### Création du serveur Windows AD2 qui contient Active Directory

Nous importons la VM "AD2" précédemment telechargée, 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

Paramètres (	de sécurité avancés pour partageP	riv		- 0	2
Nom :	C:\partages\partagePriv	/			
Propriétaire :	Administrateurs (SIEGE)	Administrateurs)	Modifier		
Autorisations	Partage Audit	Accès effectif			
sélectionnez l	'entrée et cliquez sur Modifier (si e	disponible).			
lype	Principal	Acces	Herite de	S'applique a	
Auto	Système	Modification	Aucun	Ce dossier, les sous-dossiers	et
👗 Auto	Administrateur (SIEGE\Admin	Modification	Aucun	Ce dossier, les sous-dossiers	et
🎎 Auto	Administrateurs (SIEGE\Admi	Modification	Aucun	Ce dossier, les sous-dossiers	et
🎎 Auto	G_RessPrivLocal (SIEGE\G_Res	Contrôle total	Aucun	Ce dossier, les sous-dossiers	et
Ajouter	Supprimer Modif	ïer	B		
Activer l'	héritage toutes les entrées d'autorisation c	les objets enfants p	ar des entrées d'autorisatio	n pouvant être héritées de cet objet	
				OK Annuler Appli	auer

### 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.

Entrez vos informations d'identifi MON-AD	cation pour vous cor
utilpriv	
•••••	୕
Domaine : SIEGE	٨
Mémoriser mes informations d'identification	S A
ОК	Annuler

Nous créons ensuite un fichier dans le dossier pour vérifier que "utilPriv" a bien les droits d'écriture.

	Z:)				
← → × ↑ \Xi > This PC > parta	gePriv (\\MON-AD) (Z:)			~ Ō	Search
	Name	Date modified	Туре	Size	
A Quick access	testutilpriv	1/14/2022 11:09 AM	Text Document	0	KB
Desktop					
Downloads 🖉					
Music					
	٨				
<ul> <li>OneDrive</li> </ul>		ħ			
This PC	7	-K			
3D Objects					
E. Desktop					
🖆 Documents					
🕂 Downloads					
👌 Music					
E Pictures					
🗃 Videos					
🏪 Local Disk (C:)					
🛖 partagePriv (\\MON-AD) (Z:)					
Network					
MON-AD					

## 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.

Nom :	C:\parta	ges\partagePri	VFILIALE				
Propriétaire :	Adminis	trateurs (FILIA	E\Administrateurs)	<b>Nodifier</b>			
Autorisations	Partage	Audit	Accès effectif		1.7		
Pour obtenir sélectionnez Entrées d'aut	des informations su l'entrée et cliquez s orisations :	upplémentaire ur Modifier (si	s, double-cliquez sur u disponible).	ne entrée	d autorisation. Pour m	odifier une entrée d'auto	risation,
Туре	Principal				Accès	Hérité de	S
Auto	Système				Contrôle total	Aucun	c
Section 14 Auto	Administrateurs (I	FILIALE\Admir	istrateurs)		Contrôle total	Aucun	c
Section 44 March 14 M	CREATEUR PROPE	RIETAIRE			Contrôle total	Aucun	L
State Auto	G_RessPrivLocalFi	LIALE (FILIALE	G_RessPrivLocalFiLIAL	.E)	Contrôle total	Aucun	c

### Création de la relation d'approbation

Nous allons établir une approbation unidirectionnelle entraîne, pour ce faire nous commençons par attribuée á la "monAD" un dns secondaire il s'agit de láddresse ip de "monAD2"

Général	amètres IP peuve	ont être déter	minés autor	matiqueme	ant civ	otre
réseau approp	le permet. Sinon, riés à votre admir	vous devez o histrateur rése	lemander le au.		res IP	UUC
$\bigcirc 0$	btenir une adress	e IP automati	quement	1		
OU	tiliser l'adresse IP	suivante :				
Adre	esse IP :		192 . 16	8.100.	10	
Mas	que de sous-résea	au:	255.25	5.255.	0	
Pass	erelle par défaut	:	192 . 16	8.100.	1	
0	btenir les adresse	s des serveur	s DNS auto	matiqueme	ent	
OU	tiliser l'adresse de	serveur DNS	suivante :			
Serv	eur DNS préféré :	:	127.0	. 0 .	1	
Serv	eur DNS auxiliaire	::	192 . 16	8.100.	20	
	'alider les paramèt	tres en quitta	nt		Avan	cé

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

Propriétés de : Protocole Internet vers	ion 4 (TCP/IPv4) X
Général	
Les paramètres IP peuvent être détern réseau le permet. Sinon, vous devez d appropriés à votre administrateur rése O Obtenir une adresse IP automatic	minés automatiquement si votre lemander les paramètres IP vau. quement 472
• Utiliser l'adresse IP suivante :	
Adresse IP :	192 . 168 . 100 . 20
Masque de sous-réseau :	255.255.255.0
Passerelle par défaut :	192 . 168 . 100 . 1
Obtenir les adresses des serveur	s DNS automatiquement
Serveur DNS préféré :	127.0.0.1
Serveur DNS auxiliaire :	192 . 168 . 100 . 10
Valider les paramètres en quittar	Avancé
	OK Annuler

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		
📥 Gestio	nnaire de serveur						
	Domaines et appro	bations Ac	ctive Director	У			
Fie	🛔 Gestionnaire [	NS					
-	Fichier Action	Affichage	e ?				
<b>II</b> 😹	🔶 🄿 🔁 📰	Q 📑	?				
>	🚊 DNS		Nor	m		Туре	
-	V MON-AD			iliale.dom2		Redirecteur c	
	> 📄 Zones o	le recherch	e direc				
	> Zones o	le recherch	e invei	1 1	~		
11	> Points (	approbati	itionne	$\mathbf{A}$	ノ		
0		ceurs condi	itionine .				

Nous créons un redirecteur conditionnel depuis monAD2 vers le contrôleur monAD

🕌 windo	ows-server-2	019- <mark>AD2</mark>	[En fonctio	n] - O	racle VM Vir	tua
Fichier	Machine	Écran	Entrée	Péri	iphériques	А
🎄 Gestionn	aire DNS					
Fichier Act	tion Affichage	?				
🗢 🔿 🖄	🔲 🗟 🖬	2 🖬 🗎 🕯	đ			
<ul> <li>B DNS</li> <li>✓ <ul> <li>✓ <ul> <li>✓ AD2</li> <li>&gt; <ul> <li>✓ Za</li> <li>✓ <ul> <li>✓ Za</li> <li>✓ <ul> <li>✓ <ul> <li>✓ Re</li> </ul> </li> </ul> </li> </ul></li></ul></li></ul></li></ul></li></ul>	ones de recherche d ones de recherche in oints d'approbation directeurs conditio	nne Nom	.dom1		Type Redirecteur c	

Nous créons la relations d'aprobation

ropriétés de : siege.d	om1			?
Général Approbations	Géré par			
Domaines approuvés	par ce domaine (appro	bations sort	antes) :	
Nom du domaine	Type d'ap	Transitif	Propriét	és
			Suppri	mer
Domaines qui approuv	vent ce domaine (annr	obations ent	trantes) :	
Domaines qui approuv	vent ce domaine (appro Type d'ap	obations ent Transitif	trantes) : Propriét	és
Domaines qui approuv Nom du domaine filiale.dom2	vent ce domaine (appro Type d'ap Forêt	obations ent Transitif <mark>Oui</mark>	trantes) : Propriét	és
Domaines qui approuv Nom du domaine filiale.dom2	rent ce domaine (appr Type d'ap Forêt	obations ent Transitif <mark>Oui</mark>	trantes) : Propriét Suppri	és
Domaines qui approun Nom du domaine filiale.dom2	vent ce domaine (appr Type d'ap Forèt	obations ent Transitif <mark>Oui</mark>	trantes) : Propriét Suppri	és mer
Domaines qui approuv Nom du domaine filiale.dom2	rent ce domaine (appr Type d'ap Forêt	obations ent Transitif <mark>Oui</mark>	rrantes) : Propriét Suppri	és mer
Domaines qui approuv Nom du domaine filiale.dom2	rent ce domaine (appr Type d'ap Forêt	obations en Transitif Oui	rrantes) : Propriét Suppri	és mer

# 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



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

Assistant Délégation de contrôle X	Assistant Délégation de contrôle X
Utilisateurs ou groupes           Sélectionnez un ou plusieurs groupes ou utilisateurs auxquels vous voulez déléguer le contrôle.	Tâches à déléguer           Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.
Utilisateurs et groupes sélectionnés : Administrateur (SIEGEVAdministrateur) Additional de la construction	Déléguer les tâches courantes suivantes :
< Précédent Suivant > Annuler Aide	< 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

énéral	Membres	Membre de	Géré par	Objet	Sécurité	Éditeur d'attributs	
Membre	es :						
Nom		D	ossier Serv	rices de c	domaine Ac	tive Directory	
8 G_	UtilPriv	si	iege.dom1/	Users			
₿ <mark>G</mark>	_UtilPrivLoc	alFiLIALE fil	liale.dom2/	Users			
			Λ				
			<b>A</b> 1	0			
			$\sum$				
		/-	+1	$\square$	•		
		-	71		-		
		-	71		-		
		/-	于 l				
		/-	<del>}</del>		•		
<		/-	于				>
< Aiou	ter	Supprimer	}		-		>
< Ajou	ter	Supprimer	子 I		-		>
< Ajou	ter	Supprimer	}				>

Que constatez vous ? Comment l'expliquer ?

il est impossible de faire le contraire car la délégation de contrôle a été créé 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



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