

-R304

Gestion d'annuaires unifiés

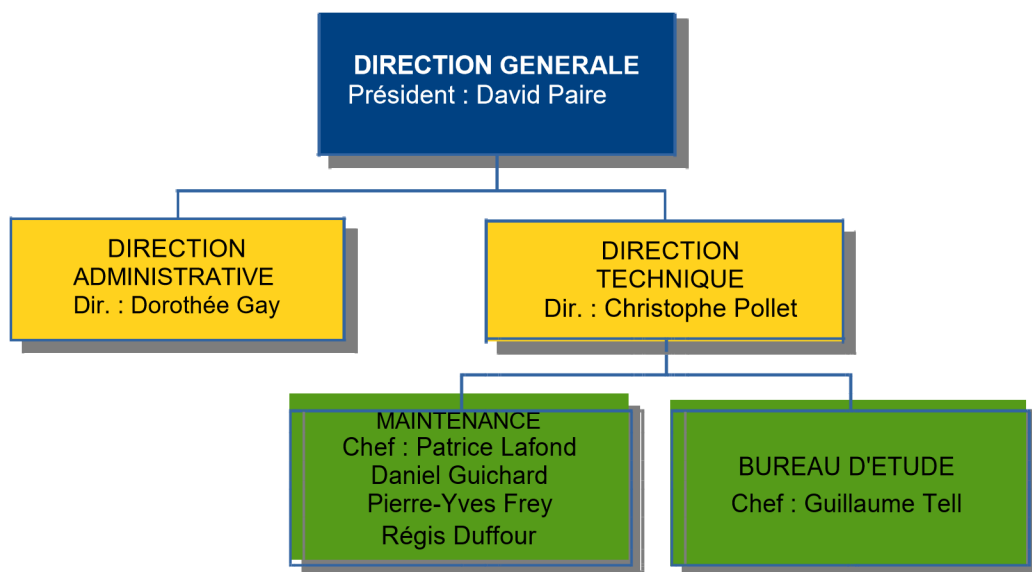
Active Directory

TP

Contexte

Vous intervenez pour le compte de la société « La Colo », qui s'informatise et nécessite la mise en place d'une infrastructure basée sur Active Directory.

Organigramme



Délégations souhaitées

1. La direction administrative est chargée de la gestion de tous les comptes utilisateurs (création, suppression, gestion), ainsi que de la gestion de tous les groupes (création, suppression, modifications d'appartenance).
2. La direction technique et le bureau d'étude doivent pouvoir réinitialiser les mots de passe de l'ensemble des personnels du pôle maintenance.

Environnement de travail

Je dispose des machines virtuelles suivantes, dont le réseau est à paramétrer et le nom ordinateur à modifier (accès depuis vcenter avec le compte login : r304 et mdp : Password)

Nom	IP	OS	Compte admin	Mot de passe
R304-W2016-x	192.168.110.139	Win2016	administrateur	Roa42300
R304-W10 -x	192.168.110.39	Win10	admin	Roa42300

Masque : /21 gateway : 192.168.104.1

Réalisation

Domaine et forêt Active Directory

Mise en place pour La Colo

Pour la création du nouveau domaine, on change d'abord l'adresse DNS au niveau de la carte réseau pour l'adresse 172.0.0.1 :

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 . 110 . 139

Masque de sous-réseau : 255 . 255 . 248 . 0

Passerelle par défaut : 192 . 168 . 104 . 1

☐ 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

Etape de l'installation :

Dans **Gérer** puis **Ajouter des rôles et fonctionnalités**.

Pour les **rôles de serveurs**, sélectionner **Services AD DS**. Pour les fonctionnalités j'ai ajouté **Services TCP/IP simples**. Et enfin cliquer sur **Installer**.

Progression de l'installation

SERVEUR DE DESTINATION
R304-W2016-SEYD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur R304-W2016-SEYD.

Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

[Promouvoir ce serveur en contrôleur de domaine](#)**Gestion de stratégie de groupe****Outils d'administration de serveur distant**

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS



Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

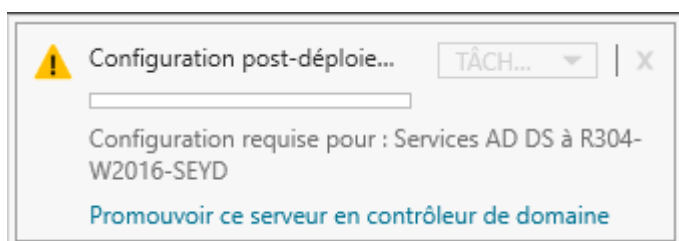
< Précédent

Suivant >

Fermer

Annuler

Après l'installation du service :



Je crée un nouveau domaine dans une nouvelle forêt :

Configuration de déploiement

SERVEUR CIBLE
R304-W2016-SEYD

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

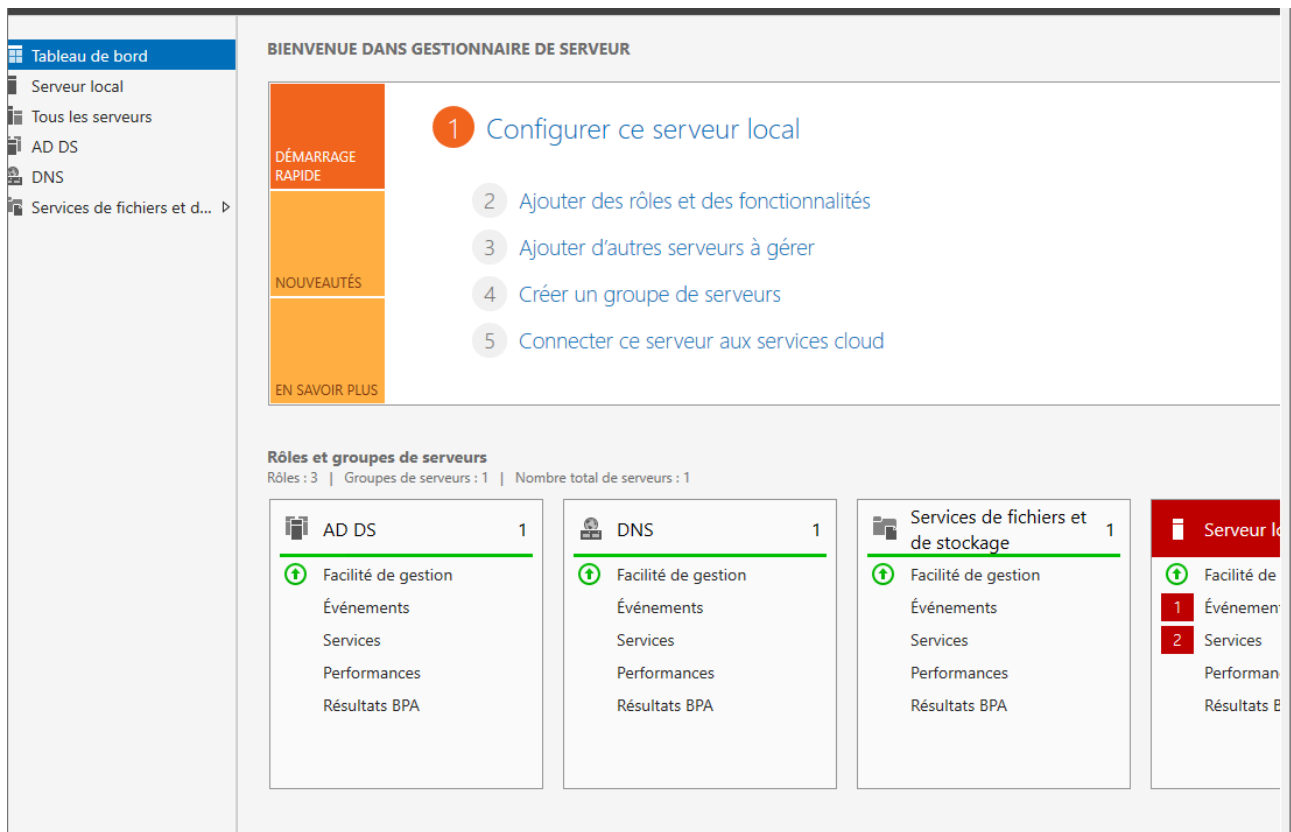
☐ Ajouter un contrôleur de domaine à un domaine existant☐ Ajouter un nouveau domaine à une forêt existante☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

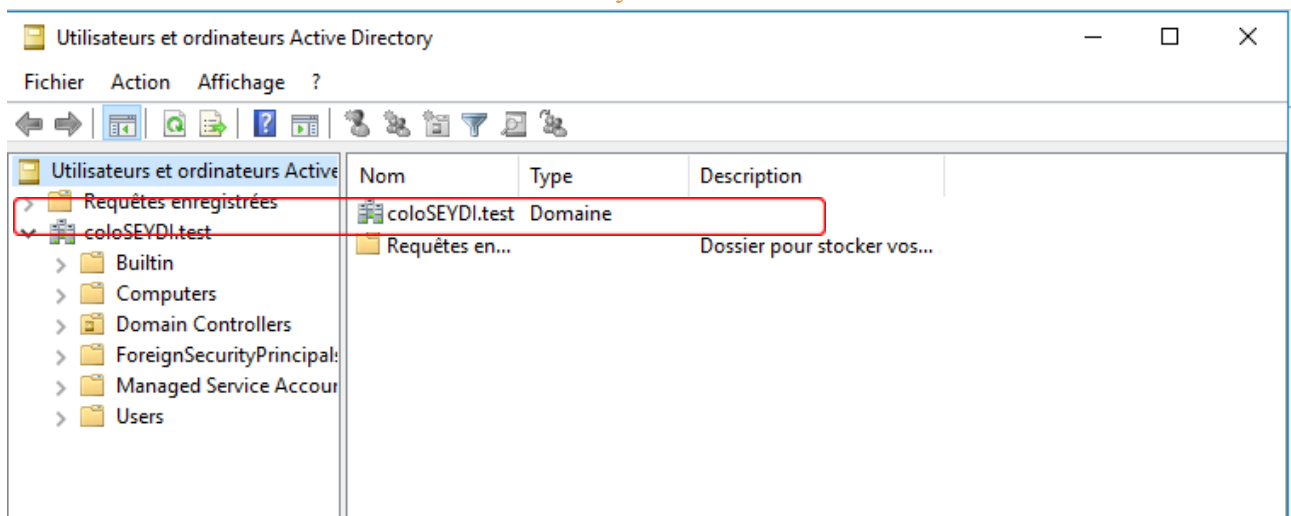
Nom de domaine racine :

coloSEYDI.test

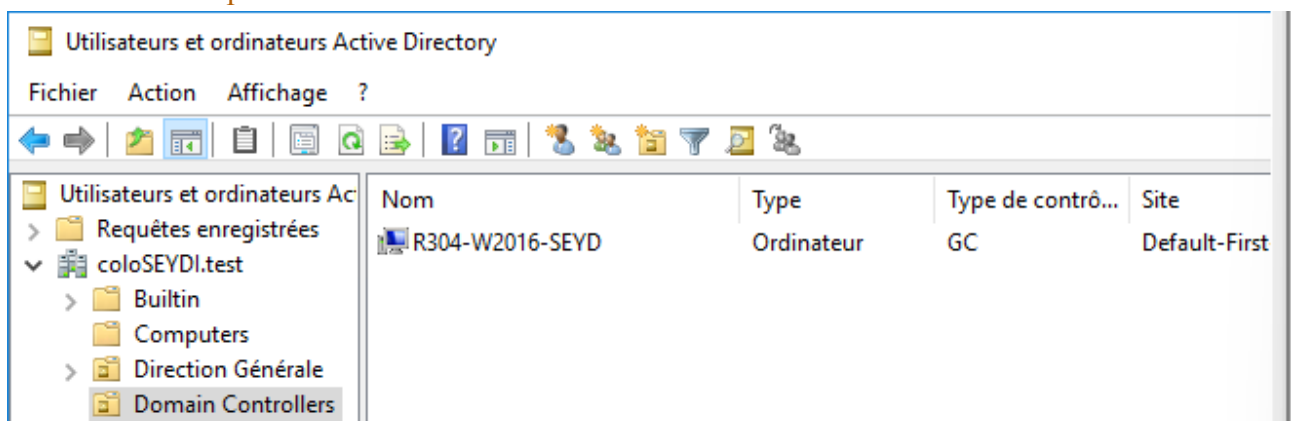
Pour l'option du contrôleur de domaine, le mot de passe renseigné est SeydiR304.
Puis cliquer sur suivant jusqu'à Installer.



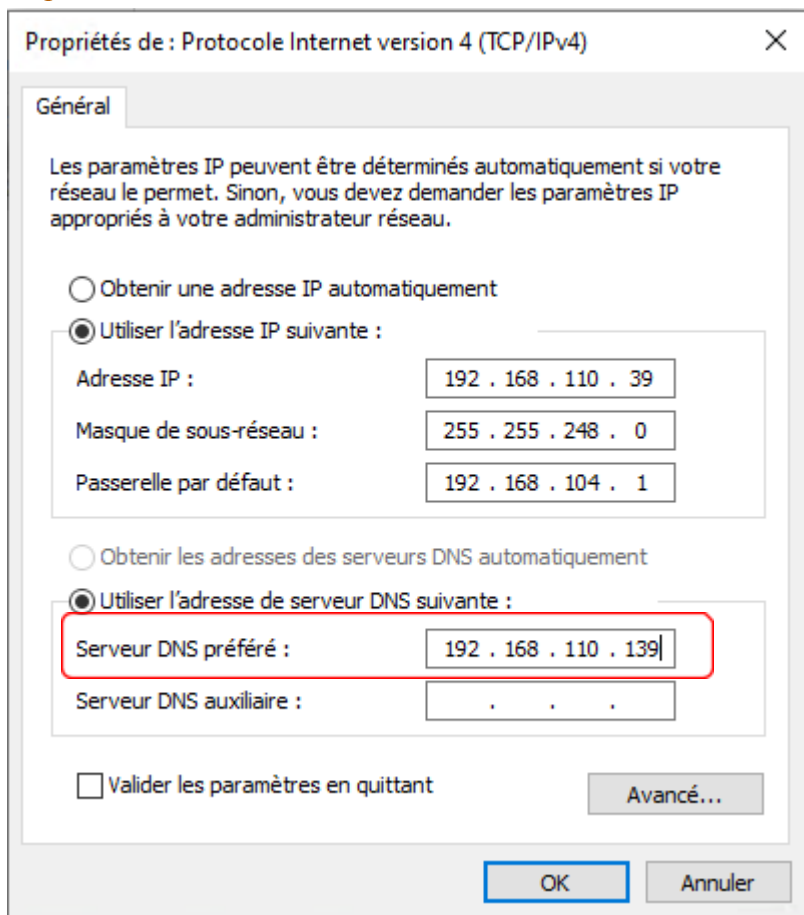
Dans Utilisateurs et ordinateurs Active Directory :



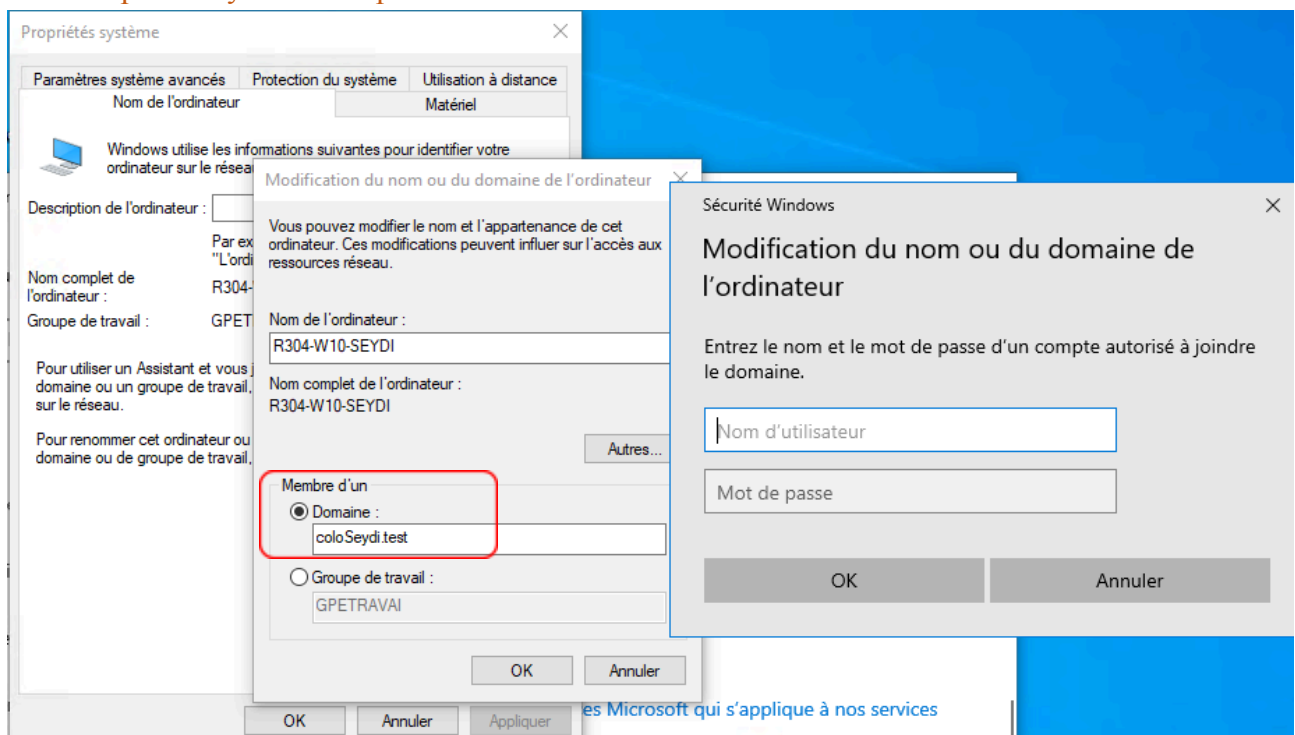
Notre domaine repose sur le contrôleur de domaine R304-W2016-SEYD:



Le poste sous Windows 10, son adresse DNS est l'adresse de notre serveur :



Joindre ce poste au domaine créé :
Dans Propriétés système des paramètres



Renseigner le nom d'utilisateur : administrateur et le mot de passe SeydiR303.

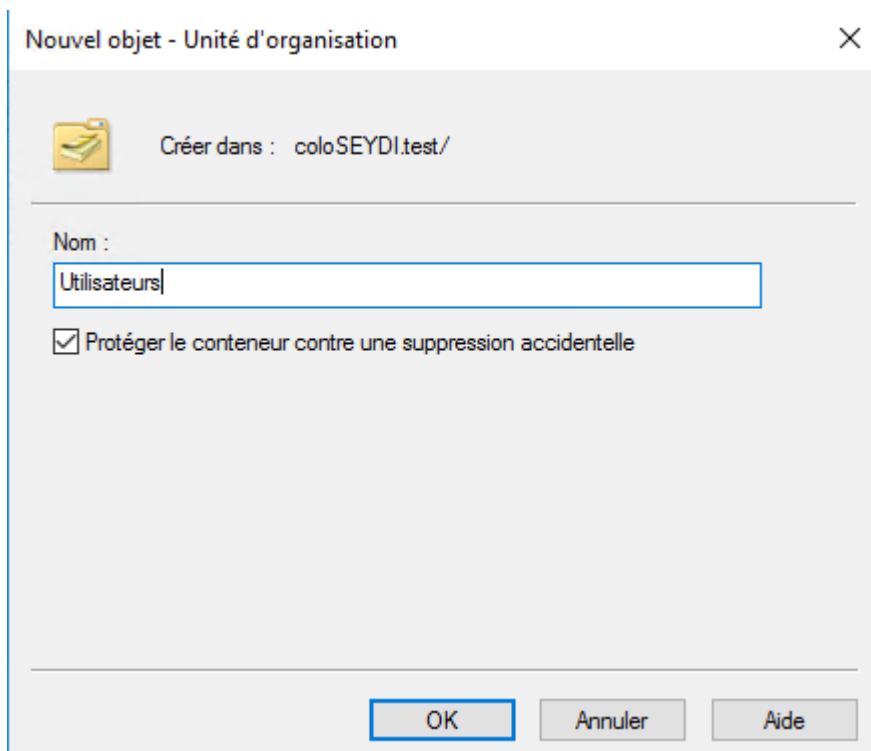
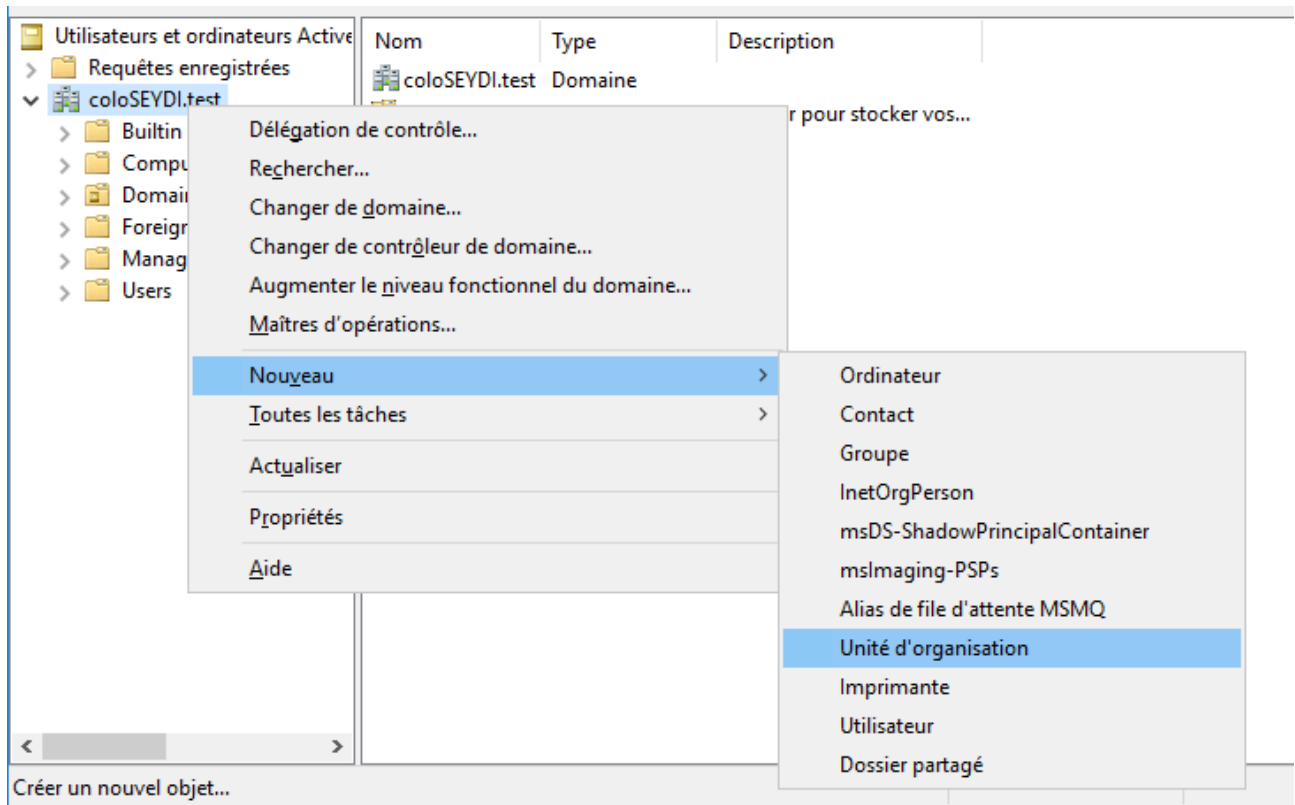
Le poste est maintenant sous le domaine **ColoSEYDI.test**.

Utilisateurs et groupes fonctionnels

Création des utilisateurs en masse:

Tout d'abord j'ai créé OU utilisateurs:

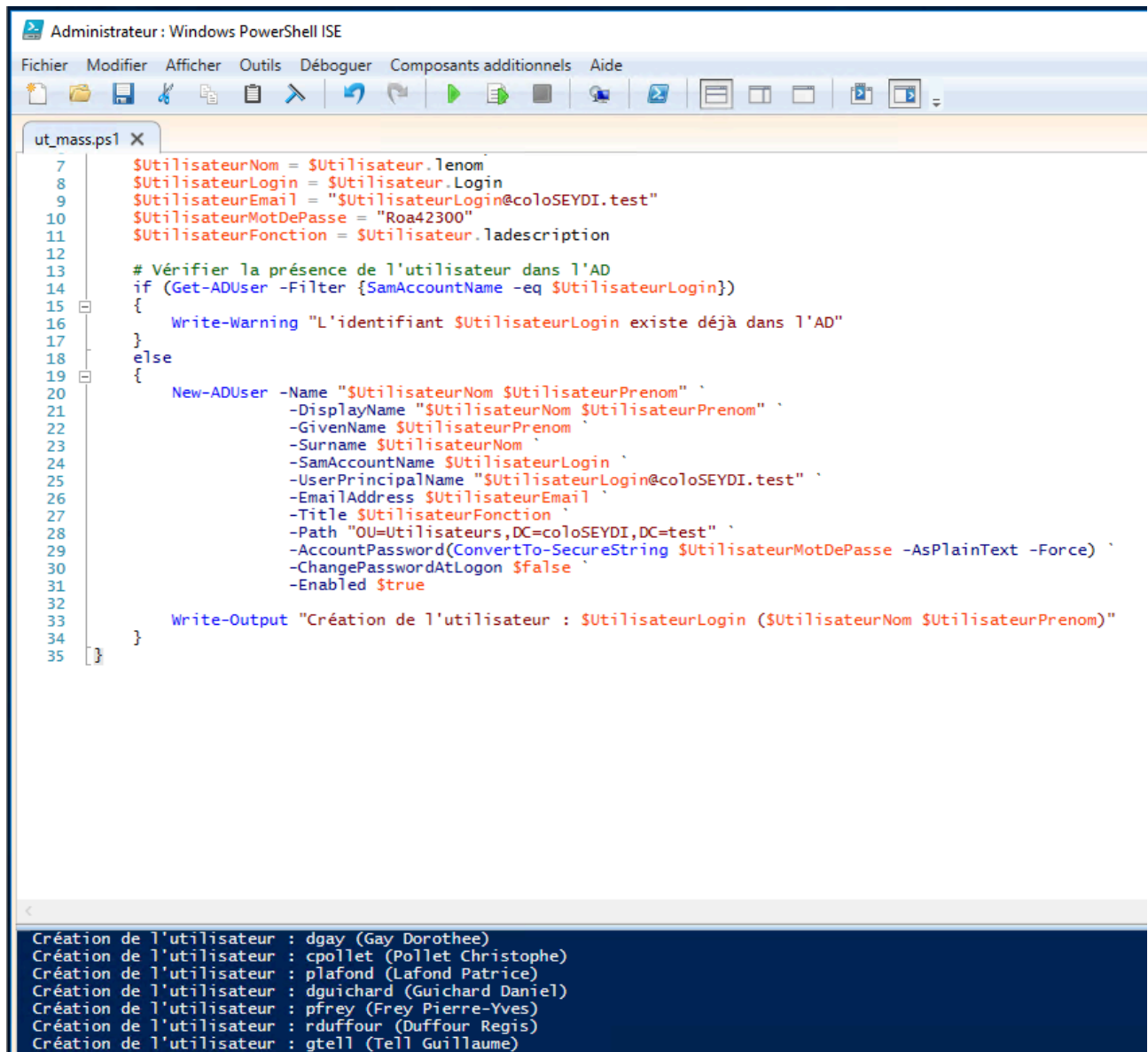
Création de l'OU :



Création des utilisateurs en masse :

<https://www.it-connect.fr/chapitres/creer-des-utilisateurs-dans-lad-a-partir-dun-csv/>

J'ai récupéré le script powershell que j'ai modifié en fonction de nos utilisateurs et de notre domaine.

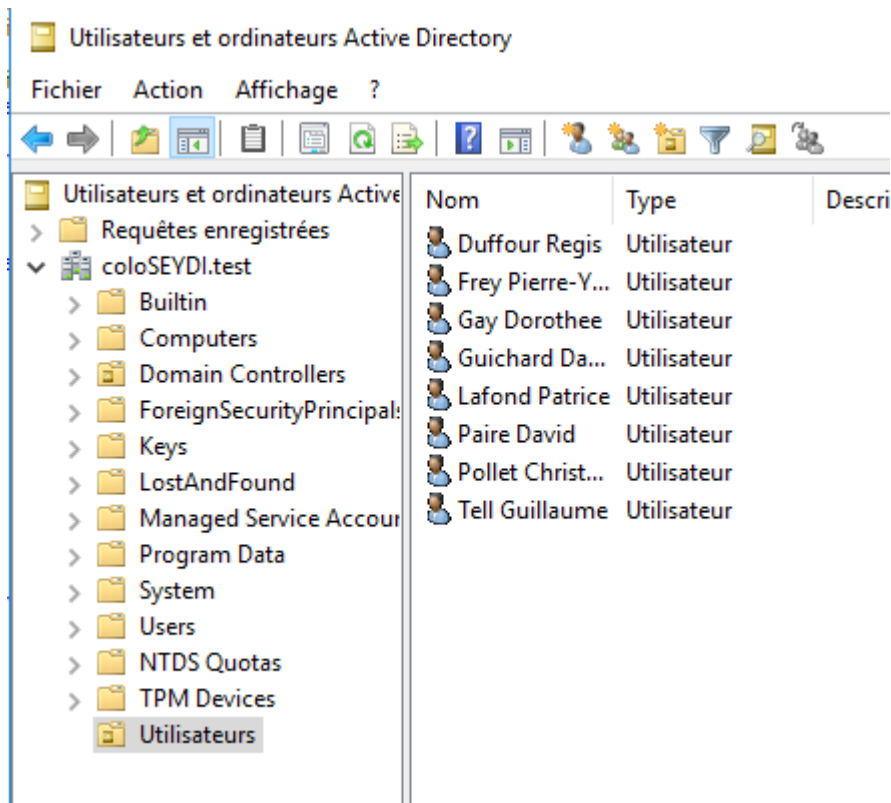


```
Administrateur : Windows PowerShell ISE
Fichier  Modifier  Afficher  Outils  Débuguer  Composants additionnels  Aide

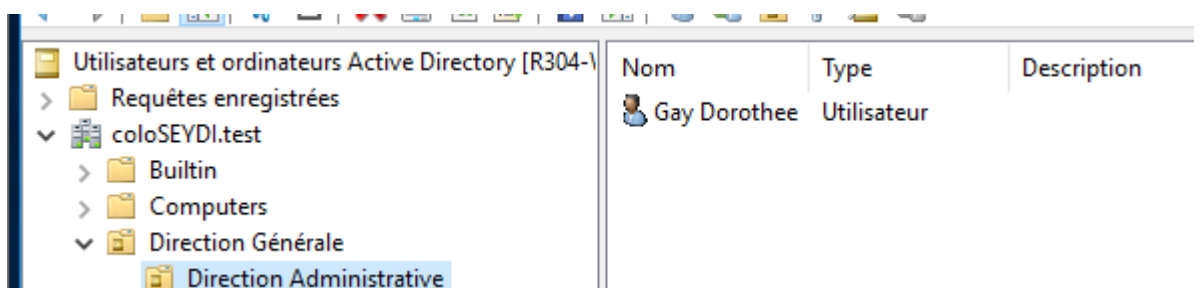
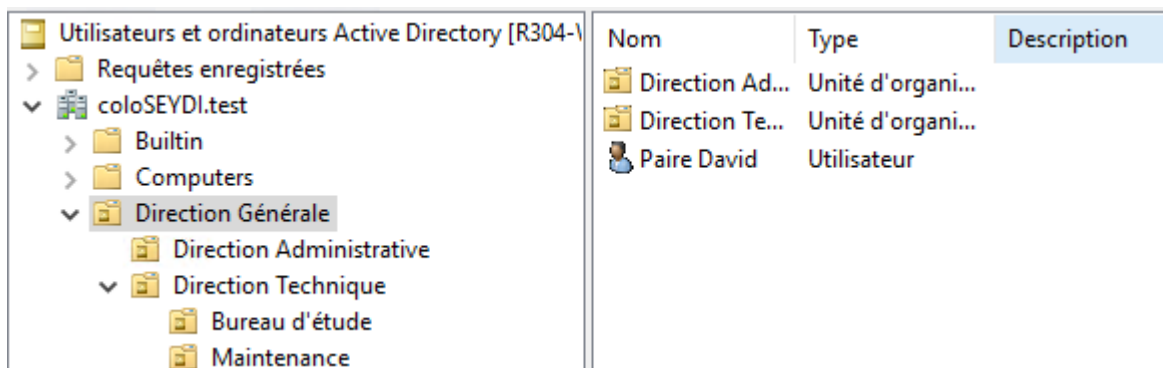
ut_mass.ps1 X
7      $UtilisateurNom = $Utilisateur.Tenom
8      $UtilisateurLogin = $Utilisateur.Login
9      $UtilisateurEmail = "$UtilisateurLogin@coloSEYDI.test"
10     $UtilisateurMotDePasse = "Roa42300"
11     $UtilisateurFonction = $Utilisateur.ladescription
12
13     # Vérifier la présence de l'utilisateur dans l'AD
14     if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin})
15     {
16         Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
17     }
18     else
19     {
20         New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
21             -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
22             -GivenName $UtilisateurPrenom `
23             -Surname $UtilisateurNom `
24             -SamAccountName $UtilisateurLogin `
25             -UserPrincipalName "$UtilisateurLogin@coloSEYDI.test" `
26             -EmailAddress $UtilisateurEmail `
27             -Title $UtilisateurFonction `
28             -Path "OU=Utilisateurs,DC=coloSEYDI,DC=test" `
29             -AccountPassword(ConvertTo-SecureString $UtilisateurMotDePasse -AsPlainText -Force) `
30             -ChangePasswordAtLogon $false `
31             -Enabled $true
32
33         Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
34     }
35 }
```

```
<
Création de l'utilisateur : dgray (Gay Dorothee)
Création de l'utilisateur : cpollet (Pollet Christophe)
Création de l'utilisateur : plafond (Lafond Patrice)
Création de l'utilisateur : dguichard (Guichard Daniel)
Création de l'utilisateur : pfrey (Frey Pierre-Yves)
Création de l'utilisateur : rduffour (Duffour Regis)
Création de l'utilisateur : gtell (Tell Guillaume)
```

Les utilisateurs ont été créés :



Une fois les utilisateurs créés, je vais créer les groupes en respectant l'arborescence comme indiqué dans le sujet. Manuellement, je mets chaque utilisateur suivant l'organigramme:



Utilisateurs et ordinateurs Active Directory [R304-1]	Nom	Type	Description
<ul style="list-style-type: none"> Requêtes enregistrées coloSEYDI.test <ul style="list-style-type: none"> Builtin Computers Direction Générale <ul style="list-style-type: none"> Direction Administrative Direction Technique 	Bureau d'étu...	Unité d'organi...	
	Maintenance	Unité d'organi...	
	Pollet Christ...	Utilisateur	

Utilisateurs et ordinateurs Active Directory [R304-1]	Nom	Type	Description
<ul style="list-style-type: none"> Requêtes enregistrées coloSEYDI.test <ul style="list-style-type: none"> Builtin Computers Direction Générale <ul style="list-style-type: none"> Direction Administrative Direction Technique <ul style="list-style-type: none"> Bureau d'étude Maintenance 	Duffour Regis	Utilisateur	
	Frey Pierre-Y...	Utilisateur	
	Guichard Da...	Utilisateur	
	Lafond Patrice	Utilisateur	

Utilisateurs et ordinateurs Active Directory [R304-1]	Nom	Type	Description
<ul style="list-style-type: none"> Requêtes enregistrées coloSEYDI.test <ul style="list-style-type: none"> Builtin Computers Direction Générale <ul style="list-style-type: none"> Direction Administrative Direction Technique <ul style="list-style-type: none"> Bureau d'étude 	Tell Guillaume	Utilisateur	

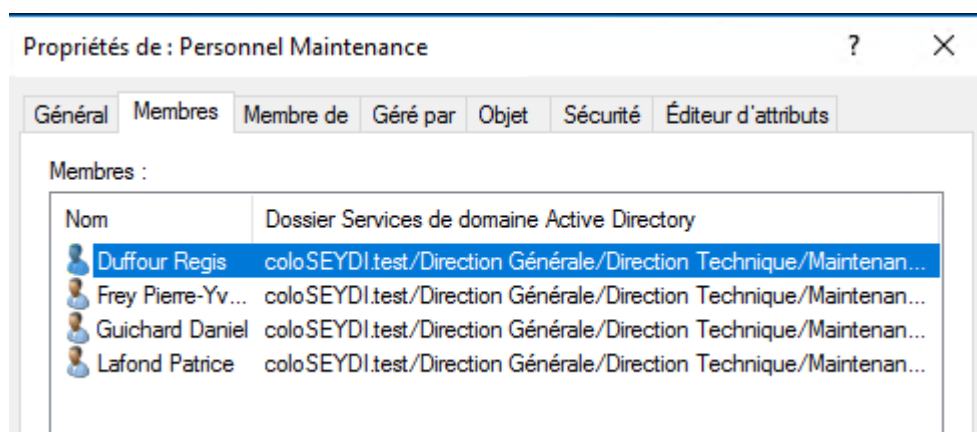
Ainsi, on a les utilisateurs dans les OU respectives.

Création d'OU nommé Groupes pour ensuite créer les différents groupes d'utilisateurs:

Utilisateurs et ordinateurs Active Directory [R304-1]	Nom	Type	De:
<ul style="list-style-type: none"> Requêtes enregistrées coloSEYDI.test <ul style="list-style-type: none"> Builtin Computers Direction Générale Domain Controllers ForeignSecurityPrincipals Groupes 	Chef Bureau...	Groupe de séc...	
	Chef Mainte...	Groupe de séc...	
	Directeur Dir...	Groupe de séc...	
	Directeur di...	Groupe de séc...	
	Personnel M...	Groupe de séc...	
	Président Dir...	Groupe de séc...	

Ensuite mettre les utilisateurs sous les différents groupes d'utilisateurs:

Exemple, pour le groupe **Personnel Maintenance**, j'ajoute tous les utilisateurs suivant l'organigramme dans ce groupe. Pour cela, je fais un clic droit sur le groupe **Personnel Maintenance** puis **Propriétés** et cliquer sur **membres**. Dans ce rubrique j'ai la possibilité d'ajouter des membres à ce groupe:

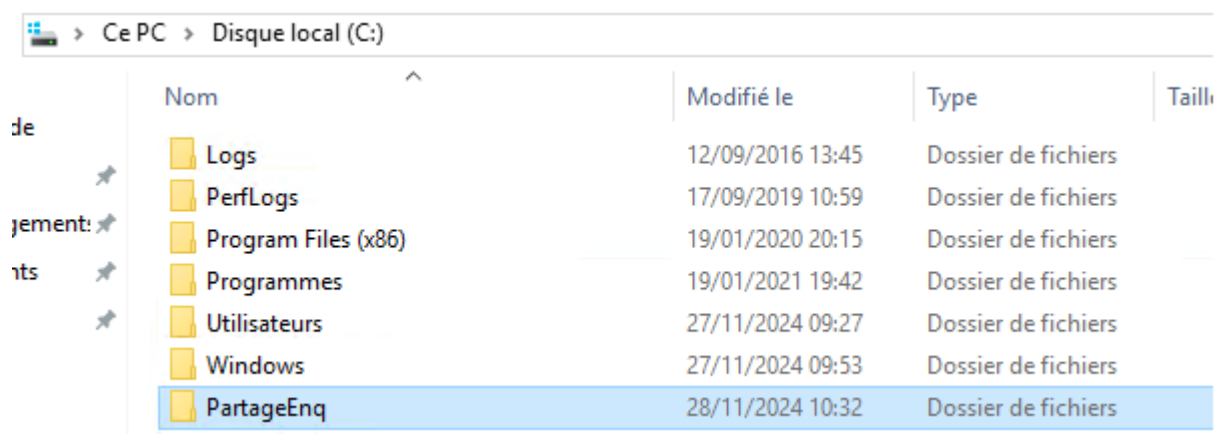


Partage réseau

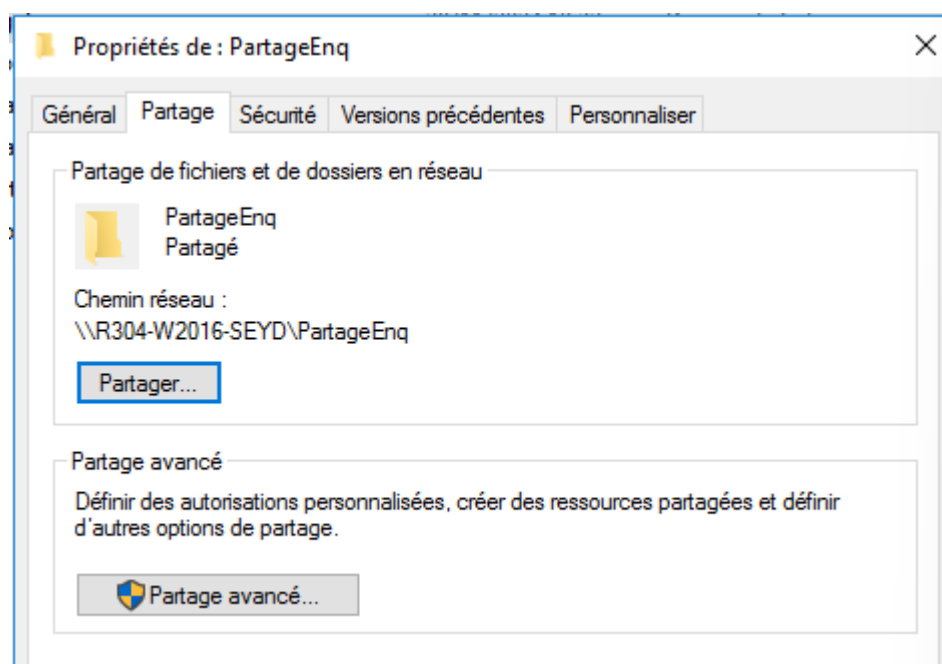
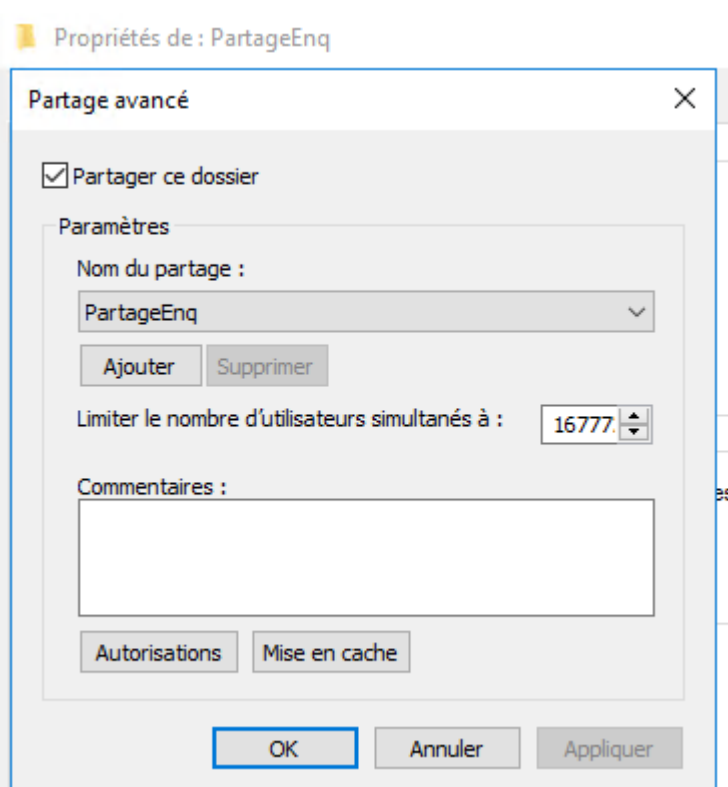
Le partage pourra être accédé d'une part en lecture, d'autre part en modification, en utilisant des groupes dédiés, afin de ne permettre les accréditations que par l'imbrication de groupes et utilisateurs.

Nom de partage	Serveur	Emplacement	Modification	Lecture
Enquetes	R304-W2016-SEYDI	C:\PartageEnq	Dir. Technique Maintenance Bureau d'étude	Dir. Générale Dir. Administrative

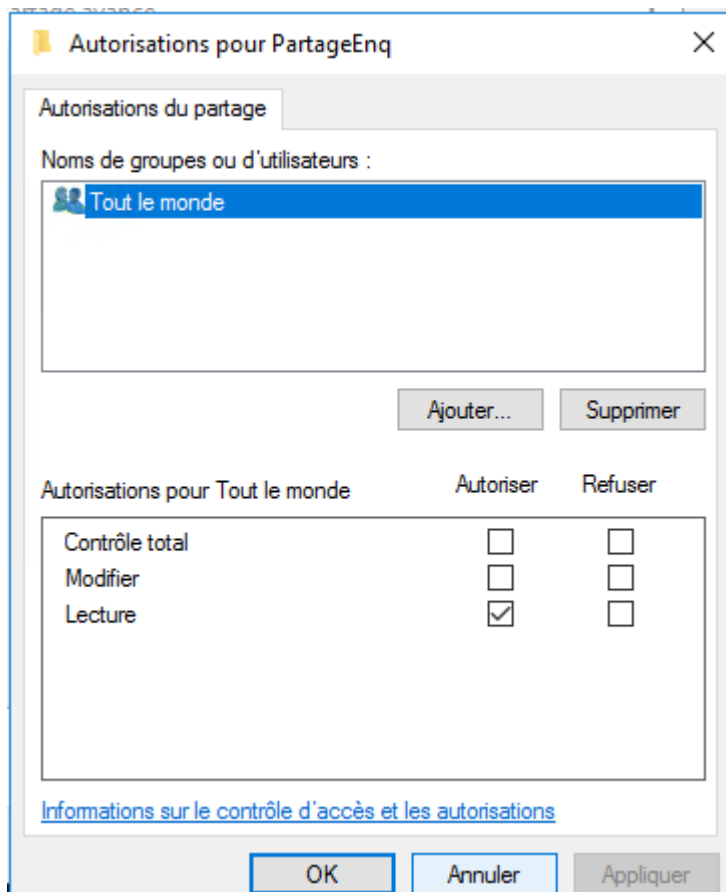
Pour cela, je crée un dossier PartageEnq avec comme emplacement C:\PartageEnq:



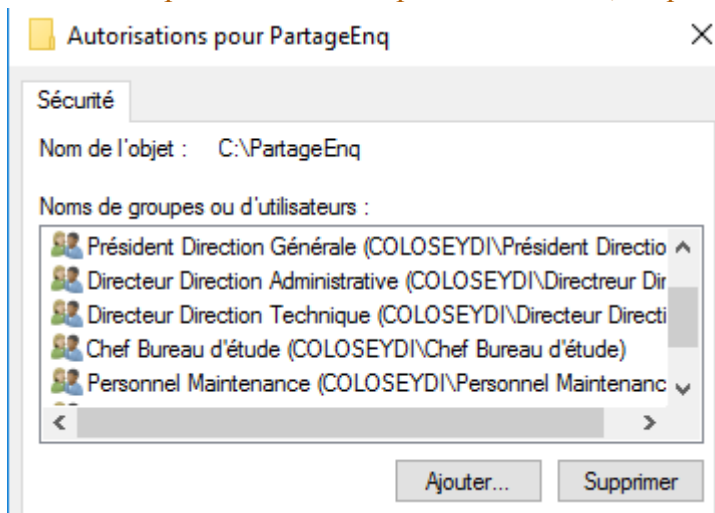
Ensuite un clic droit sur le dossier, puis dans Propriétés ensuite Partage, cliquer sur Partage avancé et active le partage dans le réseau local.



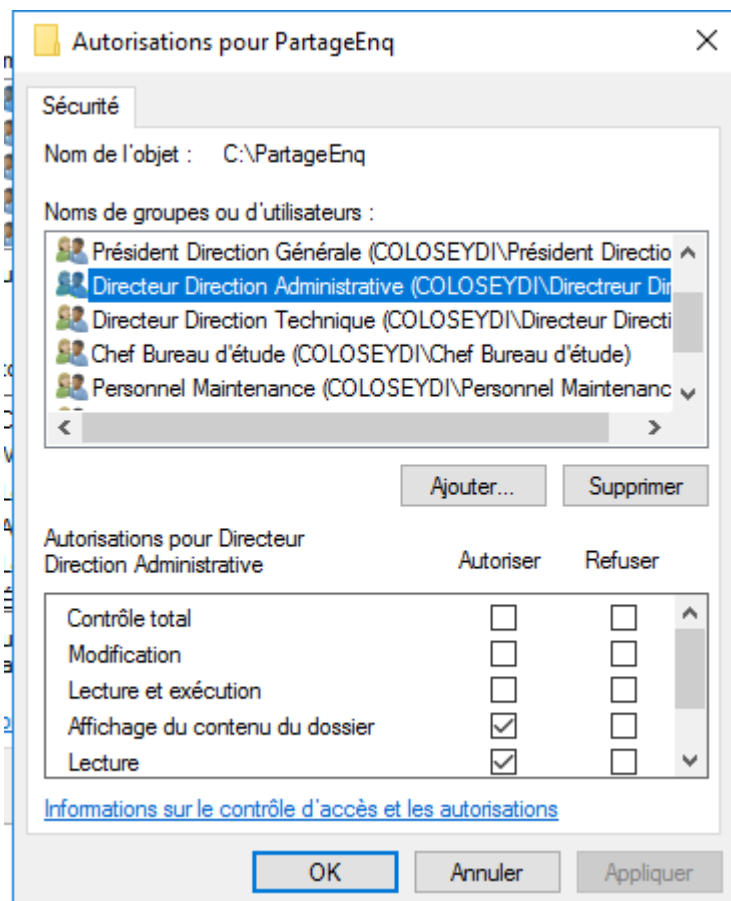
Dans Autorisations:



Maintenant je vais ajouter les groupes utilisateurs de ce dossier.
 Dans les Propriétés du dossier puis sur Sécurité, cliquer sur modifier puis sur Ajouter.

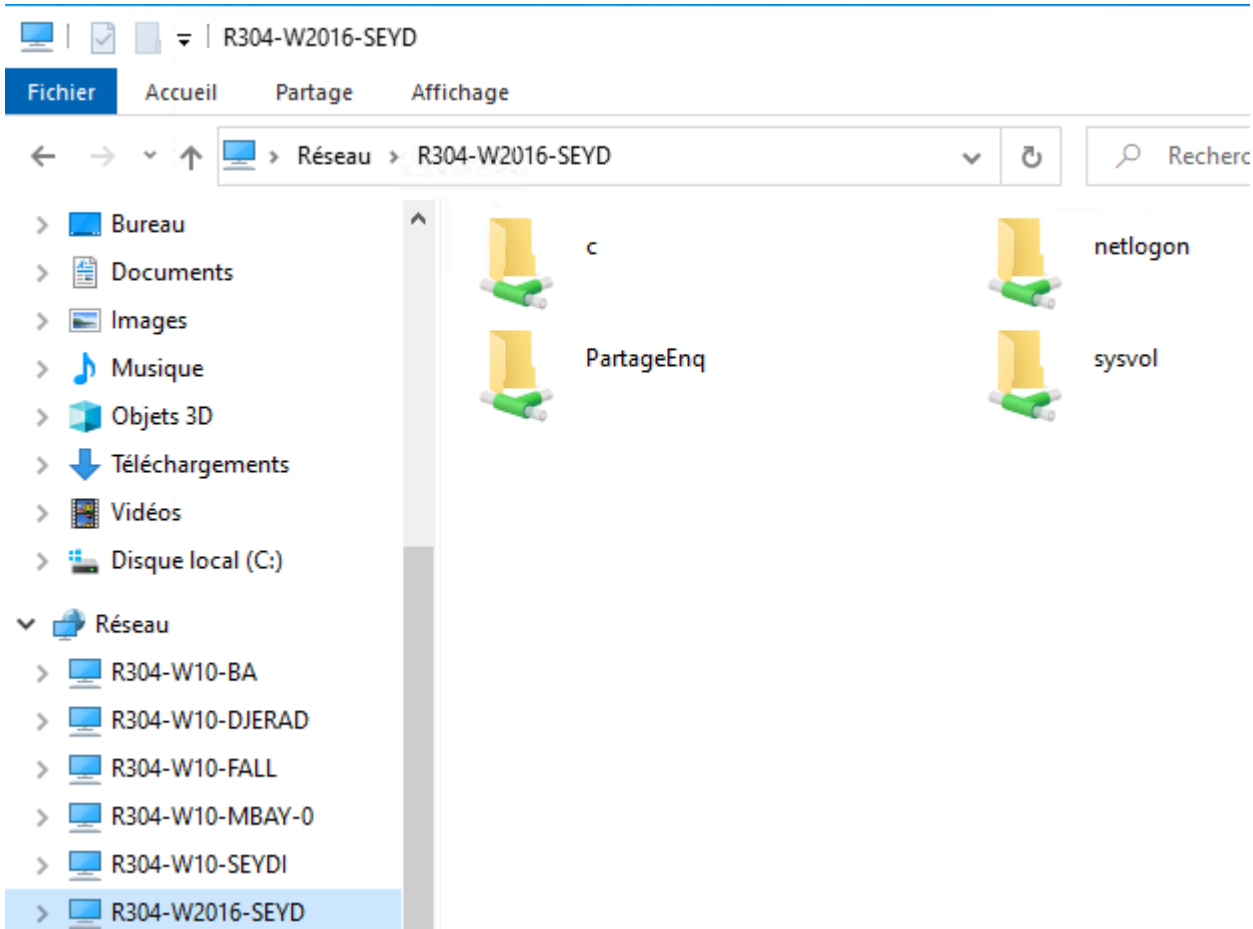


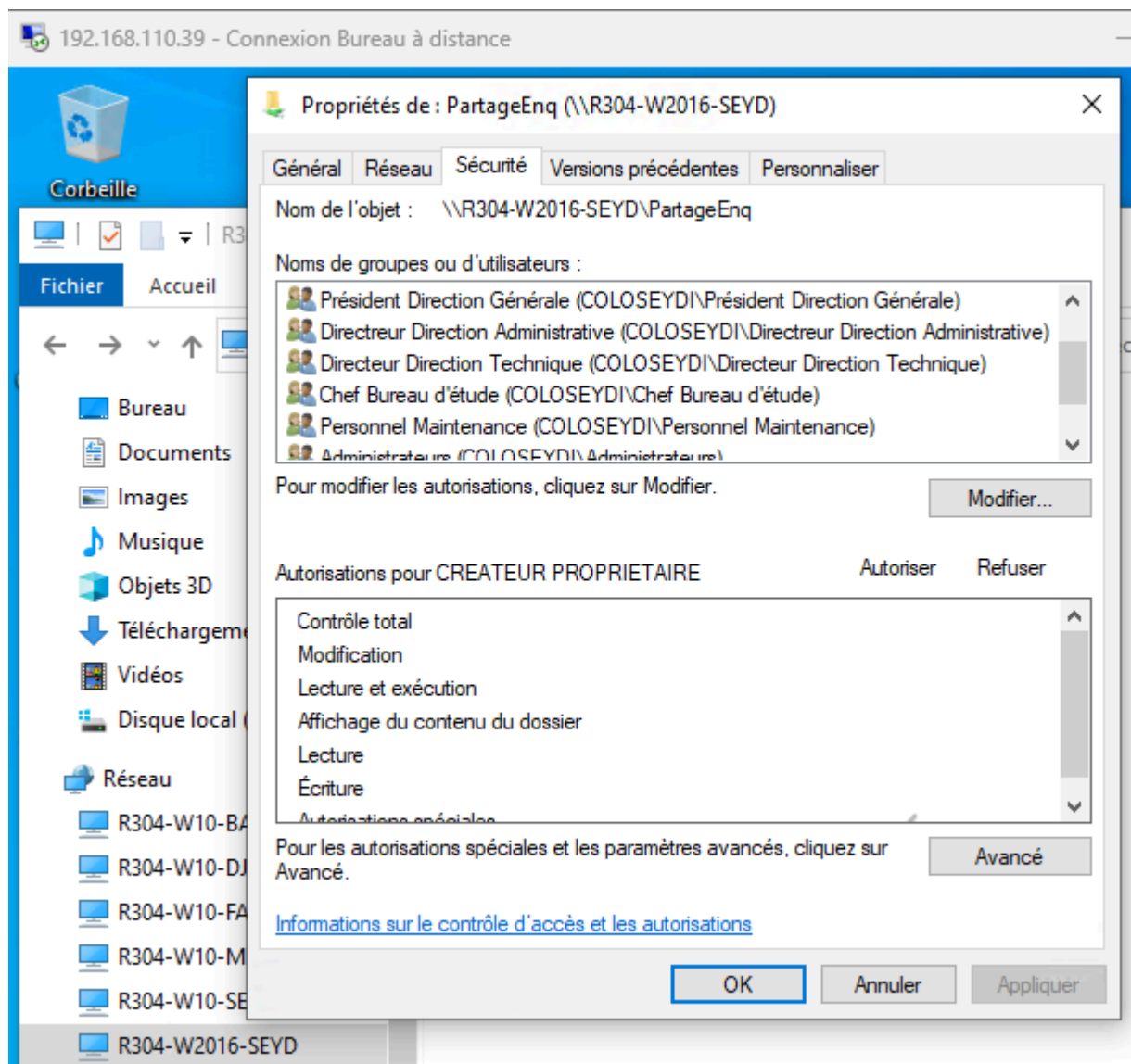
Pour attribuer les droits, cliquer sur les noms de groupe puis au niveau d' **Autorisations**, sélectionner l'autorisation voulue.
 Par exemple, pour le **Président Directeur Général**, j'ai sélectionné l'autorisation **Lecture**.



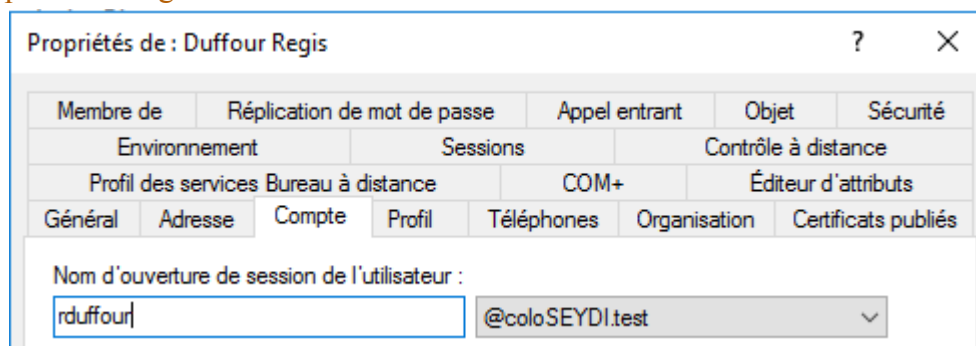
Au niveau du client, ouvrir le gestionnaire de fichiers. Au niveau de l'onglet, je me suis connecté au réseau R304-W2016-SEYD en renseignant le nom d'utilisateur et le mot de passe. Dans ce réseau, je retrouve le dossier PartageEnq créé au niveau du serveur ainsi que nos différents groupes et leurs

autoristations:



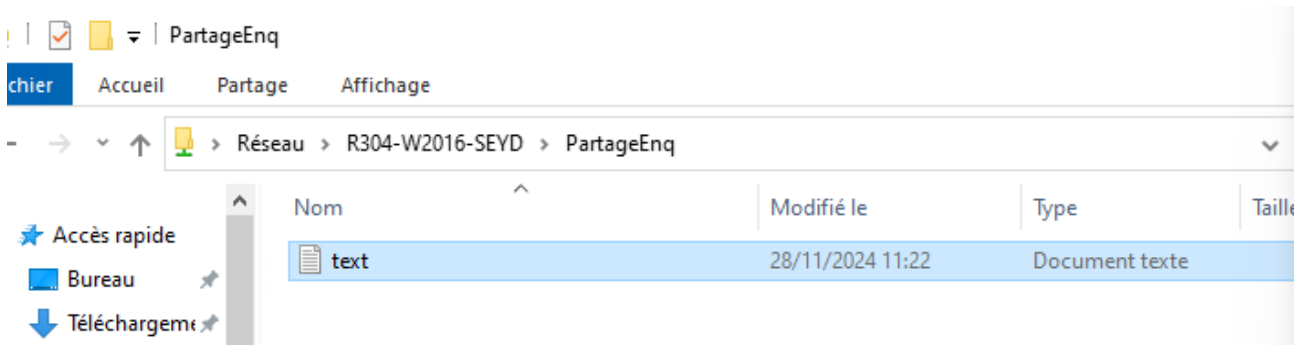


Tests des utilisateurs depuis le client, se connecter avec le nom d'ouverture de session puis le mot de passe renseigné:





Dans le réseau R304-W2016-SEYD, je peux créer un fichier texte dans le dossier partagé, sachant que Duffour Regis est un membre du personnel maintenance qui dispose des droits de modification.



Se connecter avec un utilisateur n'ayant pas les droits de modification comme David Paire:



Sécurité Windows



Entrer vos informations d'identification

Ces informations d'identification seront utilisées pour vous connecter à 192.168.110.39.

Nom d'utilisateur

dpaire@coloSEYDI.test

Mot de passe

••••••••

☐

Mémoriser mes informations



192.168.110.39 - Connexion Bureau à distance

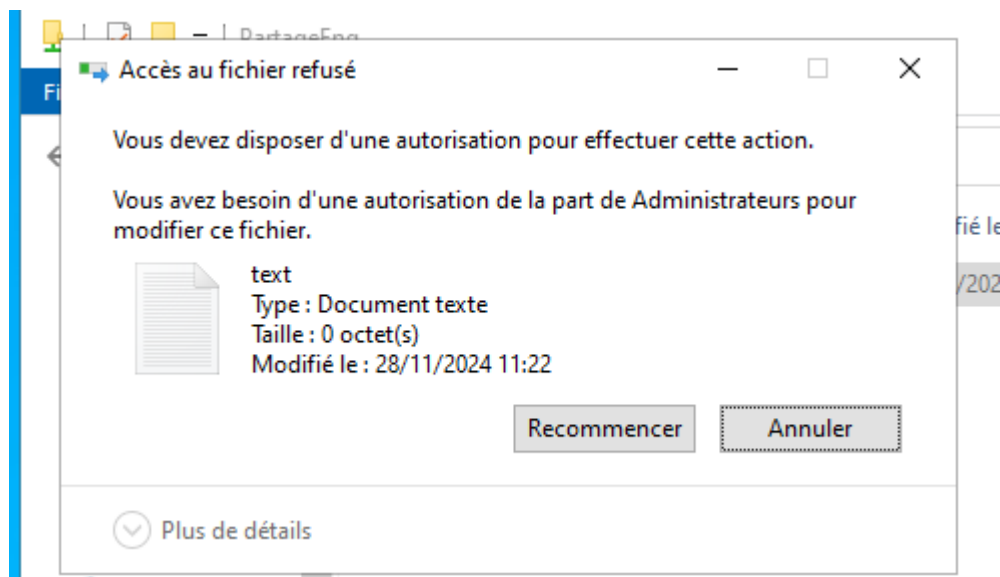


Paire David



Bienvenue

J'essaye de supprimer le fichier txt créé depuis le serveur:



Le partage ainsi que la gestion des droits pour les utilisateurs ont fonctionné.

Délégation

Mettez en place les règles de délégation demandées à l'aide de l'assistant de délégation. Vous pouvez tester le bon fonctionnement des délégations depuis le poste Windows 10, en changeant de comptes utilisateurs.

La deuxième délégation:

La direction technique et le bureau d'étude doivent pouvoir réinitialiser les mots de passe de l'ensemble des personnels du pôle maintenance:

Pour cela, faire un clic droit sur l'OU Maintenance puis cliquer sur Délégation de contrôle.

Au niveau de Utilisateurs ou groupes, cliquer sur Ajouter pour ajouter le groupe Direction Technique ainsi que le chef Bureau d'étude:

Assistant Délégation de contrôle

Utilisateurs ou groupes

Sélectionnez un ou plusieurs groupes ou utilisateurs auxquels vous voulez déléguer le contrôle.

Utilisateurs et groupes sélectionnés :

- Directeur Direction Technique (COLOSEYD\Directeur Direction Technique)
- Chef Bureau d'étude (COLOSEYD\Chef Bureau d'étude)

Ajouter... Supprimer

< Précédent Suivant > Annuler Aide

Puis au niveau Tâches à déléguer, sélectionner la tâche souhaitée:

Assistant Délégation de contrôle

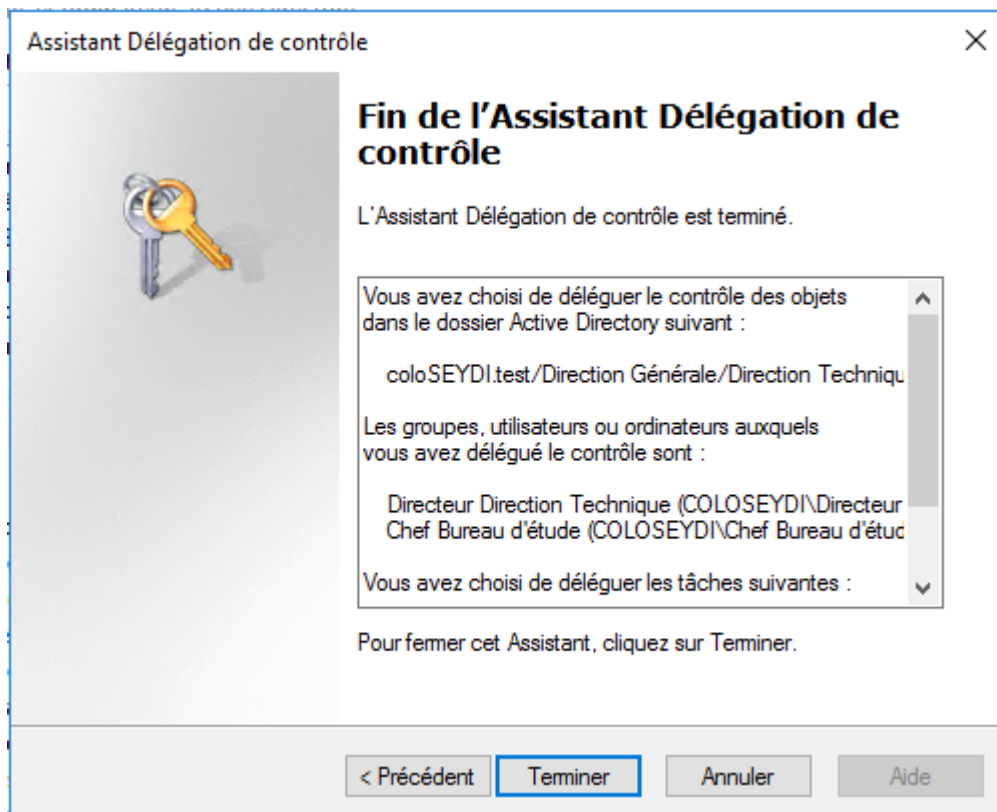
Tâches à déléguer

Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.

☒ Déléguer les tâches courantes suivantes :

- ☐ Gérer les liens de stratégie de groupe
- ☐ Générer le jeu de stratégie résultant (Planification)
- ☐ Générer le jeu de stratégie résultant (Enregistrement)
- ☐ Créer, supprimer et gérer des comptes inetOrgPerson
- ☒ Réinitialiser les mots de passe inetOrgPerson et forcer la modification d
- ☐ Lire toutes les informations inetOrgPerson

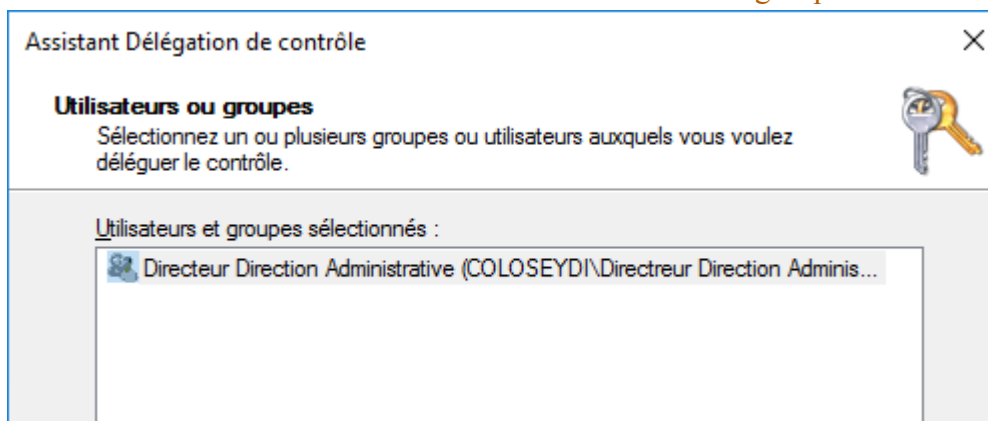
☐ Créer une tâche personnalisée à déléguer



1ère délégation:

- La direction administrative est chargée de la gestion de tous les groupes (création, suppression, modifications d'appartenance)

Au niveau de l'OU Groupes, faire un clic droit puis sur Délégation de contrôle. Ajouter le groupe de la Direction Administrative au niveau d'Utilisateurs ou groupes:



Ensuite déléguer les tâches:

Assistant Délégation de contrôle

Tâches à déléguer
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.

☒ Déléguer les tâches courantes suivantes :

- ☐ Créer, supprimer et gérer les comptes d'utilisateurs
- ☐ Réinitialiser les mots de passe utilisateur et forcer le changement de m
- ☐ Lire toutes les informations sur l'utilisateur
- ☒ Créer, supprimer et gérer les groupes
- ☒ Modifier l'appartenance à un groupe
- ☐ Gérer les liens de stratégie de groupe
- ☐ Générer le jeu de stratégie résultant (Planification)

☐ Créer une tâche personnalisée à déléguer

< Précédent Suivant > Annuler Aide

Assistant Délégation de contrôle

Fin de l'Assistant Délégation de contrôle

L'Assistant Délégation de contrôle est terminé.

Vous avez choisi de déléguer le contrôle des objets dans le dossier Active Directory suivant :

coloSEYDI.test/Groupes

Les groupes, utilisateurs ou ordinateurs auxquels vous avez délégué le contrôle sont :

Directeur Direction Administrative (COLOSEYDI\Directr

Vous avez choisi de déléguer les tâches suivantes :

Pour fermer cet Assistant, cliquez sur Terminer.

- La direction administrative est aussi chargée de la gestion de tous les comptes utilisateurs:

Stratégies de groupes (GPO)

Créez les GPOs permettant d'implémenter les paramètres ordinateurs et utilisateur demandés.

Pour gagner en clarté, vous n'utiliserez ni des filtres de sécurité personnalisés, ni ne forcerez ou bloquerez l'héritage des GPOs. Liez les OUs adéquates et testez les sur votre machine Windows 10.

✕ Vous présentez les étapes de création et d'affectation d'une des GPOs demandées (au choix)