

Créer une relation d'approbation entre deux forêts différentes.

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

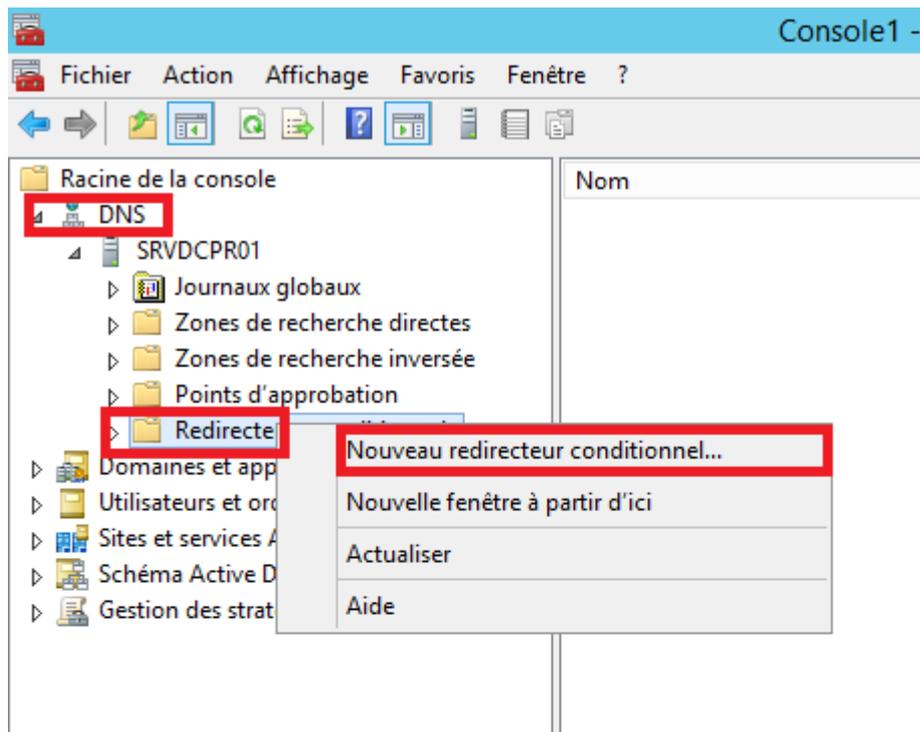
La configuration n'est pas compliquée, mais il est dans un premier temps nécessaire de s'assurer que deux prérequis soit respectés :

-Le premier concerne le niveau fonctionnel, ce dernier doit être 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.

Nouveau redirecteur conditionnel

Domaine DNS :
modomain.lan

Adresses IP des serveurs maîtres :

Adresse IP	Nom de domaine compl...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
192.168.152.180	modomain.lan	Le serveur ayant cette ...

Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit :

Tous les serveurs DNS de cette forêt

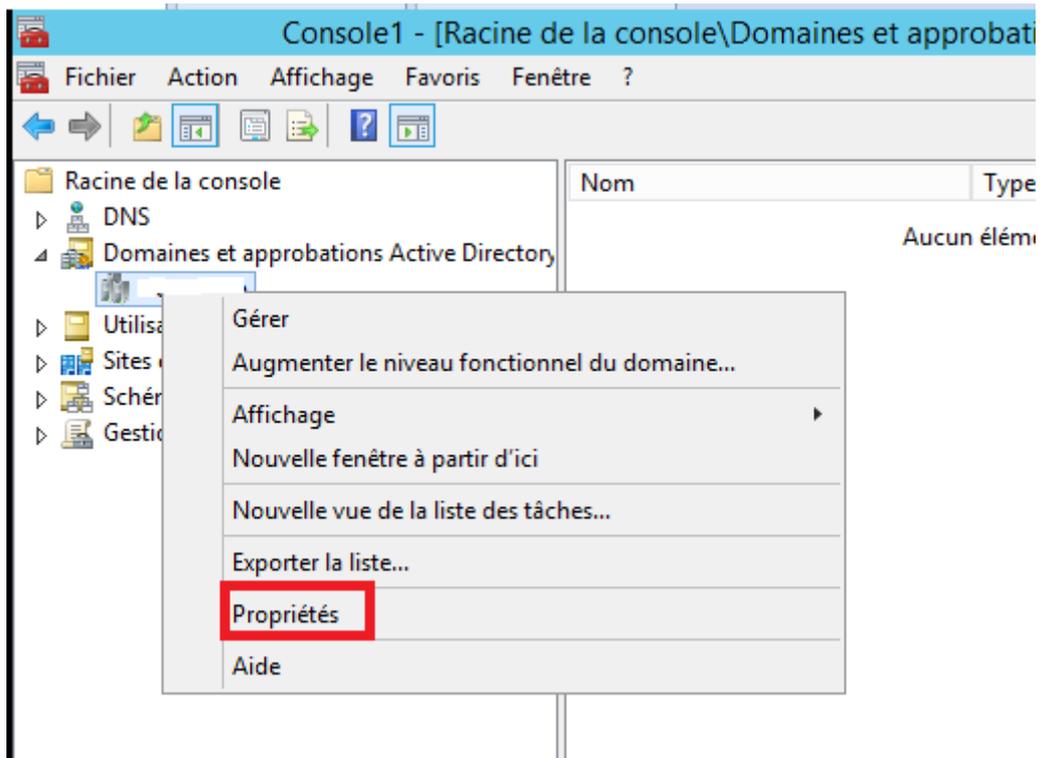
Délai d'expiration des requêtes de redirection (en secondes) : 5

Le nom de domaine complet du serveur n'est pas disponible si les entrées et les zones de recherche inversée appropriées ne sont pas configurées.

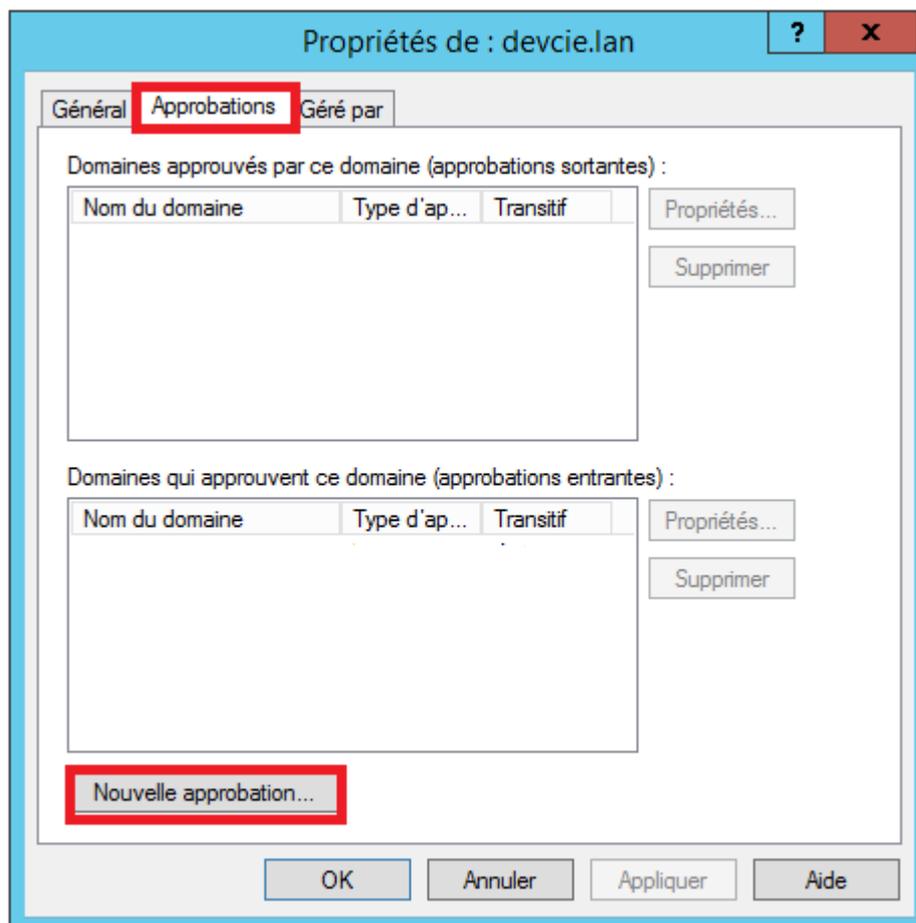
OK Annuler

Recommencez la même opération au niveau de la deuxième forêt.

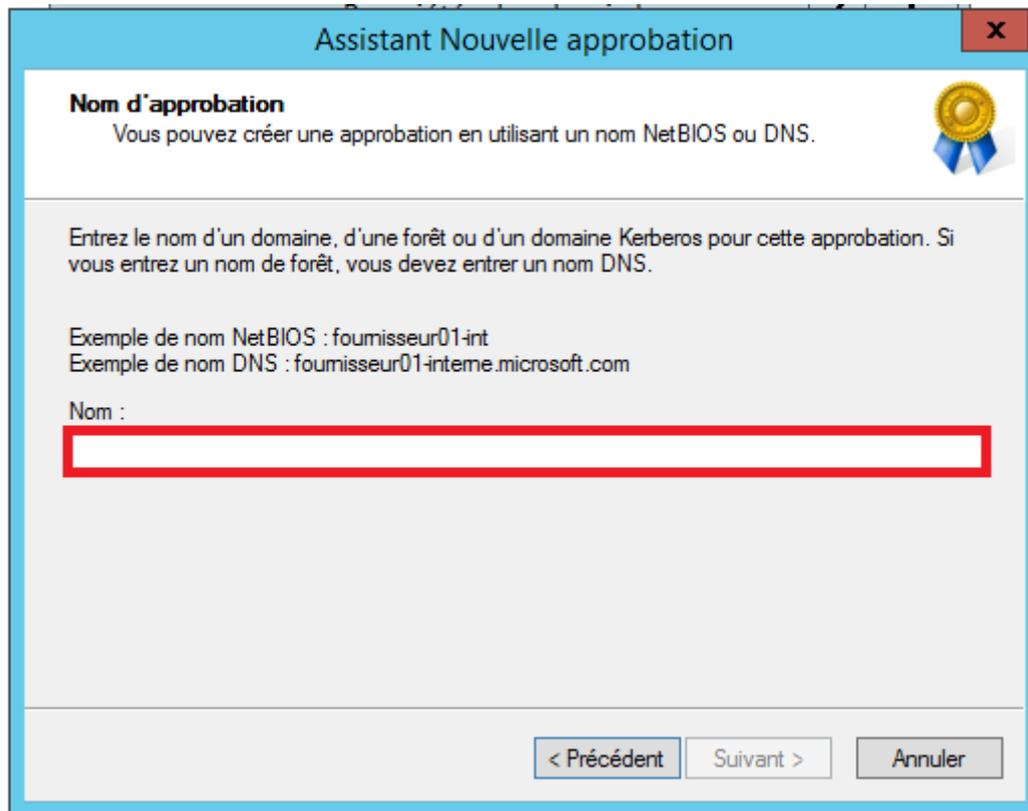
Ouvrez la console Domaine et approbations AD sur une des deux forêts puis effectuez un clic droit au niveau du domaine. Dans le menu contextuel, sélectionnez Propriétés.



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.



Assistant Nouvelle approbation

Nom d'approbation
Vous pouvez créer une approbation en utilisant un nom NetBIOS ou DNS.

Entrez le nom d'un domaine, d'une forêt ou d'un domaine Kerberos pour cette approbation. Si vous entrez un nom de forêt, vous devez entrer un nom DNS.

Exemple de nom NetBIOS : fournisseur01-int
Exemple de nom DNS : fournisseur01-inteme.microsoft.com

Nom :

< Précédent Suivant > Annuler

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

Assistant Nouvelle approbation X

Type d'approbation 

Ce domaine est un domaine racine de forêt. Si le domaine spécifié est approprié, vous pouvez créer une approbation de forêt.

Sélectionnez le type d'approbation que vous voulez créer.

Approbation externe
Une approbation externe est une approbation non transitive entre un domaine et un autre domaine en dehors de la forêt. Une approbation non transitive est liée par les domaines dans la relation.

Approbation de forêt
Une approbation de forêt est une approbation transitive entre deux forêts permettant à des utilisateurs dans n'importe quel domaine d'une forêt d'être authentifiés dans n'importe quel domaine de l'autre forêt.

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

Assistant Nouvelle approbation X

Direction de l'approbation 

Vous pouvez créer des approbations à sens unique ou bidirectionnelle.

Sélectionnez le sens de cette approbation.

Bidirectionnel
Les utilisateurs présents dans ce domaine peuvent être authentifiés dans le domaine spécifié, le domaine Kerberos ou la forêt, et les utilisateurs dans le domaine spécifié, le domaine Kerberos et la forêt peuvent être authentifiés dans ce domaine.

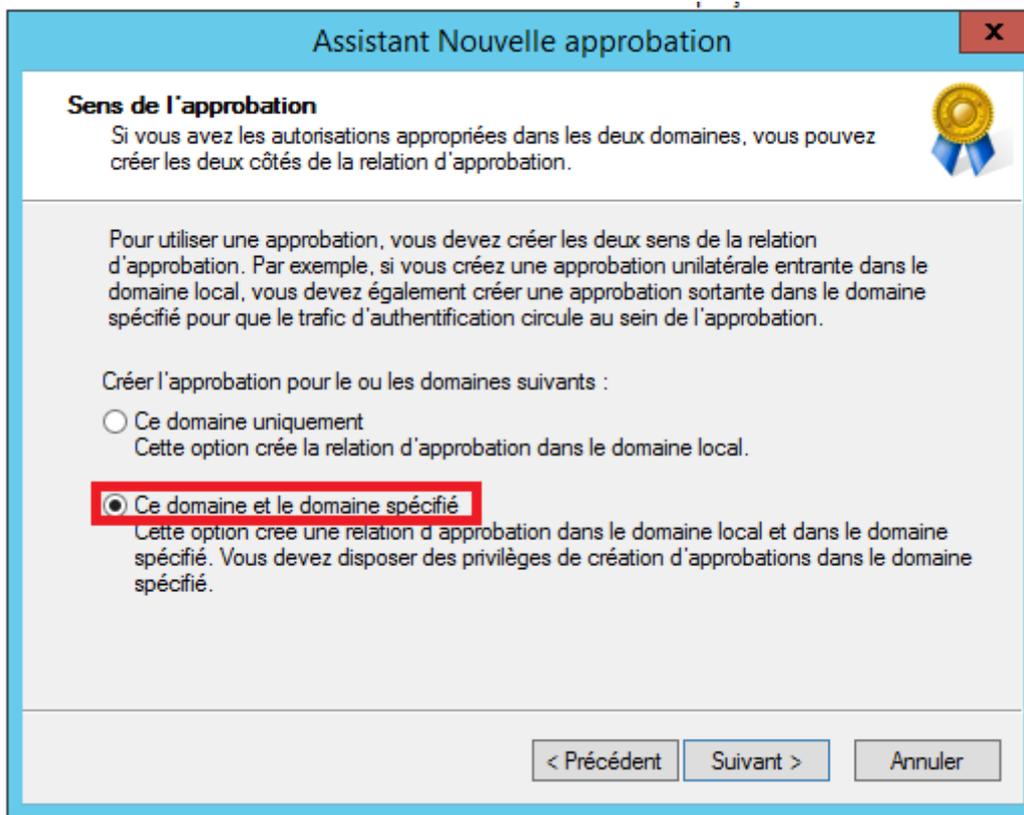
Sens unique : en entrée
Les utilisateurs présents dans ce domaine peuvent être authentifiés dans le domaine spécifié, le domaine Kerberos, ou la forêt.

Sens unique : en sortie
Les utilisateurs présents dans le domaine spécifié, le domaine Kerberos ou la forêt peuvent être authentifiés dans ce domaine.

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.

Assistant Nouvelle approbation X

Nom d'utilisateur et mot de passe 

Pour créer cette relation d'approbation, vous devez avoir les privilèges administratifs pour le domaine spécifié.

Domaine spécifié : webmaker.lan

Entrez le nom d'utilisateur et le mot de passe d'un compte disposant de privilèges d'administration dans le domaine spécifié.

Nom d'utilisateur : 

Mot de passe :

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

Assistant Nouvelle approbation X

Niveau d'authentification d'approbations sortantes – Forêt locale 

Les utilisateurs dans la forêt spécifiée peuvent être authentifiés pour utiliser toutes les ressources dans la forêt locale ou uniquement les ressources que vous spécifiez.

Sélectionner l'étendue de l'authentification pour les utilisateurs à partir de la forêt mairie.com.

Authentification pour toutes les ressources de la forêt
Windows authentifiera automatiquement les utilisateurs de la forêt spécifiée pour toutes les ressources de la forêt locale. Cette option est préférable lorsque les deux forêts appartiennent à la même organisation.

Authentification sélective
Windows n'authentifiera pas automatiquement les utilisateurs de la forêt spécifiée pour toutes les ressources dans la forêt locale. Après avoir terminé l'exécution de cet Assistant, accordez l'accès individuel à chaque serveur que vous voulez rendre disponible aux utilisateurs dans la forêt spécifiée. Cette option est préférable si les forêts appartiennent à des organisations différentes.

Confirmer l'approbation sortante puis l'approbation entrante.

Assistant Nouvelle approbation [X]

Confirmer l'approbation sortante 

Vous devez confirmer cette approbation uniquement si l'autre côté de l'approbation a été créé.

Voulez-vous confirmer l'approbation sortante ?

Non, ne pas confirmer l'approbation sortante

Oui, confirmer l'approbation sortante

Pour confirmer l'approbation maintenant, cliquez sur Suivant.

< Précédent Suivant > Annuler

Assistant Nouvelle approbation [X]

Confirmer l'approbation entrante 

Vous devez confirmer cette approbation uniquement si l'autre côté de l'approbation a été créé.

Voulez-vous confirmer l'approbation entrante ?

Non, ne pas confirmer l'approbation entrante

Oui, confirmer l'approbation entrante

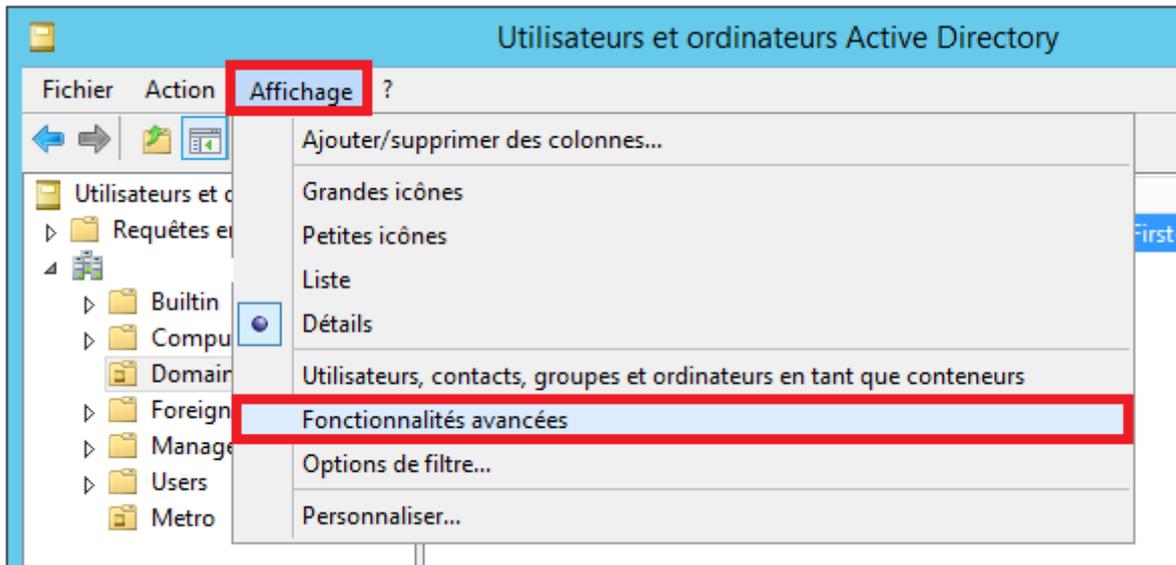
Pour confirmer l'approbation maintenant, cliquez sur Suivant.

< Précédent Suivant > Annuler

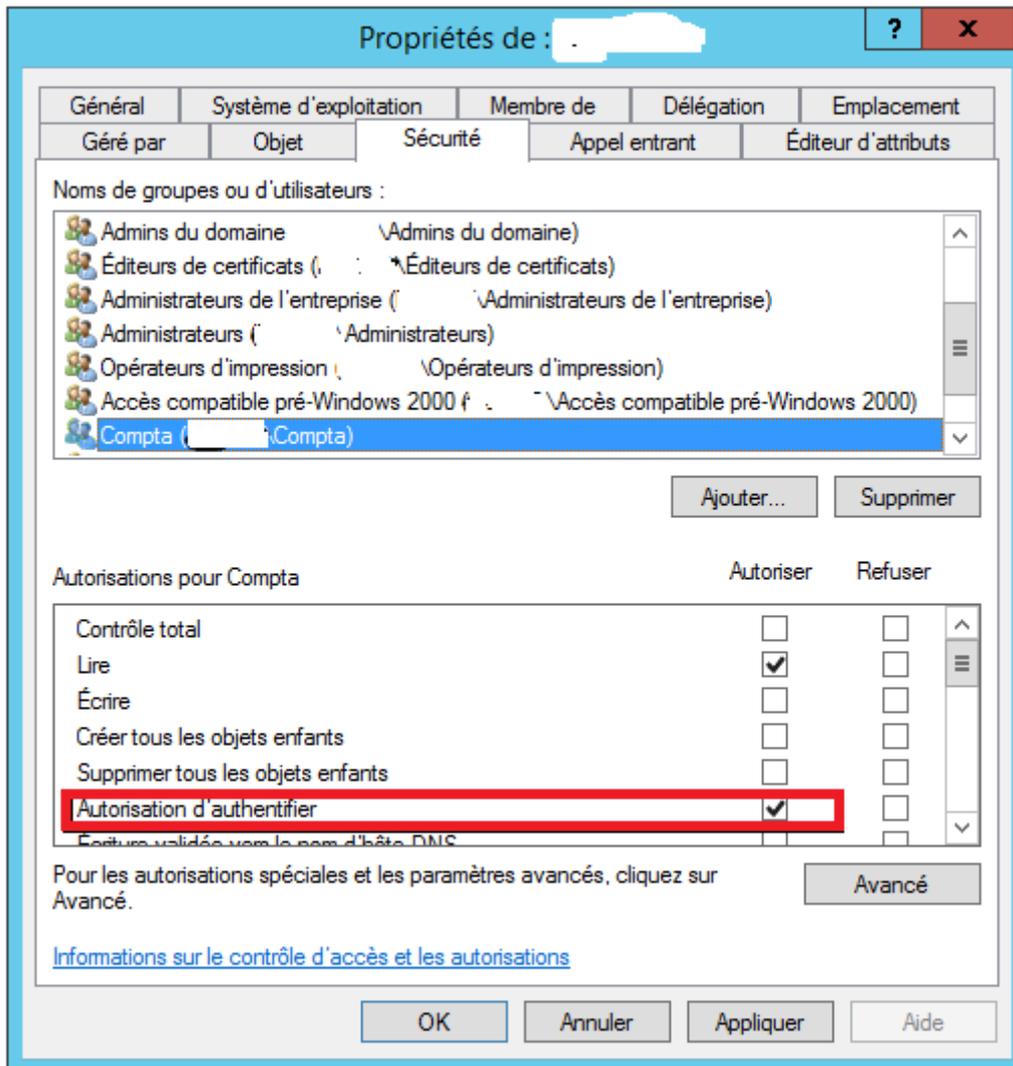
Effectuez par la suite la création de l'approbation.

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.

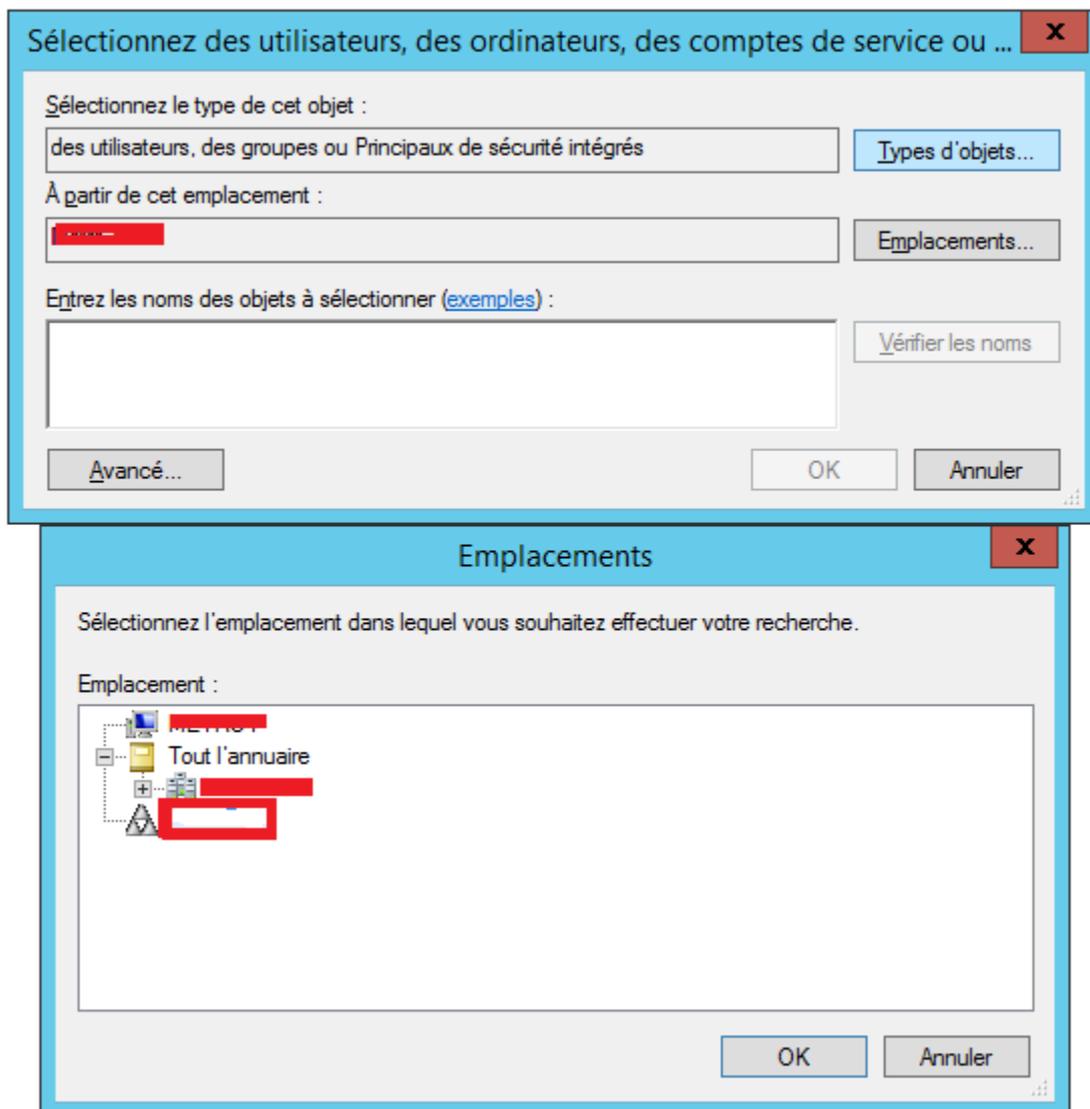


Dans les propriétés du compte ordinateur AD du serveur qui héberge la ressource, accédez à l'onglet sécurité puis ajoutez le compte ou le groupe du domaine distant qui doit accéder à la ressource. Il est nécessaire de lui attribuer le droit d'Autorisation d'authentifier.

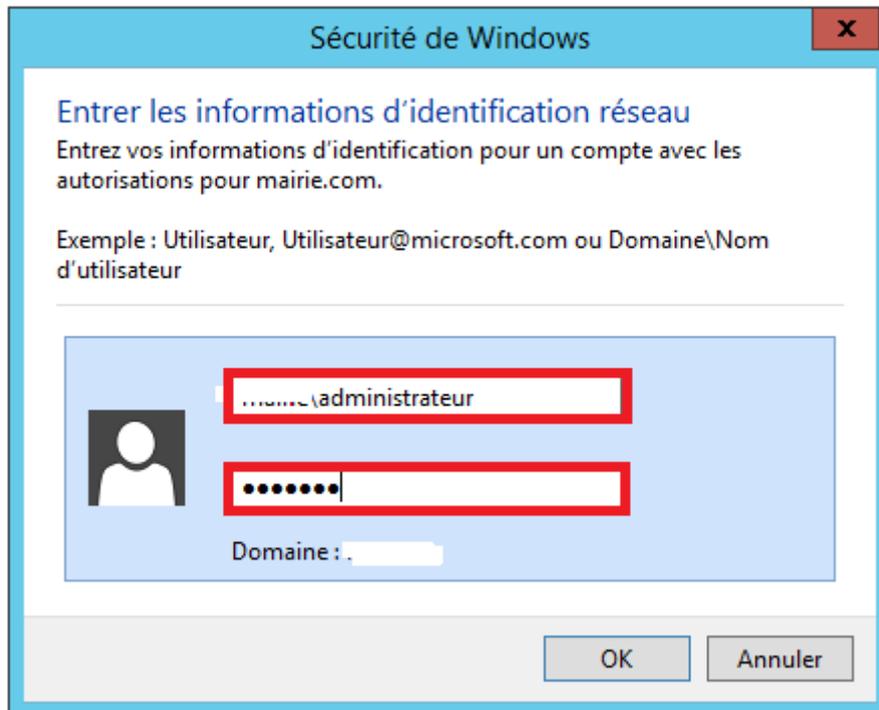


L'autorisation sur la ressource peut maintenant être donnée. Pour cela accéder à l'onglet sécurité du dossier partagé, de l'imprimante, puis cliquez sur Ajouter.

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.