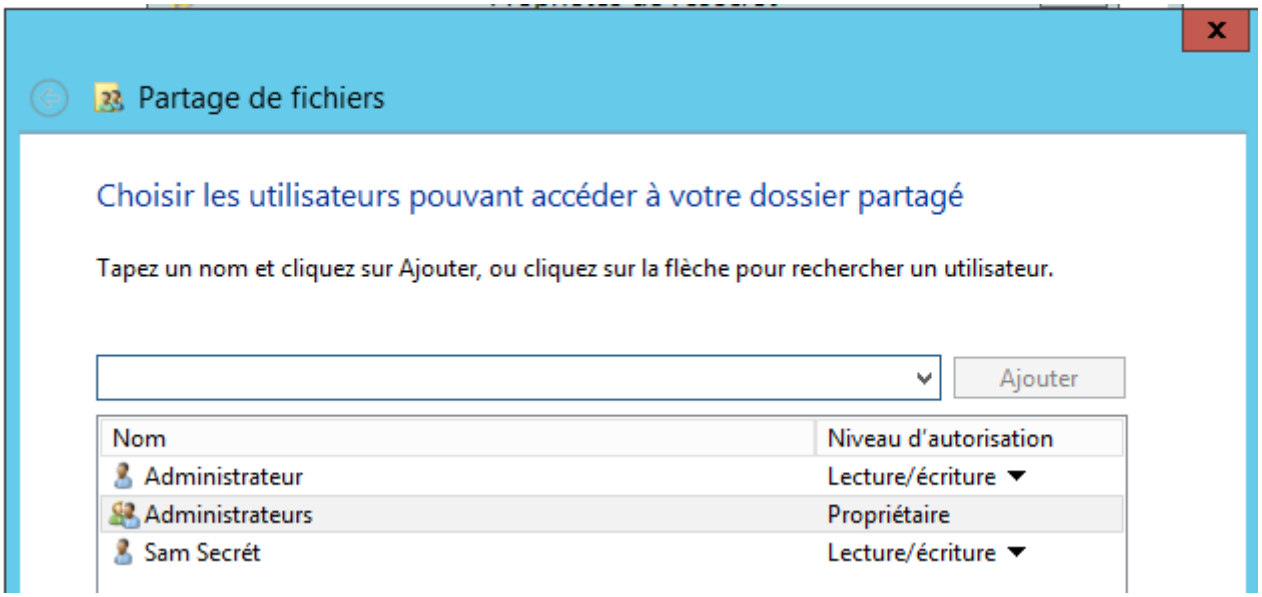
Paramétrage pour que les utilisateurs ne puissent se connecter qu'entre 8h et 18h :

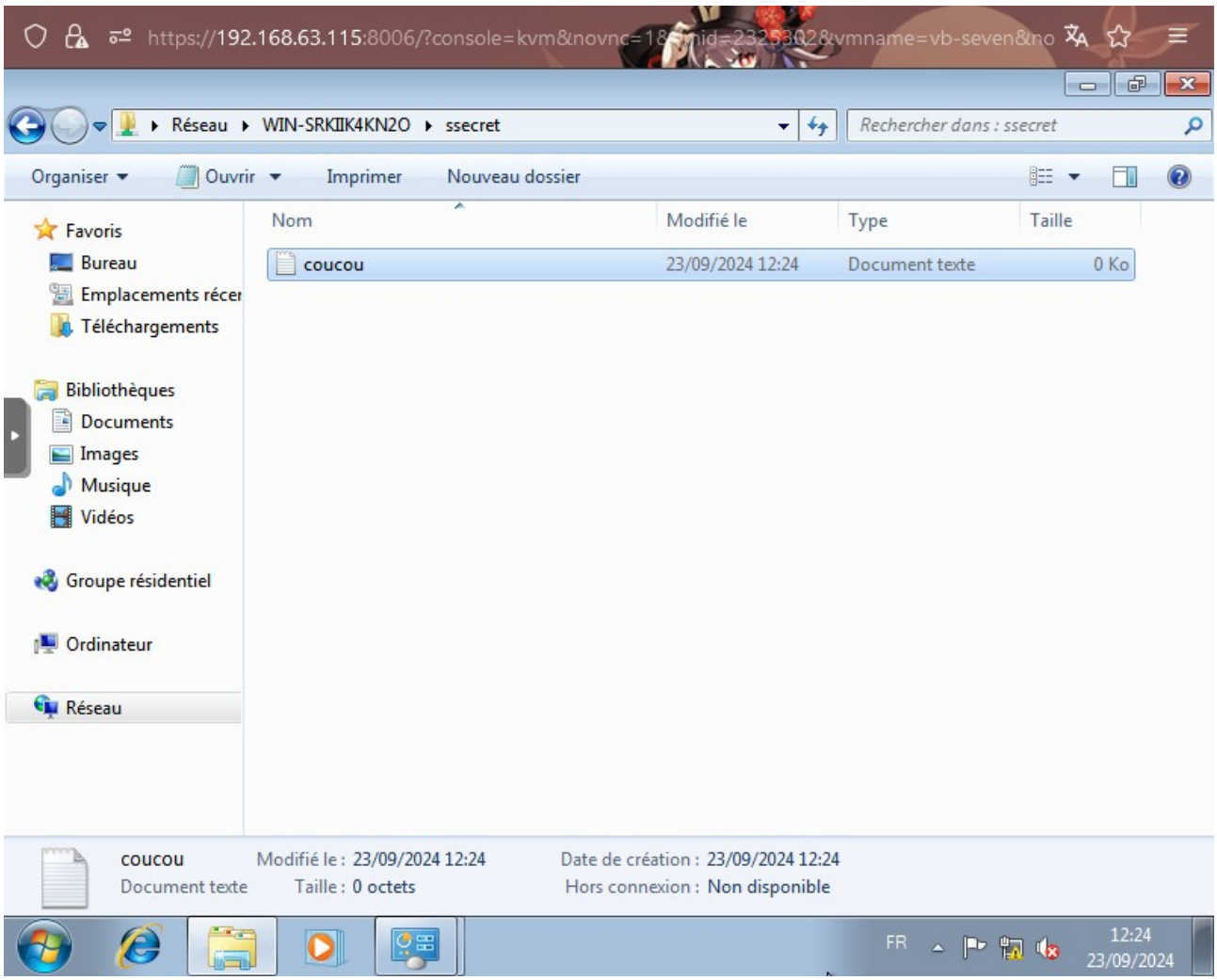


Paramétrage pour que l'utilisateur ne puisse que se connecter à l'ordinateur sur lequel il a été ajouté (SEVEN-PC) :



Le partage est créée sur le serveur et est en suite accessible depuis l'utilisateur ssecret :





NOTE : (Il est accessible depuis \\WIN-SRKIIK4KN2O\ssecret, le nom de l'ordinateur ne peut pas être modifié après la mise en place, or, les instructions indiquent que le partage doit pointer avec un nom de serveur « serveur-2012-vosinitiales », qui furent données trop tard.

Définition du terme « profil itinérant »

Un profil itinérant est simplement un profil Windows qui est stocké sur un serveur central, comme un serveur Active Directory et qui peut être servie sur n'importe quel ordinateur présent sur le réseau.

Quels sont les avantages et inconvénients des profils itinérants ?

Avantages :

L'avantage est tout d'abord la **flexibilité**, les utilisateurs peuvent se reconnecter à leur profil **depuis n'importe quel poste, n'importe quel emplacement** (différentes salles au sein de l'établissement, sur le même réseau) offrant donc la **portabilité** de leur profil.

Tous les profils sont **stockés au même endroit** sur un serveur central, et sont donc **plus faciles à gérer**, comme par exemple pour les sauvegarder.

Inconvénients :

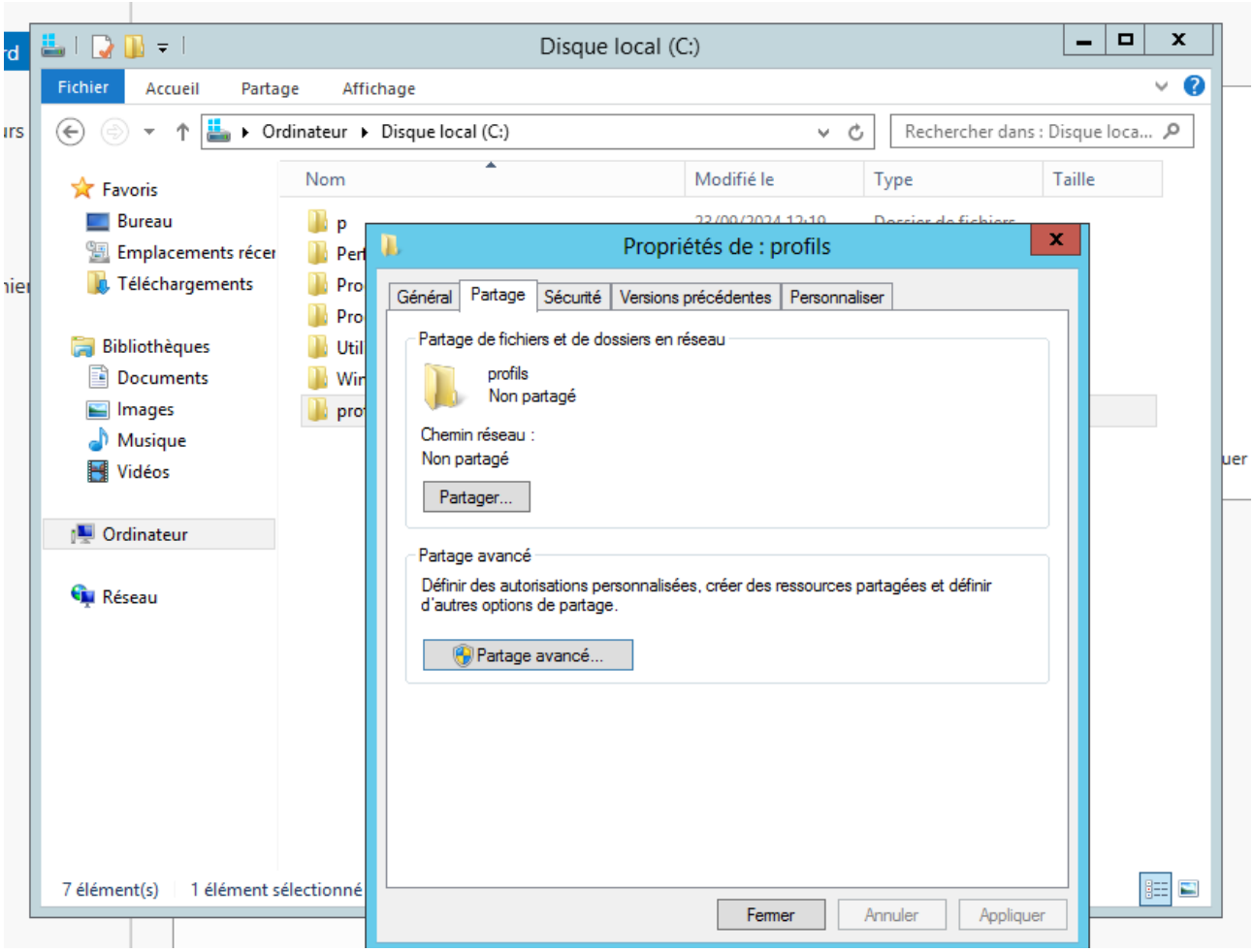
Les inconvénients sont tout d'abord la potentielle **saturation du réseau** si plusieurs personnes se connectent et récupèrent leur profil en même temps, rajoutant des délais supplémentaires, il faut donc prévoir un réseau capable de supporter le trafic dans ces situations, comme avec l'**usage de câbles et switchs 10 gbps.** (ce que l'on peut remarquer ici même au lycée, pas seulement avec les profils mais avec les machines virtuelles dont leur disque dur est stocké sur un serveur séparé, entraînant une saturation très facile du réseau.)

Les profils itinérants sont plus susceptibles de corruptions car ils sont sujet de coupures réseau durant la récupération ou la sauvegarde d'un profil.

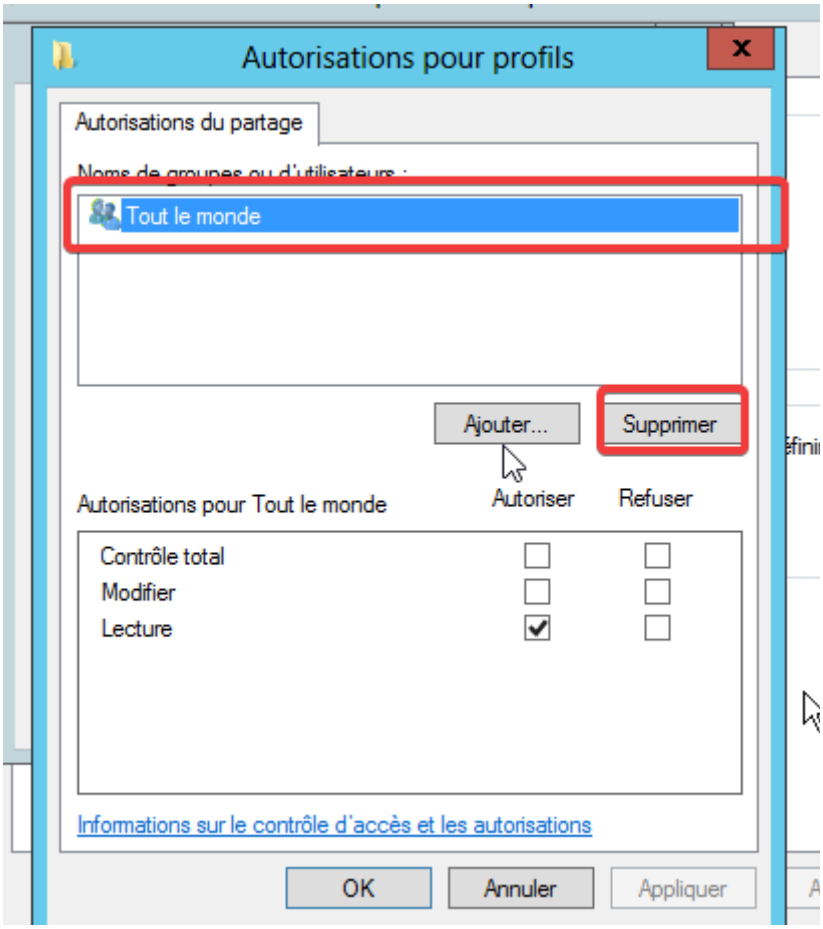
Le système de profil itinérant peut **consommer beaucoup d'espace disque** sur les postes client, il faut récupérer chaque profil de chaque utilisateur sur un même disque dur, entraînant une **utilisation importante du disque** (c'est pour cela que l'établissement du lycée les limite à 200 Mo, tout excès de cette limite fera que le profil ne sera pas sauvegardé.)

Mise en place d'un profil itinérant pour l'utilisateur Sam Secrét.

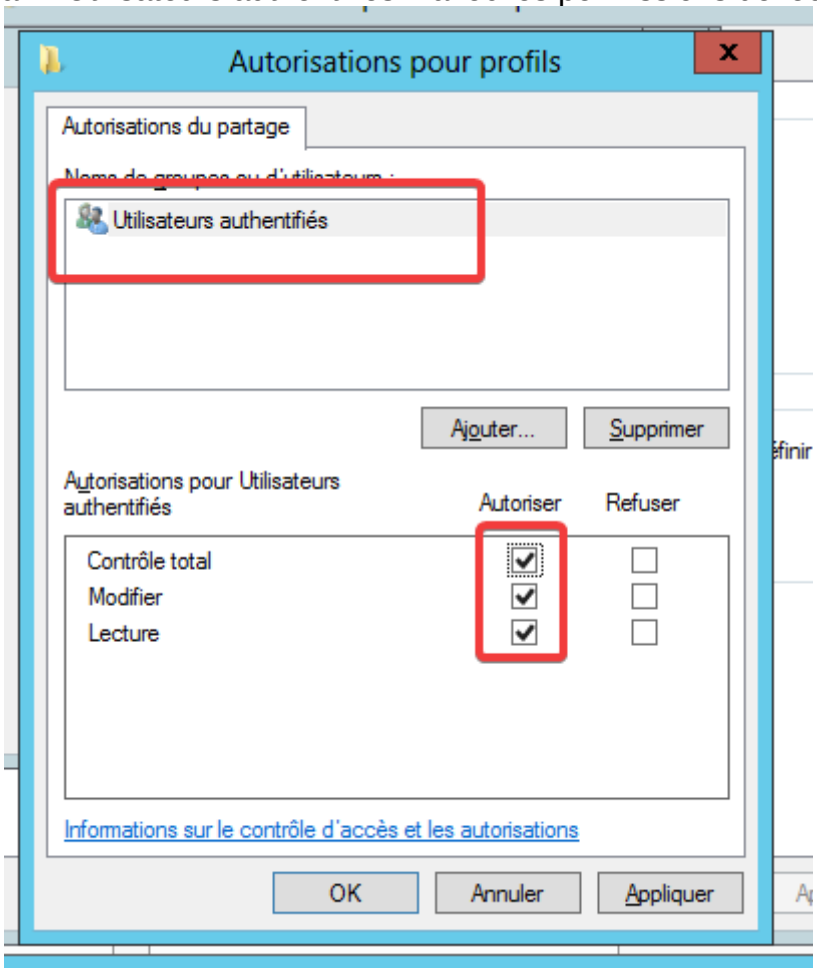
Un dossier « profils » est créée pour stocker les profils itinérant, il est alors partagé avec le mode partage avancé.



Dans les autorisations, « Tout le monde » est supprimé.

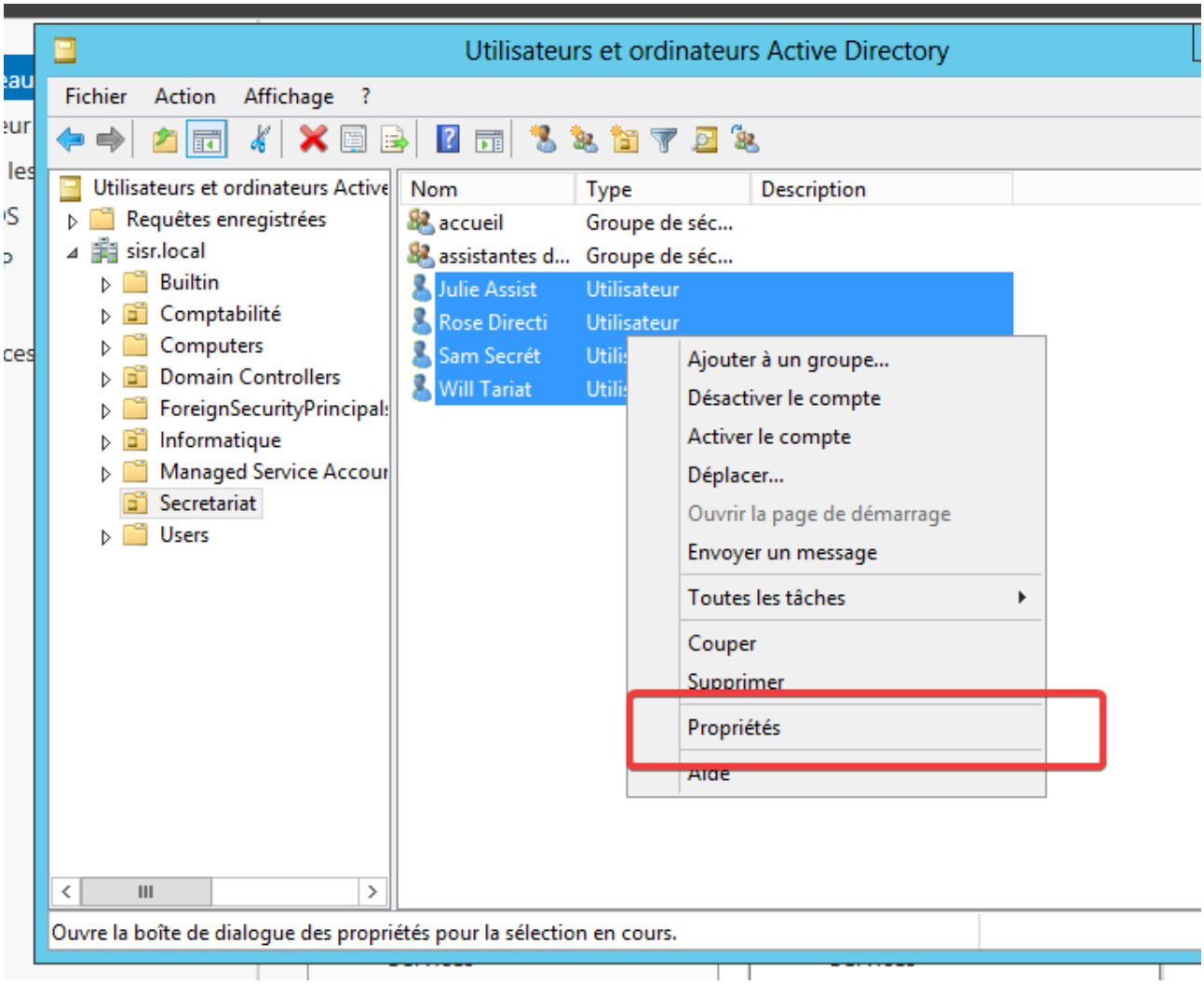


Il est remplacé par « Utilisateurs authentifiés » avec les permissions de lecture et écriture.

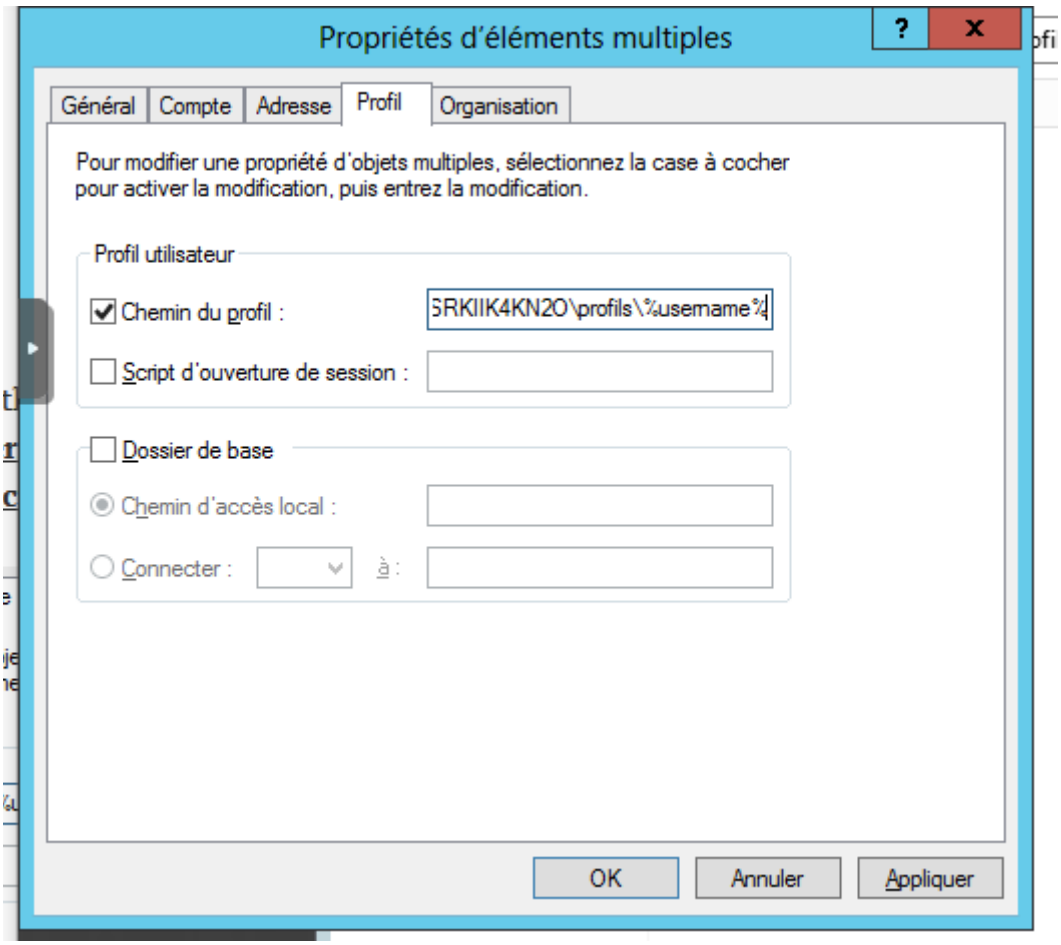


Ouverture de la console de gestion serveur, puis Outils en haut à droite > Utilisateurs et ordinateurs Active Directory

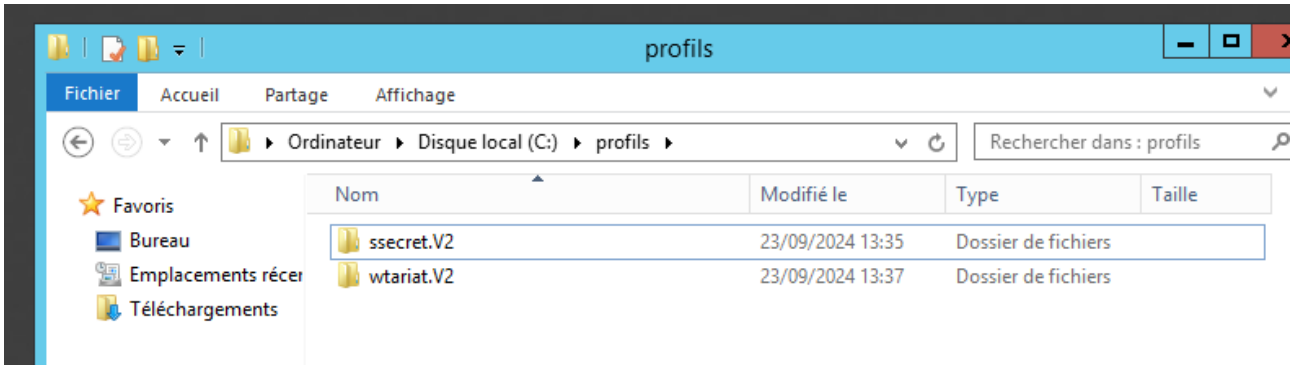
Sélection des utilisateurs :



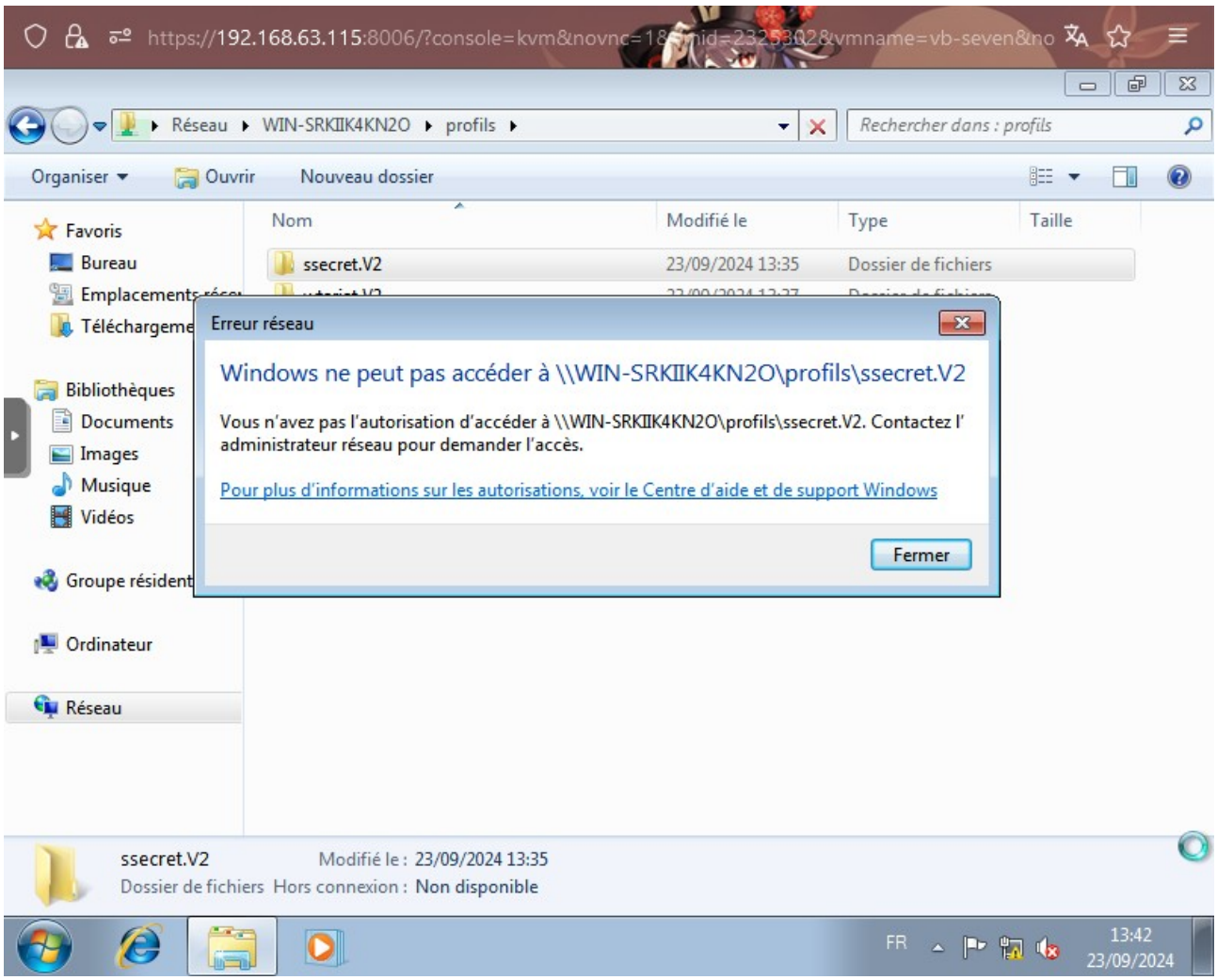
Renseignement du répertoire des profils (qui se trouve sur le serveur, comme il a été précédemment créée et configuré avec les permissions)



Test : Les profils sont bel et bien créées.



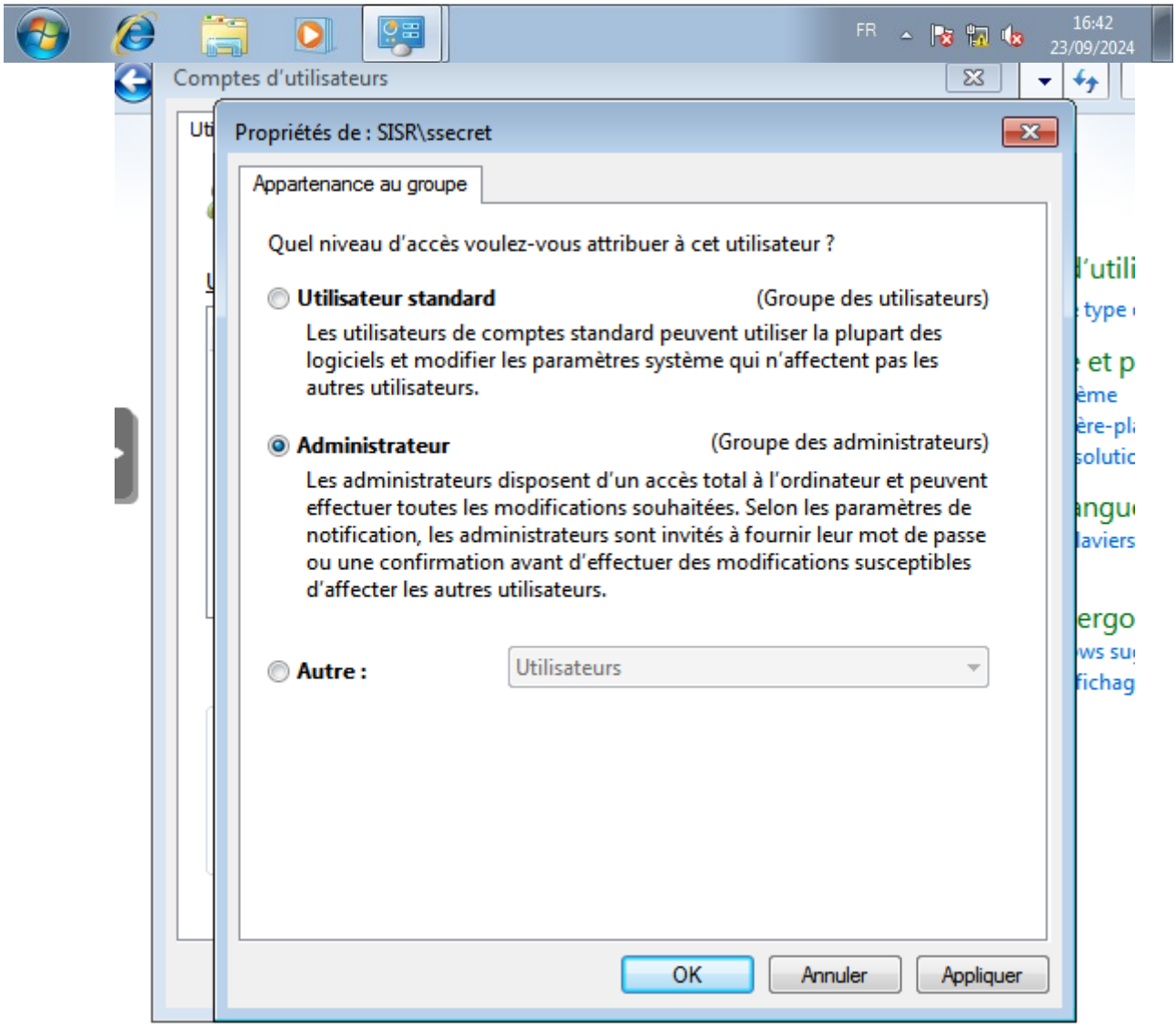
Test des autorisations depuis un autre utilisateur :



Définition de l’utilisateur Sam Secrét comme administrateur de son poste :

Panneau de configuration : Changer le type de compte


https://192.168.63.115:8006/?console=kvm&novnc=1&vmid=232530
Panneau de configuration
Rechercher
Ajuster les paramètres de l'ordinateur
Afficher par : Catégorie
Système et sécurité
Consulter l'état de votre ordinateur
Sauvegarder l'ordinateur
Rechercher et résoudre des problèmes
Réseau et Internet
Afficher l'état et la gestion du réseau
Choisir les options de groupe résidentiel et de partage
Matériel et audio
Afficher les périphériques et imprimantes
Ajouter un périphérique
Programmes
Désinstaller un programme
Obtenir des programmes
Comptes d'utilisateurs
Modifier le type de compte
Apparence et personnalisation
Modifier le thème
Modifier l'arrière-plan du Bureau
Modifier la résolution de l'écran
Horloge, langue et région
Modifier les claviers ou les autres méthodes d'entrée
Options d'ergonomie
Laisser Windows suggérer les paramètres
Optimiser l'affichage


FR
16:42
23/09/2024
Comptes d'utilisateurs
Propriétés de : SISR\ssecret
Appartenance au groupe
Quel niveau d'accès voulez-vous attribuer à cet utilisateur ?
Utilisateur standard (Groupe des utilisateurs)
Les utilisateurs de comptes standard peuvent utiliser la plupart des logiciels et modifier les paramètres système qui n'affectent pas les autres utilisateurs.
Administrateur (Groupe des administrateurs)
Les administrateurs disposent d'un accès total à l'ordinateur et peuvent effectuer toutes les modifications souhaitées. Selon les paramètres de notification, les administrateurs sont invités à fournir leur mot de passe ou une confirmation avant d'effectuer des modifications susceptibles d'affecter les autres utilisateurs.
Autre :
Utilisateurs
OK
Annuler
Appliquer

Entrer les identifiants du compte administrateur.

L’utilisateur est désormais admin sur son propre poste.

Fin.