



MENIAL Hugo

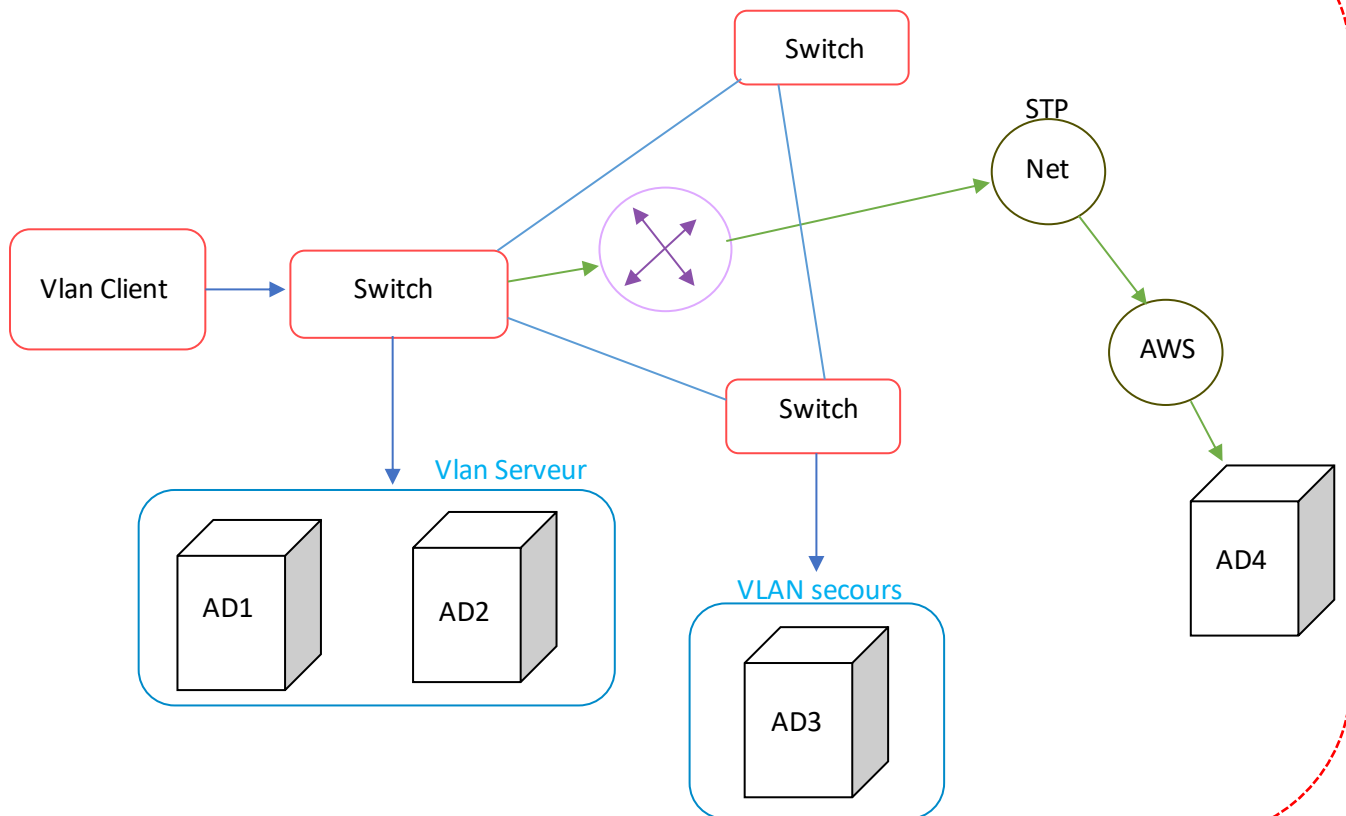
BTS SIO 2

## DFSR :

### Contextualisation :

Afin de prévoir une probable panne sur son système d'informations, l'entreprise Net Saint Luc souhaite mettre en place une réplication de son Active Directory sur son domaine principal. Vous mettez donc en place cette réplication afin d'avoir une continuité de service de l'AD.

### Schémas de réplication :



## **Sommaire :**

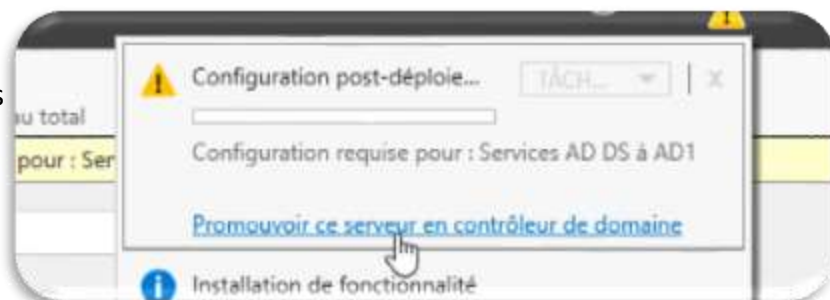
Mise en place de l'AD1	page 3-9
- Préparation de l'AD1	page 5
- Crée un dossier partager et ajouter des droits	page 6
Mise en place de l'AD2 :	page 10
- Installez le rôle AD DS sur AD2	page 12
- Configuration de déploiement	page 12
- Intégrez la machine dans le domaine	page 13
Manipulation des 2 AD :	page 14
- Créer votre pool de serveurs	page 15
- Création du Groupe de réplication	page 19
Problème du serveur de temps :	page 21

## 1) Mise en place de l'AD1 :

Donnez à votre serveur AD1 l'adresse IP voulue

The screenshot shows the 'Réseau' (Network) configuration window in Windows Server Setup. The 'Utiliser l'adresse IP suivante' (Use the following IP address) option is selected. The IP address is set to 192.168.20.116, the subnet mask is 255.255.255.0, and the default gateway is left blank. Below this, the 'Utiliser l'adresse de serveur DNS suivante' (Use the following DNS server address) option is also selected. The preferred DNS server is set to 192.168.20.116, and the auxiliary DNS server is left blank. There are additional fields for secondary DNS servers that are partially visible at the bottom.

Après l'installation de l'AD DS, Nous allons  
Ajouter une nouvelle forêt, mon nom de  
Domaine sera « menial.com »



The screenshot shows the 'Sélectionner l'opération de déploiement' (Select the deployment operation) window. Three radio buttons are present: 'Ajouter un contrôleur de domaine à un domaine existant' (Add a domain controller to an existing domain), 'Ajouter un nouveau domaine à une forêt existante' (Add a new domain to an existing forest), and 'Ajouter une nouvelle forêt' (Add a new forest). The third option is selected. Below the radio buttons, the text 'Spécifiez les informations de domaine pour cette opération' (Specify domain information for this operation) is displayed. The 'Nom de domaine racine' (Root domain name) field is filled with 'menial.com'.

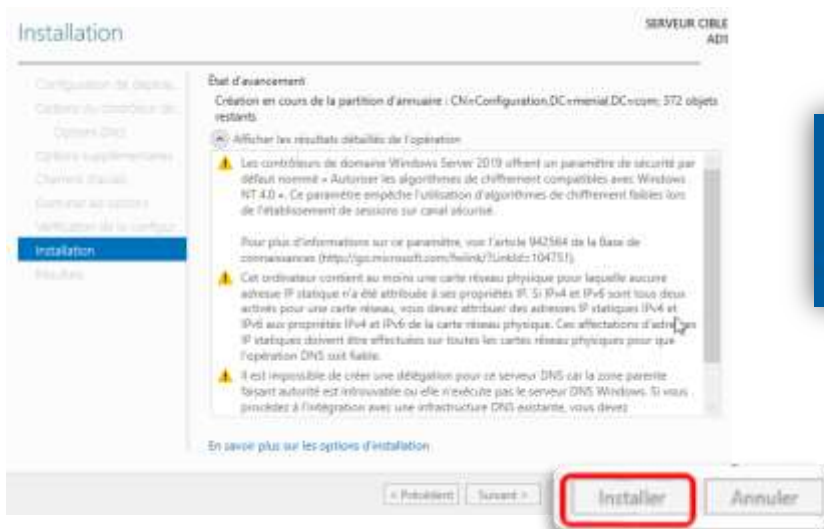
Dans l'option du contrôleur de domaine, vous devez choisir le niveau fonctionnel de la forêt :  
choisissez Windows 2012.

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

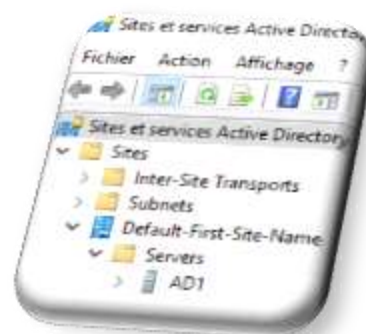
Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Puis continuer jusqu'à l'installation.



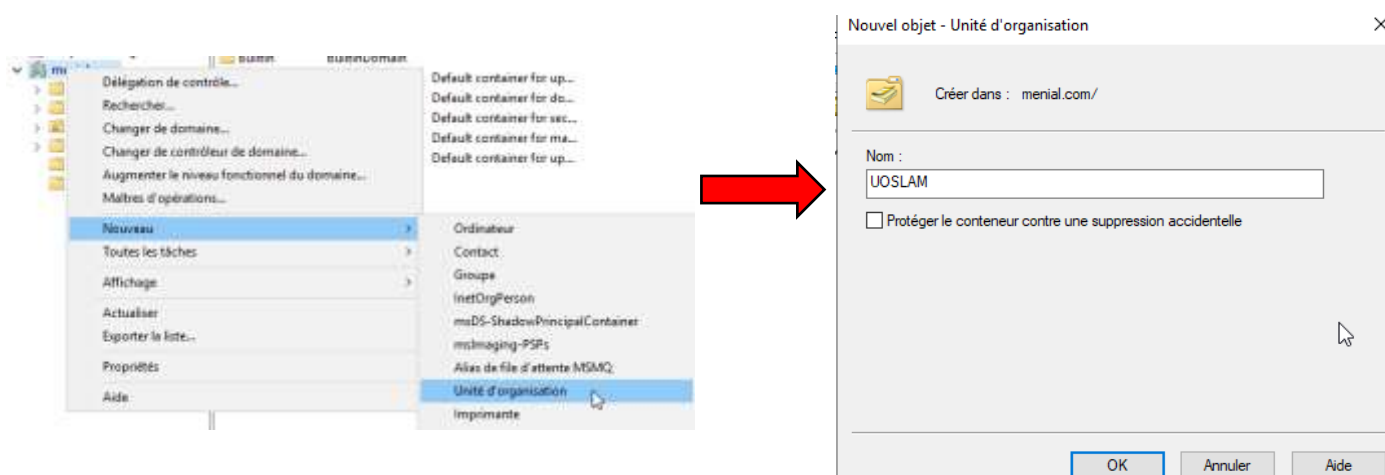
Il y a bien dans le Sites et services  
Active Directory Le serveur AD1 :  
« Default-First-Site-Name\AD1 \ »



## Préparation de l'AD1 :

Login	Groupe	UO
Laurent	SISR	UOSISR
Sebastien	SISR	UOSISR
Paul	SISR	UOSISR
Jeanne	SLAM	UOSLAM
Jérôme	SLAM	UOSLAM
Vladimir	SLAM	UOSLAM

Crée Les groupes d'Unités d'organisations Nommés « UOSISR » et « UOSLAM » :



Mon Unité d'organisation a bien été créée.

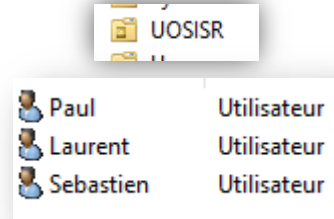
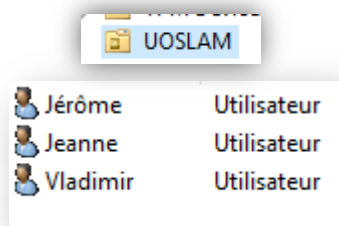
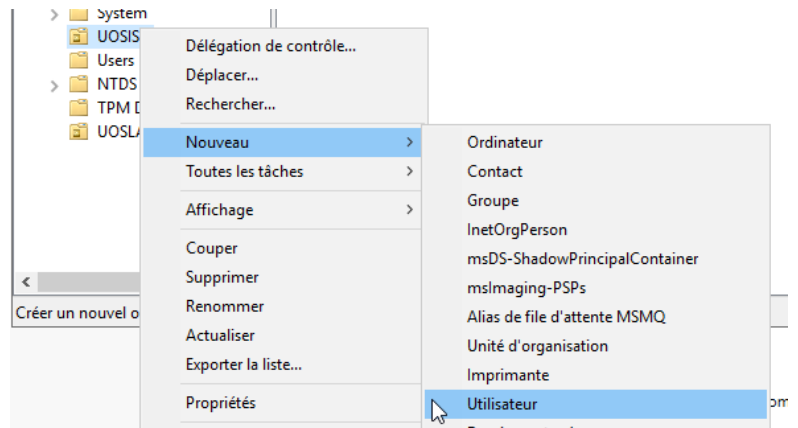


Même choses pour l'Unité d'organisation SISR.



Création de 6 comptes utilisateurs

Répartis en 2 groupes : SLAM et SISR :



Crée un dossier partager et ajouter des droits :

Ici nous avons le dossier SISR//

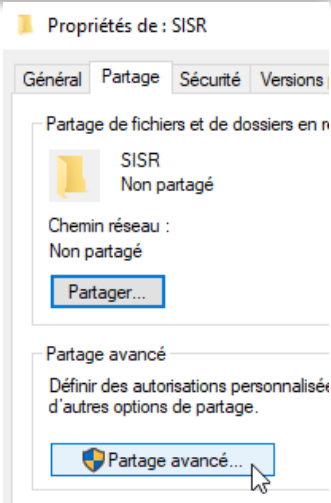
→ Commun/

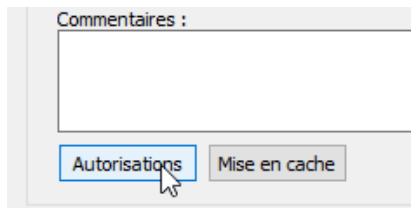
→ Cours/



Ouvrir les propriétés du dossier SISR, →

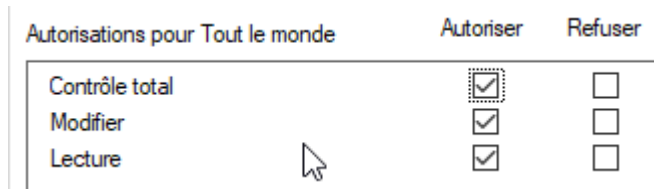
Cliquer sur «  Partage avancé... » »





Cliquer ensuite sur « Autorisations »

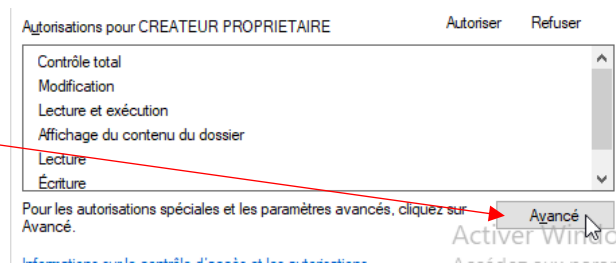
Cocher toutes les cases.



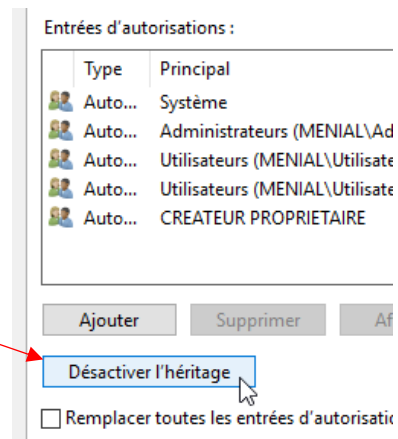
« Appliquer » puis Revenez en arrière.

Rendez-vous dans « sécurité »

« avancer »



Désactiver l'héritage



Désactiver l'héritage pour chaque dossier créé,

Ici nous avons « Commun, Cours »

J'ajoute Laurent en tant que propriétaire de SISR/Commun

Ouvrir les propriétés du dossier Commun

Aller dans – sécurité

Dans – modifier

Faite : ajouter

Puis écrire le nom du propriétaire du dossier : Laurent

Faite « Vérifier les noms» pour trouver du compte crée dans AD

Entrez les noms des objets à sélectionner (exemples) :

Laurent (laurent@menial.com); Paul (Paul@menial.com);  
Sebastien (sebastien@menial.com)

Vérifier les noms

Avancé... OK Annuler

( Dossier SISR )

Puis reproduire la même chose pour ajouter vos répertoires selon le ou les propriétaire(s).

Pour Laurent propriétaire du dossier SISR/Commun

Droit : RWX

Laurent (laurent@menial.com)

Pour modifier les autorisations, cliquez sur Modifier.

Modifier.

Autorisations pour Laurent	Autoriser	Refuser
Modification		
Lecture et exécution	✓	
Affichage du contenu du dossier	✓	
Lecture	✓	
Écriture	✓	



## ( Dossier Commun )

### Utilisateurs avec droit de Lecture

Autorisations pour Utilisateurs	Autoriser
Modification	
Lecture et exécution	
Affichage du contenu du dossier	
Lecture	✓
Écriture	

Pour Sébastien propriétaire du dossier SISR/Cours

Droit : R

Autorisations pour Sébastien	Autoriser
Modification	
Lecture et exécution	
Affichage du contenu du dossier	✓
Lecture	✓
Écriture	
Autorisations spéciales	

### Utilisateurs globaux sans droit

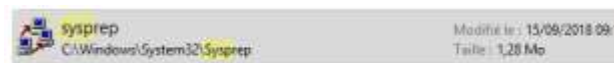
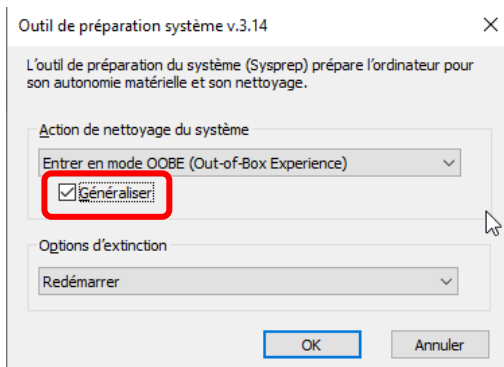
Autorisations pour Utilisateurs	Autoriser
Modification	
Lecture et exécution	
Affichage du contenu du dossier	
Lecture	
Écriture	
Autorisations spéciales	✓

## 2) Mise en place de l'AD2

Attention si vous prenez un clone de votre première AD vous aurez un problème de SSID : vos machines auront le même SSID. Donnez à votre serveur AD2 l'adresse IP voulue.

Après avoir cloner notre AD il faut modifier l'adresse MAC de Windows serveur AD2

Dans C:\Windows\System32\Sysprep\ l'application sysprep pour changer son adresse MAC.



## Adressage du réseau avant de rajouter le domaine à l'AD2 :

### AD1

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 20 . 116

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 20 . 116

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 20 . 116

Serveur DNS auxiliaire : . . .

### AD2

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 20 . 174

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 20 . 116

☐ Obtenir les adresses des serveurs DNS automatiquement

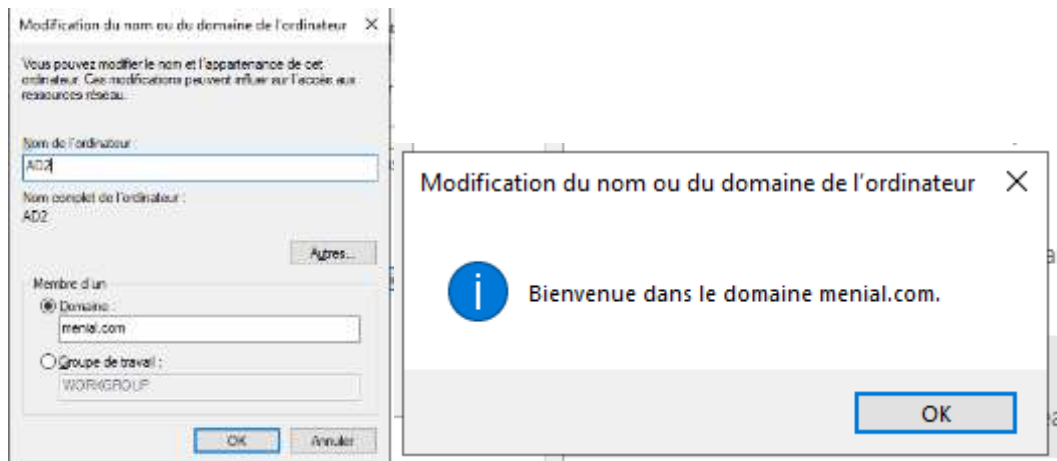
☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 20 . 116

Serveur DNS auxiliaire : . . .

Cloné ou recrée un Windows Serveur AD 2, ajouter les fonctions de l'AD, Changer de Nom de l'ordinateur et ajouter le même domaine que l'AD1,

Ici « menial.com » :



Nous pouvons remarquer que mon AD1 et mon AD2 peuvent se ping sans problème :

AD1 :

AD2 :

```
C:\Users\Administrateur>ping 192.168.20.174

Envoi d'une requête 'Ping' 192.168.20.174 avec 32 octets de données :
Réponse de 192.168.20.174 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.20.174 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.20.174 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.20.174 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.20.174:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\Administrateur>hostname
AD1
```

```
C:\Users\Administrateur>ping 192.168.20.116

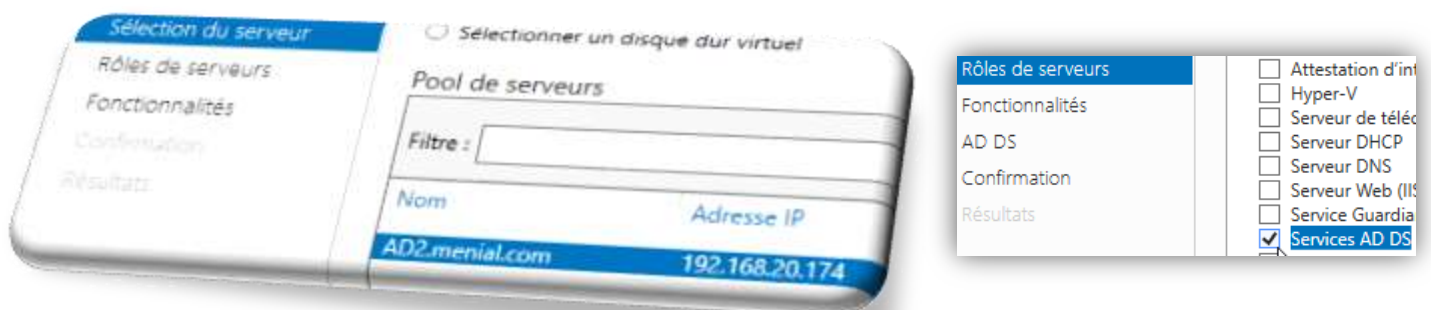
Envoi d'une requête 'Ping' 192.168.20.116 avec 32 octets de données :
Réponse de 192.168.20.116 : octets=32 temps<1ms TTL=128
Réponse de 192.168.20.116 : octets=32 temps<1ms TTL=128
Réponse de 192.168.20.116 : octets=32 temps<1ms TTL=128
Réponse de 192.168.20.116 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.20.116:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Administrateur>hostname
AD2
```

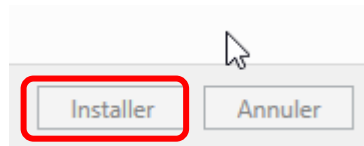
Installez le rôle AD DS sur AD2 :

Rendez vous dans « Ajouter des rôles et fonctionnalités »,



Ajout du rôle de services AD DS

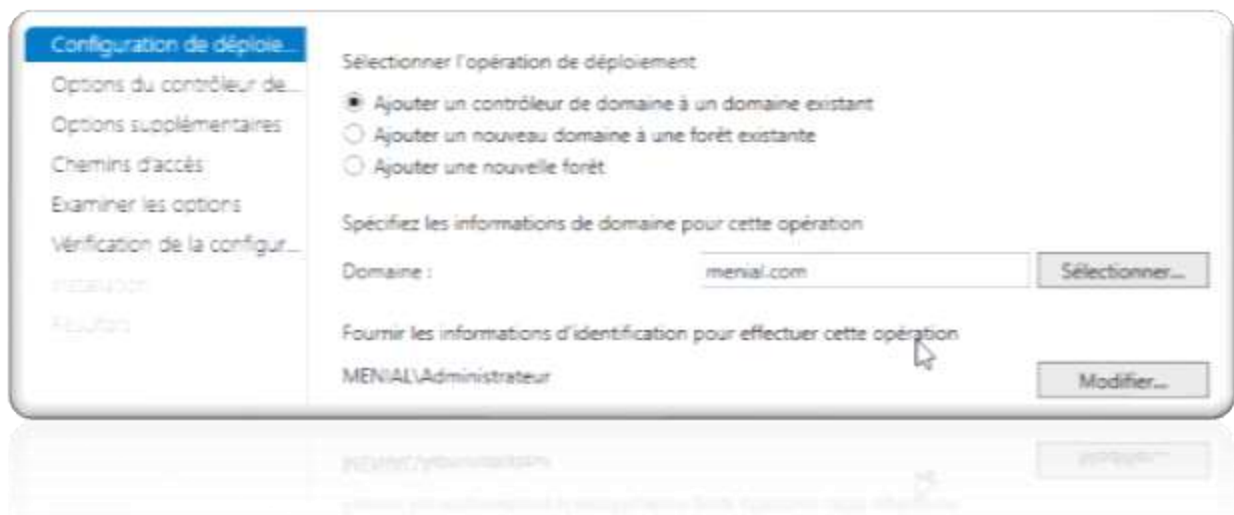
Puis installer :



## Configuration de déploiement :

Cliquez sur promouvoir ce serveur en contrôleur de domaine.

La différence se fait à la configuration du déploiement où vous devrez sélectionner "ajouter un contrôleur de domaine à un domaine existant", ensuite renseignez le nom de domaine.



Ajouter un mot de passe fort :

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

Revenez au mot de passe :

Continuer en faisant « Suivant » jusqu'à pour cliquer sur « Installer » :



Le serveur de l'AD2 est bien reconnu par l'AD1, nous pouvons vérifier ceci dans l'AD1  
Gestionnaire de serveur,

Puis « Outils » et « Utilisateurs et ordinateurs Active Directory » :

Vous pouvez retrouver AD2 connecter dans le Domain Controllers de l'AD1

Utilisateurs et ordinateurs Active Directory	Nom	Type	Type de contrôleur	Site
Requêtes enregistrées	AD1	Ordinateur	GC	Default-First-Si...
menial.com	AD2	Ordinateur	GC	Default-First-Si...
Builtin				
Computers				
Domain Controllers				

### 3) Intégrez la machine dans le domaine :

#### a) Préparation du client :

Adresse Client,

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

```
Suffixe DNS propre à la connexion. . . . : fe80::559a:b741:97fa:863c%6
Adresse IPv6 de liaison locale. . . . . : fe80::559a:b741:97fa:863c%6
Adresse IPv4. . . . . : 192.168.20.140
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
```

Client Ping AD1

```
C:\Users\Client>ping 192.168.20.116

Envoi d'une requête 'Ping' 192.168.20.116 avec 32 octets de données :
Réponse de 192.168.20.116 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.20.116 : octets=32 temps=1 ms TTL=128
```

Client Ping AD2

```
C:\Users\Client>ping 192.168.20.174

Envoi d'une requête 'Ping' 192.168.20.174 avec 32 octets de données :
Réponse de 192.168.20.174 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.20.174 : octets=32 temps=1 ms TTL=128
```

#### 4) Manipulation des 2 AD :

Retrouvez-vous les utilisateurs et UO que vous avez créés dans l'AD1 sur votre AD2 ? Que concluez-vous ?

Je retrouve bien dans mon AD2 les utilisateurs  
Que j'ai créé précédemment dans l'AD1  
La réplication Active Directory est correctement  
Configurée et fonctionne correctement.

Utilisateurs et ordinateurs Active	Nom	Type
Requêtes enregistrées		
menial.com		
> Built-in		
> Computers		
> Domain Controllers		
> ForeignSecurityPrincipal:		
> Managed Service Accour		
UOSISR	Laurent	Utilisateur
UOSLAM	Paul	Utilisateur
	Sebastien	Utilisateur

Débranchez la carte réseau de votre AD1 : votre poste client peut-il se connecter à votre domaine ? Que concluez-vous ?

- Oui il peut se connecter à mon Domaine, l'AD2 a pris le relais.

Rebranchez la carte réseau de votre AD1

Créez un utilisateur nommé billy sur votre AD2.

Débranchez la carte réseau de votre AD2 : billy peut-il se connecter à votre domaine ? Que concluez-vous ?

- Oui car AD1 prends les même configuration que AD2 donc si AD2 tombe AD1 prends le relais vis versa.

Rebranchez la carte réseau de votre AD2

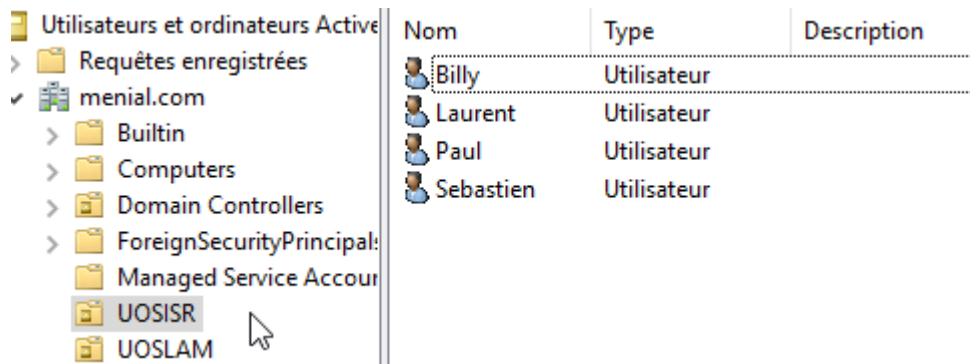
Créez sur une partition D un dossier nommé pour billy où Billy a tous les droits et où les autres ont un droit de lecture.

Débranchez la carte réseau de votre AD2 : Billy peut-il accéder à son dossier ?

Que concluez-vous ?

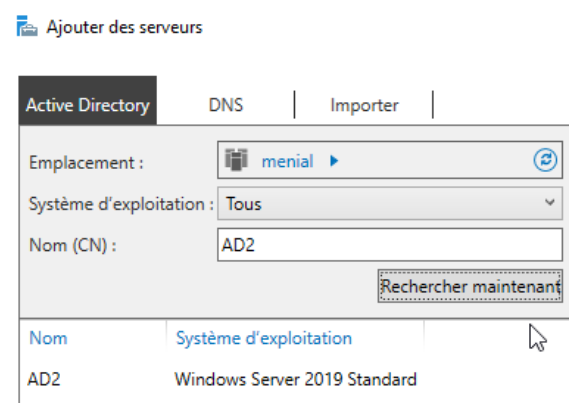
Non cela ne peut pas marcher, il faut utilisé la technique de DFSR pour que Billy puisse communiquer avec ça partition D :

Mettez Billy dans l'UOSISR

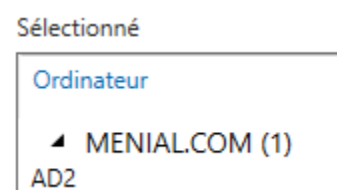


## Créer votre pool de serveurs :

Rendez-vous dans le « Gestionnaire de serveur » et  
« Tous les serveurs », cliquer droit sur « Tous les serveurs »  
Et « Ajouter des serveurs » et ajouter votre AD2  
Dans la liste de serveurs de l'AD1.



Une fois avoir ajouter AD2 vérifier bien qu'il soit bien  
sélectionné a votre droite, puis « OK ».



Filtrer			
Nom du serveur	Adresse IPv4	Facilité de gestion	
AD1	192.168.20.116	En ligne	Compteurs de performances non démarré
AD2	192.168.20.174	En ligne	Compteurs de performances non démarré

Vérifier que sur vos deux AD l'espaces et Noms et la Réplication DFS soient cocher dans « Rôles et fonctionnalités ».

Sélection du serveur  
**Rôles de serveurs**  
Fonctionnalités  
Confirmation  
Résultats

☐ Services d'activation en volume  
☐ Services d'impression et de nu  
☐ Services de certificats Active D  
☐ Services de déploiement Wind  
☐ Services de fédération Active C  
☒ Services de fichiers et de stock  
☒ Services de fichiers et iSCSI  
☒ Serveur de fichiers (Inst  
☐ BranchCache pour fichi  
☐ Déduplication des donn  
☐ Dossiers de travail  
☒ Espaces de noms DFS  
☐ Fournisseur de stockag  
☐ Gestionnaire de ressou  
☒ Réplication DFS  
☐ Serveur cible iSCSI

i Installation de fonctionnalité  
Installation réussie sur AD2.menial.com.

Outils d'administration de serveur distant  
Outils d'administration de rôles  
Outils de services de fichiers  
Outils de gestion DFS  
Services de fichiers et de stockage  
Services de fichiers et iSCSI

Gérer Outils  
Défragmenter et optimiser les lecteurs  
Diagnostic de mémoire Windows  
DNS  
Domaines et approbations Active Directory  
Éditeur du Registre  
Gestion de l'impression  
Gestion de l'ordinateur  
Gestion des stratégies de groupe  
**Gestion du système de fichiers distribués DFS**

Faite « Outils »,

Puis « Gestion du système de fichiers distribués DFS

Nouvel espace de noms :



Le Nom de mon serveur est AD1

assistant Nouvel espace de noms

Serveur d'espaces de noms

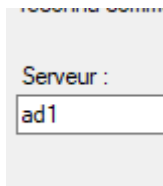
Étapes :  
Serveur d'espaces de noms  
Nom et paramètres de l'espace de noms  
Type d'espace de noms  
Sélectionnez un ordinateur  
Sélectionnez le type de cet objet :  
un ordinateur  
À partir de cet emplacement :  
menial.com  
Entrez le nom de l'objet à sélectionner (exemple)  
AD1

Entrez le nom du serveur reconnu comme le se  
Serveur :  
AD1

Avancé...

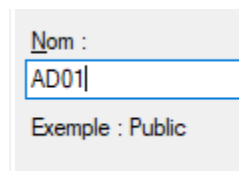


Faite suivant



Serveur :  
ad1

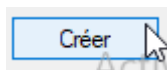
Suivant :



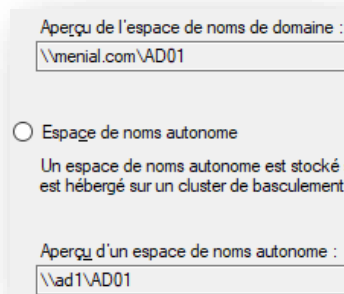
Nom :  
AD01  
Exemple : Public

Aperçu de l'espace de Noms :

Et « Créer »



Créer



Aperçu de l'espace de noms de domaine :  
\\menial.com\AD01

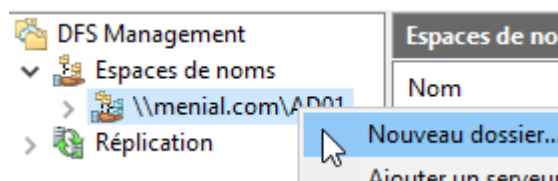
☐ Espace de noms autonome  
Un espace de noms autonome est stocké et est hébergé sur un cluster de basculement.

Aperçu d'un espace de noms autonome :  
\\ad1\AD01



Cliquer droit sur l'espaces de Noms,

Puis « Nouveau Dossier »



J'appelle mon Dossier « Partage » Je cible le dossier dans l'AD1 puis continuer :



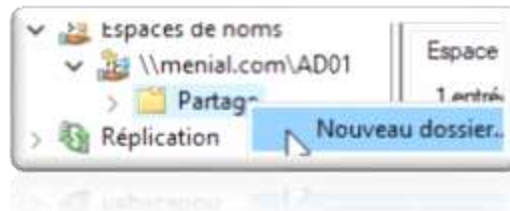
Nom :  
Partage

Aperçu de l'espace de noms :  
\\menial.com\AD01\Partage

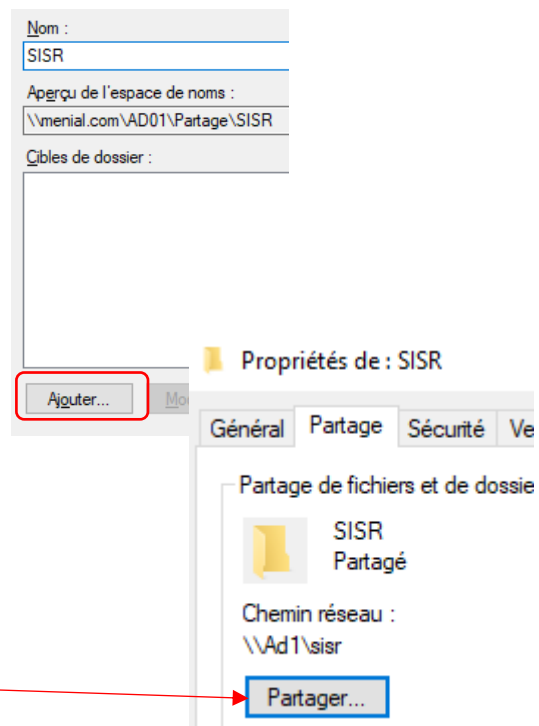
Cibles de dossier :

Ajouter... Supprimer... OK

Clique Droit sur le fichier de partage que nous venons de crée puis « Nouveau Dossier »

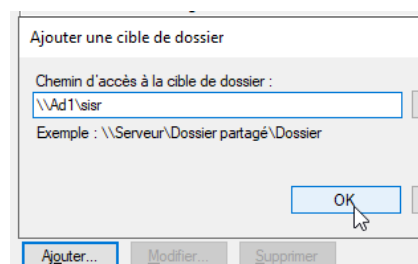


Je nomme mon fichier « SISR »,  
Puis cliquer sur « Ajouter »

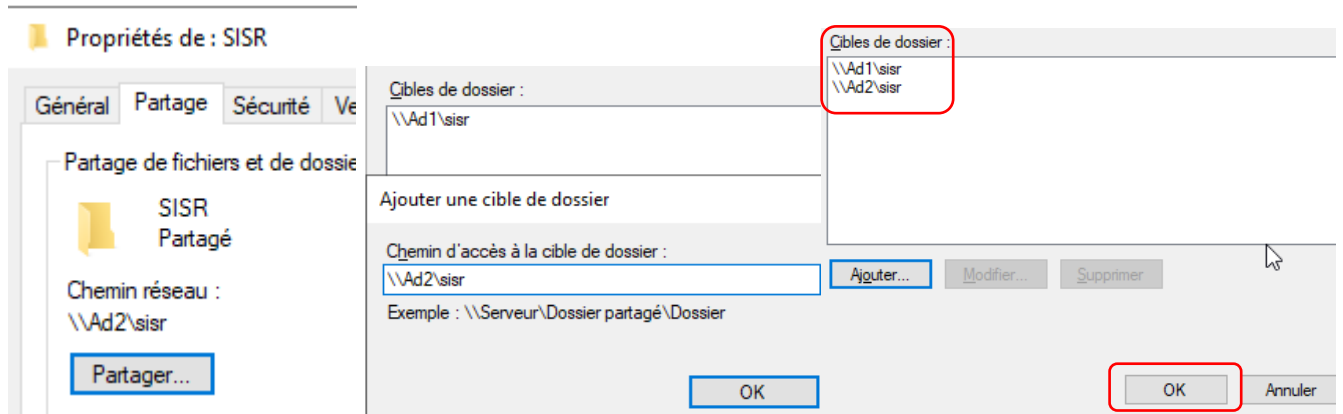


Rendez-vous dans les fichiers de votre AD1,  
Aller dans le Dossier SISR qui était déjà crée  
Au préalable dans l'AD ET l'AD2,  
Puis « propriété » et « partage »  
Copier le chemin réseau du fichier :

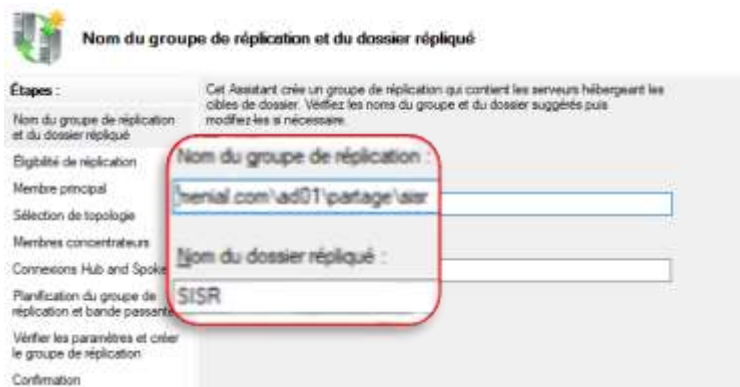
Ajouter le chemin d'accès que vous venez de copier,  
Puis faites « ok ».



Ajouter une deuxième cible « sirs » pour ajouter la réplication au dossier SIRS de AD2 :



## Création du Groupe de réplication :



On crée une planification :



Faites suivant jusqu'à arriver au choix du Membre principal :

Éligibilité de réplication

Membre principal

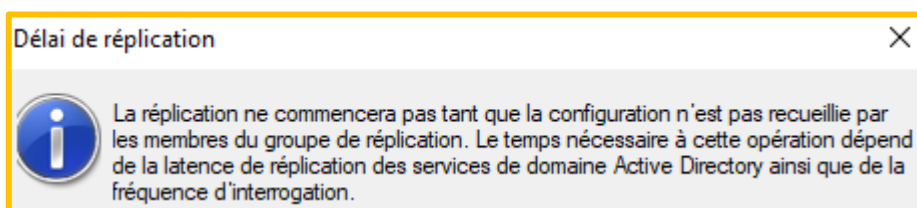
Sélection de topologie

Membre principal :

AD1



## Attention :

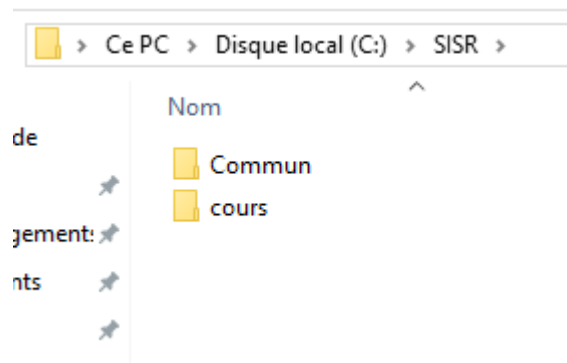


Ma réplication est bien active pour le Dossier SISR dans AD1 et AD2.

<div> <div></div> <div>Réplication</div> </div> <div> <div>Domain System Volume</div> <div>menial.com\ad01\parta</div> </div>	État	Chemin d'accè...	Statut de l'appa...	Membre	Dossier répliqué	Quota intermé...
	Dossier répliqué : SISR (2 éléments)					
		C:\SISR	Activé	AD1	SISR	4,00 Go
		C:\SISR	Activé	AD2	SISR	4,00 Go

Pour vérifier la réplication DFSR je me rends dans le dossier SISR de mon AD2 et je vérifie que mes dossiers « SISR\Commun » et « SISR\Cours » sont bien dans mon AD2 :

Je trouve bien mes dossiers que j'avais créer dans l'AD1 sur mon « \\Ad2\SISR" » de l'AD2.



#### **4) Problème du serveur de temps :**

Dans les domaines Windows, c'est le contrôleur principal de domaine qui distribue l'heure aux clients. Si nous avons plusieurs serveurs, nous allons peut-être devoir les synchroniser.

Cela se fait via powershell : `w32tm /config /manualpeerlist : @IP du serveur PDC /syncfromflags: MANUAL`

Exemple : `w32tm /config /manualpeerlist :@192.168.20.90 /syncfromflags:MANUAL`

```
C:\Users\Administrateur>w32tm /config /manualpeerlist:@192.168.20.90 /syncfromflags:MANUAL
La commande s'est terminée correctement.
```

#### ***attention aux espaces***

Restart-Service w32time

*Explication de la commande :*

- W32tm pour la gestion du service de temps
- config
- manualpeerlist pour rentrer une liste de serveurs ntp sous la forme /« nomserveurntp,nomserveur2ntp » ou :peers pour connexion à un serveur de temps sur internet en fonction de la zone géographique ou @Ip du PDC
- syncfromflags permet de dire comment on synchronise :
  - MANUAL à partir de la liste
    - DOMHIER à partir du contrôleur de domaine
    - NO on synchronise pas !!