

Sommaire:

Les manipulations sont faites avant les parties questions:

Organisationnel:	2
Questions-organisationnel:.....	3
1- : Active directory	6
1.1 Gestion de droit et autorisations:.....	6
Questions-Gestions des droits et autorisations:.....	9
1.2 sauvegardes:.....	15
2-DHCP:	19
Question de cours-dhcp:.....	19
Questions-dhcp:.....	20
3 : IIS :INTRANET:	21
-Installation d'IIS sur le serveur Windows:.....	22
-création des sites html(notamment des index.html qu'on a écrit dans le bloc notes et que on convertira ensuite en html en changeant l'extension) :.....	22
- Configuration du site web avec IIS:.....	23
Questions-intranet:.....	25
Illustration Wireshark des questions précédentes:.....	26
4 : HTTP - NetCat:	27
Questions-et pratiques -netcat:.....	27
5 : DNS:	30
Questions-et-pratique dns:.....	30
Sitographie:	36

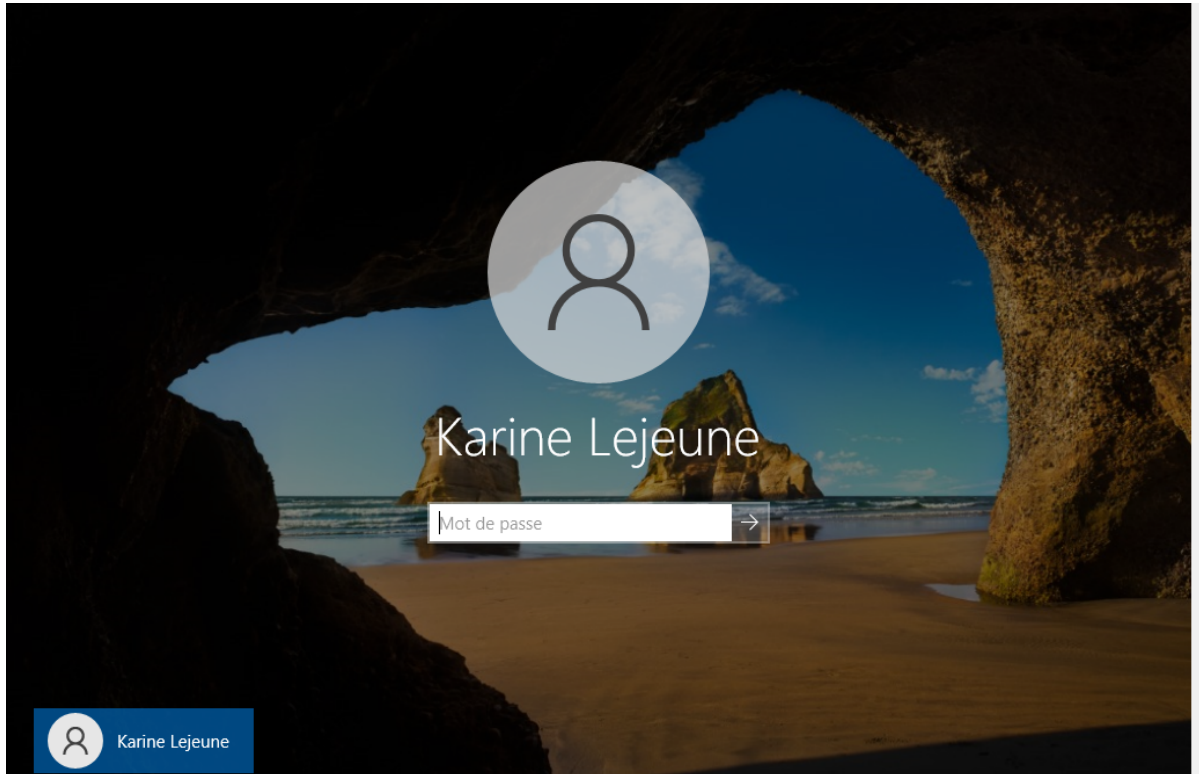
Organisationnel:

windows serveur 2019:



TP2 - Le réseau sous windows

Windows pro dont le domaine a été changé (en banconle.lan en raison de la forêt créée sur le serveur”



*Réduisons l'espace du C: de 50 Go à 25 Go pour créer de l'espace non alloué. Dès lors on crée une partition appelée **DONNEES** qui va nous permettre de gérer les partages.*

Volume	Disposition	Type	Système de ...	Statut	Capacité	Espace li...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	25,05 Go	8,08 Go	32 %
DONNEES (E:)	Simple	De base	NTFS	Sain (Parti...	24,41 Go	24,35 Go	100 %
Réservé au système	Simple	De base	NTFS	Sain (Systè...	549 Mo	133 Mo	24 %
SSS_X64FREE_FR-F...	Simple	De base	UDF	Sain (Parti...	5,29 Go	0 Mo	0 %

Questions-organisationnel:

1. Expliquez pourquoi les dossiers de partage ne se trouvent pas sur C:

La principale raison pour laquelle les dossiers de partage ne sont généralement pas situés sur la partition C:\(système) est liée à la gestion de l'espace disque et à la sécurité . En effet la partition C:\ est généralement réservée au système d'exploitation et aux programmes , et elle peut rapidement se remplir en raison des mises à jour du système , des applications installées. Donc placer les dossiers de partage sur la même partition pourrait entraîner une utilisation excessive de l'espace, affectant la stabilité du système. Donc stocker des données sur une partition distincte améliore la gestion de l'espace et protège les données contre une éventuelle corruption du système.

2. Quelles sont alors les solutions ?

Une bonne solution serait de déplacer les dossiers de partage vers une autre partition ou un autre lecteur qui dispose d'un espace de disque suffisant . Une autre solution serait de redimensionner la partition C:\ pour libérer l'espace en gérant correctement l'espace notamment la compression de fichiers.

3. Après avoir donné les divers groupes que l'on retrouve dans l'Active Directory, vous donnez la différence entre groupe et unité d'organisation ? Mettre en œuvre avec capture écran afin d'illustrer vos propos.

-liste des divers groupes:

Dans Active Directory, il existe différents types de groupes qui sont utilisés pour organiser et gérer des objets tels que des utilisateurs, des ordinateurs et d'autres groupes. Voici les principaux types de groupes dans Active Directory :

Groupes de Sécurité :

- Groupe de Sécurité Globale*
- Groupe de Sécurité Universel*
- Groupe de Sécurité Local*

Groupes de Distribution :

- Groupe de Distribution Globale*

TP2 - Le réseau sous windows





































- Groupe de Distribution Universel

Groupes Intégrés :

- Groupe Tout le Monde
- Groupe Utilisateurs Authentifiés
- Groupe Creator Owner
- Groupe Interactive
- Groupe Authentification sans Échec

Groupes Spéciaux :

- Groupe Administrateurs
- Groupe Utilisateurs
- Groupe Invités

	Accès comp...	Groupe de séc...	Un groupe de compati...
	Accès DCO...	Groupe de séc...	Les membres de ce grou...
	Administrat...	Groupe de séc...	Les membres du groupe...
	Administrat...	Groupe de séc...	Les membres de ce grou...
	Duplicateurs	Groupe de séc...	Prend en charge la répli...
	Générateurs ...	Les serveurs de ce groupe exécutent : e grou...	
	Groupe d'ac...	Groupe de séc...	Les membres de ce grou...
	IIS_IUSRS	Groupe de séc...	Groupe intégré utilisé pa...
	Invités	Groupe de séc...	Les membres du groupe...
	Lecteurs des...	Groupe de séc...	Des membres de ce gro...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres sont autor...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...
	Opérateurs ...	Groupe de séc...	Les membres peuvent a...
	Opérateurs ...	Groupe de séc...	Les membres de ce grou...
	Opérateurs ...	Groupe de séc...	Les membres du groupe...

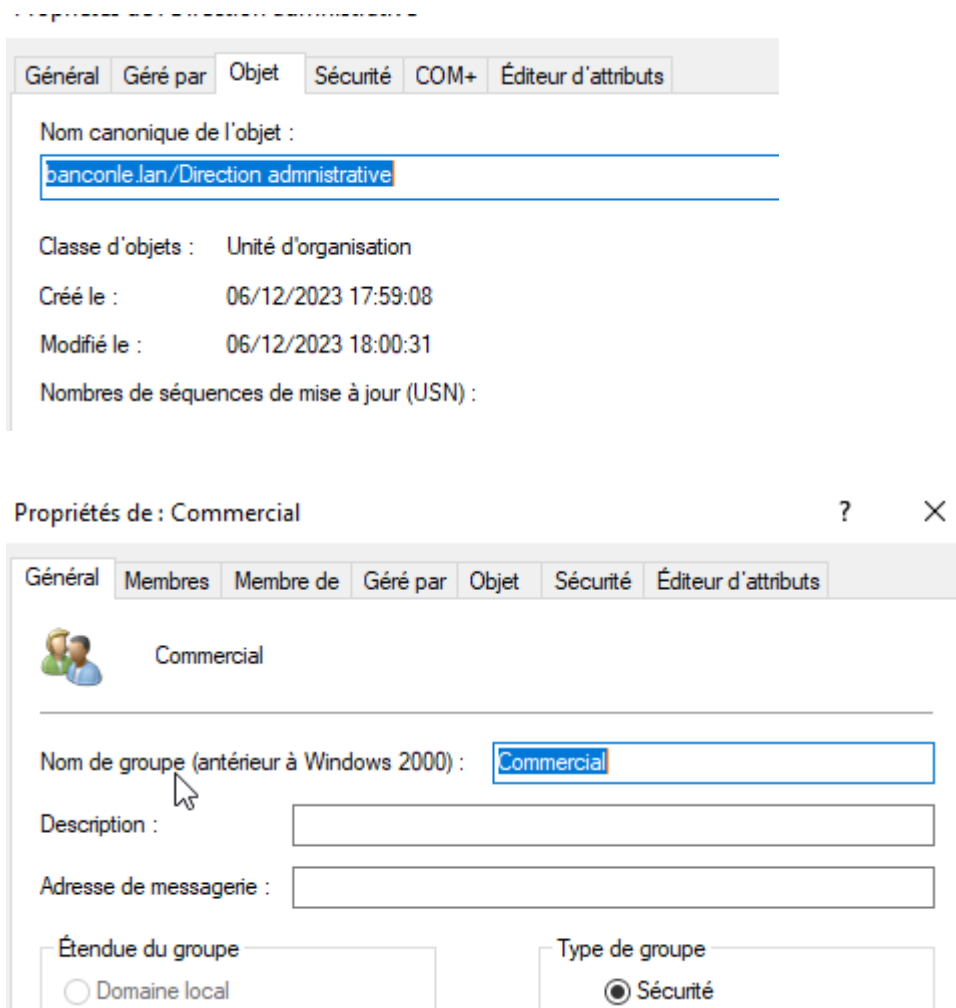
TP2 - Le réseau sous windows

Ces groupes jouent des rôles spécifiques dans la gestion des autorisations, des accès et des politiques de sécurité au sein de l'environnement Active Directory. Les administrateurs utilisent ces groupes pour simplifier la gestion des ressources et la délégation des autorisations.

-Différence entre groupe et unité d'organisation:

Un **groupe** dans Active Directory est une collection d'utilisateurs , d'ordinateurs ou d'autres groupes, utilisé pour simplifier l'administration et la gestion des autorisations. Donc elles peuvent être utilisés pour affecter des autorisations , simplifier la distribution tandis que une **unité d'organisation** est une subdivision dans la structure d'Active directory. Elle est utilisée pour organiser les utilisateurs, les groupes , les ordinateurs de manière logique

Captures de différences (propriétés):

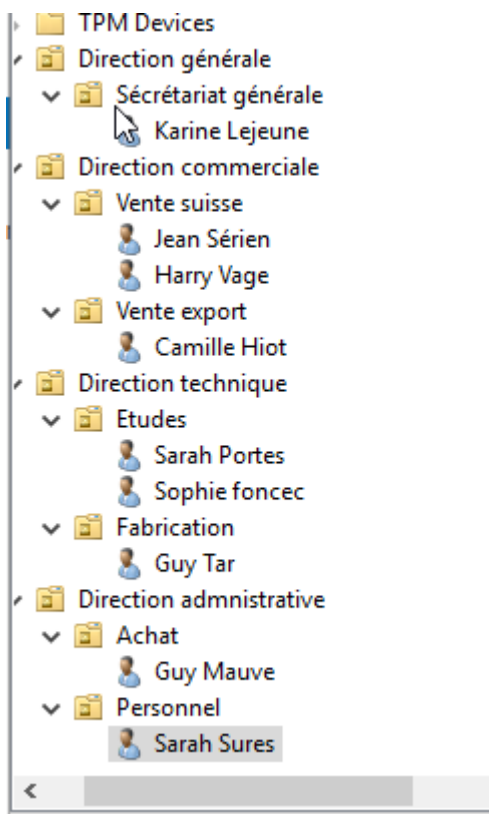


1- : Active directory

1.1 Gestion de droit et autorisations:

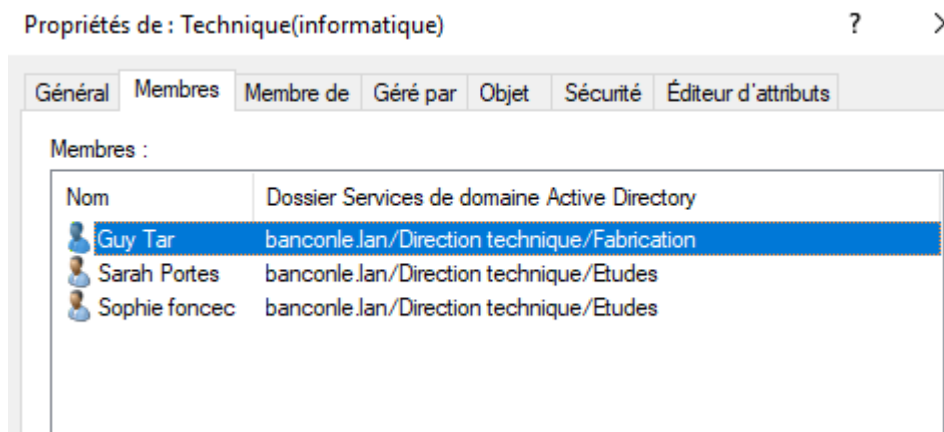
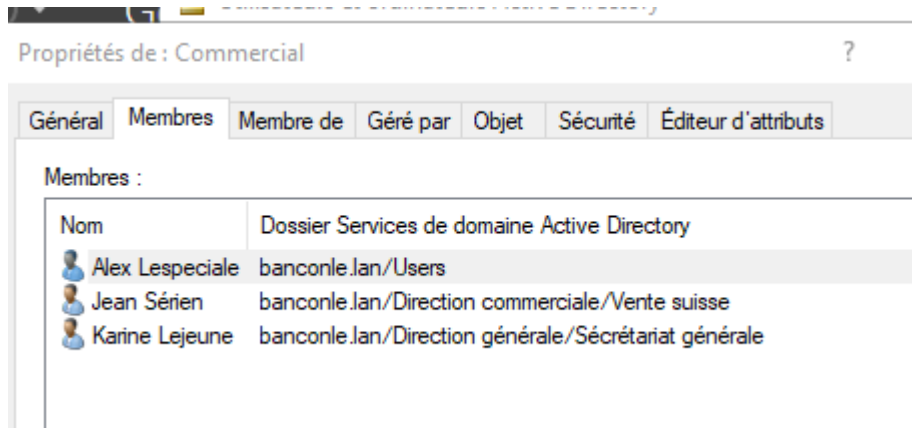
-Captures de l'organisationnel mis en place tant les UOs que les groupes selon les exigences données:

–Unités d'organisations:



















TP2 - Le réseau sous windows

-Groupes:








TP2 - Le réseau sous windows

Liste des dossiers personnels et communs créés:

nom	modifié le	type	taille
 D_commun_Achat	06/12/2023 15:16	Dossier de fichiers	
 D_commun_Etudes	06/12/2023 15:14	Dossier de fichiers	
 D_commun_Fabrication	06/12/2023 15:14	Dossier de fichiers	
 D_commun_Personnel	06/12/2023 15:16	Dossier de fichiers	
 D_commun_Secretariat_general	06/12/2023 15:13	Dossier de fichiers	
 D_commun_Vente export	06/12/2023 15:16	Dossier de fichiers	
 D_commun_Vente suisse	06/12/2023 15:17	Dossier de fichiers	
 D_perso_KLejeune	06/12/2023 18:35	Dossier de fichiers	
 D_perso_JSérien	06/12/2023 18:36	Dossier de fichiers	
 D_perso_HVage	06/12/2023 18:36	Dossier de fichiers	
 D_perso_CHiot	06/12/2023 18:36	Dossier de fichiers	
 D_perso_SPortes	06/12/2023 18:36	Dossier de fichiers	
 D_perso_Sfoncec	06/12/2023 18:37	Dossier de fichiers	
 D_perso_Gtar	06/12/2023 18:37	Dossier de fichiers	
 D_perso_Gmauve	06/12/2023 18:37	Dossier de fichiers	
 D_perso_SSures	06/12/2023 18:37	Dossier de fichiers	

Tous les droits ont également attribués , par exemple celui de Harry Vage dans son groupe est:

 Harry Vage (HVage@banconle.lan)
 Système
 Jean Sérien (JSérien@banconle.lan)
 Administrateurs (BANCONLE\Administrateurs)
 Utilisateurs (BANCONLE\Utilisateurs)

utorisations pour Harry Vage	Autoriser	Refuser
Lecture et exécution	<input type="checkbox"/>	<input type="checkbox"/>
Affichage du contenu du dossier	<input type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Écriture	<input type="checkbox"/>	<input type="checkbox"/>
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>

Questions-Gestions des droits et autorisations:

1-Donnez la différence entre contrôle total et cocher tous les droits.

Le contrôle total accorde tous les droits possibles sur un dossier, tandis que cocher tous les droits nécessite de spécifier individuellement les droits à attribuer

2-Donnez la différence entre contrôle total et cocher tous les droits.

L'héritage des droits NTFS est un mécanisme qui permet à un dossier ou à un fichier de recevoir automatiquement les autorisations de son dossier parent. Par défaut, les nouveaux objets héritent des autorisations du dossier parent. Si on modifie les autorisations sur un dossier parent, ces modifications peuvent être automatiquement appliquées aux objets enfants.

Lorsqu'on active l'héritage sur un dossier, les autorisations définies sur ce dossier sont transmises aux objets enfants.

3-Expliquez les différences entre les groupes (universel et local...). Quel groupe devons nous prendre ici (justifiez)?

-Les groupes locaux sont spécifiques à un ordinateur, utilisés pour définir des autorisations locales.

Les groupes globaux sont utilisés à l'échelle d'un domaine AD pour organiser des utilisateurs avec des besoins similaires.

-Les groupes universels offrent une portabilité globale à travers la forêt AD pour des besoins d'accès entre plusieurs domaines.

Dans notre cas, on choisira un groupe global car on ne gère que des utilisateurs de notre domaine(banconle.lan) qui ont besoin d'accéder à des ressources partagées.

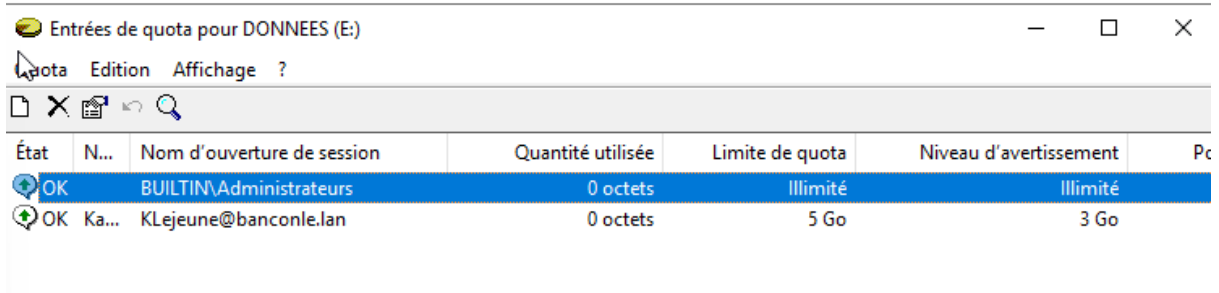
4. Expliquez les quotas NTFS (mettre en place un quota pour un utilisateur)

Les quotas NTFS (New Technology File System) sont des fonctionnalités permettant de définir des limites d'utilisation de l'espace disque pour des utilisateurs ou des groupes spécifiques sur un volume NTFS. Cela permet de contrôler la quantité d'espace disque qu'un utilisateur peut consommer,

TP2 - Le réseau sous windows

prévenant ainsi l'utilisation excessive et garantissant une gestion efficace des ressources de stockage.

Définissons donc par exemple un quota à **Karine Lejeune** de 5 Go et un avertissement lorsqu'elle aura atteint les 3Go.



État	N...	Nom d'ouverture de session	Quantité utilisée	Limite de quota	Niveau d'avertissement	Pc
OK		BUILTIN\Administrateurs	0 octets	Illimité	Illimité	
OK	Ka...	KLejeune@banconle.lan	0 octets	5 Go	3 Go	

5-Après avoir énoncé les différences, expliquez l'intérêt des profils dans l'organisation Mettre en place un profil itinérant pour Jean et obligatoire pour Camille.

Un profil obligatoire est un modèle de profil utilisateur que chaque utilisateur reçoit lors de sa connexion, mais toute modification apportée par l'utilisateur n'est pas enregistrée entre les sessions. Cela signifie que toutes les modifications apportées par l'utilisateur pendant sa session sont ignorées lorsqu'il se déconnecte. Les profils obligatoires sont généralement utilisés dans des environnements où une configuration standardisée et immuable est nécessaire. Ce type de profil est souvent utilisé pour garantir que chaque utilisateur bénéficie d'une expérience identique et sécurisée.

Un profil itinérant, en revanche, est un profil utilisateur qui est stocké sur un serveur réseau et est accessible depuis n'importe quel ordinateur sur le réseau. Lorsqu'un utilisateur se connecte à n'importe quelle machine, il retrouve son environnement de bureau, ses paramètres et ses fichiers personnels. Les modifications apportées par l'utilisateur sont enregistrées sur le serveur, garantissant une cohérence d'expérience utilisateur d'un poste de travail à l'autre. Les profils itinérants sont particulièrement utiles pour les utilisateurs qui se déplacent fréquemment entre différents ordinateurs au sein d'une organisation.

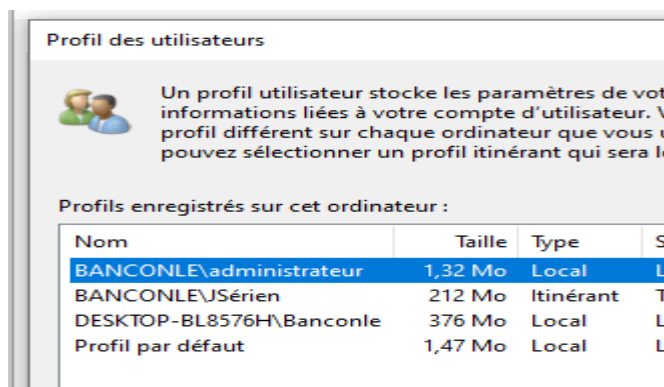
TP2 - Le réseau sous windows

La mise en place d'un profil assure une expérience utilisateur cohérente et flexible d'un ordinateur à l'autre. En effet il simplifie principalement la gestion en imposant des configurations standardisées pour renforcer la sécurité et faciliter l'administration des utilisateurs.

-Mise en place du profil itinérant pour Jean sérien:

Pour ce faire , on va mettre en tant que chemin du profil ,le chemin du dossier personnel de Jean vu qu'il a tous les droits la dessus et le partager . Puis on vérifiera dans les profils de l'ordinateur , les différents types.

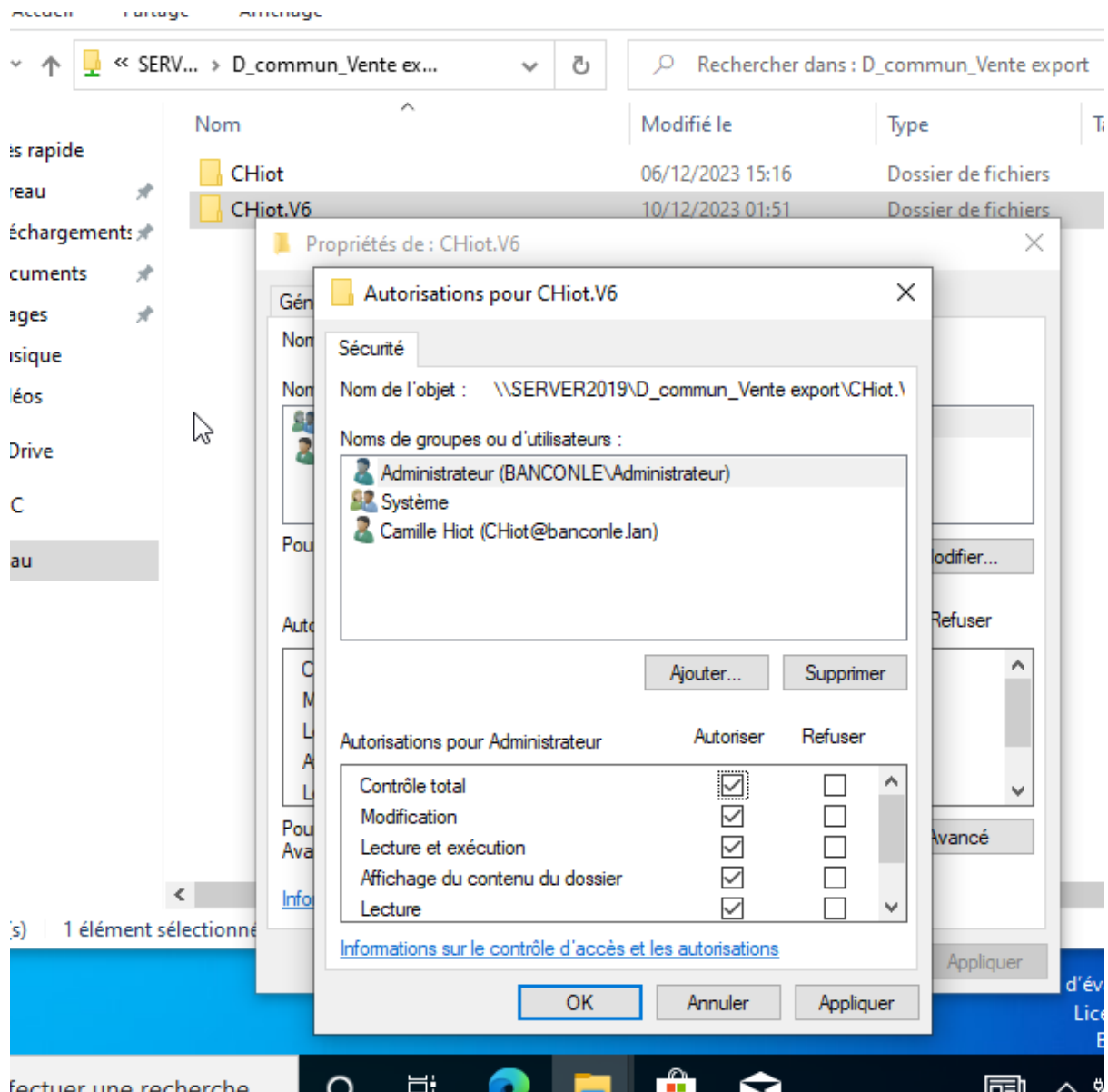
Ainsi on a:



-Profil obligatoire pour camille:

Pour Camille Hiot , on fera pareil mais le changement se fera au niveau du changement d'extension de DAT en MAN d'un fichier NTuser , pour ainsi créer un profil obligatoire pour Camille et fixer ses connexions exclusivement à ce PC. En effet on va d'abord partager le dossier commun vente_export par exemple , puis ajouter le chemin CNU dans le chemin profil de Camille. Ainsi quand on se connecte avec le compte de camille on remarque un dossier CHiot.V6 qui n'est accessible que par elle . Donc on accède à ses propriétés pour donner un contrôle total à l'administrateur(notre serveur) pour enfin pouvoir modifier l'extension de NTuser de DAT à MAN ,ce qui rendra le profil de Camille obligatoire :

TP2 - Le réseau sous windows



Ainsi le on a le profil de camille qui désormais obligatoire:

TP2 - Le réseau sous windows

Profils enregistrés sur cet ordinateur :

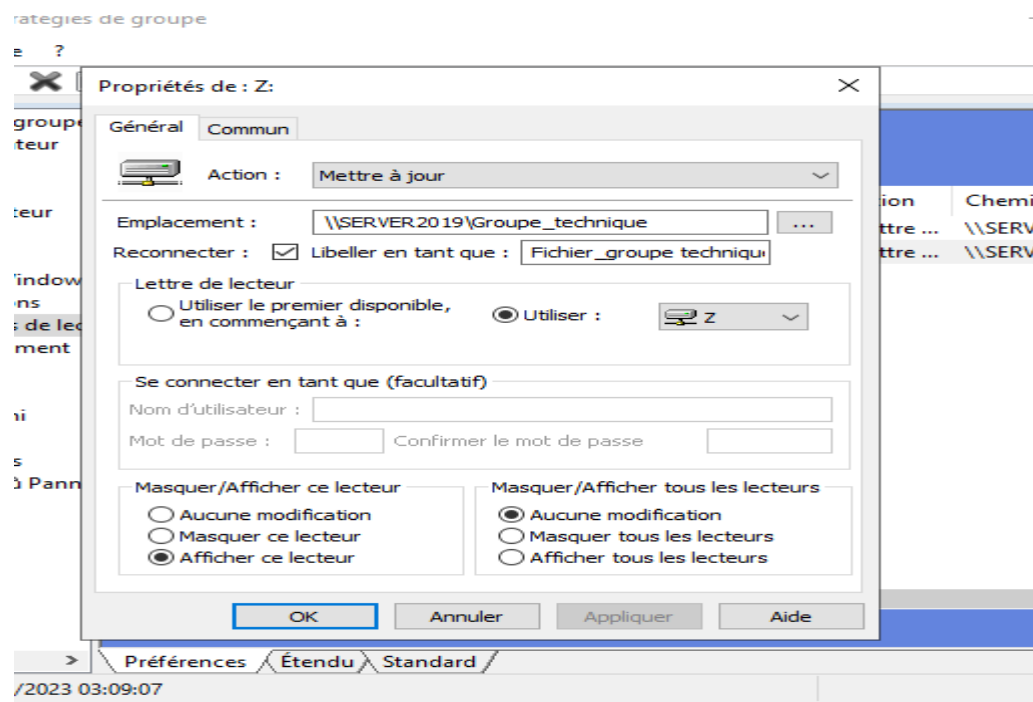
Nom	Taille	Type	Statut	Mod...
BANCONLE\Administrateur	1,36 Mo	Local	Local	10/1...
BANCONLE\CHiot	3,02 Mo	Obligat...	Obligat...	10/1...
DESKTOP-BL8576H\Banconle	376 Mo	Local	Local	10/1...
Profil par défaut	1,47 Mo	Local	Local	06/1...

Modifier le type... Supprimer Copier dans

Pour faciliter l'accès à son dossier personnel et au dossier(s) du groupe (Comptabilité et Informatique), l'utilisateur se verra monter un lecteur réseau J:\ et Z:\ au démarrage de sa session. Montrez l'intérêt de travailler dans un domaine et d'utiliser une session utilisateur:

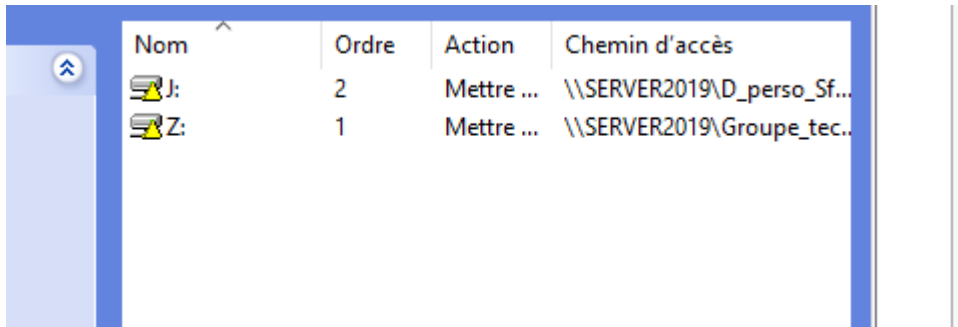
Vu qu'on a un groupe informatique, on pourra faire un partage de dossier à tout le groupe en même temps, ce qui reflète d'ailleurs l'intérêt des groupes.

La méthode sera de créer un GPO:



TP2 - Le réseau sous windows

On fait de même pour le lecteur J pour un dossier personnel (de Sophie par exemple) et on a ceci:



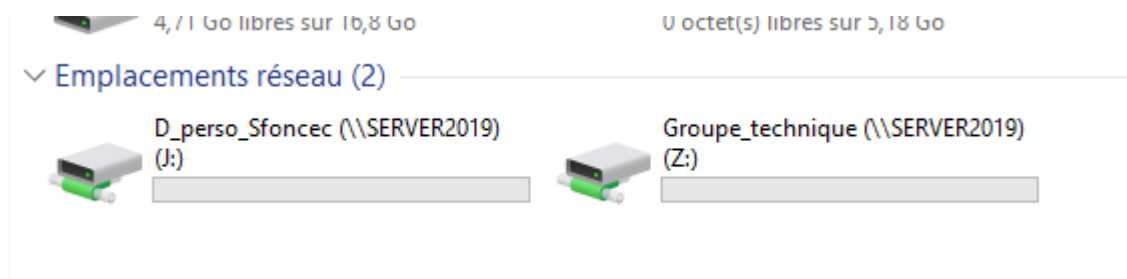
Nom	Ordre	Action	Chemin d'accès
J:	2	Mettre ...	\\SERVER2019\D_perso_Sf...
Z:	1	Mettre ...	\\SERVER2019\Groupe_tec..

Dès lors s'assure que tout soit appliqué avec la commande `gpupdate/force`

```
C:\Users\Administrateur>gpupdate/force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
```

Et on peut remarquer tout s'est bien passé:



Intérêt de Travailler dans un Domaine avec une Session Utilisateur :

TP2 - Le réseau sous windows

Les sessions utilisateur dans un domaine permettent une gestion centralisée des droits d'accès et des politiques de sécurité. En effet l'administration centralisée facilite la gestion des utilisateurs, des groupes et des ressources.

De plus les lecteurs réseau montés au démarrage de la session simplifient l'accès aux ressources partagées.

Travailler dans un domaine offre une infrastructure plus robuste, facilitant la gestion des utilisateurs, la mise en œuvre de politiques de sécurité et la fourniture d'un accès aux ressources partagées de manière plus efficace. Utiliser des sessions utilisateur et des profils adaptés améliore l'expérience et la sécurité des utilisateurs.

1.2 sauvegardes:

Questions-sauvegardes:

a-)Ecrire un script qui permet de faire la sauvegarde sur le serveur

et b) Lancer le script à chaque fin de journée (fermeture de session):

Pour ce faire on va écrire un script de sauvegarde dans un fichier avec l'extension ps1 ensuite on va spécifier les dossiers communs puis les dossiers personnels à sauvegarder(on a préalablement créer deux dossiers , un qui contient tous les communs et un pour tous les personnels pour me faciliter la tâche) . On crée aussi un fichier sur le serveur indépendamment des fichiers de partage(DONNEES(E:)) de sauvegarde dont le chemin sera également utilisé dans le script

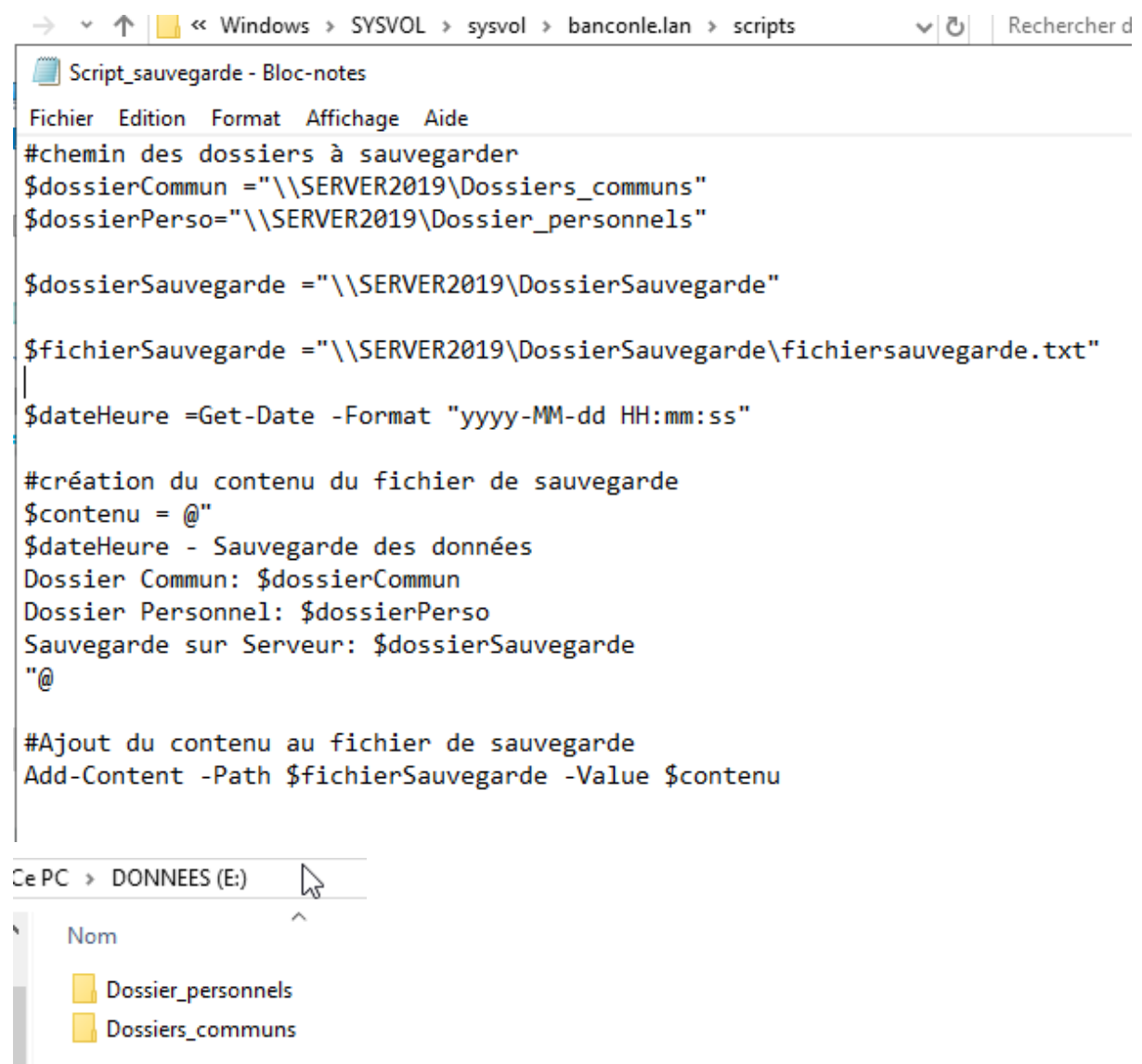
*Ensuite on crée un **GPO** pour déployer le script dans la section script située dans la partie configuration des ordinateurs (afin de permettre à tous les ordinateurs du domaine de lancer la sauvegarde en fin de*

TP2 - Le réseau sous windows

session vu que cette section propose de options qui sont "Ouverture de session" et "fermeture de session".

On s'assure que le script est accessible par les utilisateurs (via le partage réseau) et que les autorisations sont correctement configurées.

Enfin on forcera la mise à jour de la stratégie de groupe sur les ordinateurs clients en utilisant la commande ``gpupdate /force`` dans l'invite commandes.



```
Script_sauvegarde - Bloc-notes
Fichier Edition Format Affichage Aide
#chemin des dossiers à sauvegarder
$dossierCommun ="\\SERVER2019\Dossiers_communs"
$dossierPerso ="\\SERVER2019\Dossier_personnels"

$dossierSauvegarde ="\\SERVER2019\DossierSauvegarde"
$fichierSauvegarde ="\\SERVER2019\DossierSauvegarde\fichiersauvegarde.txt"

$dateHeure =Get-Date -Format "yyyy-MM-dd HH:mm:ss"

#création du contenu du fichier de sauvegarde
$contentu = @"
$dateHeure - Sauvegarde des données
Dossier Commun: $dossierCommun
Dossier Personnel: $dossierPerso
Sauvegarde sur Serveur: $dossierSauvegarde
"@

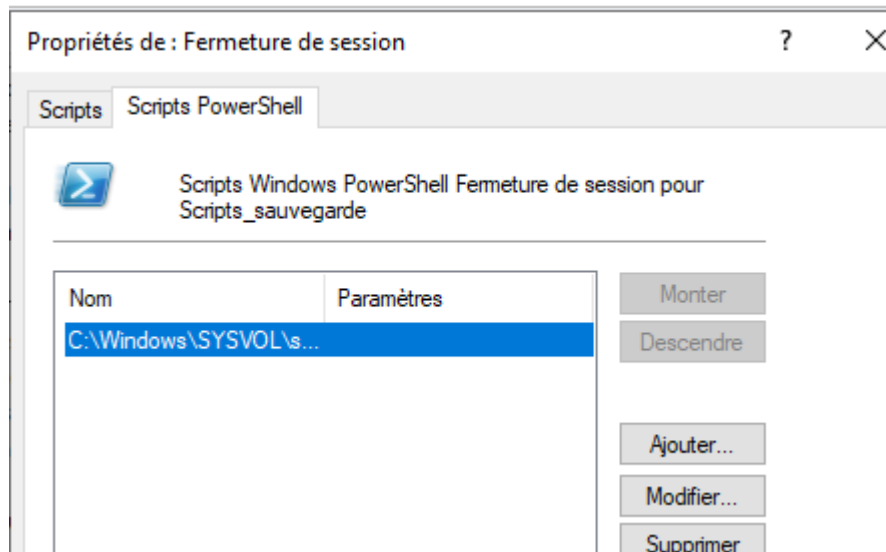
#Ajout du contenu au fichier de sauvegarde
Add-Content -Path $fichierSauvegarde -Value $contentu
```

Ce PC > DONNEES (E:)

Nom
Dossier_personnels
Dossiers_communs

Pour la fermeture de session , on a:

TP2 - Le réseau sous windows



3-Est ce que cette politique de sauvegarde est suffisante ?

La politique de sauvegarde mise en œuvre, consistant à sauvegarder les données sur le serveur à la fin de chaque journée, est une première étape importante vers la protection des données. Cependant, la suffisance de cette politique dépend de la nature critique des données, des exigences de reprise. Nous devrions évaluer régulièrement cette politique en tenant compte de la fréquence des sauvegardes, de la méthode de sauvegarde utilisée, de la facilité de restauration des données et des éventuelles exigences de conformité. Il pourrait être nécessaire d'ajuster la politique de sauvegarde en fonction de l'évolution des besoins de l'entreprise pour garantir une protection optimale des données et une reprise efficace en cas de perte.

2-DHCP:

Question de cours-dhcp:

1. Bail DHCP :

Un bail DHCP est la durée pendant laquelle une adresse IP est attribuée à un périphérique sur le réseau par le serveur DHCP. Pendant ce bail, le périphérique peut utiliser cette adresse IP pour communiquer sur le réseau. Une fois le bail expiré, le périphérique doit renouveler son bail pour continuer à utiliser la même adresse IP ou en obtenir une nouvelle.

2. Réservation DHCP :

Une réservation DHCP est une configuration spécifique dans laquelle le serveur DHCP attribue toujours la même adresse IP à un périphérique particulier. Cela garantit que le périphérique obtient toujours la même adresse IP lorsqu'il demande une adresse DHCP. Les réservations sont souvent utilisées pour les serveurs ou les périphériques nécessitant une adresse IP fixe.

3. Exclusion DHCP :

L'exclusion DHCP consiste à spécifier une plage d'adresses IP qui ne doit pas être attribuée par le serveur DHCP. Cela peut être utilisé pour exclure certaines adresses IP du pool DHCP, garantissant qu'elles restent disponibles pour des configurations spécifiques, telles que des serveurs réseau statiquement configurés. Les exclusions permettent d'éviter les conflits d'adresses IP entre les attributions statiques et dynamiques.

Questions-dhcp:

2.1 Expliquez pourquoi le poste informatique ne reçoit pas d'adresse DHCP ?

Le poste informatique du VLAN2 ne reçoit pas d'adresse DHCP car le serveur DHCP se trouve dans le VLAN1, et les requêtes DHCP ne sont pas routées entre les VLAN par défaut.

2.2 Expliquez en quoi la mise en œuvre d'un relais DHCP dans le VLAN2 peut remédier au problème ?

La mise en œuvre d'un relais DHCP dans le VLAN2 permettrait de résoudre le problème en redirigeant les requêtes DHCP vers le serveur DHCP du VLAN1. Le relais DHCP agit comme un intermédiaire pour transférer les requêtes DHCP entre les VLAN.

2.3 Afin de pouvoir répondre aux contraintes de sécurité de l'entreprise celle-ci vous demande de rédiger une note en expliquant les termes relatifs aux DHCP : Le poste de Karine possédera toujours la même adresse DHCP, le poste de Guy sera en IP fixe 192.168.1.3, l'adresse du serveur DHCP sera exclu en 192.168.1.15

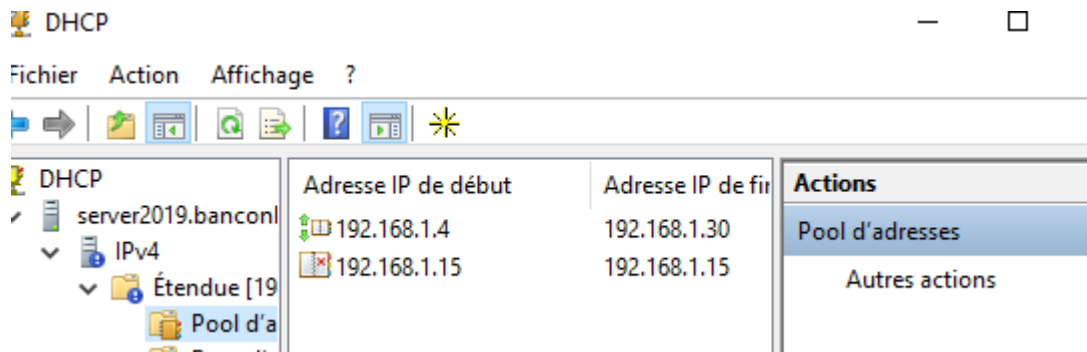
Pour éviter l'achat de matériel supplémentaire, il est possible de configurer l'interface du switch 3750 (qui sera un switch de niveau 3) dans le vlan2 avec l'instruction ip helper sur le serveur dhcp du vlan1 ainsi le switch fera office de relai DHCP et transmettra les requêtes au serveur DHCP du VLAN1.

2.4 Mettre en place le plan DHCP sans VLAN, montrez et expliquez la configuration du serveur

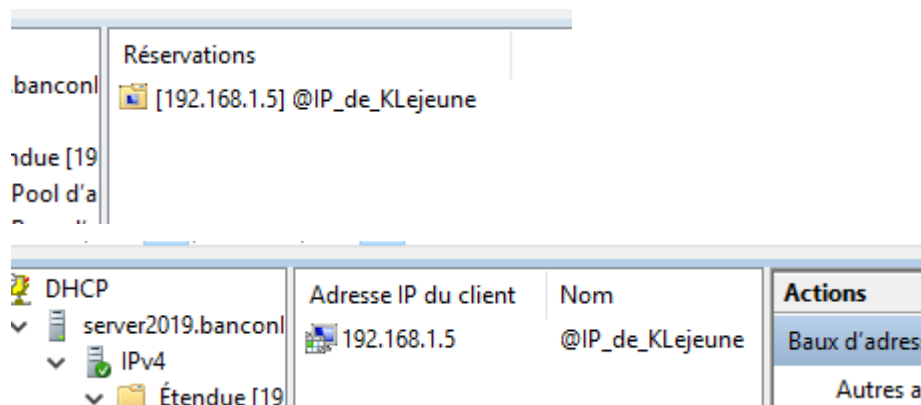
On installe le service DHCP dans notre gestionnaire de serveurs et on exécute respecte les notes de Karine Lejeune:

Définissons donc un pool entre 192.168.1.4 et 192.168.1.30 et une exclusion de l'adresse 192.168.1.15

TP2 - Le réseau sous windows



Ensuite on met une adresse en fixe à JEAN Sérien puis on fait une réservation pour karine le jeune (pour qu'elle puisse avoir la même adresse Ip tout le temps:



3 : IIS :INTRANET:

Pour mettre en place une autorité de certification sur votre serveur Windows et configurer un site web avec IIS en utilisant des certificats SSL, on suivra étape par étape:

TP2 - Le réseau sous windows

-Installation d'IIS sur le serveur Windows:

-création des sites html(notamment des index.html qu'on a écrit dans le bloc notes et que on convertira ensuite en html en changeant l'extension) :

1-<http://banconle.lan>

```
<html>
<head>
<title>
Banconle site
</title>
</head>
<body>
<h1>Hello banconle, travailles dur dans la vie</h1><form>
<input type="text" name="banconle">
<input type="submit" value="envoyer"></form>
</body>
</html>
```

2-<https://banconlesecurity.lan>:

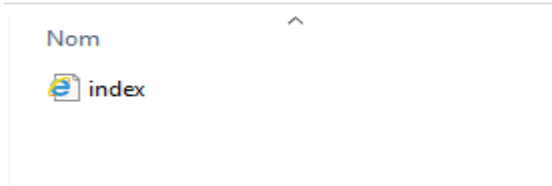
```
<html>
<head>
<title>
Banconle site
</title>
</head>
<body>
<h1>Bienvenue sur la page sécurisée</h1>

<form>
<input type="text" name="banconlesecu">
<input type="submit" value="envoyer"></form>
</body>
</html>
```

I

TP2 - Le réseau sous windows

PC > Bureau > banconle



- Configuration du site web avec IIS:

création des sites Pour le site HTTP et HTTPS(bien sur on mettra en place un certificat):



Certificats de serveur

Utilisez cette fonction pour demander et gérer les certificats servant au serveur Web pour accéder aux sites Web configurés pour le protocole SSL.

Filter :	Atteindre
Nom	Délivré à
Banconle	Server2019.banconle.lan

Nom du site :	Pool d'applications :	Sélectionner
Banconleauthentification	Banconleauthentification	

Répertoire de contenu

Chemin d'accès physique :
C:\Users\Administrateur\Desktop\banconleauthentificati ...

Authentification directe

Se connecter en tant que... Tester les paramètres...

Liaison

Type :	Adresse IP :	Port :
http	192.168.10.2	80

Nom de l'hôte :
www.Banconleauthentification.lan

Exemple : www.contoso.com ou marketing.contoso.com

TP2 - Le réseau sous windows

Nom du site : Pool d'applications :

Répertoire de contenu

Chemin d'accès physique :

Authentification directe

Liaison

Type : Adresse IP : Port :

Nom de l'hôte :

☐ Exiger l'indication de nom du serveur

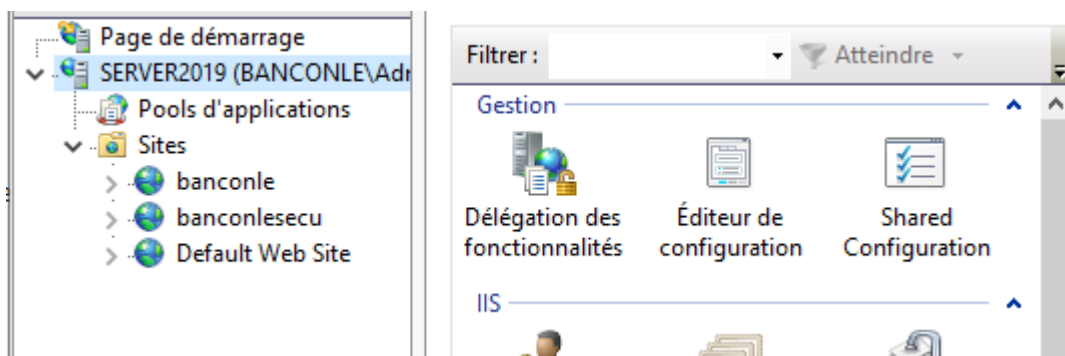
☐ Désactiver HTTP/2

☐ Désactiver l'association OCSP

Certificat SSL :

☒ Démarrez le site Web immédiatement

Ainsi on a :



TP2 - Le réseau sous windows

En consultant les pages , on a ceci :

-Page en http:



-page en https:



Questions-intranet:

1- Donnez la différence entre http et https, de quoi avons-nous besoin ?

-HTTP (Hypertext Transfer Protocol) :

C'est un protocole de communication utilisé pour le transfert de données sur le web.

AKOBI BANCONLE

L2-informatique

TP2 - Le réseau sous windows

Les données sont transmises en texte clair, ce qui signifie qu'elles ne sont pas chiffrées.

Vulnérable aux attaques de type interception où les données peuvent être capturées par des tiers.

HTTPS (Hypertext Transfer Protocol Secure) :

C'est une version sécurisée d'HTTP. Les données sont chiffrées à l'aide de protocoles tels que SSL ou TLS .De plus , il protège contre l'interception des données, assurant la confidentialité et l'intégrité des informations échangées.

2- de quoi avons-nous besoin pour une sécurisation par compte utilisateur windows ?

Pour sécuriser un compte utilisateur Windows, on a besoin de d'un mot de passe fort , une politique de groupe (s'applique des stratégies de sécurité via les politiques de groupe).

On pourrait aussi limiter l'accès aux ressources en fonction des besoins.

3- Expliquez l'intérêt de la mise en place d'un certificat ? Est-ce réellement sécurisé ?

Il permet d'authentifier le serveur web auprès du client et chiffrer les données échangées entre le client et le serveur.

Mais il n'est pas très très sécurisé car si la machine est compromise, l'autorité de certification peut également l'être , ce qui n'est pas donc très avantageux.

Illustration Wireshark des questions précédentes:

-Lors de l'authentification sans SSL, les informations d'identification peuvent être capturées en clair lors de la transmission.

Exemple :

TP2 - Le réseau sous windows

Entrons dans la barre de saisie du site http une phrase: "je suis présent", on constate que le message est présent en clair sur wireshark donc la sécurité n'est pas du tout garantie.

40	17.292381	:::1	:::1	DNS	82 Standard query response 0xa67c Server failure A www.bing.com
41	24.994773	192.168.10.2	192.168.10.2	HTTP	453 GET /?banconle=je+suis+present HTTP/1.1
42	24.995055	192.168.10.2	192.168.10.2	TCP	44 80 → 62377 [ACK] Seq=144 Ack=759 Win=2619136 Len=0
43	25.010512	192.168.10.2	192.168.10.2	HTTP	187 HTTP/1.1 304 Not Modified
44	25.010765	192.168.10.2	192.168.10.2	TCP	44 62377 → 80 [ACK] Seq=759 Ack=287 Win=261632 Len=0

-Par contre avec SSL/TLS, même si la capture est effectuée, les informations d'identification restent chiffrées, renforçant la sécurité de l'authentification.

9	0.010816	192.168.10.2	192.168.10.2	TCP	44 62501 → 443 [ACK] Seq=2 Ack=2 Win=1015 Len=0
10	0.011669	192.168.10.2	192.168.10.2	TLSv1.2	194 Server Hello, Change Cipher Spec, Encrypted Handshake Message
11	0.011977	192.168.10.2	192.168.10.2	TCP	44 62506 → 443 [ACK] Seq=228 Ack=151 Win=261888 Len=0
12	0.012434	192.168.10.2	192.168.10.2	TLSv1.2	95 Change Cipher Spec, Encrypted Handshake Message

4 : HTTP - NetCat:

Questions-et pratiques -netcat:

Nous allons ici installer netcat sur notre windows plutôt que télécharger kali linux. Ainsi pour vérifier que ça a réussi:

```
C:\Users\Administrateur>ncat --version
Ncat: Version 7.92 ( https://nmap.org/ncat )
C:\Users\Administrateur>
```

1. Expliquez la commande utilisée ci-dessous:

TP2 - Le réseau sous windows

```
root@kali:~# nc -v -w2 192.168.1.2 1-300
192.168.1.2: inverse host lookup failed: Unknown server error : Co
out
(UNKNOWN) [192.168.1.2] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.2] 135 (loc-srv) open
```

- nc: Commande pour lancer Netcat.
- -v: Mode verbeux, affiche plus d'informations pendant l'exécution.
- -w2: Délai d'attente de 2 secondes pour la connexion.
- 192.168.1.2: Adresse IP du serveur Windows.
- 1-300: Plage de ports à scanner, de 1 à 300 inclus.

2. Expliquez à quoi correspond les ports 'OPEN':

Les ports "OPEN" font référence aux ports qui sont actuellement ouverts et accessibles sur un système ou un réseau.

Un port ouvert signifie qu'il y a un service ou un programme en cours d'exécution sur le système distant et qu'il est prêt à accepter des connexions entrantes sur ce port spécifique. Ces connexions entrantes peuvent être utilisées pour échanger des données, exécuter des commandes, ou permettre l'accès à des services spécifiques.

2.1-Utiliser Netcat pour capturer les informations :

On exécute donc la commande ncat sur le serveur:

```
C:\Users\Administrateur>ncat -v -w2 192.168.10.2 443
ncat: Version 7.92 ( https://nmap.org/ncat )
ncat: Connected to 192.168.10.2:443.
```

2.2 Que se passe-t-il ?

TP2 - Le réseau sous windows

```
C:\Users\Administrateur>ncat -v -w2 192.168.10.2 443
ncat: Version 7.92 ( https://nmap.org/ncat )
ncat: Connected to 192.168.10.2:443.
```

Si un port est ouvert, Netcat peut établir une connexion à ce port. Il peut être utilisé pour envoyer des données au serveur et recevoir des données du serveur.

2.3 Expliquer rapidement quel service « tourne » derrière chaque port ouvert :

Pour déterminer quel service tourne derrière un port ouvert, vous va utiliser Nmap pour effectuer une analyse de service sur ces ports.

```
C:\Users\Administrateur>nmap -p 1-300 192.168.10.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-15 23:59 Paris, Madrid
Nmap scan report for 192.168.10.2
Host is up (0.0024s latency).
Not shown: 294 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
137/tcp   filtered netbios-ns
139/tcp   open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 14.70 seconds
```

Donc avec cette commande on voit que les ports 53,80,88,135,139 sont ouverts avec les services associés

5 : DNS:

**Modifier le fichier de votre client afin d'entrer facebook et d'accéder à la page <http://www.uphf.fr/>
Déterminons l'adresse de www.uphf.fr avec nslookup et ensuite exécutons la commande suivante .**

```
5 él 194.167.248.41 facebook.com|
192.168.10.2 www.jerome.ridet.free.fr
<
```

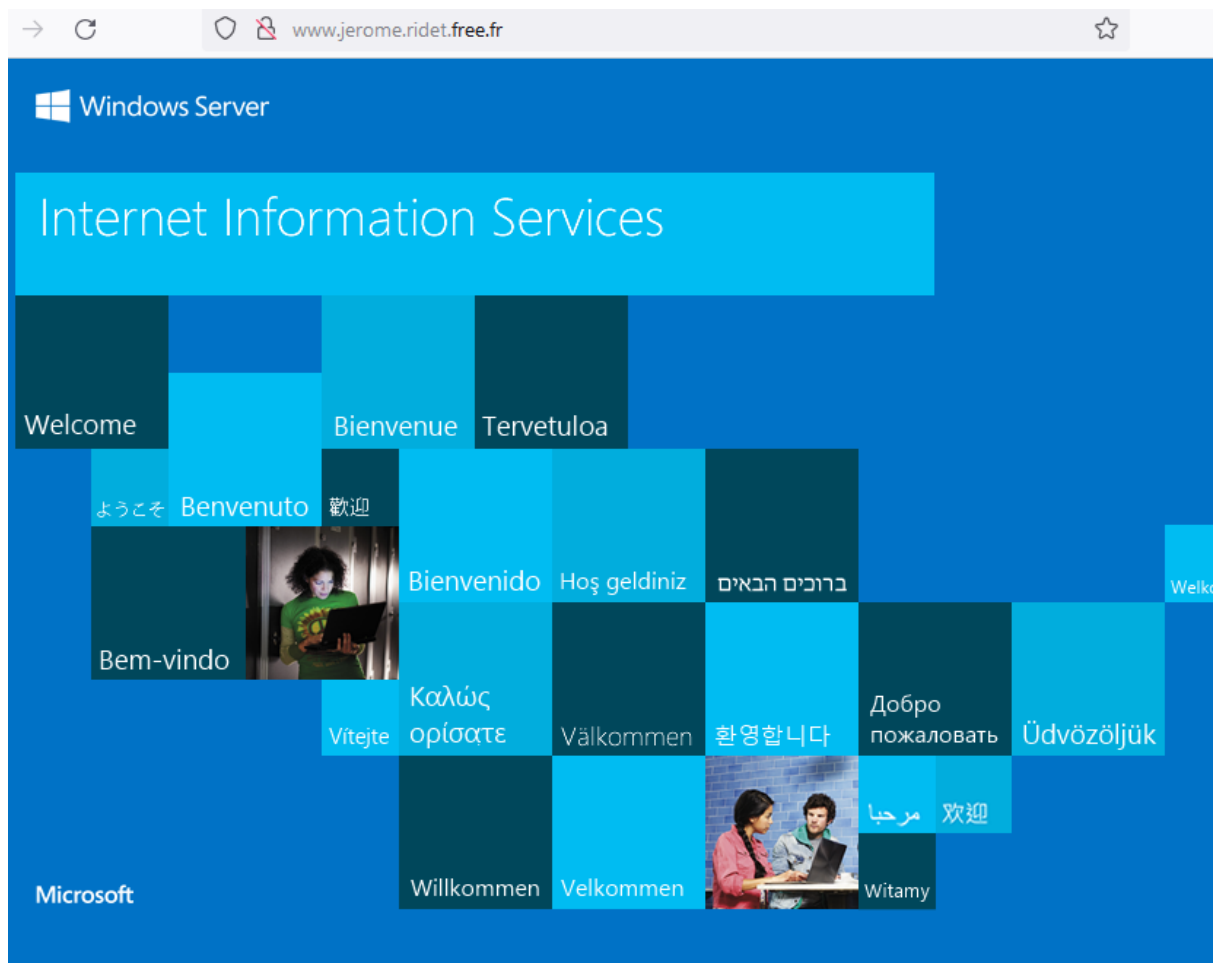
Imaginons que votre serveur Intranet possède l'adresse 192.168.1.10 Ajouter l'entrée 192.168.1.10 www.jerome.ridet.free.fr

Questions-et-pratique dns:

Que se passe t-il lorsque vous tapez www.jerome.ridet.free.fr dans chrome ?

TP2 - Le réseau sous windows

on a ceci 👍



A quoi sert la commande `ipconfig/displaydns` ? Faites une capture écran

La commande `ipconfig/displaydns` affiche le cache DNS local sur un système Windows, montrant les enregistrements DNS récemment résolus et leurs durées de vie. Cela permet de visualiser les informations DNS stockées localement, utile pour le dépannage réseau et la gestion des résolutions DNS.

TP2 - Le réseau sous windows

```
C:\Users\Administrateur>ipconfig /displaydns

Configuration IP de Windows

usbeketrica.com
-----
Échec du serveur de type A

www.jerome.ridet.free.fr
-----
Nom d'enregistrement. : www.jerome.ridet.free.fr
Type d'enregistrement : 1
Durée de vie . . . . : 589043
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 192.168.10.2

www.jerome.ridet.free.fr
-----
Aucun enregistrement de type AAAA
```

Que se passe t il avec la commande IPCONFIG /FLUSHDNS?

La commande `ipconfig /flushdns` permet de vider le cache DNS local sur un système Windows, supprimant ainsi toutes les entrées enregistrées. Cela peut être utile pour résoudre certains problèmes de résolution DNS en forçant le système à actualiser sa base de données DNS.

Expliquez rapidement la hiérarchie du DNS, Qu'est ce qu'un serveur qui fait autorité dans sa zone:

Le DNS fonctionne selon une hiérarchie composée de plusieurs niveaux. Au sommet, se trouvent les serveurs racines, qui dirigent les requêtes vers les serveurs de premier niveau (TLD, Top-Level Domain), tels que .com, .org, et ainsi de suite. Les serveurs de niveau supérieur

TP2 - Le réseau sous windows

renvoient ensuite vers les serveurs autoritaires gérant des domaines spécifiques.

Un serveur faisant autorité dans sa zone est responsable de la gestion des enregistrements DNS pour un domaine particulier. Il détient des informations actualisées concernant les noms de domaine sous sa responsabilité et répond directement aux requêtes DNS pour ces domaines, fournissant ainsi des informations fiables et à jour sur les adresses IP associées aux noms de domaine de sa zone.

5-2 Sécurisation d'un poste :

Imaginons que vous ne souhaitiez pas que les salariés de la société accèdent à live.fr <http://live.fr/> mais avec l'IP 127.0.0.1 -----> alors le site est interdit !

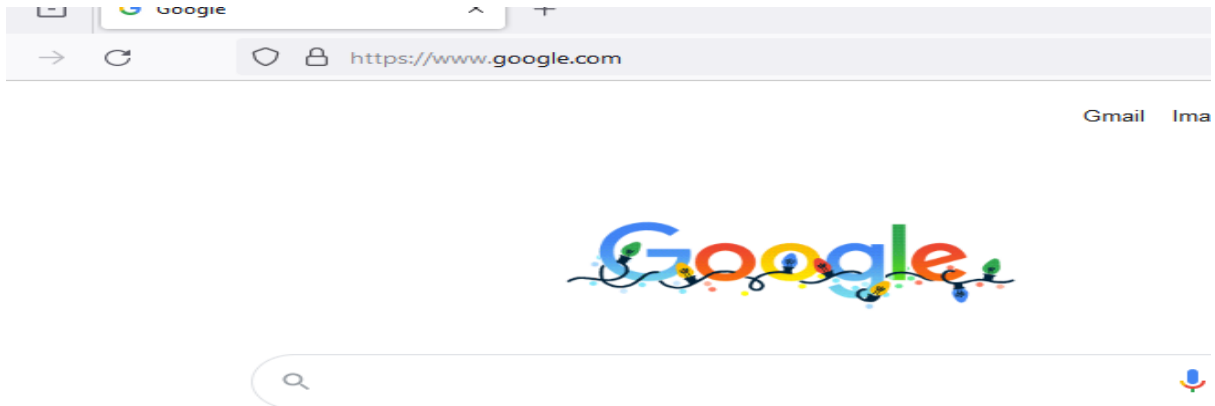
Faites la même manipulation avec google.fr ? que se passe t-il ?

Le site n'est plus accessible:



Faites la même manipulation avec google.com? que se passe t-il ?
Malgré le blocage , google.com fonctionne toujours .

TP2 - Le réseau sous windows



5.4 EXERCICE - Wireshark DNS

Installez un outil de capture de trames sur votre ordinateur (par exemple Wireshark), et lancez la capture.

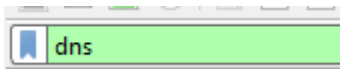
Videz votre cache local DNS.

```
C:\Users\Administrateur>ipconfig /flushdns  
Configuration IP de Windows  
Cache de résolution DNS vidé.
```

Lancez ensuite une résolution du FQDN www.jerome.ridet.free.fr

Que doit-on écrire dans la zone de texte Filter : pour n'obtenir que les requêtes DNS ?

On n'écrit juste "DNS " et le filtre sera fait.



Dans Wireshark, trouvez la ligne correspondant à la bonne requête (car il peut en apparaître plusieurs, en général la bonne est vers la fin), clic droit, Copy Summary (Text)

, A quelle adresse IP est associé le FQDN www.jerome.ridet.free.fr (notez juste l'adresse IP et pas toute la ligne) ?

TP2 - Le réseau sous windows

Index	Source	Port	Target	Port	Protocol	Length	Details
11	0.140322	::1	::1	DNS	94	Standard query 0x0004 A www.jerome.ridet.free.fr	

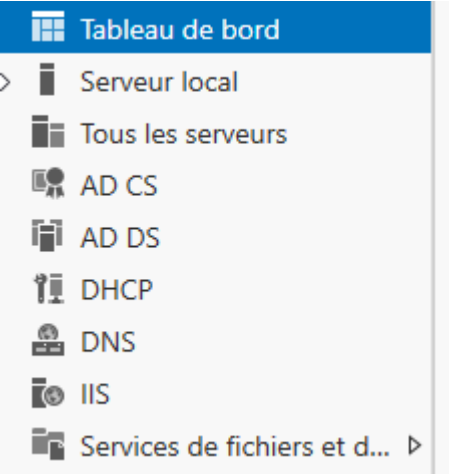
```
C:\Users\Administrateur>nslookup www.jerome.ridet.free.fr
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
    primary name server = 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
    responsible mail addr = (root)
    serial      = 0
    refresh     = 28800 (8 hours)
    retry       = 7200 (2 hours)
    expire      = 604800 (7 days)
    default TTL = 86400 (1 day)

Serveur :   UnKnown
Address:  ::1

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur UnKnown est dépassé.
```

Fin

Ensemble des services installés (situation finale):



Sitographie:

<https://www.ibm.com/docs/fr/rpa/23.0?topic=ldap-installing-configuring-microsoft-active-directory>

<https://www.microsoft.com/fr-fr/windows-server/trial>

<https://www.dell.com/support/kbdoc/fr-fr/000143677/creation-ou-modification-dune-partition-dans-microsoft-windows#:~:text=Ouvrez%20la%20Gestion%20des%20disques,taille%2C%20puis%20cliquez%20sur%20Suivant.>

<https://www.developpez.net/forums/d536964/systemes/windows/windows-serveur/faire-difference-entre-groupe-unite-d-organisation/>

<https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory>

https://help.claris.com/archive/help/16/fmp/fr/index.html#page/FMP_Help/example-backup-script.html

<https://www.ubackup.com/fr/articles/sauvegarde-automatique-avec-fichier-de-commandes.html>

<https://openclassrooms.com/fr/courses/2035806-virtualisez-votre-architecture-et-vos-environnements-de-travail/6313956-faites-communiquer-vos-machines-entre-elles>

<http://www.ordinateur.cc/réseaux/Réseaux-locaux/73211.html>

<https://web.maths.unsw.edu.au/~lafaye/CCM/intranet/resintro.htm>

<https://www.configserverfirewall.com/windows-10/netcat-windows/>

TP2 - Le réseau sous windows

<https://www.01net.com/hebergeur/transferer-nom-domaine/>