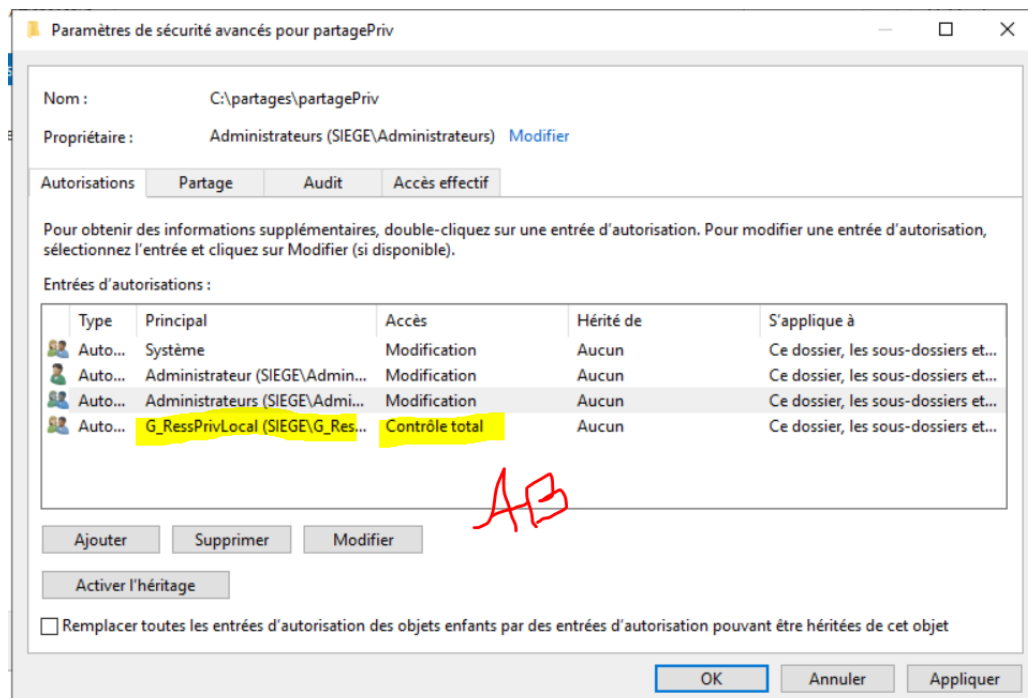


Création du serveur Windows AD2 qui contient Active Directory

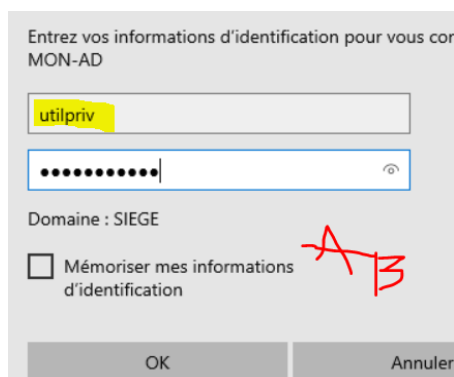
Nous importons la VM "AD2" précédemment téléchargée, lui assignons le mode accès réseau "interne" sur l'interface "COEUR"

Nous créons ensuite le groupe de sécurité dans le domaine SIEGE "G_RessPrivLocal" en local avec un contrôle total au dossier **partagePriv** et supprimer "G_RessPriv" des autorisation

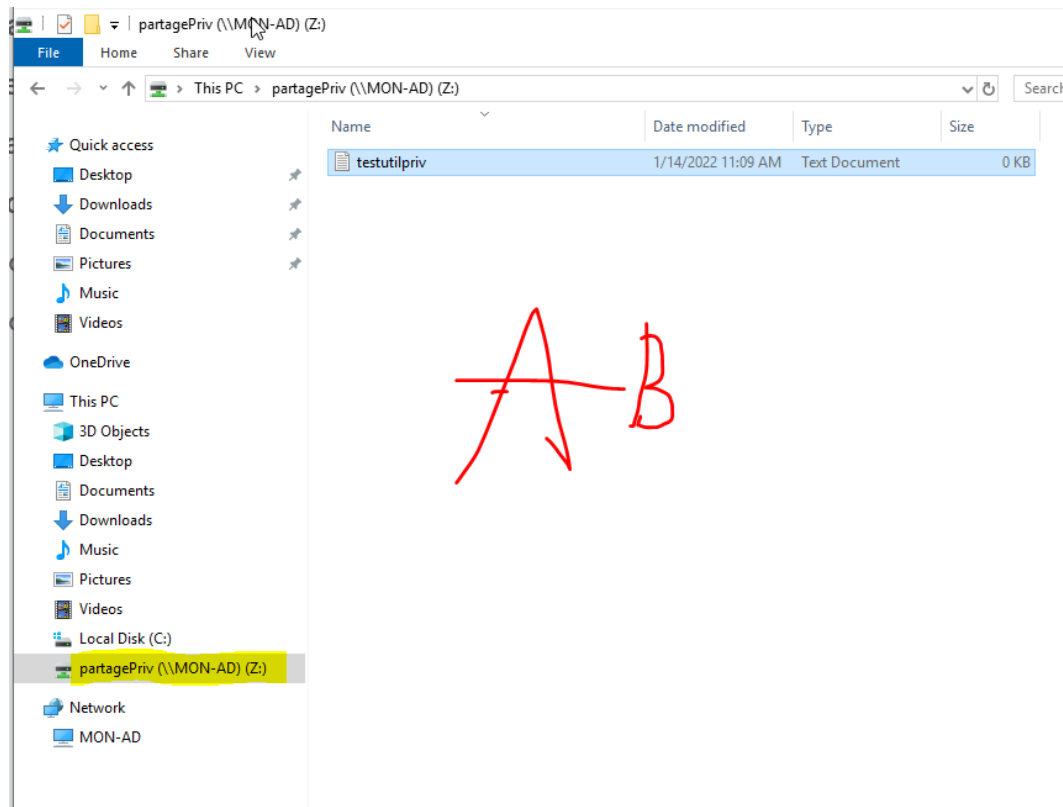


Test du nouveau groupe de sécurité renforcée

A l'aide de l'utilisateur "utilPriv", on se connecte à "partagePriv" et vérifions que nous avons les droits d'écriture.



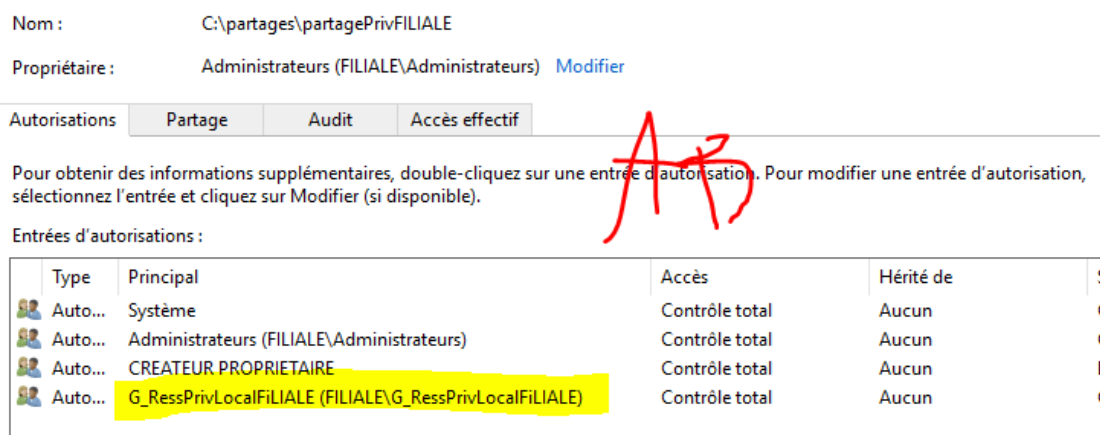
Nous créons ensuite un fichier dans le dossier pour vérifier que “utilPriv” a bien les droits d’écriture.



Création des utilisateurs et ressources dans le domaine FILIALE

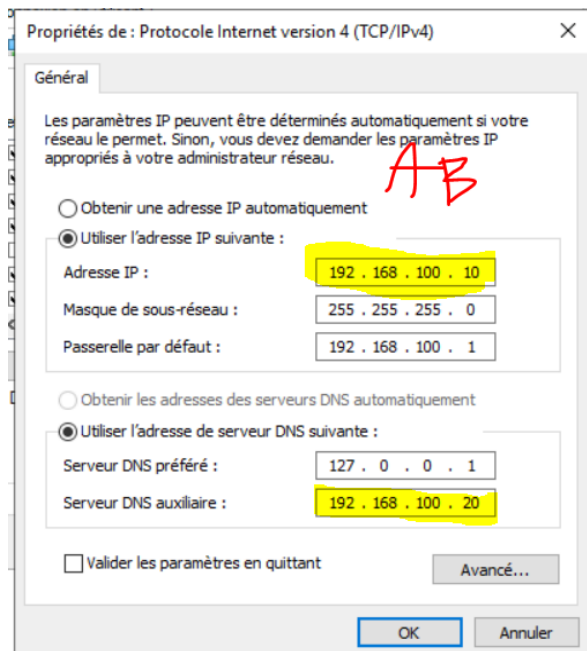
Nous créons les groupes “**G_RessPrivLocalFILIALE**” et “**G_UtilPrivFILIALE**” membre de “**G_RessPrivLocalFILIALE**” et l'utilisateur “**utilPrivFILIALE**” membre de “**G_UtilPrivFILIALE**”.

Nous créons ensuite un répertoire de partage avec comme chemin absolu “**c:\partages\partagePrivFILIALE**” en attribuant les droits au bon groupe.

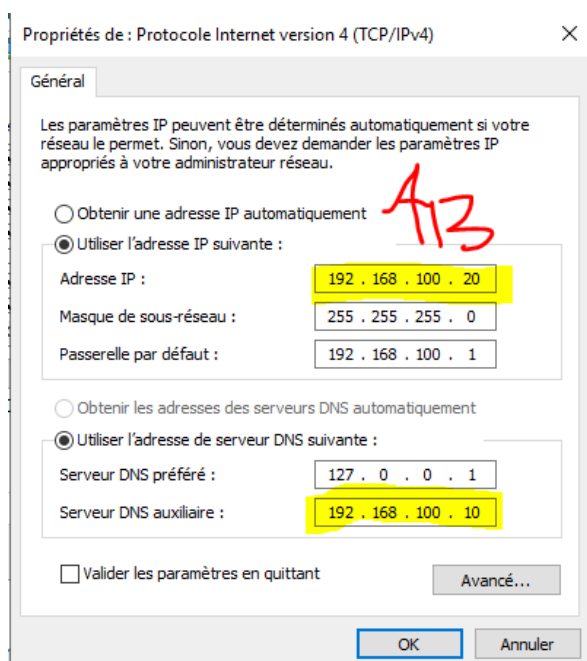


Création de la relation d'approbation

Nous allons établir une approbation unidirectionnelle entraîne, pour ce faire nous commençons par attribuer à la “monAD” un dns secondaire il s'agit de l'adresse ip de “monAD2”



Sur “monAD2”, Nous créons redirecteur conditionnel similaire vers le contrôleur ”monAD”

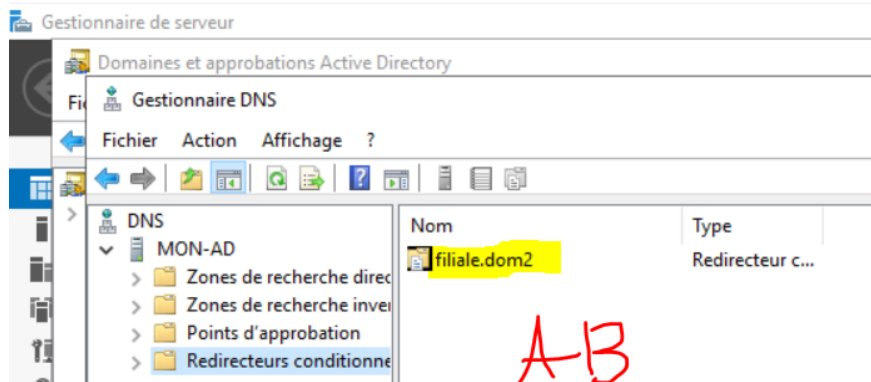


Création de la relation d'approbation dans MONDOMAINE

Nous créons un redirecteur conditionnel depuis monAD vers le contrôleur monAD2

windows-server-2019-modele [En fonction] - Oracle VM VirtualBox

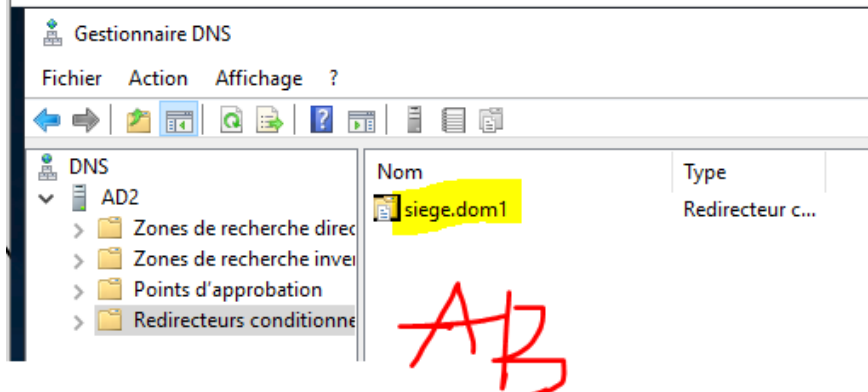
Fichier Machine Écran Entrée Périphériques Aide



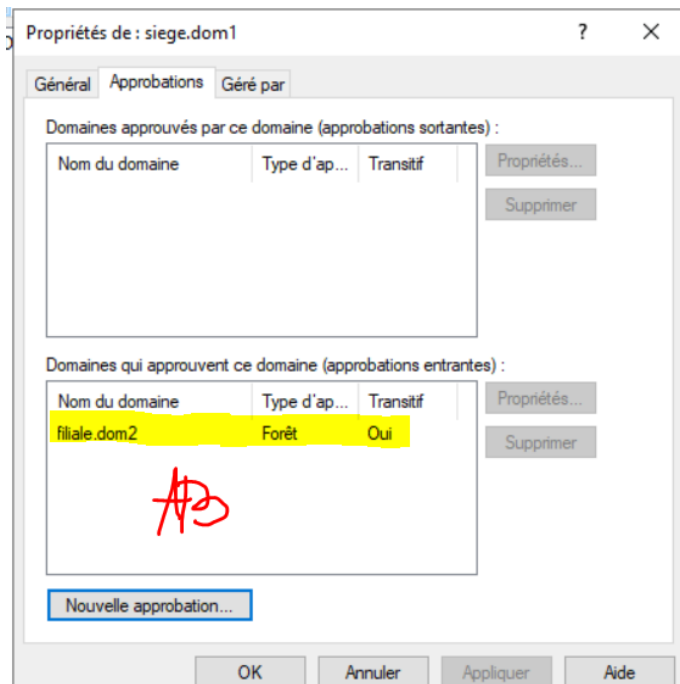
Nous créons un redirecteur conditionnel depuis monAD2 vers le contrôleur monAD

windows-server-2019-AD2 [En fonction] - Oracle VM Virtual

Fichier Machine Écran Entrée Périphériques A



Nous créons la relations d'approbation



Donner l'accès aux ressources de FILIALE pour les utilisateurs de SIEGE

Nous créons une délégation de contrôle pour L'administrateur de siège du domaine SIEGE depuis monAD2

Sélectionnez des utilisateurs, des ordinateurs ou des groupes

Sélectionnez le type de cet objet :
des utilisateurs ou des groupes

À partir de cet emplacement :
siege.dom1

Requêtes communes

Sécurité Windows

Entrer les informations d'identification ré

Entrez vos informations d'identification pour un compte a
autorisations pour siege.dom1.

Exemple : Utilisateur, Utilisateur@microsoft.com ou Doma
\Nom d'utilisateur

Rés : SIEGE\Administrateur

Nom :

Domaine : SIEGE

OK Annuler

nous sélectionnons l'administrateur du domaine siege et nous selection la bonne tâche

Assistant Délégation de contrôle

Utilisateurs ou groupes

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

Utilisateurs et groupes sélectionnés :

Administrateur (SIEGE\Administrateur)

Ajouter... Supprimer

< Précédent Suivant > Annuler Aide

Assistant Délégation de contrôle

Tâches à déléguer

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

☒ Déléguer les tâches courantes suivantes :

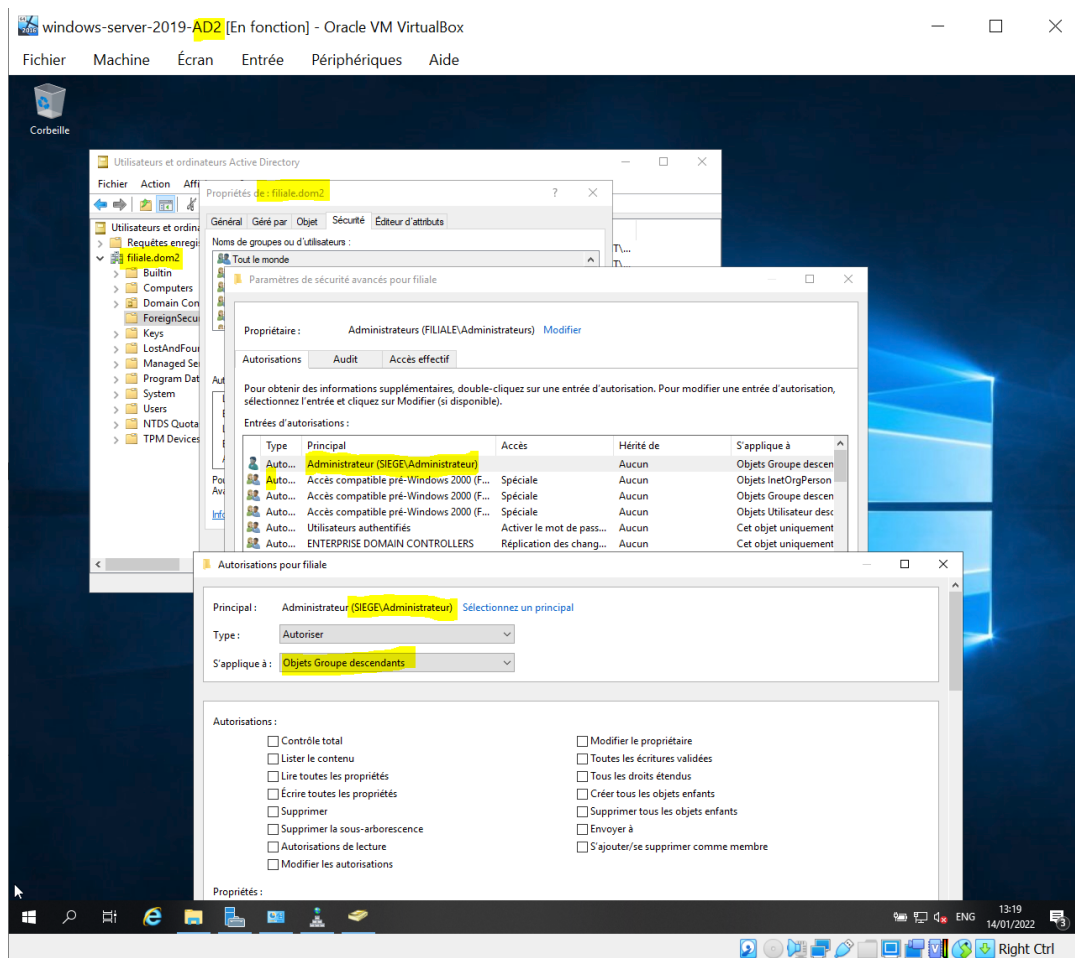
- ☐ Créer, supprimer et gérer les comptes d'utilisateurs
- ☐ Réinitialiser les mots de passe utilisateur et forcer le changement de m
- ☐ Lire toutes les informations sur l'utilisateur
- ☒ Modifier l'appartenance à un groupe
- ☐ Joindre un ordinateur au domaine
- ☐ Gérer les liens de stratégie de groupe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

☐ Créer une tâche personnalisée à déléguer

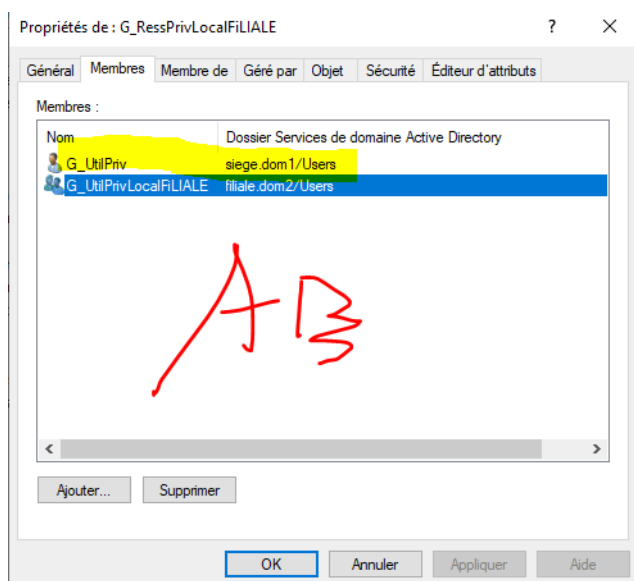
< Précédent Suivant > Annuler Aide

Vérifier et modifier les délégations accordées

les autorisations accordées on bien était prisent en compte



on associe G_UtilPriv du domaine "SIEGE" au groupe G_RessPrivLocalFILIALE depuis monAD2



Que constatez vous ? Comment l'expliquer ?

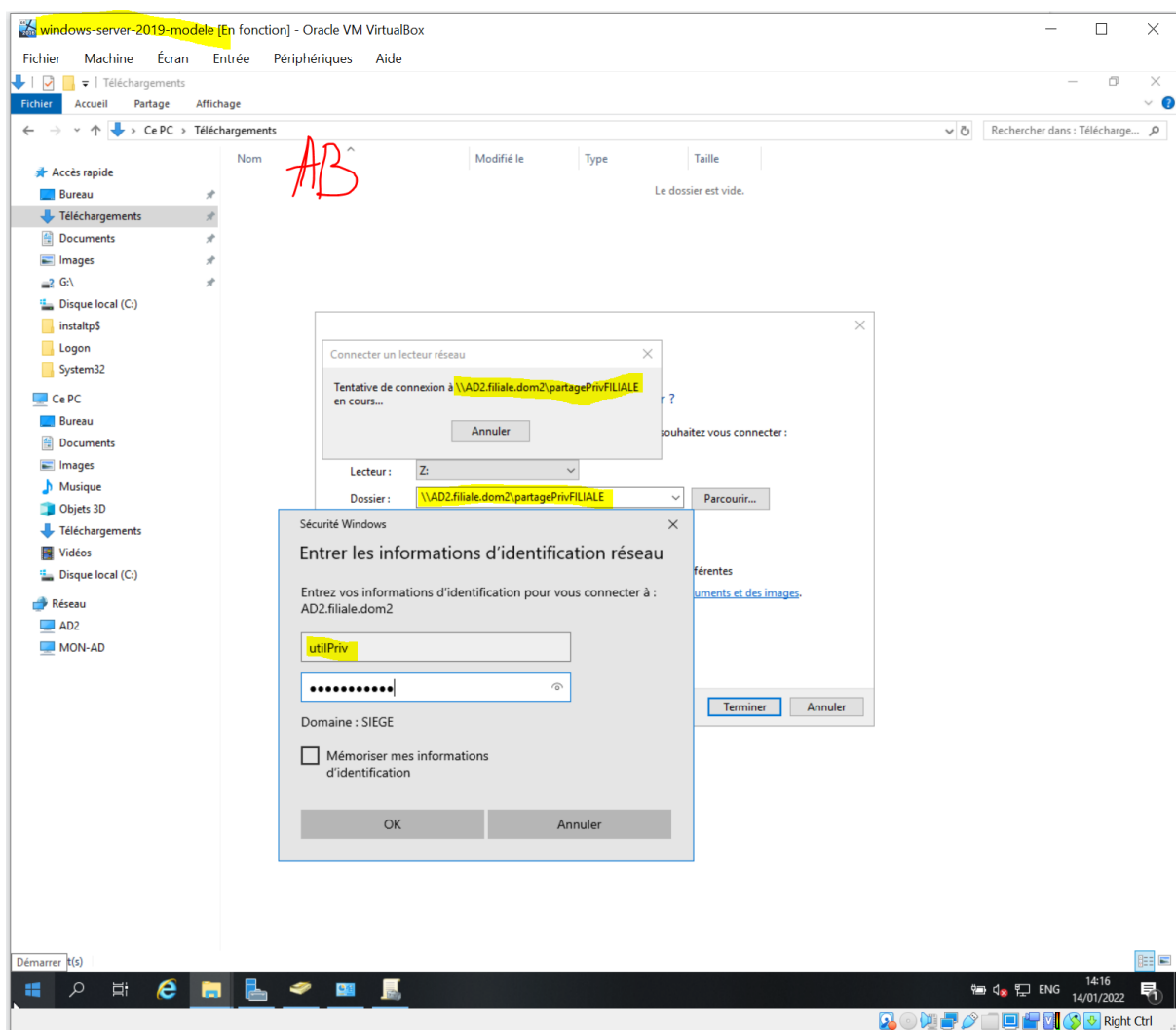
il est impossible de faire le contraire car la délégation de contrôle a été créée seulement sur AD2

Test de la relation d'approbation

Test de l'accès des utilisateurs de SIEGE aux ressources de FILIALE

Nous nous connectons à un nouveau lecteur réseau dans le chemin

"\\AD2.filiale.dom2\partagePrivFILIALE" depuis notre AD avec l'utilisateur utilPriv

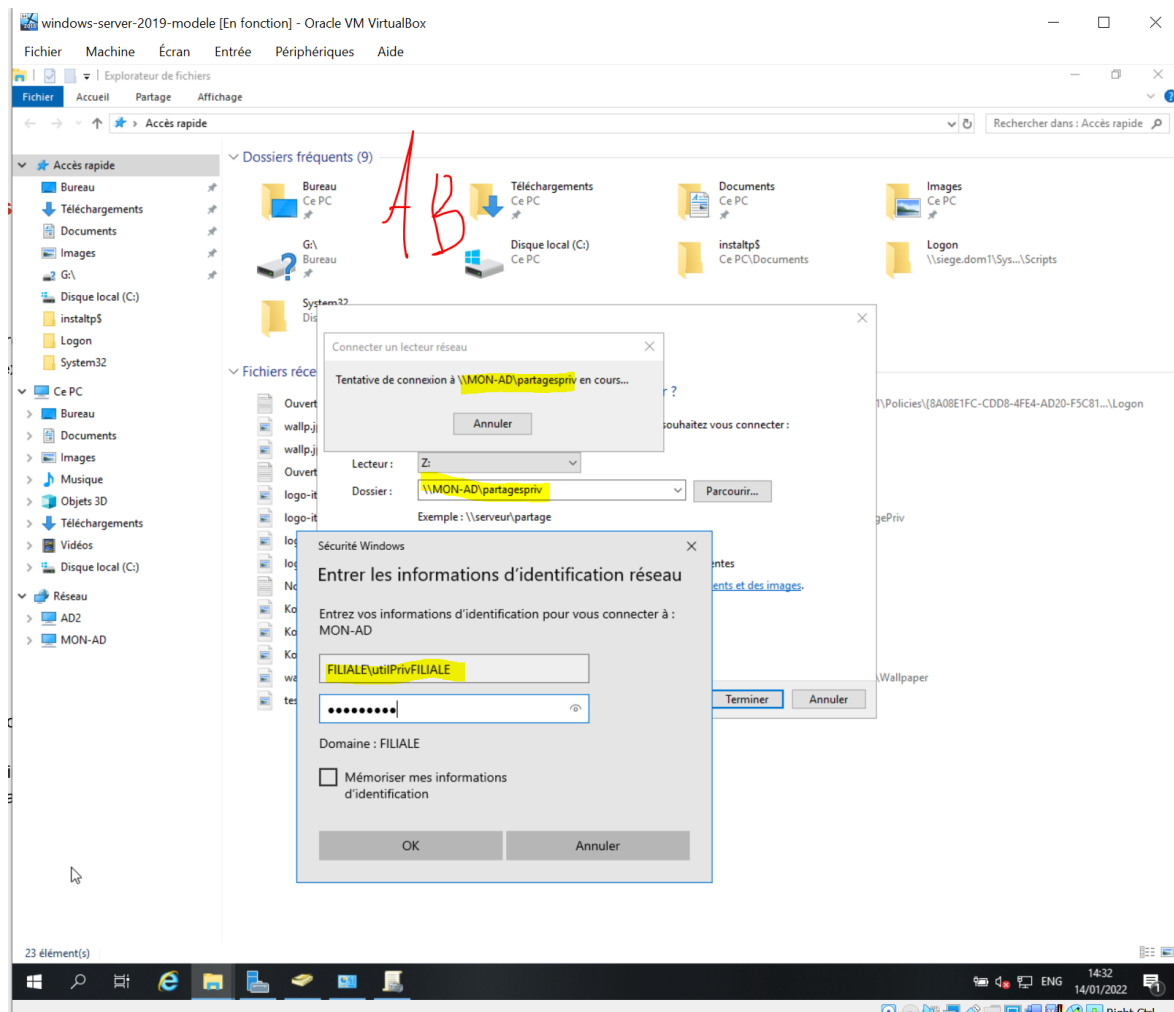


partagePrivFILIALE (\\AD2.filiale.c

Quel est le résultat observé ? oui

Est-ce le résultat attendu et pourquoi ? Cela correspond au paramètre qu'on a mis en place

Test de l'accès des utilisateurs de FILIALE aux ressources de SIEGE



Quel est le résultat observé ? Avec l'utilisateur utilPrivFILIALE la conection au lecteur mpartagePriv ne se fait pas

Est-ce le résultat attendu et pourquoi ? Cela correspond au paramètre qu'on a mis en place