Mr ROTH



Compte rendu TP4

Active Directory - Serveur de fichier -Droits NTFS - GPO

TEWES Arnaud BTS SIO SISR 1ÈRE ANNÉE

1. Introduction

Dans ce TP, j'ai procédé à la mise en place d'un domaine Active Directory avec création d'unités d'organisation, d'utilisateurs, de groupes et j'ai mis en place un serveur de fichier avec droits NTFS sur mes groupes d'utilisateurs. J'ai ensuite établi une stratégie de groupe pour que mes utilisateurs puissent avoir accès à mon partage de fichier en passant par un lecteur réseau sans avoir à taper le chemin UNC.

Dans un premier temps, j'ai installé les rôles Active Directory (AD DS) et DNS sur mon serveur, et je l'ai ensuite promu en contrôleur de domaine. J'ai ensuite pu spécifier un nom à mon domaine (étant donné que j'ai créé un tout nouveau domaine dans une toute nouvelle forêt). J'ai ensuite configuré DNS pour qu'il fasse la résolution entre mon nom de domaine et l'adresse IP de mon contrôleur de domaine et inversement. En créant dans un premier temps une zone de recherche inversée, qui elle fera la résolution entre adresse IP et nom de domaine, puis en configurant les propriétés du serveur DNS pour qu'il écoute seulement sur IPv4 (comme je fonctionne en IPv4 dans mon cas).

Dans un second temps, j'ai organisé mes utilisateurs, groupes et ordinateurs dans différentes unités d'organisations que j'ai créées : une principale sur le domaine avec le nom de l'organisation (pour laquelle je travaille virtuellement), et dans celle-ci j'en ai créé trois autres pour les ordinateurs, utilisateurs et groupes. Cela me permet d'avoir une base de travail plus claire pour la création de mes utilisateurs et de mieux m'y retrouver lorsque je voudrais appliquer des stratégies de groupes sur mes UOs.

Enfin, j'ai ajouté le rôle serveur de fichiers à mon serveur, créé des dossiers à partager entre les utilisateurs ou groupes d'utilisateurs, puis géré leurs droits NTFS respectivement pour chaque groupe, avec un groupe « direction » ayant un peu plus de droit que les autres.

Dans mon cas, j'ai utilisé le même serveur pour AD et pour le serveur de fichier car je suis en test. Mais dans un cas réel, il est important d'utiliser un serveur dédié pour chaque rôle que l'on souhaite installer pour des raisons de sécurité.

Prérequis

- Installation sur Windows Server
- Adresse IP fixe et serveur DNS : Active Directory a besoin de DNS pour fonctionner car il
 permet aux clients de localiser les contrôleurs de domaine, ou aux contrôleurs de domaine
 de se localiser entre eux. Sans DNS, les clients ne pourraient pas trouver les contrôleurs de
 domaine et donc ne pourraient pas être identifiés. DNS permet de faire la conversion du nom
 de domaine vers IP et inversement. Sans une adresse IP fixe et DNS, il serait impossible de se
 connecter au domaine
- **Matériel** : Un processeur 1,4 GHz 64 bits ou plus rapide, 512 Mo de RAM ou plus, 32 Go d'espace disque ou plus, et un adaptateur réseau Ethernet sont recommandés.

Pourquoi installe-t-on Active Directory ?

Active Directory est un service d'annuaire qui utilise le protocole LDAP (Lightweight Directory Access Protocol). Il est utilisé pour centraliser, référencer, identifier et authentifier les utilisateurs, les ordinateurs ou tout objet dans un domaine Active Directory. Il permet de simplifier l'administration des utilisateurs, de sécuriser l'accès aux ressources et de mettre en place des stratégies de groupe pour appliquer un paramétrage sur des unités d'organisation (une UO est un dossier dans lequel on range nos objets AD). On l'installe pour faciliter la gestion des utilisateurs et des ressources au sein d'un réseau d'entreprise.

Un serveur de fichiers est un serveur qui permet de centraliser un partage de fichiers/dossiers dans un réseau. Grâce à lui, nous pouvons stocker les ressources à un seul et même endroit et pouvons gérer les droits d'accès de manière centralisée grâce à l'annuaire Active Directory.

Une stratégie de groupe permet quant à elle, de créer un paramétrage sur nos unités d'organisations (Nous pouvons créer des UOs dans des UOs si on veut des paramétrages pour certains utilisateurs seulement). Nous pouvons par exemple, définir le même fond d'écran pour tout le monde, configurer un lecteur réseau, déployer un logiciel, forcer les MAJ Windows update, etc...

2. Mise en place et procédé pas à pas

Dans un premier temps il faut définir un adresse IP fixe sur notre serveur ou l'on va installer AD qui deviendra le contrôleur de domaine. Dans mon cas, j'ai défini 192.168.1.10/24, puis définir en serveur DNS préféré nous-même, qui peut aussi se noter 127.0.0.1 (car notre contrôleur de domaine fera aussi serveur DNS, car AD en a besoin pour fonctionner comme je l'ai mentionné plus haut).

Propriétés de : Protocole Internet ve	ersion 4 (TCP/IPv4)	×
Général		×
Les paramètres IP peuvent être dét réseau le permet. Sinon, vous deve appropriés à votre administrateur ré	erminés automatiquement si votre z demander les paramètres IP íseau.	
Obtenir une adresse IP automa	atiquement	
• Utiliser l'adresse IP suivante :		
Adresse IP :	192.168.1.10	
Masque de sous-réseau :	255 . 255 . 255 . 0	
Passerelle par défaut :	192.168.1.1	
Obtenir les adresses des serve	urs DNS automatiquement	
• Utiliser l'adresse de serveur DN	IS suivante :	- 11
Serveur DNS préféré :	127.0.0.1	
Serveur DNS auxiliaire :		
Valider les paramètres en quit	tant Avancé	
	OK Annuk	er
	ОК	Annuler

Ensuite, nous pouvons passer à l'installation des rôles en passant par le gestionnaire de serveur, ajout de rôles et fonctionnalités, et cocher les rôles « serveur DNS » et « Services AD DS », nous pouvons ensuite valider et faire suivant pour terminer l'installation.

🚡 Assistant Ajout de rôles et de fon	nctionnalités	– 🗆 X
Sélectionner des r	ôles de serveurs	SERVEUR DE DESTINATION SRV-V-FS-AT
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec	tionné.
Type d'installation	Rôles	Description
Sélection du serveur	Accès à distance	Les services de domaine Active
Rôles de serveurs	Attestation d'intégrité de l'appareil	Directory (AD DS) stockent des
Fonctionnalités	Hyper-V	le réseau et rendent ces
Serveur DNS	Serveur DHCP	informations disponibles pour les
AD DS	Serveur DNS	réseau. Les services AD DS utilisent
Confirmation	Service Guardian hôte	les contrôleurs de domaine pour
Résultats	Services AD DS Services AD RNS (Active Directory Lightweight Dire Services AD RNS (Active Directory Rights Manager Services d'activation en volume Services d'activation en volume Services d'activation en volume Services d'activation en volume Services de déploiement Windows Services de déploiement Windows Services de déploiement Windows Services de fáchaiton Active Directory (AD FS) Services de fáchaiton Active Directory (AD FS) Services de stratégie et d'accès réseau Services de stratégie et d'accès réseau Services de stratégie et d'accès réseau	donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
	< Précédent Suivant	t > Installer Annuler

Une fois les rôles installer, nous avons deux nouveaux onglets à gauche sur notre gestionnaire de serveur « AD DS » et « DNS », qui certifient que les rôles sont bien installés. Et nous avons un petit symbole jaune « attention » en haut à droite qui nous avertit qu'il faut finir la configuration d'Active Directory (nous devons le passer en tant que contrôleur de domaine). Il faut donc cliquer dessus et cliquer sur « promouvoir ce serveur en contrôleur de domaine ».

🚡 Gestionnaire de serveur	- N			- 0 ×
Gestionna	ire de serveur • Se	rveur local		🔹 🕃 🎢 Gérer Outils Afficher Aide
🎹 Tableau de bord	PROPRIÉTÉS Pour SRV-V-FS-AT			Configuration post-déploie
Serveur local Tous les serveurs AD DS DNS	Nom de l'ordinateur Groupe de travail	SRV-V-FS-AT WORKGROUP	Dernières mises à jo Windows Update Dernière recherche c	Configuration requise pour : Services AD D'S à SRV- VER ar Promouvoir ce serveur en contrôleur de domaine uniquement à l'aide de Windows Upc installation de fonctionnalité
Services de fichiers et d >	Pare-feu Windows Defender Gestion à distance Bureau à distance	Privé : Inactif Activé Désactivé	Antivirus Windows D Commentaires et dia Configuration de séc	Configuration requise. Installation réussie our SRV-V- FS-AT. Ajouter des rôles et fonctionnalités
	Association de cartes réseau Ethernet	Désactivé 192.168.1.10, Compatible IPv6	Fuseau horaire ID de produit (Produ	Détails de la tâche

Maintenant le configurateur nous demande si l'on veut ajouter le contrôleur de domaine à un domaine existant, si l'on veut ajouter un nouveau domaine à un foret existant, ou si l'on veut créer une toute nouvelle forêt. Dans notre cas, c'est une toute nouvelle foret étant donné que c'est notre premier domaine, nous prenons donc la dernière option. Il faut maintenant définir un nom à notre domaine, étant donné que c'est un domaine local, il ne faut pas mettre un nom trop compliqué ni trop long, et finir par « .local » ou « .lan » pour ne pas le confondre avec un nom de domaine publique.

Assistant Configuration des servi	ces de domaine Active Directory	-		×
Assistant Configuration des servi Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	ces de domaine Active Directory déploiement Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter un nouveau domaine à une forêt existante Ajouter un nouveau domaine à une forêt existante Spécifiez les informations de domaine nour cette opération Nom de domaine racine : AT.local	-	GERVEUR C	X IBLE S-AT
	En savoir plus sur les configurations de déploiement	er	Annule	er

L'installeur nous demande si l'on veut que le contrôleur de domaine soit rétro compatible avec d'anciennes versions de Windows Server, dans notre cas nous n'en avons pas d'autres donc nous laissons les options par défaut. Nous pouvons aussi spécifier si nous voulons qu'il soit aussi serveur DNS, dans notre cas vu que c'est le premier il doit obligatoirement être serveur DNS aussi, si on veut qu'il soit catalogue global (qu'il stock tous les objet de mon annuaire), pareil que pour DNS vu que c'est notre premier il doit être CG, et l'option « contrôleur de domaine en lecture seule » permet d'avoir un contrôleur de domaine où l'on ne peut faire aucune modification, il répondra seulement au demande d'authentification ou autres des clients (utiles si l'on veut le mettre dans un site distant). Nous devons ensuite définir un mot de passe qui nous servira à la restauration en cas de panne d'Active Directory, seul ce mot de passe pourra être utilisé. (Il permet d'accéder en admin au serveur)

📥 Assistant Configuration des servi	ices de domaine Active Directory		-		×
Options du contrô Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès	Sélectionner le niveau fonctionnel de Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine : Spécifier les fonctionnalités de contre	la nouvelle forêt et du domaine ra Windows Server 2016 Windows Server 2016 Sleur de domaine	v v	SERVEUR (SRV-V-I	CIBLE FS-AT
Examiner les options Vérification de la configur Installation Résultats	✓ Serveur DNS (Domain Name Syst ✓ Catalogue global (GC) ☐ Contrôleur de domaine en lectur Taper le mot de passe du mode de re Mot de passe : Confirmer le mot de passe :	em) e seule (RODC) stauration des services d'annuaire 	(DSRM)		
	En savoir plus sur les options pour le	contrôleur de domaine Précédent Suivant >	Installer	Annu	ler

Il nous est ensuite possible de créer une délégation DNS (Si l'on veut qu'un autre serveur gère DNS), ce n'est pas notre cas, on peut donc cliquer sur suivant

📥 Assistant Configuration des serv	ces de domaine Active Directory	-		×
Options DNS	e délégation pour ce serveur DNS car la zone parente faisant autorité est intro…	Affiche	SRV-V-I	CIBLE FS-AT
Configuration de déploie Options du contrôleur de Options Supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Spécifier les options de délégation DNS			
	En savoir plus sur la délégation DNS			
	< Précédent Suivant >	ller	Annu	ler

Il faut ensuite attendre que l'installateur définisse le nom de domaine NetBIOS (alternative à DNS plutôt ancienne)

Assistant Configuration des servi	ces de domaine Active Directory		-		×
Options suppléme	entaires		SE	RVEUR C	IBLE S-AT
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires	Vérifiez le nom NetBIOS attribué au Le nom de domaine NetBIOS :	u domaine et modifiez-le si nécessaire. AT			
Chemins d'accès Examiner les options Vérification de la configur Installation Résultats					
	En savoir plus sur d'autres options	< Précédent Suivant > Inst	aller	Annule	r

Maintenant, le configurateur nous avertit que nous n'avons pas défini de délégation DNS, et que nous n'aurons pas de rétrocompatibilité avec les anciens OS Windows Server.

Katter de la s	C SERVEUR	CIB
erification de la c	configuration requise srv-v-	FS-/
Toutes les vérifications de la	configuration requise ont donné satisfaction. Cliquez sur Installer pour comme Afficher plus	×
Configuration de déploie Options du contrôleur de	La configuration requise doit être validée avant que les services de domaine Active Directory s installés sur cet ordinateur	oier
Options DNS	Réexécuter la vérification de la configuration requise	
Options supplémentaires		
Chemins d'accès	Voir les résultats	
Examiner les options	A Les contrôleurs de domaine Windows Server 2019 offrent un paramètre de sécurité par	^
Vérification de la configur	NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors	
Installation	de l'établissement de sessions sur canal sécurisé.	
Résultats	Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?Linkld=104751).	T
	Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer des adresses IP statiques IPv4 et IPv6 et la contraction de site de la contraction de la cont	~
	 Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération promotion. En savoir plus sur les conditions préalables 	de

Le serveur redémarre, applique les modifications que l'on a effectué et nous pouvons maintenant nous connecter en tant qu'administrateur sur le domaine



Nous passons à la configuration du DNS, il faut dans un premier temps définir une zone de recherche inversée, qui fera la liaison entre l'adresse IP et le nom de domaine pour tous les objets de notre domaine. Il faut donc aller dans les paramètres DNS, clic droit sur « zone de recherche inversé » et crée une nouvelle zone « zone principale »

🚊 Gestionnaire DNS	
Fichier Action Affichage ?	
🗢 🔿 🙍 📅 🧟 👘	1 🛛 🛱
 DNS SRV-V-FS-AT Zones de recherche direc Zones de recherche inver Points d'approbation Redirecteurs conditionne 	Ajouter une nouvelle zone DNS (Domain Name System) permet la division d'un espace de noms DNS en zones. Pour ajouter une nouvelle zone, ouvrez le menu Action et cliquez sur Nouvelle zone.
	Assistant Nouveile zone Assistant Nouveile zone Le serveur DNS prend en charge différents types de zones et de stockages.
	Sélectionnez le type de zone que vous voulez créer : © Zone principale Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur. O zone secondaire Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à
	équiliter la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes. Zone de stub Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone
	Entregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)
	< Précédent Suivant > Annuler

Nous pouvons définir si l'on veut que la zone de recherche inversée soit répliqué sur le domaine ou sur la forêt, nous pouvons laisser l'option par défaut et cliquer sur suivant.

Vous pouvez sélectionner la façon dont sur votre réseau.	les données DNS doivent être répliquées	THUR IT
Choisissez la façon dont les données de	la zone doivent être répliquées :	
O Vers tous les serveurs DNS exécutés AT.local	sur des contrôleurs de domaine dans cette	e forê
Vers tous les serveurs DNS exécutés domaine : AT.local	sur des contrôleurs de domaine dans ce	
O Vers tous les contrôleurs de ce doma	ine (compatibilité avec Windows 2000) : AT	r.local
 Vers tous les contrôleurs de domaine d'annuaire : 	spécifiés dans l'étendue de cette partition	
O Vers tous les contrôleurs de domaine d'annuaire :	spécifiés dans l'étendue de cette partition	
O Vers tous les contrôleurs de domaine d'annuaire :	spécifiés dans l'étendue de cette partition	
O Vers tous les contrôleurs de domaine d'annuaire :	spécifiés dans l'étendue de cette partition	

Nous indiquons sur quel type d'IP nous travaillons (IPv4) dans notre cas et spécifions dans la fenêtre d'après l'adresse réseau de l'IP de votre serveur (dans notre cas 192.168.1).

Assistant Nouvelle zone X	Assistant Nouvelle zone X
Nom de la zone de recherche inversée Une zone de recherche inversée traduit les adresses IP en noms DNS.	Nom de la zone de recherche inversée Une zone de recherche inversée traduit les adresses IP en noms DNS.
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6. © Zone de recherche inversée IPv <u>4</u> O Zone de recherche inversée IPv <u>6</u>	Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.
< <u>P</u> récédent <u>S</u> uivant > Annuler	< <u>P</u> récédent <u>S</u> uivant > Annuler

Nous pouvons laisser cocher la case par défaut qui est recommandé pour Active Directory et qui permettra que le serveur DNS mette à jour les enregistrements de ressources dès qu'une modification à lieu sur le domaine, puis nous terminons la configuration. La zone de recherche inversée est correctement paramétrée et nous le voyons dans la zone avec notez l'IP du réseau à l'envers.

2
2
r



Nous devons maintenant aller dans la zone de recherche direct, faire un clic droit sur notre serveur est cocher la case « Mettre à jour l'enregistrement de pointeur PTR associé » qui permettra à notre zone de recherche inversé de retourner le nom DNS d'un hôte à partir de son adresse IP.

🍰 Gestionnaire DNS						F	Propriétés de : sr	v-v-fs-at			?	×
Fichier Action Affichage ?							•					
← ⇒ 2 □ × □ ≥ 1							Hôte local (A) S	écurité				
🚊 DNS	Nom	Туре	Données		Horodateur							
SRV-V-FS-AT	_msdcs						Hôte (utilise le d	Iomaine parer	nt si ce champ est vi	de) :		
Zones de recherche direction	sites						srv-v-fs-at					
V C AT.local	_tcp											
> 🔂 _msdcs	_udp						Nom de domain	e pleinement	qualifié (FQDN) :			
> 🦳 _sites							enverte-at AT lo	ocal				
> 🦲 _tcp	(identique au dossier parent)	Source de nom (SOA)	[22] cn/-y-fr	satat local h	statique		314-413-01.711.10					
>udp	(identique au dossier parent)	Serveur de noms (NS)	sry-y-fs-at.a	t.local.	statique		Adresse IP -					
> ForestDnsZones	(identique au dossier parent)	Hôte (A)	192.168.1.10		30/11/2023 19:00:00		100 100 1 10					
✓ I Zones de recherche inver	(identique au dossier parent)	Hôte IPv6 (AAAA)	2a02:8428:18	Bbc:5501:a489:	30/11/2023 19:00:00		192.168.1.10					
> 🛐 1.168.192.in-addr.arp	srv-v-fs-at	Hôte (A)	192.168.1.10	i i i i i i i i i i i i i i i i i i i	statique			11	DTI			
> Points d'approbation	srv-v-fs-at	Hôte IPv6 (AAAA)	2a02:842	Supprimer	ue		Mettre a jour	lenregistrem	nent de pointeur (PTI	R) associe		
Kedirecteurs conditionne				Propriétés								
				Aide								
									OK	Annuler	Appli	quer

Et lorsque l'on retourne dans la liste de zone de recherche inversé, on voit bien que le PTR a été pris en compte



Nous pouvons maintenant terminer la configuration du serveur DNS en allant dans les propriétés du serveur DNS, dans l'onglet « Interface » cocher la case « Uniquement les adresses IP suivantes » et ne laisser cocher que les cases qui nous intéressent avec l'IP de notre serveur, ce qui permettra au serveur DNS de n'écouter que les requêtes provenant des adresses IP spécifié.

-		-					
Enregistrement de o	lébogage	Enregistre	ment des événeme	ints	Analyse	Sécu	urite
Interfaces	Redire	cteurs	Avancé	, l	ndications de	e racine	•
Sélectionnez les ac requêtes DNS sur t limiter aux adresses Écouter sur : O Toutes les adre (a) Uniquement les	dresses IP q outes les ad s IP sélection sses IP adresses IF	ui serviront le Iresses IP dé Innées. 9 suivantes :	es requêtes DNS. L finies pour cet ordi	e serv nateur	reur peut éca , ou vous po	outer le: ouvez le	5
Adresses IP : 2a02:842 fe80::12f6 2 192.168.1	8:18bc:550 3:2975:3298	1:a489:c6e6 :5d4a	:e626:5304				
1	ł						
		ОК	Annuler	Ann	liquer	Aide	e

Ensuite, nous pouvons définir un redirecteur, c'est un autre serveur DNS qui se trouve coté internet cette fois, que notre serveur DNS interrogera s'il ne connaît pas les noms de domaine que nous lui demandons.

Enregistrement de	débogage	Enregist	rement des événem	ents	Analyse	Sécurit
Interfaces	Redire	cteurs	Avancé	1	ndications de	e racine
Les redirecteurs s résoudre les requé résolus.	ont des serve êtes DNS liée	eurs DNS q es aux enre	ui permettent à ce s gistrements n'ayant	erveur pu être	de	
Adresse IP		No	om de domaine com	plet du	ser	
9.9.9.9		dn	s9.quad9.net			
9.9.9.9		dn	s9.quad9.net			
9.9.9.9		dn	s9.quad9.net			
9.9.9.9		dn	is9.quad9.net			
9.9.9.9		dn	is9.quad9.net			
9.9.9.9		dr	s9.quad9.net			
9.9.9.9 Utiliser les indi n'est disponibl	cations de ra	dn cine si auc	s9.quad9.net	Modi	fier	

La configuration DNS est maintenant terminée, nous pouvons tester un ping vers notre nom de domaine pour vérifier que le serveur DNS répond bien aux requêtes et fait bien la conversion vers la bonne adresse IP



Le serveur DNS fait bien la conversion nom de domaine vers IP, tout fonctionne correctement.

Active Directory

Nous pouvons donc passer maintenant à la configuration de nos premiers objets (utilisateurs, groupes, UO) sur Active Directory. Dans un premier temps, nous allons créer des unités d'organisation propre et claire pour mieux nous y retrouver.

Utilisateurs et ordinateurs Active Directory	-	×
Fichier Action Affichage ?		
🗢 🔿 🚾 🔏 📋 🗙 🖾 🕰 😖 🔯 📷 🗏 🍇 🧯 🍸 💆 🍇		
Utilisateurs et ordinateurs Active Nom Type Description > ☐ Requêtes enregistrées Unité d'organi Unité d'organi > ☐ Builtin ☐ Ordinateurs Unité d'organi > ☐ Domain Controllers ☐ Ordinateurs Unité d'organi > ☐ ForeignSecurityPrincipal: ☐ Utilisateurs Unité d'organi > ☐ Managed Service Accour ☐ Utilisateurs ☐ Ordinateurs > ☐ Ordinateurs ☐ Ordinateurs		

Ensuite, nous pouvons créer notre premier utilisateur du domaine. Nous créons l'utilisateur AT01, et spécifions qu'il doit changer son mot de passe à la première connexion (pour qu'il puisse définir son propre mot de passe).

Nouvel objet - Utilisateur		×	Nouvel objet - Utilisateur		×
Créer dans : AT.k	ocal/AT/Utilisateurs		Créer dans : AT Jo	ocal/AT/Utilisateurs	
Prénom : AT01 Nom : Nom complet : AT01 Nom d'ouverture de session o at01 Nom d'ouverture de session o AT\	de l'utilisateur : @AT.Jocal de l'utilisateur (antérieur à Windows at01 < Précédent Suivant >	2000) :	Mot de passe : Confirmer le mot de passe : L'utilisateur doit changer le L'utilisateur ne peut pas ch Le mot de passe n'expire ja Le compte est désactivé		re de session
	 Utilisateurs et ordinateurs Active Fichier Action Affichage ? 	Directory	ک کے تک کی Description teur	- 0 X	

Nous allons créer un groupe, on peut imaginer que ATO1 fait partie de la direction, nous créons donc le groupe AT.direction (les groupes permettent de gérer les droits). Nous ajoutons donc ATO1 au groupe AT.direction (chacun sont dans leurs UO respective)

Créer dans : AT	.local/AT/Groupes	
om du groupe :		
AT.direction		
om de groupe (antérieur à Wi	ndows 2000) :	
AT.direction	10010 2000) 1	
Étendue du groupe	Type de groupe	
O Domaine local	Sécurité	
Globale	ODistribution	

<

Propriété	s de : AT.d	irection				?	×
Général	Membres	Membre de	Géré par				
Membre	es :						
Nom	F01	Dossier S AT.local/	ervices de do AT/Utilisateu	maine Active D s	lirectory		
Ajou	ıter	Supprimer					

Notre utilisateur et notre groupe sont maintenant bien créer un sein de notre domaine Active Directory.

Client pour tests

Nous passons maintenant sur une machine cliente pour l'intégrer au domaine et vérifier qu'elle peut se connecter avec l'utilisateur que nous venons de créer.

Dans un premier temps, il faudra de nouveau spécifier une adresse IPv4 fixe pour notre machine cliente qui fait partie de la même adresse réseau que notre serveur contrôleur de domaine (pour qu'ils puissent communiquer), et dans la partie « DNS préféré », nous pouvons maintenant définir l'adresse IP de notre contrôleur de domaine (192.168.1.10) qui fait aussi serveur DNS maintenant et peut donc répondre aux requête concernant notre domaine, et dans DNS secondaire, un serveur DNS public tel que 9.9.9.9.

Propriétés de : Protocole Internet v	version 4 (TCP/IPv4) ×
Les paramètres IP peuvent être dé réseau le permet. Sinon, vous dev appropriés à votre administrateur r	iterminés automatiquement si votre ez demander les paramètres IP réseau.
Obtenir une adresse IP autom	natiquement
• Utiliser l'adresse IP suivante :	
Adresse IP :	192.168.1.100
Masque de sous-réseau :	255.255.255.0
Passerelle par défaut :	192.168.1.1
Obtenir les adresses des serv	eurs DNS automatiquement
• Utiliser l'adresse de serveur D	NS suivante :
Serveur DNS préféré :	192.168.1.10
Serveur DNS auxiliaire :	9.9.9.9
Valider les paramètres en qui	ttant Avancé
	OK Annuler

Une fois cela valider, nous pouvons tester si le serveur répond et si le DNS fonctionne correctement en faisant un ping sur le nom de domaine que nous avons créé. Et vérifier avec la commande « nslookup » qui interroge notre serveur DNS et nous fait le rapprochement entre l'IP du contrôleur de domaine et le nom de domaine.



Le serveur répondant correctement à nos requêtes, nous pouvons maintenant ajouter l'ordinateur client au domaine. Il faut tout d'abord allez dans le gestionnaire de fichier Windows ou l'on a le disque local C:, clic droit et allez dans les propriété. Sur cette page, nous avons la possibilité de changer le nom du PC (ce que nous allons faire pour mieux le retrouver ensuite dans Active Directory, il faut qu'il ait un nom unique et reconnaissable au sein du domaine, pour une meilleure gestion), et dans la case juste en dessous cocher « membre d'un domaine » et spécifier le nom du domaine que l'on veut rejoindre.

	Nom de l'or	Modification du nom ou du domaine de l'ordinates	ur X
	Windows ut ordinateur s	Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès ressources réseau.	aux
Description	de l'ordinate		
		Nom de l'ordinateur :	
Nom comple	t de	CLI-V-01-AT	
ordinateur : Groupe de tr	ravail :	Nom complet de l'ordinateur : CLI-V-01-AT	
Pour utilise domaine ou sur le résea Pour renom	r un Assistar u un groupe au. nmer cet ord	Membre d'un	:s
domaine ou	u de groupe	ATJOCAI	
		⊖ Groupe de travail :	
		WORKGROUP	
		OK Annu	uler
			es terr
			0-44

Le domaine nous demande un utilisateur autorisé à nous faire intégrer le domaine, typiquement le compte administrateur du domaine et sur Windows cela se note « AT\Administrateur » qui veut dire l'administrateur du domaine « AT ». Nous validons et rejoignons donc notre domaine !

Propriétés s Paramètres	système X système av Nom de l'ordinication du nom ou du domaine de l'ordinateur X	
	Sécurité Windows X	
Descriptic	Modification du nom ou du domaine de l'ordinateur	Modification du nom ou du domaine de l'ordinateur $$ $ imes$
Nom com l'ordinateu Groupe de	Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.	Bienvenue dans le domaine AT.local.
Pour utili domaine	AT\Administrateur	
sur le rés Pour ren domaine	••••••	ОК
	OK Annuler	
	OK Annuler s termes du contrat	
	O-AA303 OK Annuler Appliquer	

Le PC client redémarre, et nous pouvons essayer de nous connecter avec l'utilisateur ATO1 que nous avons créé juste avant.



Con	beille										
=	DÉMARRER	×	Productivité	55 M	CC icrosoft Edge	Microsoft Stor	re				
8	AT01										
D	Documents										
	Images										
Ö	Paramètres										
Φ	Marche/Arrêt										
		une recher	che	1		:			^ 단 🐅	21:19 30/11/2023	-

Le PC client à bien rejoint le domaine et nous pouvons nous connecter sur ce PC avec l'utilisateur du domaine que nous avions créé préalablement sur Active Directory. Nous avons toujours la possibilité de nous connecter en local avec le compte local du PC si nécessaire.

Serveur de fichier + droit NTFS

Le PC client ayant bien rejoint le domaine, nous allons maintenant ajouter le rôle serveur de fichier à notre serveur Active Directory (Encore une fois, dans un cas réel il est important de créer un serveur dédié pour chaque rôle que nous installons, mais dans notre cas comme nous sommes en test, nous faisons tout sur le même serveur).

Comme pour les rôles Active Directory, nous nous rendons sur le gestionnaire de serveur, ajout de fonctionnalité. Le rôles serveur de fichier étant déjà installé de base, nous avons simplement besoin de rajouter le gestionnaire de ressource du serveur de fichier pour ce serveur-là.



Une fois cela fait, nous devons nous rendre dans le gestionnaire de fichier, et en faisant un clic droit sur le « disque local C: », nous avons la possibilité d'activer les clichés instantanée. Les clichés instantanés est une technologie Windows qui nous permettent d'avoir un retour en arrière possible sur l'ensemble du disque dur, ou sur l'ensemble de la machine. Cela crée une sauvegarde du système au moment où le cliché est pris. En les activant, nous avons un nouvel onglet dans les propriétés de chaque dossier et sous dossier d'où son activé les clichés instantanée « version antérieur ». Très utile lorsqu'on fait des modifications et que l'on souhaite revenir en arrière. Nous avons également la possibilité de planifier à quelles fréquences sont pris les clichés.

Clichés instantanés	X Paramèteor	
Clichés instantanés	C:\	? ×
Les clichés instantanés permettent de voir le contenu des dossiers partagés tel qu'il existait dans le passé. Pour obtenir plus d'informations sur les clichés instantanés, <u>cliquez tel</u> . Sélectionnez un volume : Volume Heure de la procha Partages Utilisé	Planfication 1. Å 07:00 tous les lun., mar., mer., jeu., ven. 1. Å 07:00 tous les lun., mar., mer., jeu., ven. 2. Å 12:00 tous les lun., mar., mer., jeu., ven.	de chaque semaine, débu 💙 de chaque semaine, début : 3 de chaque semaine, début : 3
	Tâche planifiée : Heure de début :	
Activer Désactiver Paramètres Uiches instantanes du volume sélectionné 30/11/2023 22:30 Créer Supprimer Rétablr	Planification hebdomadaire Toutes 1 semaine(s) U Lu MM M Je Ve	n Sam Ir Dim Ir Ju
OK Annul	Afficher les différents horaires.	OK Annuler

Nous pouvons maintenant aller dans les paramètres Active Directory, retrouver la configuration des unités d'organisation précédente que nous avions créé (quelques étapes au-dessus). J'ai décidé de supprimer l'utilisateur « ATO1 » et de reprendre sur une base saine, en créant de nouveaux utilisateurs et groupes, pour pouvoir gérer leurs droits de manière plus compréhensible. Dans un premier temps, j'ai créé trois groupes (un par service).



Puis, j'ai créé trois nouveaux utilisateurs (un par groupe).



J'ai ensuite ajouté les utilisateurs à leurs groupes respectifs (les groupes nous permettent de gérer les droits de manière plus simple, sans avoir à gérer les droits pour chaque utilisateur un par un, alors qu'une stratégie de groupe s'applique uniquement sur des unités d'organisation).



Nous pouvons maintenant créer les dossiers à partager. Il est recommandé de créer les dossiers à partager à la racine d'un disque dur pour éviter les chemins d'accès trop long et d'atteindre la limite de caractère imposée par Windows lorsqu'on voudra y accéder. Nous créons donc le dossier partage à la racine de notre disque dur, puis dans le dossier "partage", nous pouvons créer un dossier pour chaque groupe d'utilisateur que nous avons créé (un pour compta, un pour direction, un pour informatique).

I Image Fichier Accueil Partage \leftarrow \rightarrow \uparrow Image	ige Affichage PC > Disque local (C:) > Partage >			
	Nom	Modifié le	Type	Taille
 ✓ Accès rapide ■ Bureau ✓ Téléchargement: ✓ Documents ✓ Images ✓ System32 	Comptabilité Direction Informatique	30/11/2023 22:44 30/11/2023 22:44 30/11/2023 22:44	Dossier de fichiers Dossier de fichiers Dossier de fichiers	
🛄 Ce PC 💣 Réseau				

Dans un premier temps, nous devons partager le dossier « parent » de notre partage, dans notre cas, le dossier partage. Nous nous rendons donc sur ce dossier, clic droit, propriété, partage, partage avancé. Nous voyons que le groupe « tout le monde » à accès au partage par défaut. Tout le monde veut dire que n'importe quelle personne connectée au réseau même si elle n'est pas identifiée pourra voir le partage (ce que n'est pas très sécurisé). Nous supprimons donc « tout le monde » et ajoutons à la place « utilisateurs du domaine », et leur laissons le droit en modification et en lecture. (Les droits dans partage avancée ne concerne seulement qui a le droit de voir le dossier via le réseau, et non qui peut faire quoi. On gèrera les vrais droits à l'étape suivant)



Nous pouvons maintenant gérer les droits d'accès au dossier, nous nous rendons donc dans le dossier partage, et sur chaque dossier respectif, nous avons la possibilité de gérer les droits d'accès au dossier en question. Pour cela, il faut clic droit sur le dossier, propriété, onglet « sécurité », « Avancé ». Il faut tout d'abord désactiver l'héritage pour que notre dossier n'hérite plus des droits de son dossier parent (dans notre cas le dossier « partage »), puis supprimer les groupes utilisateurs (il faut cependant bien laisser les groupes « administrateur » et « système »). Nous pouvons maintenant ajouter les groupes ou les utilisateurs qui auront accès au dossier. Ensuite, nous devons configurer ce que ce groupe pourra faire sur le dossier. Dans notre cas, nous voulons que chaque groupe puisse avoir les accès en lecture et modification/écriture sur leurs dossiers respectifs.

ntrées d'aut	orisations :			
Туре	Principal	Accès	Hérité de	S'applique à
Auto	Système	Contrôle total	C:\	Ce dossier, les sous-dossiers et
Auto	Administrateurs (AT\Administ	Contrôle total	C:\	Ce dossier, les sous-dossiers et
🚨 Auto	Utilisateurs (AT\Utilisateurs)	Lecture et exécution	C:\	Ce dossier, les sous-dossiers et
& Auto	Utilisateurs (AT\Utilisateurs)	Spéciale	C:\	Ce dossier et les sous-dossiers
🔏 Auto	CREATEUR PROPRIETAIRE	Contrôle total	C:\	Les sous-dossiers et les fichiers.

Principal :	AT_compta (AT\AT.compta) Sélectionnez un principal				
Type :	Autoriser \checkmark				
S'applique à :	: Ce dossier, les sous-dossiers et les fichiers $$				
Autorisations	s de base :	Afficher les a	utorisatio	ons avand	cée
	Contrôle total				
	⊴ Lecture et execution ☑ Affichage du contenu du dossier				
	✓ Lecture				
	⊡ Écriture				
	Autorisations spéciales				
Appliquer c	ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur		Eff	acer tout	t
Ajoutez une co	condition pour limiter l'accès. Les autorisations spécifiées ne seront accordées au principal que si les conditions s	ont remplies.			
Aiouter une co	condition				

Nous vérifions que chaque groupe a accès à son dossier en Modification.

Nom : Ci/Partage/Comptabilité Propriétaire : Administrateurs (AT\Administrateurs) Autorisations Partage Audit Accès effectif Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, selectionnez l'entrée et cliquez sur Modifier (si disponible). Entrées d'autorisations :	Nom : C:\Partage\Direction Propriétaire : Administrateurs (AT\Administrateurs) Autorisations Partage Autorisations Partage Autorisations Partage Autorisations Partage Autorisations Partage Autorisations Partage Autorisations Accès effectif Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible). Entrées d'autorisations : Entrées d'autorisations :
Type Principal Accès Hérité de S'applique à & Auto Système Contrôle total Aucun Ce dossier, les sous-dossiers et & Auto Administrateurs (AT\Administ Contrôle total Aucun Ce dossier, les sous-dossiers et & Auto CREATUR PROPRITAIRE Contrôle total Aucun Les sous-dossiers et les fichiers & Auto AT_compta (AT\AT.compta) Modification Aucun Ce dossier, les sous-dossiers et	Type Principal Accès Hérité de S'applique à & Auto Système Contrôle total Aucun Ce dossier, les sous-dossiers et. & Auto Administrateurs (AT\Administ: Contrôle total Aucun Ce dossier, les sous-dossiers et. & Auto CREATERIBER Contrôle total Aucun Ce dossier, les sous-dossiers et. & Auto CREATERIBER Contrôle total Aucun Les sous-dossiers et. & Auto At_direction (AT\AT.direction) Modification Aucun Ce dossier, les sous-dossiers et.
Ajouter Supprimer Modifier Activer l'héritage	Ajouter Supprimer Modifier Activer l'héritage Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet

Nom : Propriétaire :	C:\Partage\Informatiqu Administrateurs (AT\Ad	e Iministrateurs)	😌 Modifier	
utorisations	Partage Audit	Accès effectif		
electionnez intrées d'aut	l'entree et cliquez sur Modifier (si o torisations : Principal	disponible). Accès	Hérité de	S'applique à
Auto	Système	Contrôle total	Aucun	Ce dossier les sous-dossiers et.
Auto	Administrateurs (AT\Administ	Contrôle total	Aucun	Ce dossier, les sous-dossiers et.
Auto	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers.
Auto	AT_informatique (AT\AT.infor	Modification	Aucun	Ce dossier, les sous-dossiers et.
Ajouter Activer I	Supprimer Modif	ier		

Nous pouvons aussi vouloir que, par exemple, le groupe « direction » ait des accès en lecture seulement sur les dossiers d'un autre service. Nous pouvons le faire en retournant dans les paramètres de sécurité avancés pour « Compta » par exemple, et en ajoutant le groupe « direction » en laissant les paramètres par défaut (Lecture et exécution, affichage du contenu du dossier, Lecture)

Autorisation	s pour <mark>Comptabilité</mark>				;
Principal :	AT_direction (AT\AT.direction) Sélectionnez un principal				
ype :	Autoriser ~				
applique à :	Ce dossier, les sous-dossiers et les fichiers $\qquad \lor$				
Autorisations	de base :	Afficher les au	torisatio	ins avand	cée
	Contrôle total				
	Modification				
	Affichage du contenu du dossier				
	Lecture				
	Êcriture				
	Autorisations spéciales				
Appliquer o	ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur		Eff	acer tout	t
joutez une c	condition pour limiter l'accès. Les autorisations spécifiées ne seront accordées au principal que si les conditions sor	t remplies.			
Aiouter une ci	rendition				

lom :	C:\Partage\Comptabilit	é		
ropriétaire	: Administrateurs (AT\Ad	lministrateurs) 🛛 🎈 Modif	ier	
utorisation	s Partage Audit	Accès effectif		
ntrées d'au Type	torisations : Principal	Accès	Hérité de	S'applique à
Auto	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et
Auto	Administrateurs (AT\Administ	Contrôle total	Aucun	Ce dossier, les sous-dossiers et
& Auto	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers
Auto	AT_compta (AT\AT.compta)	Modification	Aucun	Ce dossier, les sous-dossiers et
& Auto	AT_direction (AT\AT.direction)	Lecture et exécution	Aucun	Ce dossier, les sous-dossiers et
Ajouter Activer	Supprimer Modif l'héritage er toutes les entrées d'autorisation d	ier	entrées d'autorisation	n pouvant être héritées de cet objet

Nous avons bien géré les droits d'accès de chaque groupe sur leurs dossier respectif, avec direction qui a un peu plus de droit que les autres. Il faut maintenant gérer les droits du dossier « partage » (le dossier parent qui contient tous les autres dossiers que l'on partage). Nous retournons donc dans les paramètres de sécurité avancés du dossier « Partage », désactivons l'héritage, et supprimons également « utilisateurs » pour ajouter « utilisateurs du domaine ». Nous ne voulons cependant pas que n'importe quels utilisateurs puissent modifier ou créer des dossiers dans notre dossier « Partage », on peut donc laisser les droits en lecture, affichage du contenu du dossier, et lecture pour ce dossier.



Nom	1:	C:\Partage			
rop	riétaire :	Administrateurs (AT\Ad	lministrateurs)	Modifier	
uto	risations	Partage Audit	Accès effectif		
intré	tionnez ées d'aut Type	rentree et ciiquez sur Modifier (si o orisations : Principal	Accès	Hérité de	S'applique à
2	Auto	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et
	Auto	Administrateurs (AT\Administ	Contrôle total	Aucun	Ce dossier, les sous-dossiers et
97	Auto	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers
62	Auto	Utilisateurs du domaine (AT\	Lecture et exécu	tion Aucun	Ce dossier seulement
) j	Ajouter Activer l'	Supprimer Affich	er		

Nous pouvons aussi vouloir que chaque groupe voit seulement les dossiers où ils ont au moins des droits en lecture et qu'ils ne voient pas les autres dossiers partagés. C'est possible grâce à l'option ABE (énumération basée sur l'accès) qui cache les dossiers où l'on n'a pas au minimum un droit de lecture ou équivalent. Il s'active dans le gestionnaire de serveur, onglet « partage », clic droit sur le dossier partagé et dans l'onglet « paramètres » nous pouvons cocher l'ABE



Nous allons nous connecter avec l'utilisateur AT Direction » (étant donné qu'il a un peu plus de droits que les autres) pour vérifier que tout ce que l'on à appliquer fonctionne correctement.





AT direction ne voit que les dossiers ou-il à les droits grâce à l'option ABE.

Il peut créer un document texte dans son propre dossier

I I I I I I Fichier Accueil Partage	Affichage			
← → × ↑ 🔒 > Réseau	u > srv-v-fs-at > Partage > Dire	ection	ٽ ~	
🕈 Accès ranide	Nom	Modifié le	Туре	Taille
Bureau 🖈	Test	01/12/2023 02:11	Document tex	te O Ko
Téléchargements *				
E Images				
h Musique				

🖳 | 🖸 📑 🖛 | Partage o × r Accueil Partage Affichage ? ✓ ♂ Rechercher dans: Partage Nom Modifié le Туре Taille 📌 Accès rapide Comptabilité 30/11/2023 22:44 Dossier de fichiers E Bureau * Direction 01/12/2023 02:11 Dossier de fichiers 🕂 Téléchargements 🖈 Documents * Images) Musique Vidéos Accès au dossier de destination refusé × Vous devez disposer d'une autorisation pour effectuer cette action OneDrive Partage Ce PC 💣 Réseau Recommencer Annuler

Il ne peut pas créer de dossiers dans le dossier parent « Partage »

Il ne peut pas créer de dossier dans le dossier « Comptabilité »

$\leftarrow \rightarrow \land \uparrow \square \rightarrow Rés$	eau > srv-v	-fs-at > Partage > Con	nptabilité		~	Ū,	© Recherch
📌 Accès rapide	Nom	^	Modifié I	e	Туре		Taille
📃 Bureau 🛛 🖈		Accès au dossier de desti	nation refusé				×
 Construction of the second seco		Vous devez disp	ooser d'une autorisatio Comptabilita Type : Dossie Modifié le : 3	n pour effectuer é er de fichiers 30/11/2023 22:44	cette actio	'n	
Ce PC				Recomment	cer	Annuler	

Je me suis connecté avec l'utilisateur « AT Informatique » pour vérifier ses droits, et il ne voit bien que le dossier où il a des droits, et ne peut pas créer de dossiers dans le dossier parent « Partage ».

↓ ↓ Partage Fichier Accueil Partage				-	
\leftarrow \rightarrow \checkmark \uparrow \fbox « srv-v-fs-at » Partage » \checkmark	ē	, Rechercher d	ans : Partage		
★ Accès rapide Bureau ★ Téléchargements ★ Documents ★ Images ★ Musique Vidéos		Modifié le 30/11/2023 22:44	Type Dossier d	le fichiers	Taille
Image Image Fichier Accueil Partage Affichage Image Affichage Image Image Image Image Image Image	م ا	Rechercher dans : Pa		- 🗆	× ~ 2
Accès rapide	Ma 30/	difié le 11/2023 22:44	Type Dossier de fichier	Taille	
 ↓ Téléchargementz △ Documents ✓ Images ✓ Vidéos ✓ OneDrive ✓ Ce PC ✓ Réseau 	pour effe	ectuer cette action	a. X		

Tous les droits que l'on a attribués sont correctement configurés !

Mise en place d'une stratégie de groupe (GPO)

Nous allons maintenant ajouter une stratégie de groupe pour que les utilisateurs puissent avoir accès à notre partage de fichiers directement via un lecteur réseau de manière beaucoup plus simple (qui se trouvera directement dans le gestionnaire de fichiers en dessous du « Disque local C: »).

Pour ce faire, il faudra aller dans les outils d'administration, et dans « Gestion de stratégie de groupe ». Dans cette console, nous allons retrouver nos unités d'organisation (je rappelle qu'une GPO s'applique seulement sur une unité d'organisation, et non sur un groupe ou un utilisateur). Nous retrouvons nos unités d'organisation créées précédemment.



Nous décidons d'appliquer cette GPO sur l'unité d'organisation « Utilisateurs », qui s'appliquera donc à tous les objets se trouvant dans cette UO. Il faut faire un clic droit sur l'UO voulu, « Créer un objet GPO dans ce domaine, et le lier ici... »

🚡 Fichier Action Affichage	Fenêtre ?			
 Gestion de stratégie de groupe A Forêt : AT.local Domaines AT.local Conupes Condinateurs Condinateurs Cobjets de st Filtres WMI Objets GPO Sites Modélisation de sti Résultats de stratégie 	Créer un objet Lier un objet d Bloquer l'hérit. Mise à jour de Assistant Mod Nouvelle unité Affichage Nouvelle fenét Supprimer Renommer Actualiser Propriétés Ajde	Utilisate Objets de Service GPO dans c e stratégie d disation de d'organisat re à partir d'	eurs stratégie de groupe liés Ordre des liens le domaine, et le lier ici le groupe existant de groupe stratégie de groupe ion 'ici	Héntage de s Objet de st

Nous devons lui ajouter un nom, vu que ce sera un lecteur réseau, nous pouvons l'appeler « LecteurReseau ».

Nouvel objet GPO	×
Nom :	
LecteurReseau	
Objet Starter GPO course :	

Il apparaîtra ensuite dans l'UO ou nous l'avons créé. Il faut faire un clic droit sur la GPO, et modifier.



Dans « Configuration des utilisateurs », « Préférences » (Préférence qui permet de réaliser un paramétrage rapide, une nouvelle fonctionnalité de Windows Server), « Paramètres Windows », « Nouveau > Lecteur mappé », nous pouvons créer notre lecteur réseau.



Dans la configuration du lecteur mappé, il est recommandé de laisser l'option « Mettre à jour » activée. Cette option permet de remplacer le lecteur s'il existe déjà, sinon de le créer. Ensuite, nous indiquons le chemin de notre partage (\\srv-v-fs-at\partage\). Nous avons ensuite la possibilité de donner un nom à notre lecteur, ce qui nous évite d'afficher tout le chemin (je conseille donc de le faire). De plus, nous avons la possibilité de choisir une lettre pour notre lecteur réseau. Pour éviter de choisir une lettre déjà utilisée par une clé USB ou autre, il est préférable de commencer par la fin de l'alphabet, ce qui permet d'éviter les problèmes.

ا الله 🎝 🖌 🔂 🖄 🗠	Propriétés de <mark>:</mark> Z:	×	-		_
Stratégie LecteurReseau [SRV-V- Configuration ordinateur Stratégies	Général Commun	~	ecteurs	5	
 Préférences Configuration utilisateur Stratégies Préférences Préférences Applications Mappages de lec Invironnement Fichiers Fichiers Fichiers.ini Raccourcis Rarcourcis Paramètres du Panne 	Emplacement : \\prv-v-fs-at' Reconnecter : \Delta Ubeller en tan Lettre de lecteur Utiliser le premier disponible, en commençant à : Se connecter en tant que (facult Nom d'utilisateur : \Delta Confir Mot de passe : \Delta Confir	atif)	Ordre 1	Action Mettre	Chi
	Masquer/Afficher ce lecteur	Masquer/Afficher tous les lecteurs Aucune modification Masquer tous les lecteurs Afficher tous les lecteurs nuller Appliquer Aide			>

Nous pouvons ensuite choisir l'ordre de lancement des GPOs, dans notre cas nous n'en avons qu'une.



Pour que notre stratégie de groupe s'applique, il est nécessaire de laisser la case « Lien activé » cochée. La case située au-dessus, « Appliquer », ne sert pas à appliquer la stratégie de groupe, mais à la forcer. On l'utilise dans le cas où nous aurions une deuxième stratégie de groupe qui serait contraire à celle que nous paramétrons (comme un fond d'écran, par exemple)



Notre lecteur réseau est correctement configuré et nous avons appliqué la stratégie de groupe sur l'ensemble de notre unité d'organisation « Utilisateurs ». Nous pouvons vérifier qu'elle s'est bien appliquée et que nous avons toujours accès au dossier respectif de chaque groupe en nous connectant avec un utilisateur et en allant dans « PC ». Le lecteur réseau apparaît bien, et l'utilisateur « AT Direction » a bien accès au dossier pour lequel il a les droits, et ne voit que ceuxci grâce à l'option ABE.



┳ 🖓 🔜 ╤ Fichier Accueil Partage Affichage	Gérer Outils de lecteur	Partage (Z:)			
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Ce PC \rightarrow Partage (Z:)	>		~	ē	, Recherc
 Accès rapide Bureau Téléchargements * Documents * Images * Musique Vidéos 		Modifié le 30/11/2023 22:44 01/12/2023 02:11	Type Dossier Dossier	de fichie de fichie	Taille rs rs

Nous avons deux commandes intéressantes sur les stratégies de groupe :

- gpresult /r : nous donne le résultats des GPOs appliquée à notre utilisateur et de voir les groupes/OU auxquels il appartient. Très utile si la GPO ne s'applique pas, nous pouvons vérifier plusieurs paramètres différents.
- gpupdate /force qui force l'ordinateur et l'utilisateur a interroger le serveur pour voir si une mise à jour de la GPO a eu lieu

A noter qu'une stratégie de groupe ne s'applique sur :

- Un ordinateur que si on le redémarre
- Un utilisateur : à la fermeture/ouverture de session.

Invite de commandes		-	0	×
				^
Configuration du système d'exploitation : Station de travail membre				
Version du système d'exploitation : 10.0.19045				
Nom du site N/A				
Profil itinérant : N/A				
Profil local Vision lists				
connexion via une liaison iente ? : Non				
PARAMÈTRES UTILISATEURS				
CN=AT Direction,OU=Utilisateurs,OU=AT,DC=AT,DC=local				
Heure de la dernière application de la stratégie de groupe : 01/12/202	3 à 02:38:54			
Stratégie de groupe appliquée depuis : SRV-V-FS-AT.AT.local				
Seuil de liaison lente dans la stratégie de groupe : 500 kbps				
Nom du domaine : AT				
Type de domaine : Windows 2008 ou superieur				
Objets Stratégie de groupe appliqués				
LecteurReseau				
Les objets stratégie de groupe n'ont pas été appliqués				
car ils ont été refusés				
Charteful de annue land.				
Filtname : Non appliqué (vide)				
rittinge . Hon appilde (vide)				
L'utilisateur fait partie des groupes de sécurité suivants				
Utilisateurs du domaine				
Tout le monde				
Utilisateurs				
Utilicatours authentifiés				
Cette organisation				
LOCAL				
AT.direction				
Identité déclarée par une autorité d'authentification				
Niveau obligatoire moyen				
C:\Users\atdirection>				~
🗄 🔎 Tapezici pour effectuer une 🛛 🚈 🛱 💽 📄 💼		^ ₽ 4 01/1	2:41	鬲



3. Conclusion

Et voilà, nous avons procédé à la mise en place d'un domaine avec Active Directory, promu notre serveur AD en contrôleur de domaine et créé des utilisateurs dans ce domaine. Nous avons ensuite mis en place un partage de fichier avec des droits d'accès NTFS pour chaque utilisateur, avons laissé afficher les dossiers partagés qu'aux personnes ayant au minimum des droits en lecture sur ces derniers grâce à l'option ABE et avons déployé ce partage sous forme de lecteur réseau grâce à une GPO.

Test de bon fonctionnement :

Pour le test, il suffit de tenter d'entrer un ordinateur au domaine précédemment créé, de créer un utilisateur et d'essayer de se connecter avec ce dernier sur un poste client. Ensuite, nous pouvons vérifier que les GPOs s'appliquent bien en vérifiant dans « Ce PC » leurs droits d'accès à ce même endroit. Si nous arrivons à accéder avec un utilisateur à un dossier auquel il n'a pas accès ou qu'il le voit alors que l'option ABE est activée, c'est qu'il faut revoir ces points directement sur le serveur.

Point de vigilances

- Dans ce TP, j'ai rencontré un souci avec DNS qui ne faisait la résolution de mon nom de domaine uniquement vers mon adresse en IPv6 et non en IPv4. Pour pallier ce souci, il faut bien penser à décocher l'IPv6 dans les propriétés du serveur DNS pour n'avoir que des adresses en IPv4
- Bien vérifier le DNS sur le poste client si nous n'arrivons pas à l'entrer dans le domaine, le souci peut venir d'un DNS mal renseigné
- Un nom de domaine local, par convention, doit toujours se terminer par « .local » ou « .lan » pour ne pas le confondre avec un nom de domaine public.
- Il faut bien faire attention : les stratégies de groupes peuvent uniquement être mises en place sur des unités d'organisation. Les groupes quant à eux, servent à gérer les droits NTFS (accès aux dossiers ou ressources). A ne pas confondre !
- Pour se connecter au domaine, il faut utiliser cette façon d'écrire sur la page de connexion : AT\administrateur (qui veut dire l'administrateur du domaine AT). Ajouter un poste à un domaine n'empêche pas de se connecter en local, en écrivant le login de cette façon : .\UtilisateurduPC (qui veut dire l'utilisateur du poste en local)
- Lorsque l'on met en place une stratégie de groupe, pour l'appliquer il faut bien laisser la case « lien activé » cochée qui veut simplement dire que cette dernière est activée, et ne pas utiliser « appliqué » (qui se traduit « forced » sur un Windows Server anglais) et qui forcerait la GPO. On utilise « appliqué » dans le cas où on a une stratégie de groupe « parente » à celle

qu'on paramètre (comme un fond d'écran différent par exemple).

- Dans la configuration d'un lecteur mappé, il faut bien laisser l'option « mettre à jour » qui fait que si le lecteur existe déjà, on le remplace, sinon on le crée.
- Lorsqu'on paramètre un lecteur réseau, il faut bien penser à lui attribuer une lettre et de plutôt commencer par la fin, ce qui évite de tomber sur la même lettre qu'une clé USB ou autre par exemple.
- La commande « nslookup » est intéressante car elle interroge notre serveur DNS et nous fait le rapprochement entre l'IP du contrôleur de domaine et le nom de domaine.
- Les dossiers à partager sont à créer uniquement à la racine du disque local pour éviter les chemins d'accès trop longs et éviter d'atteindre la limite de caractères imposée par Windows qui peut nous causer des soucis lors de renommage ou de copie de fichiers.
- Nous avons deux commandes intéressantes sur les stratégies de groupe :

gpresult /r : nous donne le résultat des GPOs appliquées à notre utilisateur et de voir les groupes/OU auxquels il appartient. Très utile si la GPO ne s'applique pas, nous pouvons vérifier plusieurs paramètres différents.

gpupdate /force qui force l'ordinateur et l'utilisateur à interroger le serveur pour voir si une mise à jour de la GPO a eu lieu (Attention, ça ne l'appliquera pas, pour qu'une stratégie de groupe s'applique il faut :

- Redémarrer le poste quand c'est une GPO ordinateurs.
- Déconnecter et reconnecter la session quand c'est une GPO utilisateurs.

Conseils de sécurité

- Le premier conseil est de bien laisser coché l'option pour que les nouveaux utilisateurs qu'on crée puisse choisir eux même leurs mots de passes lors de la première connexion.
- Il faut bien évidemment et comme toujours créer un serveur dédié pour chaque rôle que l'on souhaite installer, donc un serveur Active Directory, et un serveur de partage de fichier dans notre cas
- Sur un serveur de fichier, il est impératif d'activer les clichés instantanés qui nous permettent d'avoir une antériorité sur nos fichiers à un moment donné et une solution de récupération ou de restauration en cas de souci
- L'option « partager ce dossier » ne sert qu'à définir qui peut voir le partage via le réseau et non qui peut faire quoi sur ce dernier. Pour gérer les droits d'accès, il faut gérer les droits NTFS dans l'onglet sécurité. Les permissions NTFS déterminent qui peut accéder, modifier ou supprimer des fichiers.
- Il est ESSENTIEL de supprimer le groupe « Tout le monde » dans les options de partage avancées qui veut bien dire que tout le monde pourra voir le dossier sur le réseau,

et ajouter à la place « utilisateurs authentifié » ou « utilisateurs du domaine » qui est bien plus sécurisé.

- De même, pour les droits NTFS, il faut bien supprimer les utilisateurs et créer des groupes dédiés pour gérer les droits sur ces dossiers, selon qui peut y avoir accès ou non (Ne pas oublier de désactiver l'héritage comme mentionné dans le procédé pas à pas).
- Les droits en contrôle total sur des dossiers sont uniquement à laisser pour les administrateurs et le système (pour les MAJ ou autres), et ne jamais laisser de droits en contrôle totale à d'autres personnes qui leur permettrait de modifier les droits d'accès, ce qu'on ne veut surtout pas.
- L'option ABE est très intéressante en matière de sécurité car elle permet de ne laisser afficher les dossiers que des utilisateurs qui ont des droits en lecture au minimum sur ces derniers. Si un utilisateur n'a pas de droit, il ne verra pas le dossier lors de sa connexion au partage.
- Il faut définir un mot de passe fort pour la restauration en cas de panne d'Active Directory (lors de l'installation du rôle), seul ce mot de passe pourra être utilisé. (Il permet d'accéder en admin au serveur)