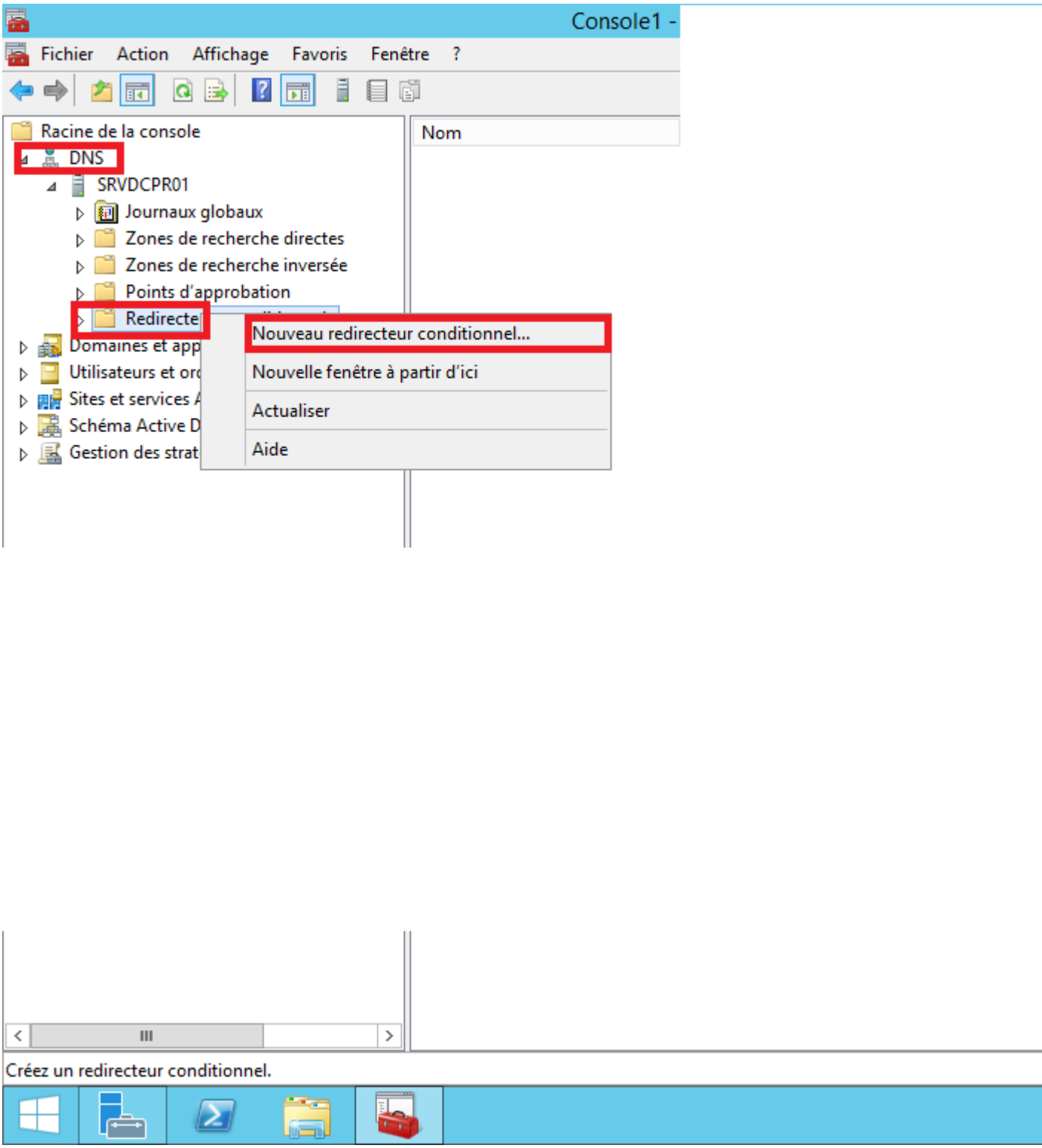
Créer une relation d'approbation entre deux forets différentes.

Cette opération a pour but de pouvoir authentifier des utilisateurs issues d'un domaine appartenant à une foret extérieur a l'entreprise pour qu'ils accèdent aux ressources de votre domaine.

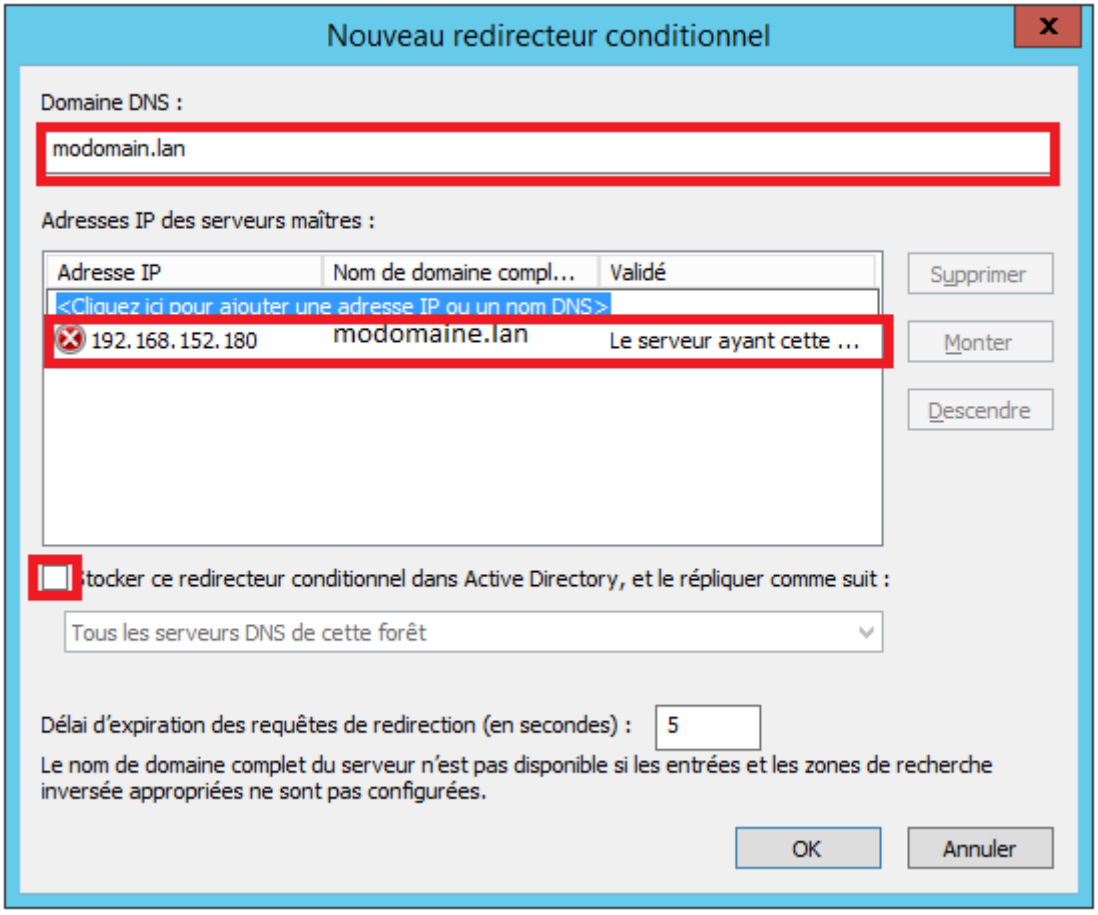
La configuration n'est pas compliquée, mais il est dans un premier temps nécessaire de s'assurer que deux prérequis soit respectés :
-Le premier concerne le niveau fonctionnel, ce dernier doit égal à Windows server 2003.
-Le deuxième point concerne la mise en place de redirecteur au niveau du serveur DNS.
Ces derniers doivent être créés sur les serveurs DNS des deux forêts.

Dans la console du serveur DNS, effectuez un clic droit sur Redirecteur conditionnel puis sélectionnez l'option Nouveau redirecteur conditionnel.



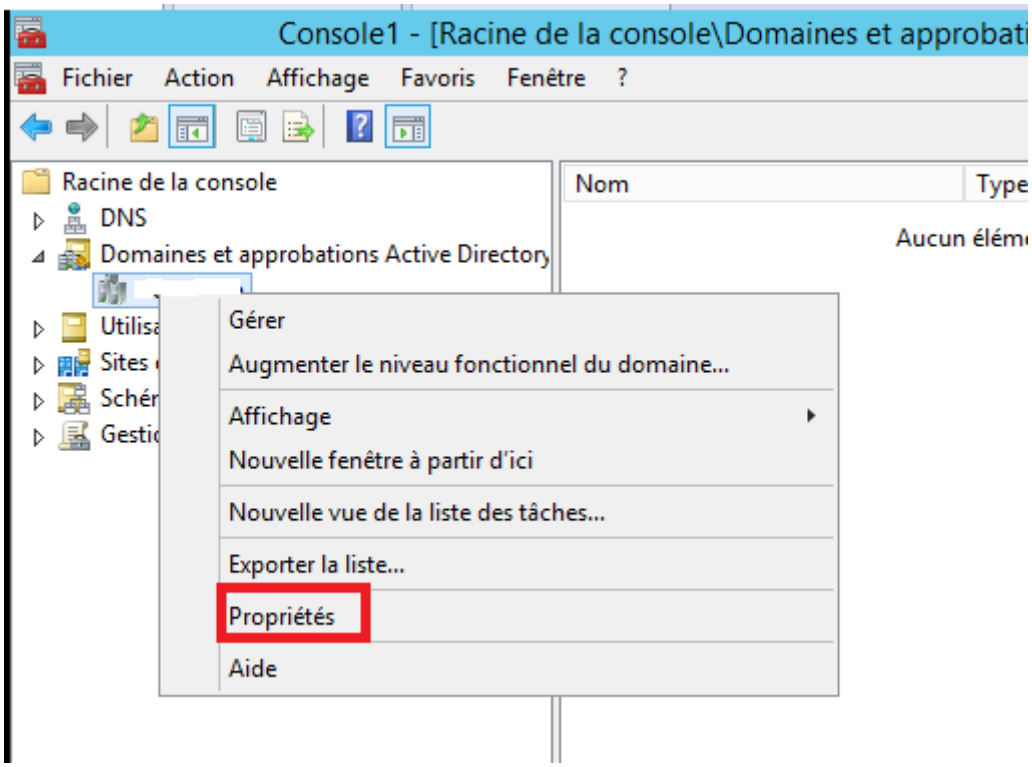
Saisissez le nom de domaine AD de la forêt approuvée ainsi que le nom du serveur DNS.

Enfin cochez la case permettant de stocker le redirecteur dans l'annuaire Active Directory.

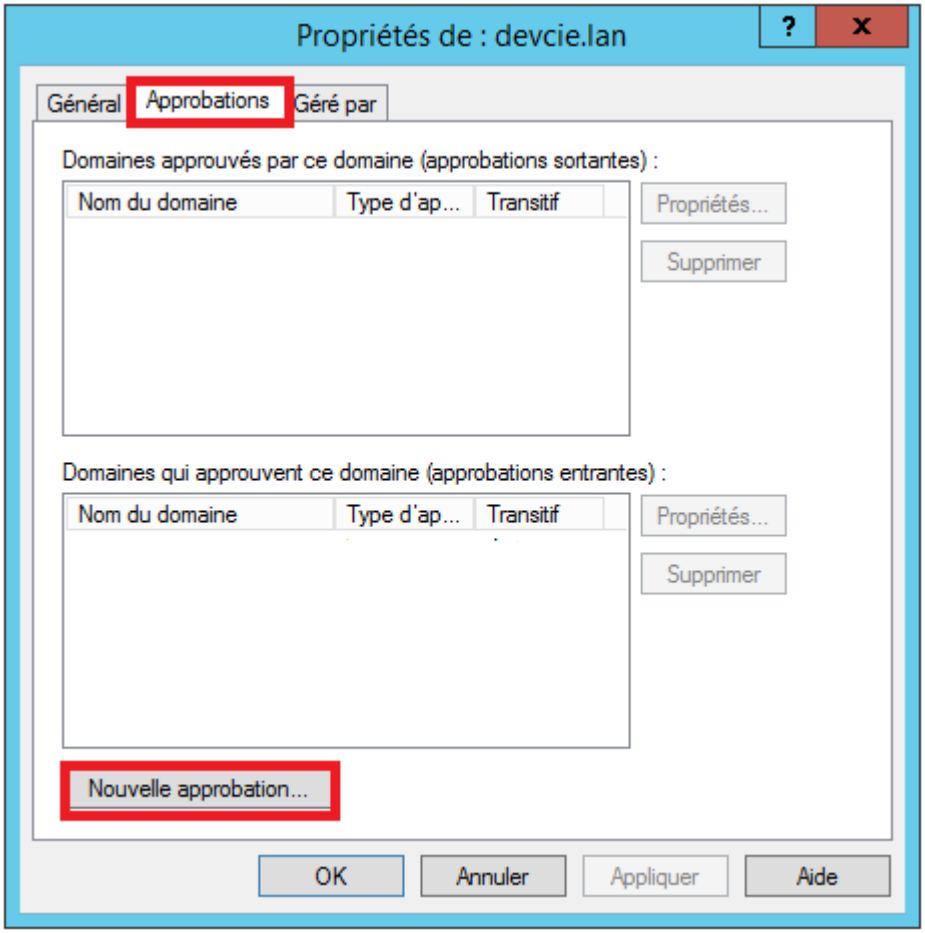


Recommencez la même opération au niveau de la deuxième forêt.

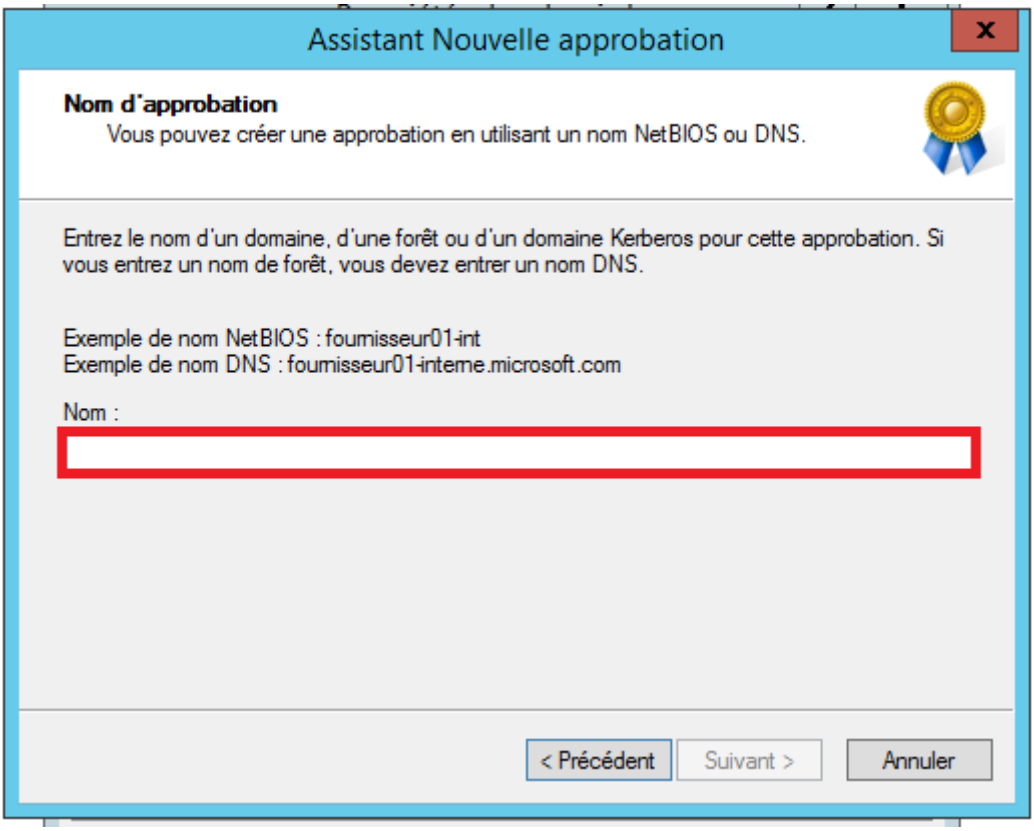
Ouvrez la console Domaine et approbations AD sur une des deux forêts puis effectuez un clic droit au niveau du domaine. Dans le menu contextuel, sélectionnez Propriétés.



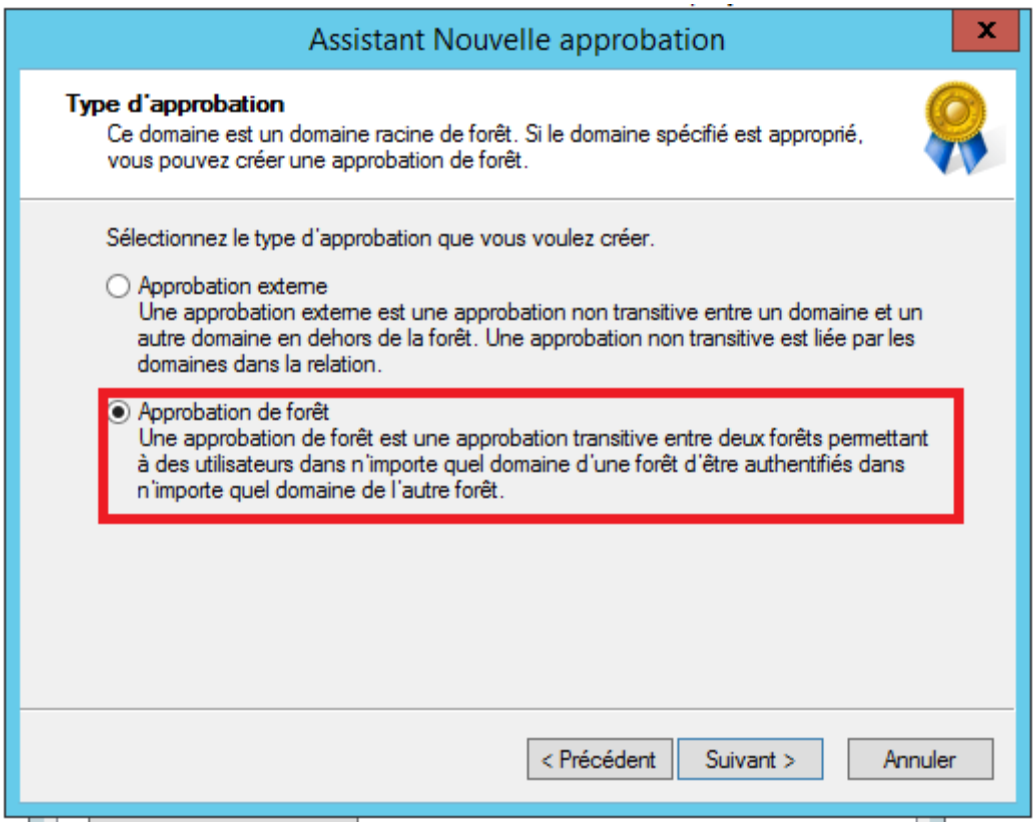
Sélectionnez l'onglet Approbations puis cliquez sur le bouton Nouvelle approbation



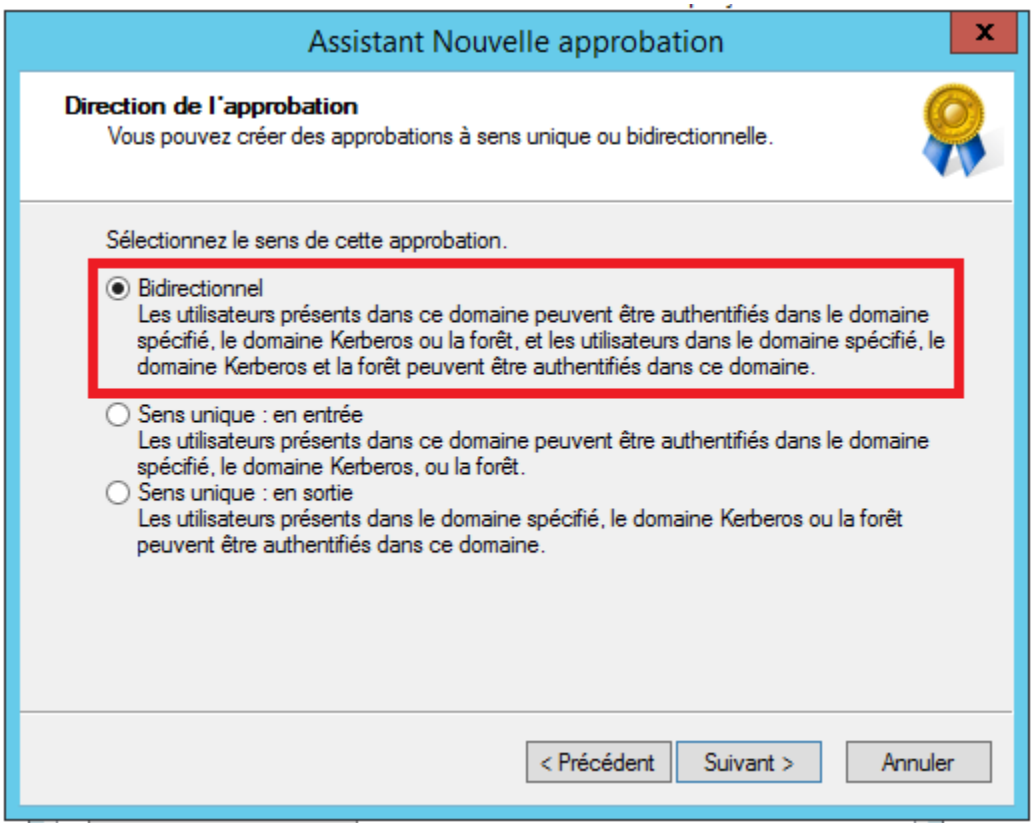
Un assistant se lance, cliquez sur Suivant dans la fenêtre de Bienvenue. Dans la fenêtre Nom d'approbation, saisissez le nom de la forêt qui doit être approuvée.



Dans le choix du type d'approbation, sélectionnez el type qui vous convient pour j'ai choisi approbation de foret puis cliquez sur suivant.



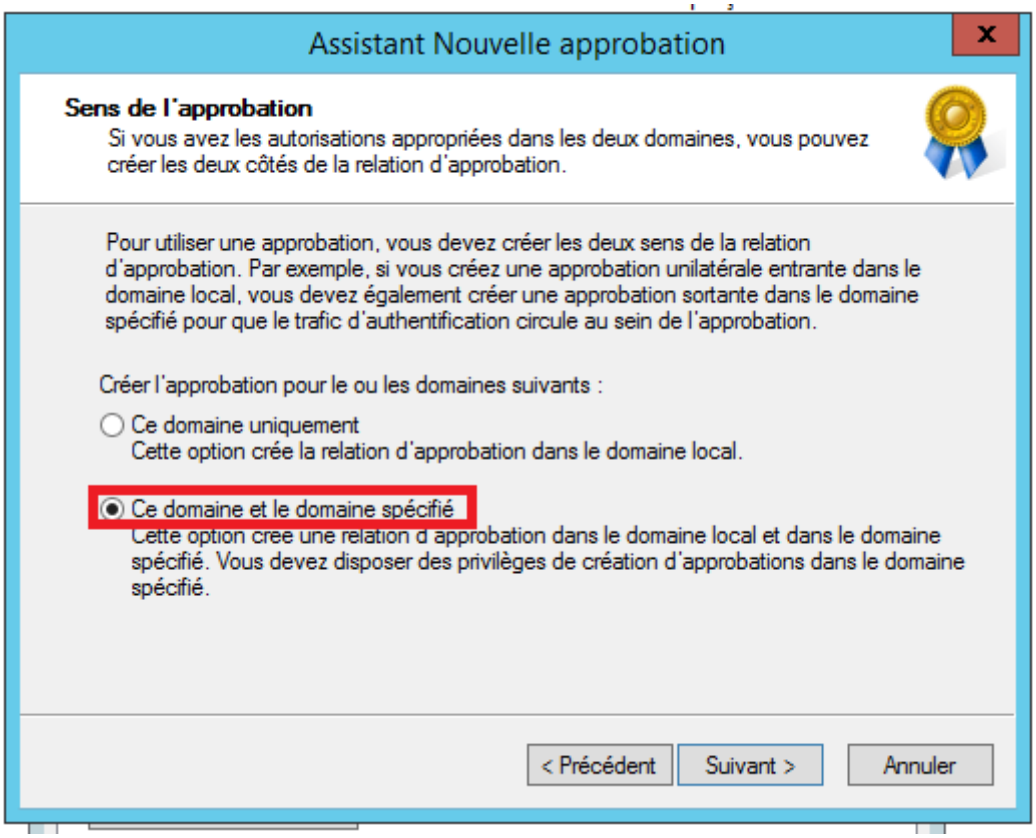
L'approbation pourra être de type bidirectionnel ou d'un seul sens (entrante ou sortante).



La création va être effectuée au niveau des deux forêts.

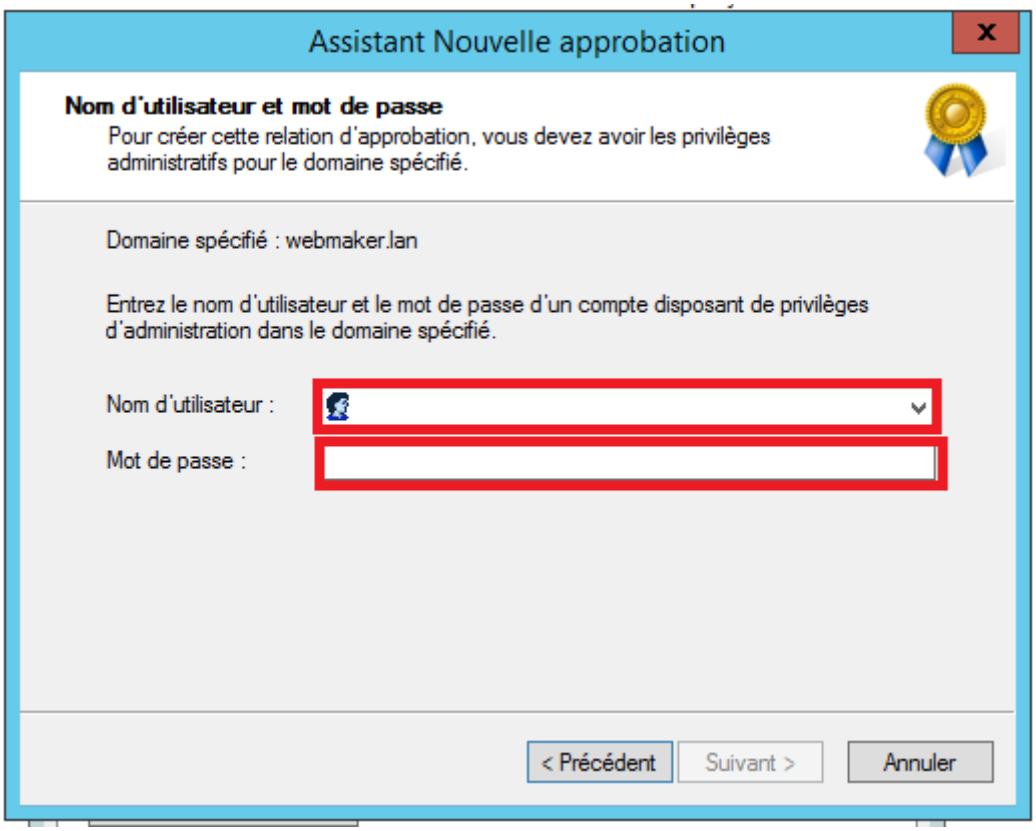
Pour cela, il est nécessaire d'avoir un compte d'administration sur la deuxième forêt.

Dans la fenêtre Sens de l'approbation, sélectionnez l'option Ce domaine et le domaine spécifié puis cliquez sur Suivant.

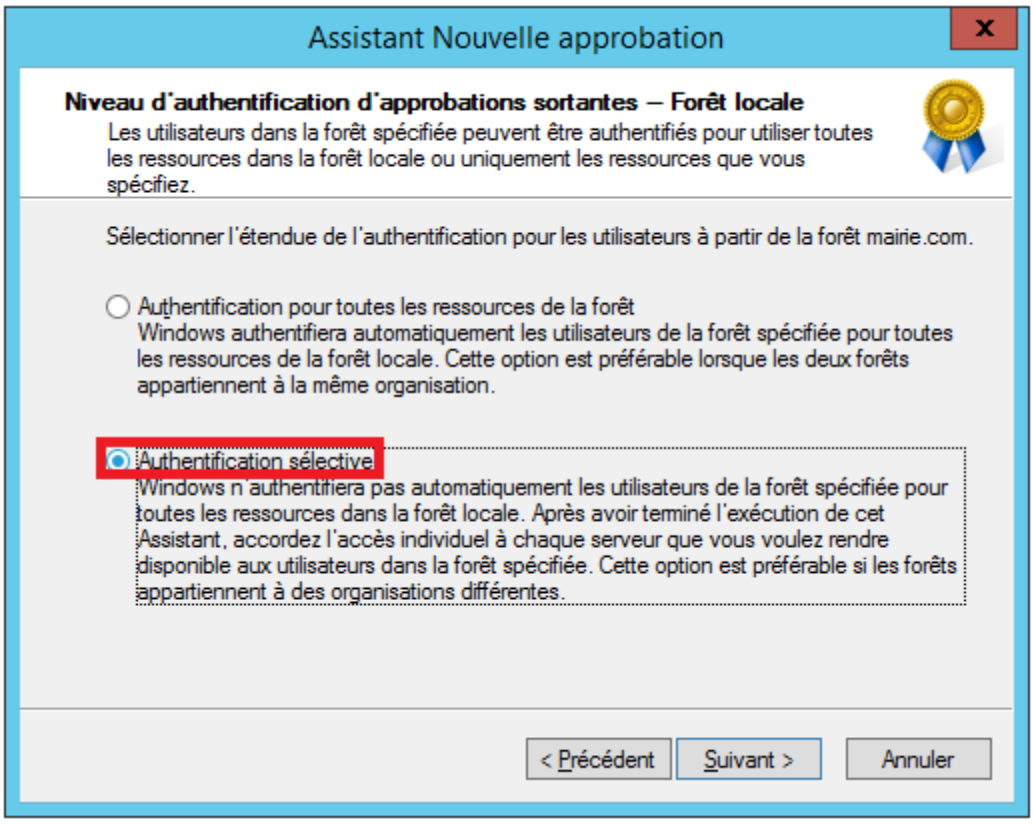


Saisissez l'identifiant et mot de passe d'un compte qui possède des droits d'administrations au niveau de la deuxième forêt.

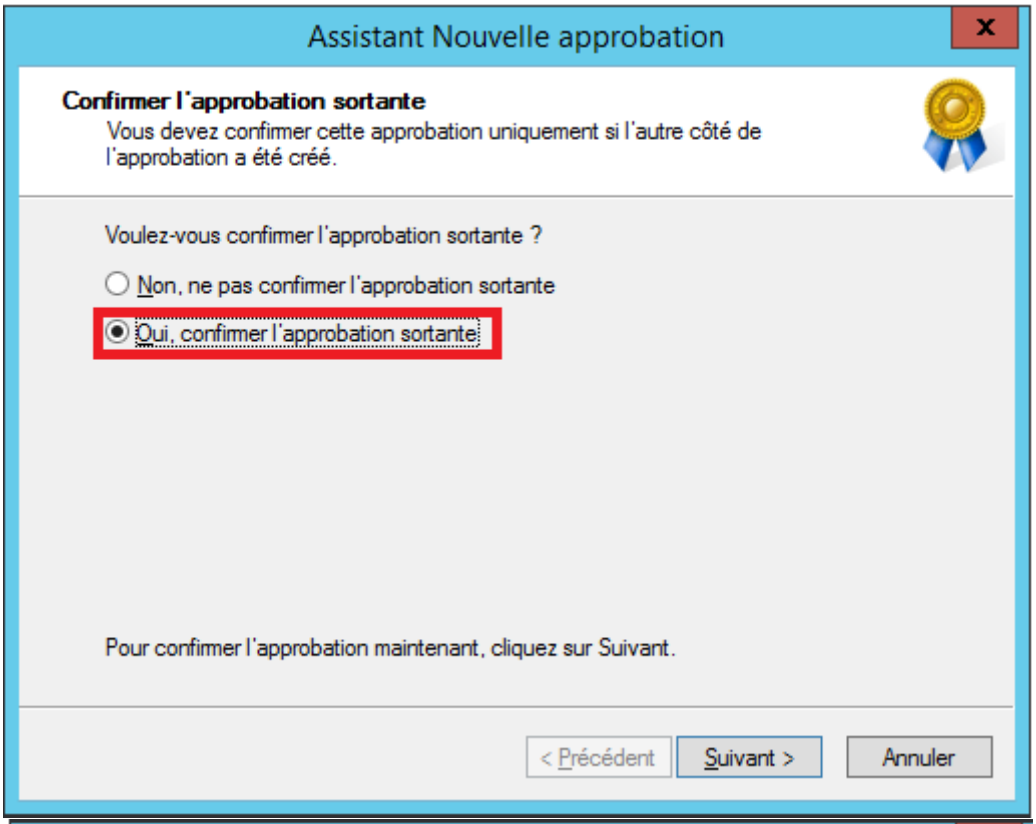
Cela va permettre de procéder à la création de la relation d'approbation.

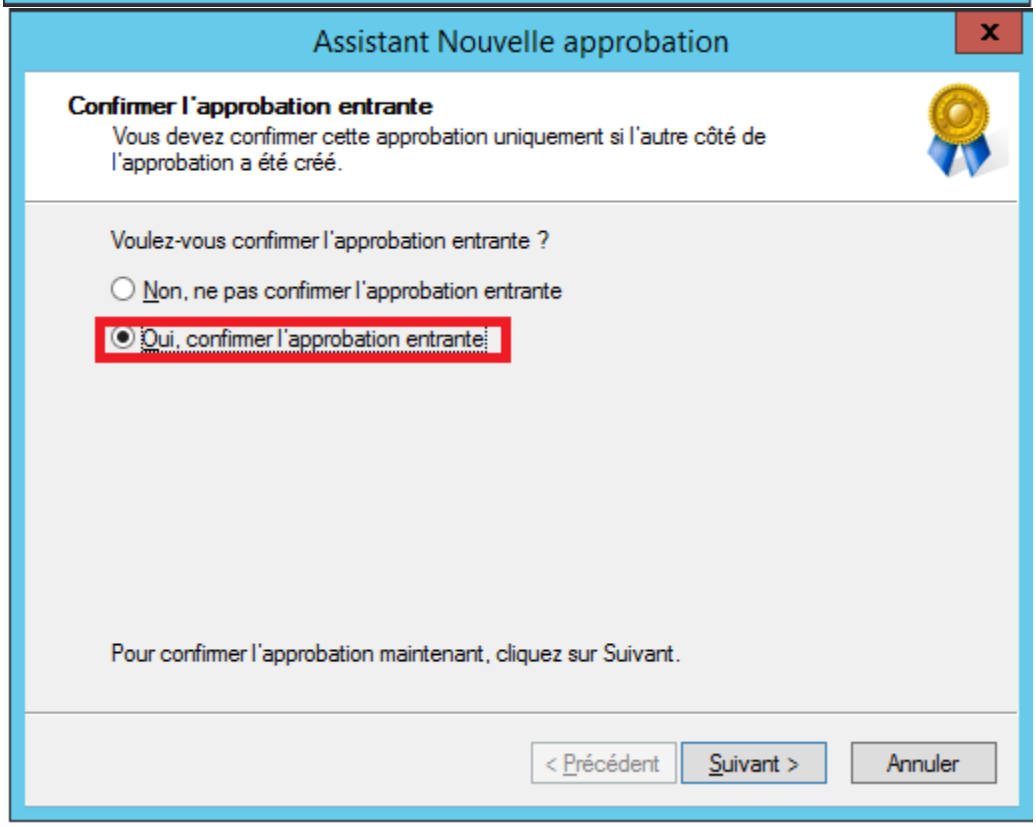


Afin de s'assurer de limiter l'accès aux ressources à quelques utilisateurs de la forêt approuvée, l'authentification sélective doit être sélectionnée.



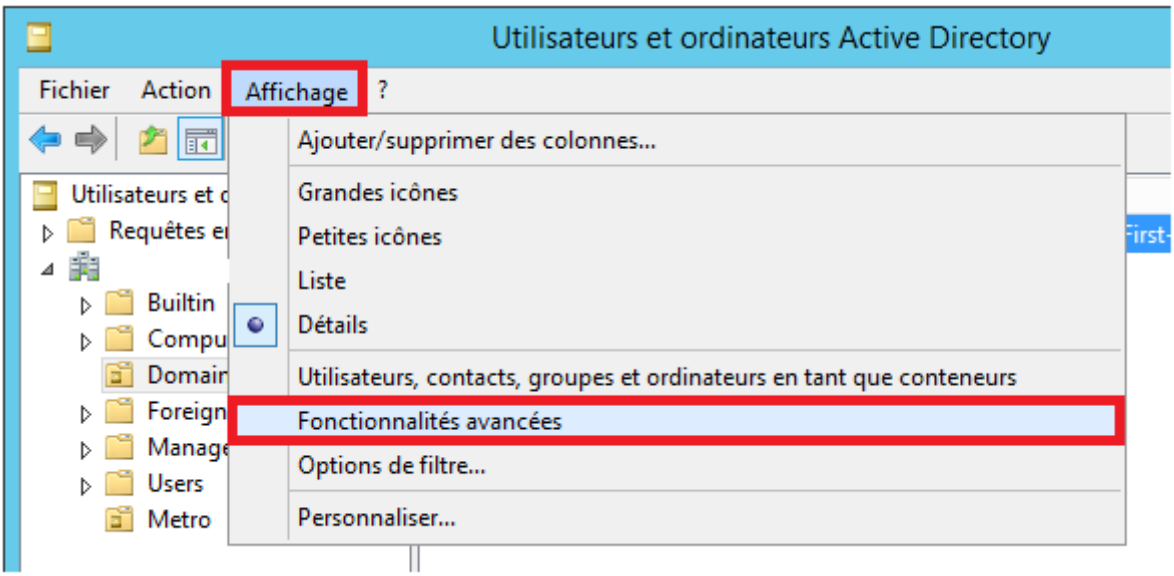
Confirmer l'approbation sortante puis l'approbation entrante.



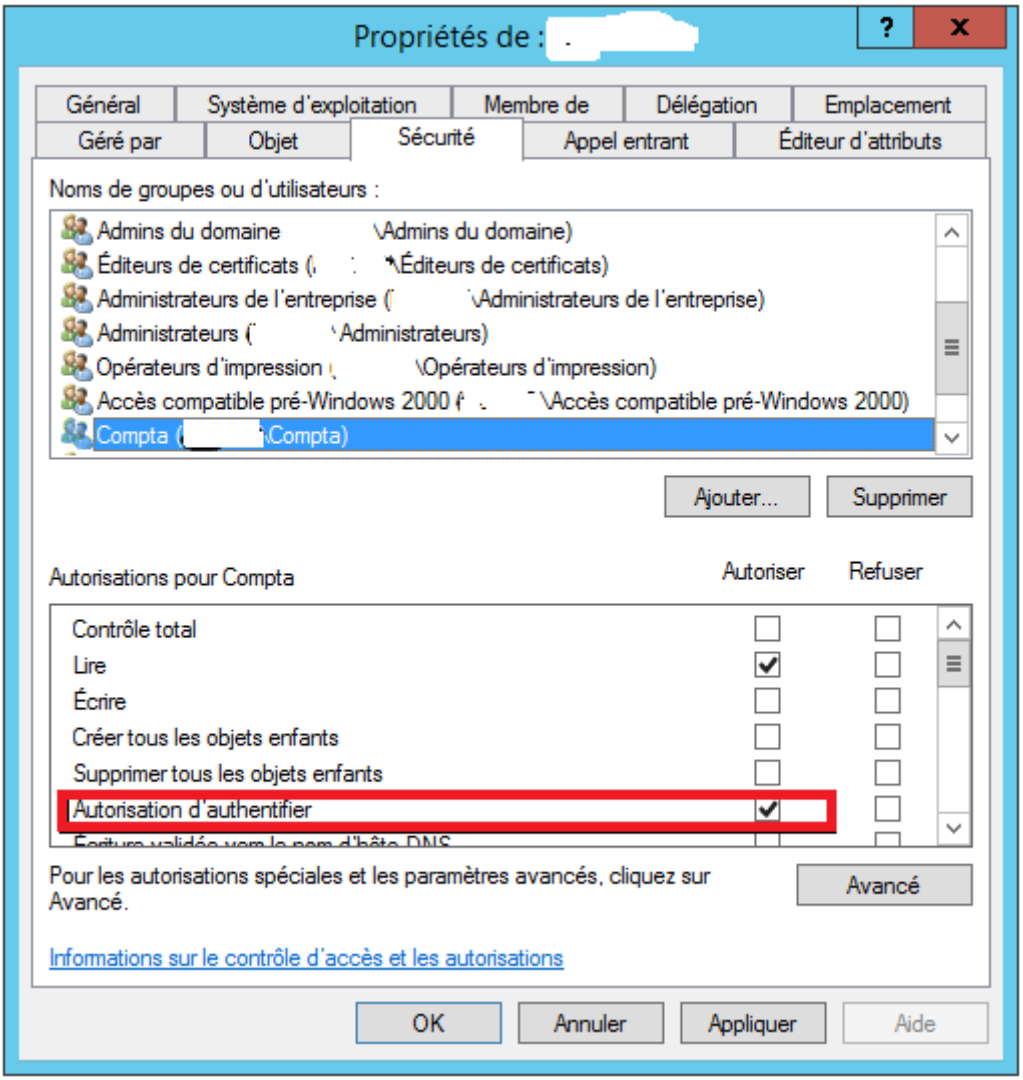


Effectuez par la suite la création de l'approbation.

Afin que les utilisateurs puissent accéder aux ressources, il est nécessaire de modifier l'ACL du compte ordinateur AD du serveur qui contient les ressources.
Afin d'afficher l'onglet Sécurité, il est nécessaire d'afficher les fonctionnalités avancées.

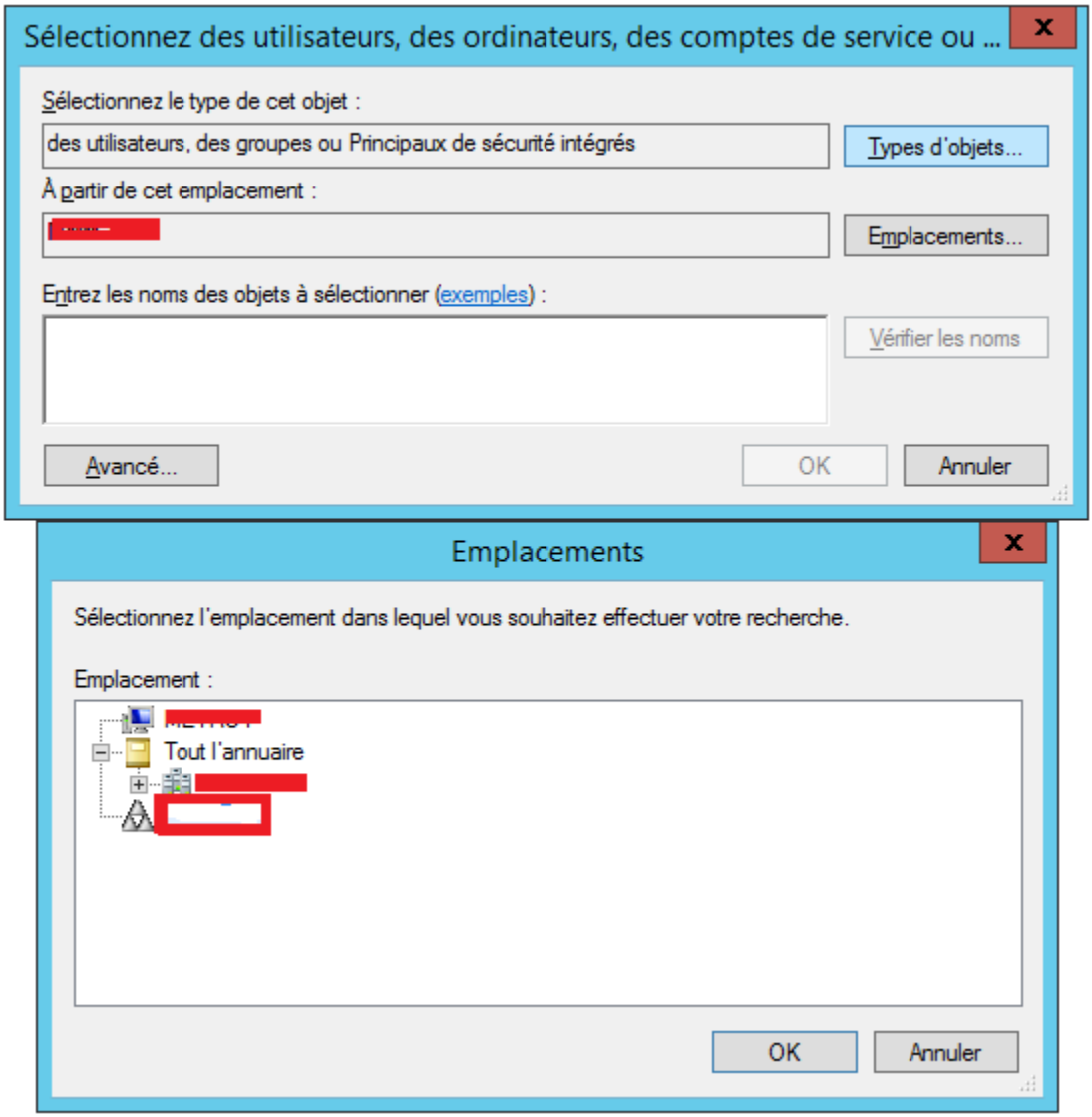


Dans les propriétés du compte ordinateur AD du serveur qui héberge la ressource, accédez à l'onglet sécurité puis ajoutez le compte ou le groupe du domaine distant qui doit accéder à la ressource. Il est nécessaire de lui attribuer le droit d'Autorisation d'authentifier.

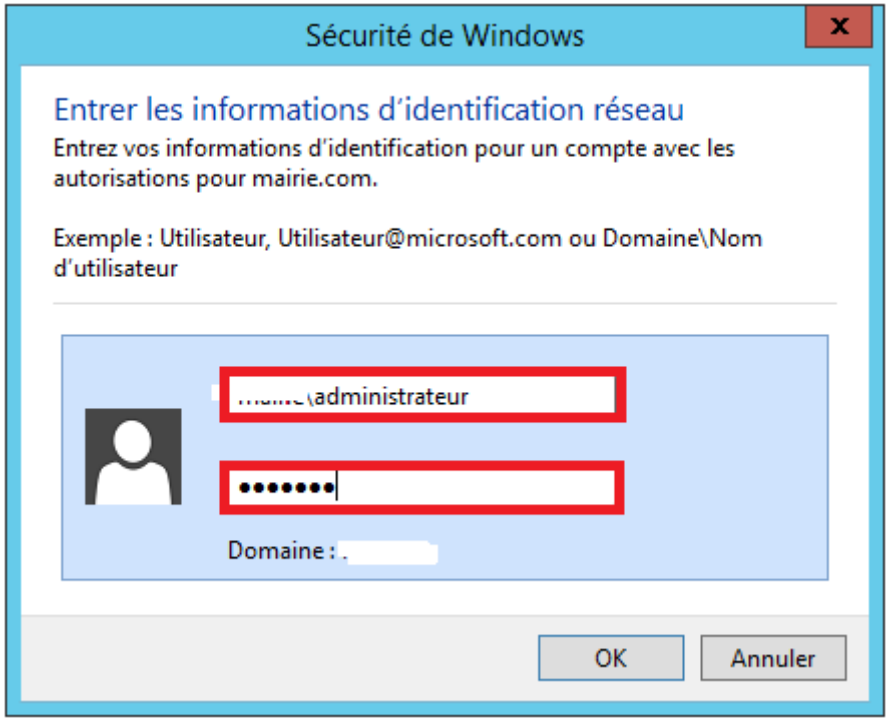


L'autorisation sur la ressource peut maintenant être donnée. Pour cela accéder à l'onglet sécurité du dossier partagé, de l'imprimante, puis cliquez sur Ajouter.

Dans la fenêtre de sélection, cliquez sur Emplacement puis sélectionnez le domaine approuvé.



Une authentification est nécessaire, saisissez les identifiants d'un compte ad du domaine approuvé.



Saisissez le nom du compte ou groupe souhaité puis cliquez sur Vérifier Maintenant puis donner les autorisations nécessaires. L'utilisateur peut maintenant accéder à la ressource.

Votre relation d'approbation est mise en place.