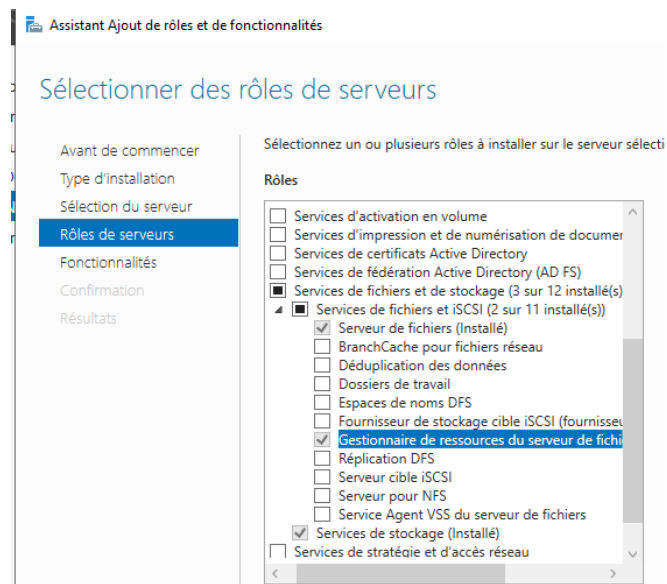




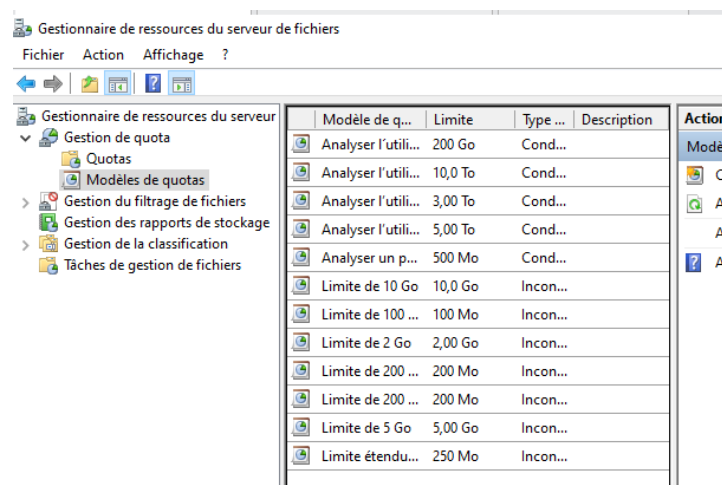
Procédure : Créer un quota inconditionnel

Objectif : Apprendre à créer un quota inconditionnel avec des alertes

- I. Dans le gestionnaire du serveur, appuyer sur ajouter un rôle ou fonctionnalité
Puis ajouter Gestionnaire de ressources du serveur de fichiers



- II. Après l'installation, dans outils appuyer sur Gestionnaire de ressources du serveur de fichiers



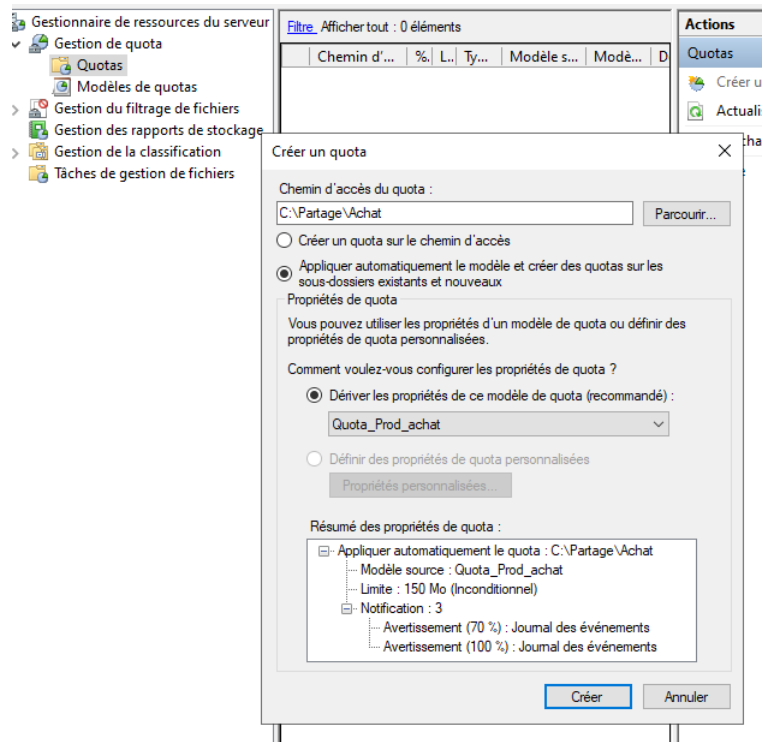
- III. Puis dans modèles de quotas, clic droit créer un modèle de quota... saisir les informations requises

The screenshot shows the 'Créer un modèle de quota' dialog box. At the top, it says 'Copier les propriétés du modèle de quota (facultatif) : Analyser l'utilisation de volume de 200 Go' with a 'Copier' button. Below is the 'Paramètres' section with fields for 'Nom du modèle : Quota_Prod_achat' and 'Description (facultatif) :'. The 'Limite d'espace' section has 'Limite : 150 Mo' and two radio buttons: 'Quota inconditionnel : empêcher les utilisateurs de dépasser la limite' (selected) and 'Quota conditionnel : autoriser les utilisateurs à dépasser la limite (utilisé pour l'analyse)'. At the bottom, there is a table for 'Seuils de notification' with columns 'Seuil', 'Adresse d...', 'Journal de...', 'Commande', and 'Rapports'. Below the table are 'Ajouter...', 'Modifier...', and 'Supprimer' buttons.

- IV. Ensuite dans Seuil de notification faire ajouter puis à nouveau saisir 70 % et alerte dans le journal d'événement + une alerte à 100 %

The first screenshot shows the 'Ajouter un seuil' dialog box with 'Générer des notifications lorsque l'utilisation atteint (%) : 70'. The 'Message électronique' tab is selected. It has checkboxes for 'Envoyer un courrier électronique aux administrateurs suivants : [Admin Email]' and 'Envoyer un message à l'utilisateur qui dépasse le seuil'. The 'Objet' field contains 'Seuil de quota de [Quota Threshold] % dépassé'. The 'Corps du message' field contains a template text with variables like [Source], [Owner], [Quota Threshold], [Quota Path], [Server], [Quota Limit MB], and [Quota Used MB]. There is a 'Sélectionnez la variable à insérer : [Admin Email]' dropdown and an 'Insérer une variable' button. The second screenshot shows the same dialog box with the 'Journal des événements' tab selected. The 'Générer des notifications lorsque l'utilisation atteint (%) : 70' is still present. The 'Envoyer un avertissement au journal des événements' checkbox is checked. The 'Message d'avertissement' section has a text area for the journal entry with a template similar to the first screenshot. It also has a 'Sélectionnez la variable à insérer : [Admin Email]' dropdown and an 'Insérer une variable' button.

V. On applique ensuite le quota au dossier Achat et Production



Chemin d'accès du quota	% utilisé	Limite	Type de quota	Modèle source	Modèle correspondant	Description
Modèle source : Quota_Prod_achat (2 éléments)						
C:\Partage\Achat	63%	150 Mo	Inconditionnel	Quota_Prod_achat	Oui	
C:\Partage\Production	0%	150 Mo	Inconditionnel	Quota_Prod_achat	Oui	

VI. TEST Achat

L'utilisateur LEARN\AchatL a dépassé le seuil de quota de 100 % dans C:\Partage\Achat sur le serveur DC1. La limite de quota est de 150,00 Mo alors que 143,06 Mo sont actuellement utilisés (95 % de la limite).

L'utilisateur LEARN\AchatL a dépassé le seuil de quota de 70 % dans C:\Partage\Achat sur le serveur DC1. La limite de quota est de 150,00 Mo alors que 143,06 Mo sont actuellement utilisés (95 % de la limite).

VII. TEST Production

L'utilisateur LEARN\ProductionL a dépassé le seuil de quota de 100 % dans C:\Partage\Production sur le serveur DC1. La limite de quota est de 150,00 Mo alors que 0,02 Mo sont actuellement utilisés (0 % de la limite).

L'utilisateur LEARN\ProductionL a dépassé le seuil de quota de 100 % dans C:\Partage\Production sur le serveur DC1. La limite de quota est de 150,00 Mo alors que 0,02 Mo sont actuellement utilisés (0 % de la limite).



Procédure : Créer un quota inconditionnel

Objectif : Apprendre à créer un quota inconditionnel avec des alertes

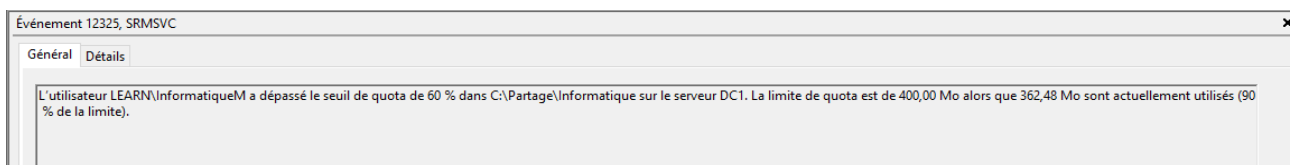
- I. Dans modèles de quotas, clic droit créer un modèle de quota... saisir les informations requises
Ensuite dans Seuil de notification faire ajouter puis à nouveau saisir 60 % et alerte dans le journal d'événement + une alerte à 100 %

Seuil	Adresse d...	Journal de...	Commande	Rapports
Avertissement (60 %)		✓		
Avertissement (100 %)		✓		

- II. On applique ensuite le quota au dossier Achat et Production

Chemin d'accès du quota	% utilisé	Limite	Type de quota	Modèle source	Modèle correspondant	Description
Modèle source : Quota_IT_dir (2 éléments)						
C:\Partage\Direction	0%	400 Mo	Conditionnel	Quota_IT_dir	Oui	
C:\Partage\Informatique	0%	400 Mo	Conditionnel	Quota_IT_dir	Oui	
Modèle source : Quota_Prod_achat (2 éléments)						
C:\Partage\Achat	63%	150 Mo	Inconditionnel	Quota_Prod_achat	Oui	
C:\Partage\Production	0%	150 Mo	Inconditionnel	Quota_Prod_achat	Oui	

- III. TEST Informatique



L'utilisateur LEARN\InformatiqueM a dépassé le seuil de quota de 100 % dans C:\Partage\Informatique sur le serveur DC1. La limite de quota est de 400,00 Mo alors que 476,93 Mo sont actuellement utilisés (119 % de la limite).

IV. TEST Direction

Général Détails

L'utilisateur LEARN\DirectionL a dépassé le seuil de quota de 60 % dans C:\Partage\Direction sur le serveur DC1. La limite de quota est de 400,00 Mo alors que 333,80 Mo sont actuellement utilisés (83 % de la limite).

Général Détails

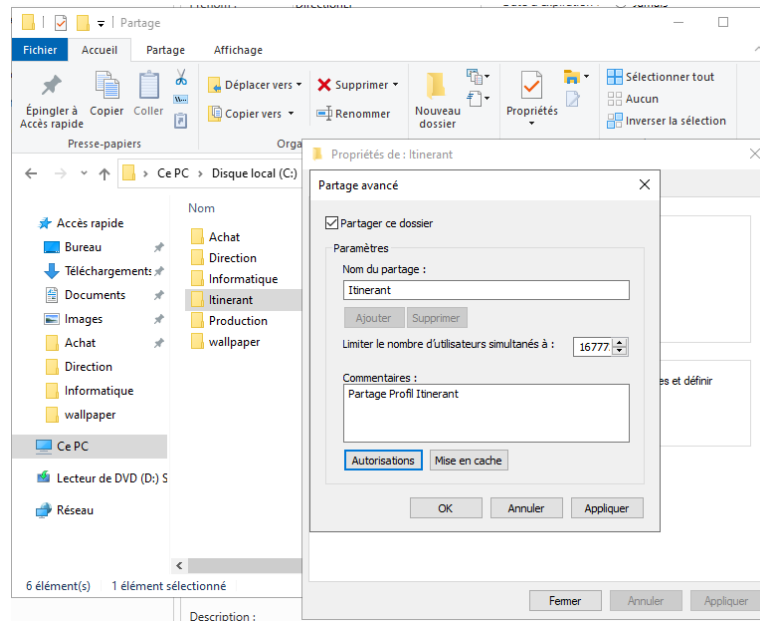
L'utilisateur LEARN\DirectionL a dépassé le seuil de quota de 100 % dans C:\Partage\Direction sur le serveur DC1. La limite de quota est de 400,00 Mo alors que 667,59 Mo sont actuellement utilisés (166 % de la limite).



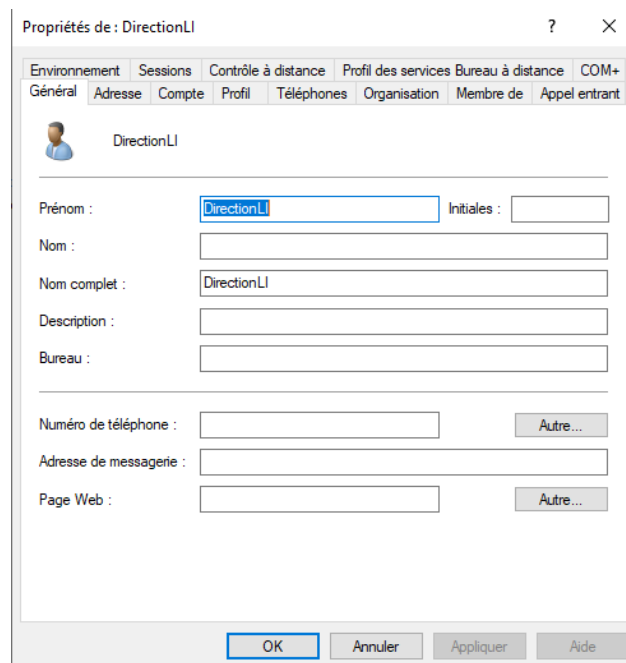
Procédure : Créer un utilisateur itinérant

Objectif : Apprendre à créer un utilisateur itinérant

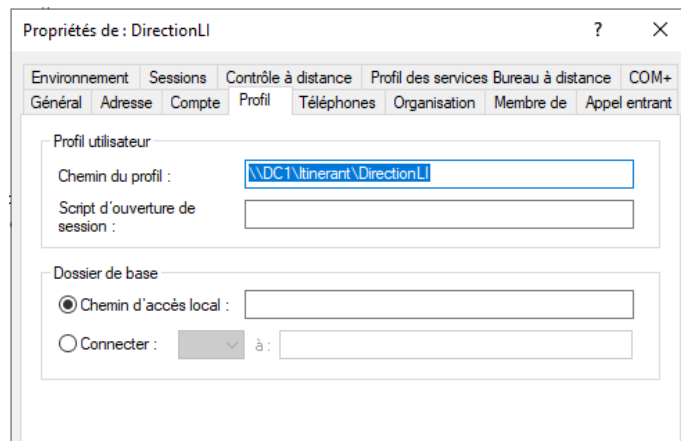
I. Dans un premier temps crée un dossier partagé pour le profil itinérant



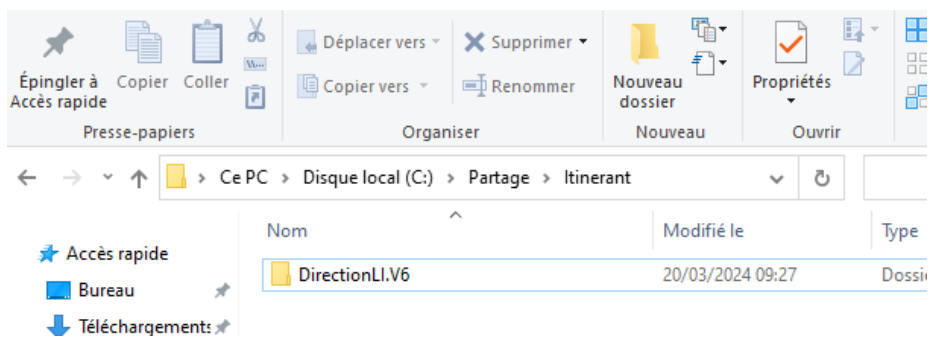
II. Ensuite crée un utilisateur ici DirectionLI



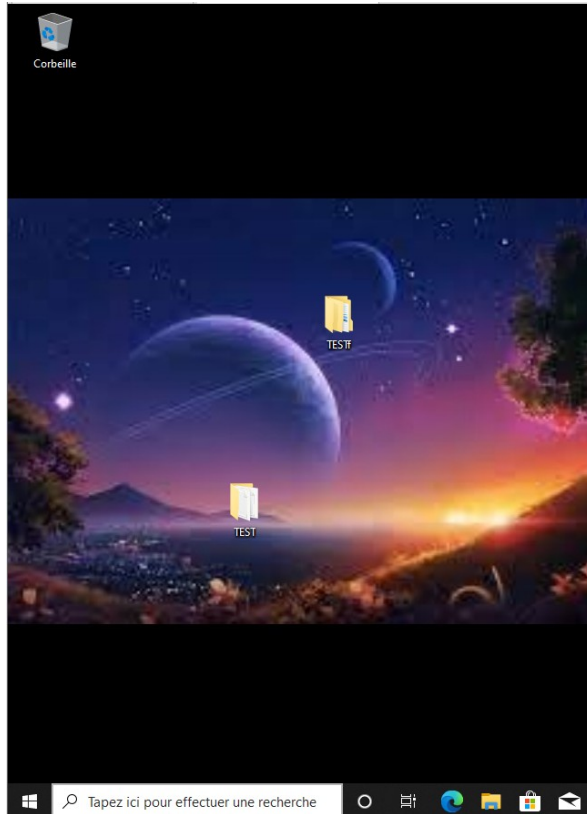
- III. Dans le profil, rajouter le chemin du dossier partagé \\DC1\Itinerant\%username % ← prend le nom du profil



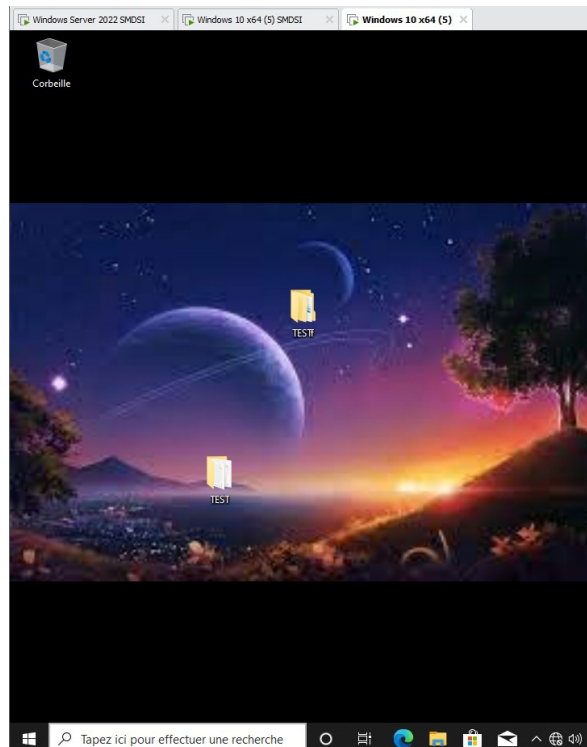
- IV. On peut voir qu'après le démarrage de la session DirectionLI, un dossier (DirectionLI.V6) se crée dans le dossiers itinerant partagé



V. TEST sur l'ordinateur CL1, il y a deux fichiers



VI. TEST sur l'ordinateur CL2 (nouvellement créée) , on retrouve bien le bureau

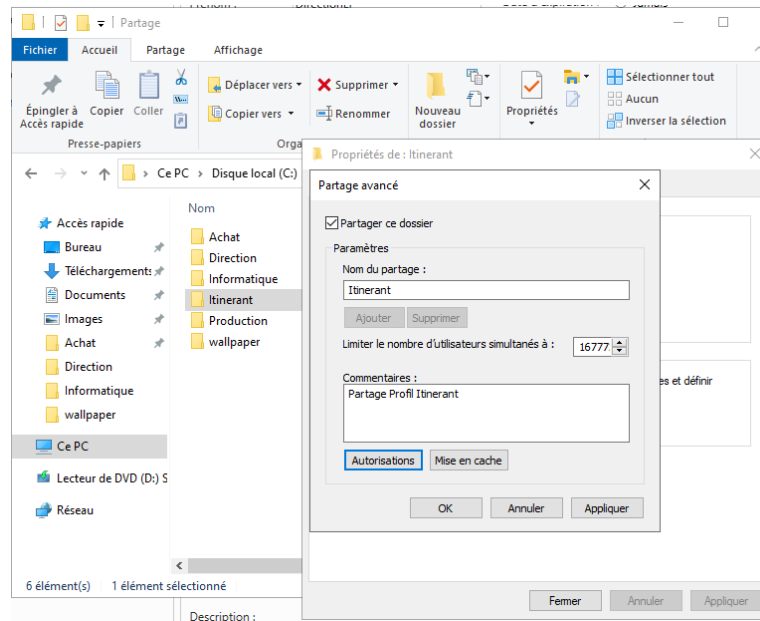




Procédure : Créer un utilisateur obligatoire

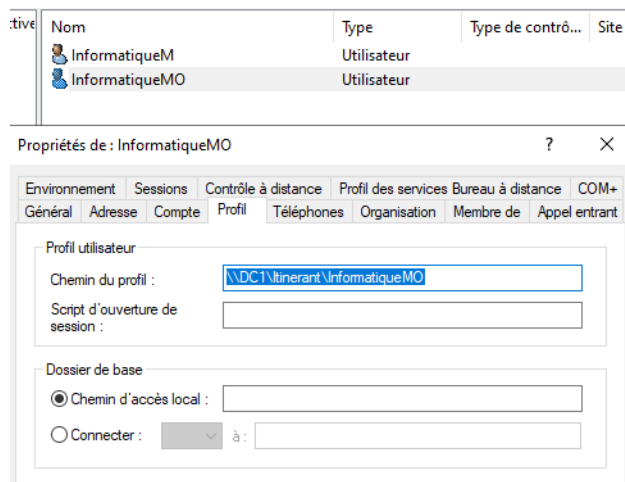
Objectif : Apprendre à créer un utilisateur obligatoire

I. Dans un premier temps crée un dossier partagé pour le profil itinérant




II. Ensuite crée un utilisateur ici InformatiqueMOB

Dans le profil, rajouter le chemin du dossier partagé \\DC1\Itinerant\%username % ← prend le nom du profil



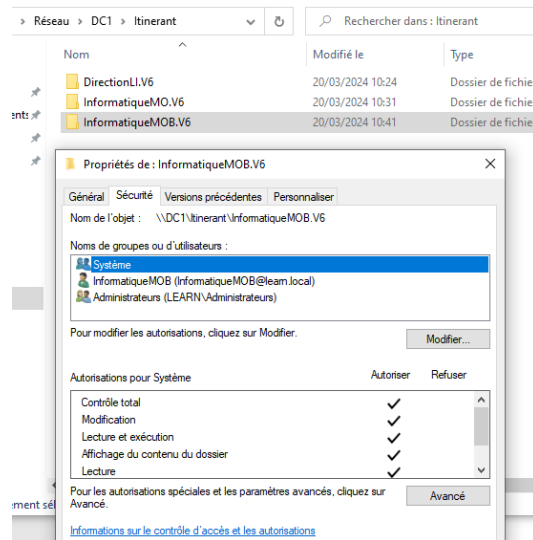
- III. On peut voir qu'après le démarrage de la session InformatiqueMOB, un dossier (InformatiqueMO .V6) se crée dans le dossiers itinérant partagé

 InformatiqueMOB.V6

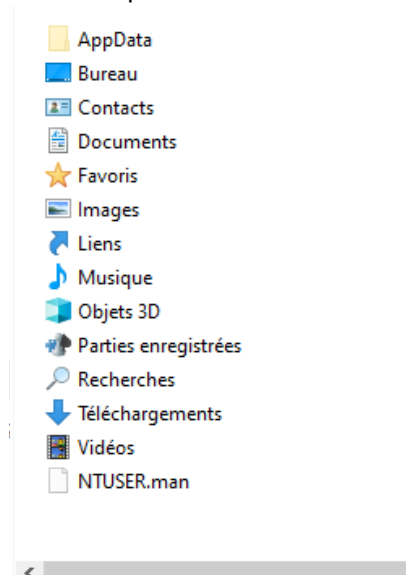
20/03/2024 10:41

Dossier de fichiers

- IV. Il faut ensuite rentrer dans le fichier InformatiqueMOB mais on a pas l'autorisation
Pour éviter cela, se connecter à son profil InformatiqueMOB puis changer les autorisations



Enfin avec la session Administrateur on peut renommer le fichier nuser.dat → nuser.man



- V. On peut ensuite se connecter à la session InformatiqueMOB, dans les paramètres système avancé on peut voir que le profil est bien en obligatoire

LEARN\InformatiqueMOB

3,16 Mo

Obligatoire

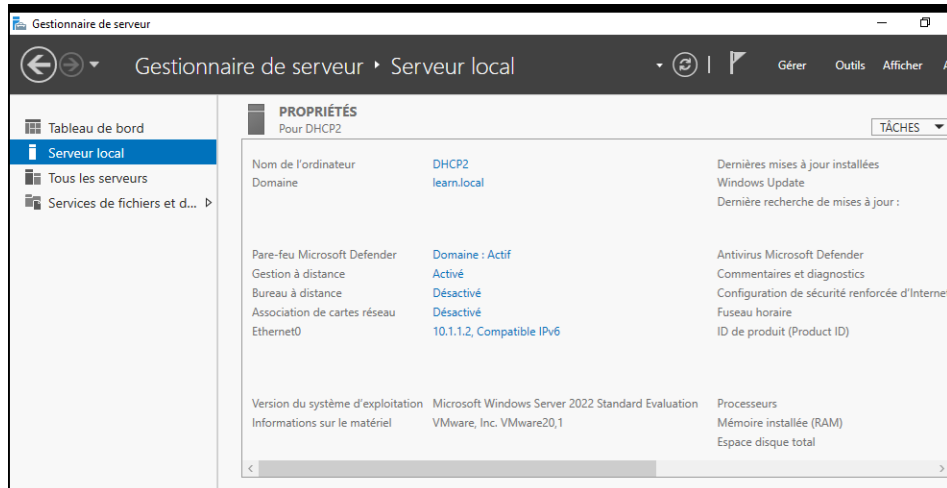
Obligat...



Procédure : DHCP Failover

Objectif : Configurer le DHCP Failover

I. Création et installation d'un Windows server 2022 et joindre le domaine learn.local

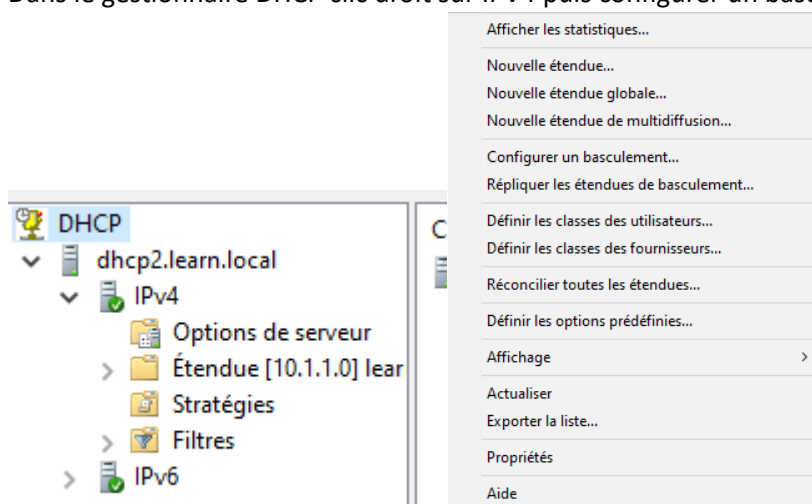


II. Installer le rôle DHCP

Dans le gestionnaire des serveurs cliquez sur Gérer puis ajouter des rôles et fonctionnalités puis cliquez sur serveur DHCP pour installer

III. Configurer un basculement

Dans le gestionnaire DHCP clic droit sur IPV4 puis configurer un basculement



Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire 10.1.1.2

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Pourcentage d'équilibrage de charge

Serveur local : %

Serveur partenaire : %

Intervalle de basculement d'état : minutes

Activer l'authentification du message

Secret partagé :

< Précédent Suivant > Annuler

IV. FIN

Configurer un basculement

Un basculement va être configuré entre dc1.learn.local et 10.1.1.2 avec les paramètres suivants.

Étendues :

Nom de la relation : dc1.learn.local
 Délai de transition maximal du client (MCLT) : 1 h 0 min
 Mode : Équilibrage de charge
 Intervalle de basculement d'état : Désactivé

Pourcentage d'équilibrage de charge

Serveur local : 50 %
 Serveur partenaire : 50 %

< Précédent Terminer Annuler

Contenu du serveur DHCP	État	Description	Relation de basculement
Options de serveur			
Étendue [10.1.1.0] learnDHCP	** Actif **		dc1.learn.local-10.1.1.2
Stratégies			
Filtres			

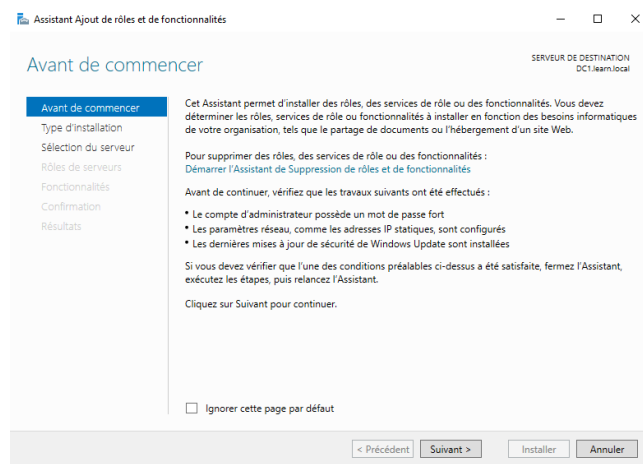


Procédure : DHCP

Objectif : Mise en place d'un DHCP

I. Installer le rôle DHCP

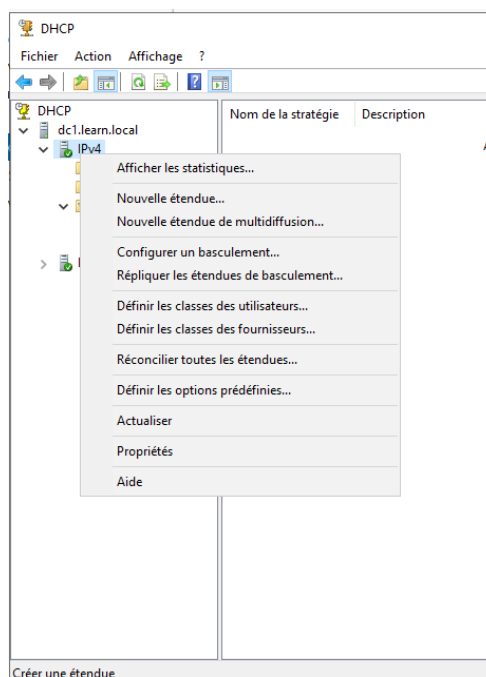
Depuis l'interface gestionnaire de serveur faire gérer puis ajouter des rôles et fonctionnalités ensuite ajouter le rôle serveur DHCP



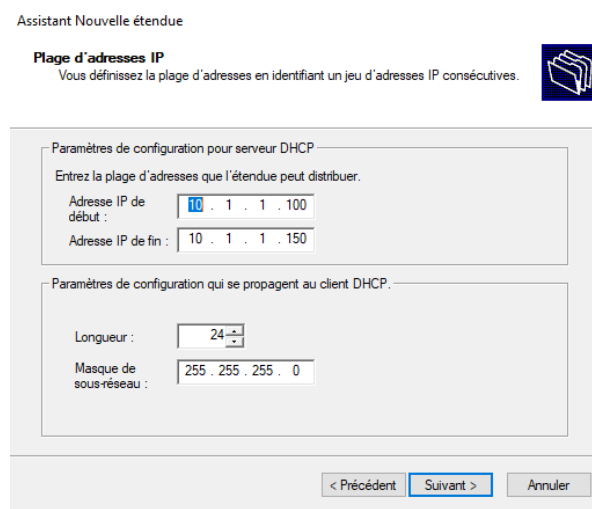
II. Après l'installation l'icone nous indique qu'il faut terminer la configuration du DHCP

Après la configuration, on clique sur outils puis DHCP pour entrer dans le gestionnaire DHCP

III. Dans le gestionnaire DHCP, on clique droit sur IPV4 puis nouvelle étendue



IV. Paramétrage de l'étendue

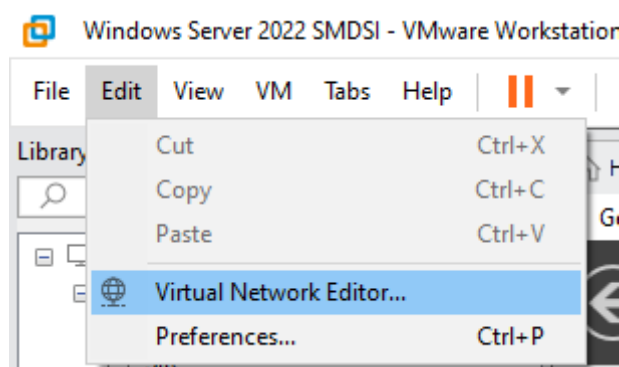


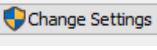
V. On paramètre la carte réseau de CL1 en DHCP puis on regarde

```
Carte Ethernet Ethernet0 :  
  
Suffixe DNS propre à la connexion. . . : learn.local  
Adresse IPv6 de liaison locale. . . . : fe80::3d0f:f3b:7e9f:37a0%12  
Adresse IPv4. . . . . : 10.1.1.100  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 10.1.1.1
```

NB : Dans mon cas le logiciel VMware à activer un DHCP local sur les VM ce qui prenait la place du DHCP précédemment crée pour résoudre ce problème

Dans VMWare en haut à droit edit -> Virtual Network Editor



Puis change setting 

name	type	external connection	host connection	DHCP	subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	-	192.168.10.0
VMnet8	NAT	NAT	Connected	-	192.168.67.0

Et ici désactiver les DHCP

Est-ce que le DHCP répond au requête DHCP d'un PC hors domaine ?

Oui

```
Invite de commandes
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . : fe80::ccf3:b446:9862:a443%11
Adresse d'autoconfiguration IPv4 . . . . : 169.254.164.67
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . :

C:\Users\TESTVPN>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . :

C:\Users\TESTVPN>ipconfig

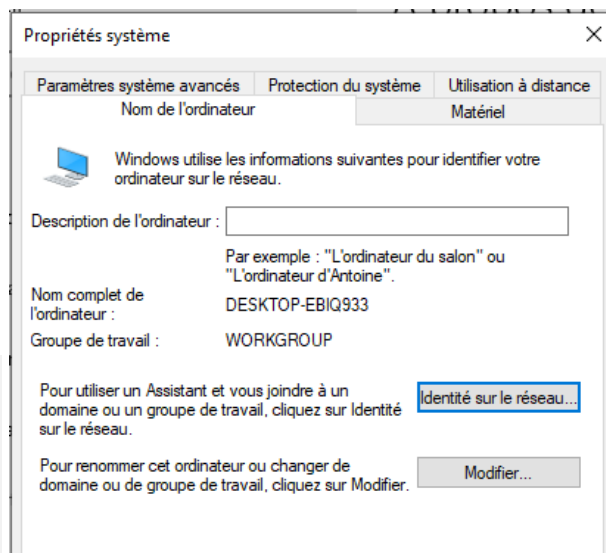
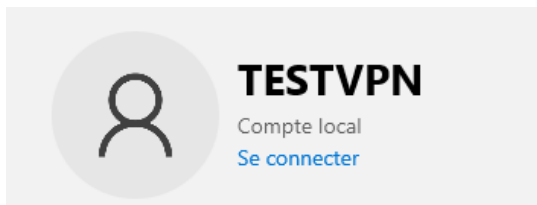
Configuration IP de Windows

Carte Ethernet Ethernet0 :

Suffixe DNS propre à la connexion. . . . : learn.local
Adresse IPv6 de liaison locale. . . . : fe80::ccf3:b446:9862:a443%11
Adresse IPv4. . . . . : 10.1.1.101
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.1.1.1

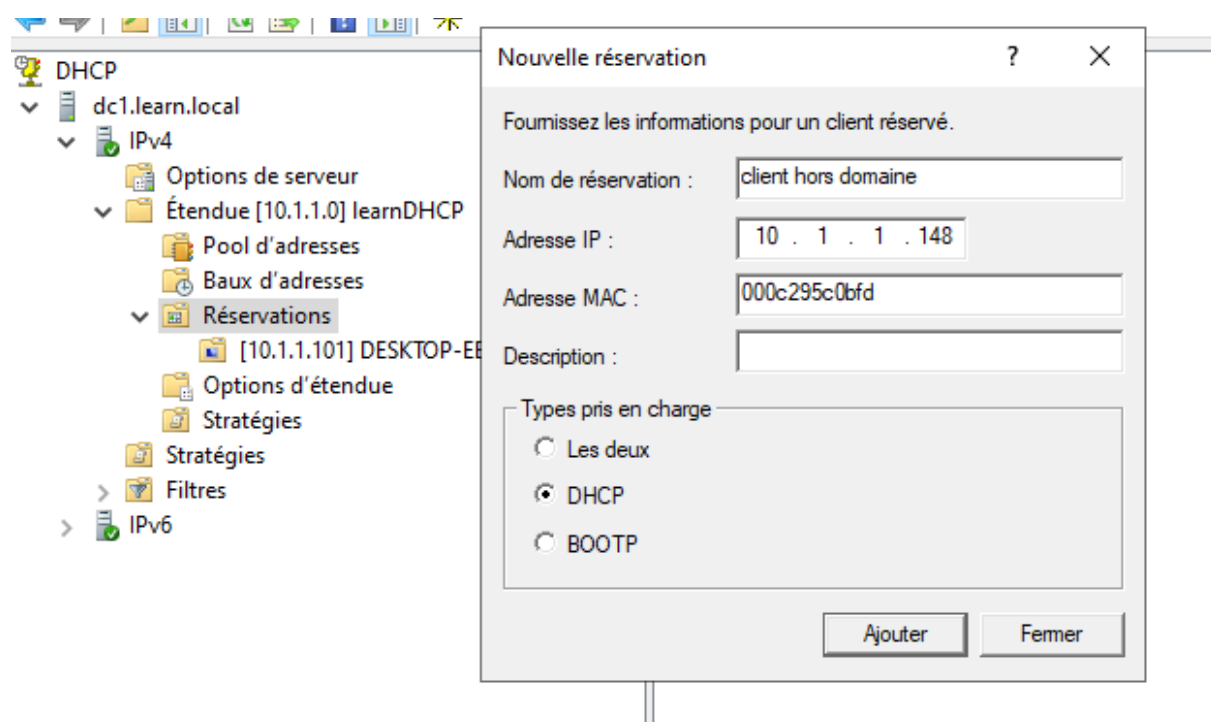
C:\Users\TESTVPN>
```

Le compte n'est pas connecté au domaine



VI. Réserveation

Clic droit sur réserveation -> nouvelle réserveation puis on saisit les données nécessaire



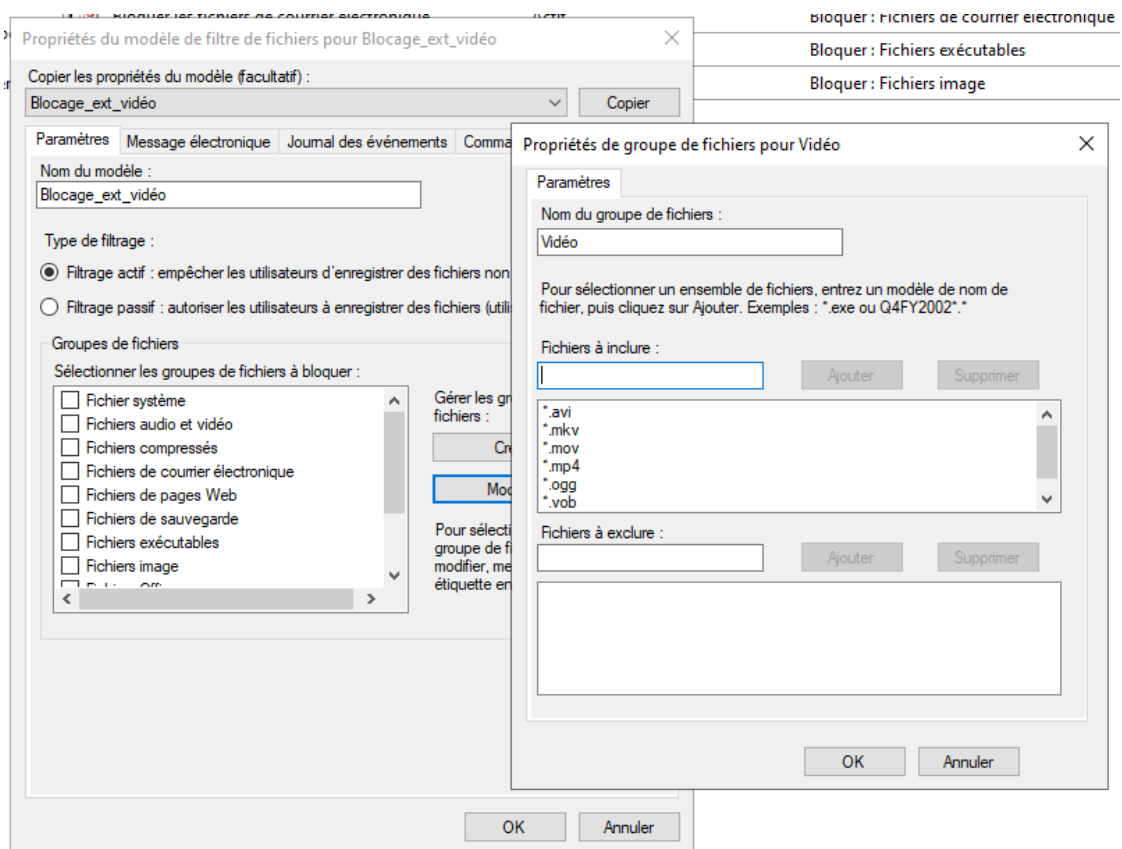
```
Carte Ethernet Ethernet0 :  
  
Suffixe DNS propre à la connexion. . . : learn.local  
Adresse IPv6 de liaison locale. . . . . : fe80::ccf3:b446:9862:a443%11  
Adresse IPv4. . . . . : 10.1.1.148  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 10.1.1.1  
  
C:\Users\TESTVPN>
```



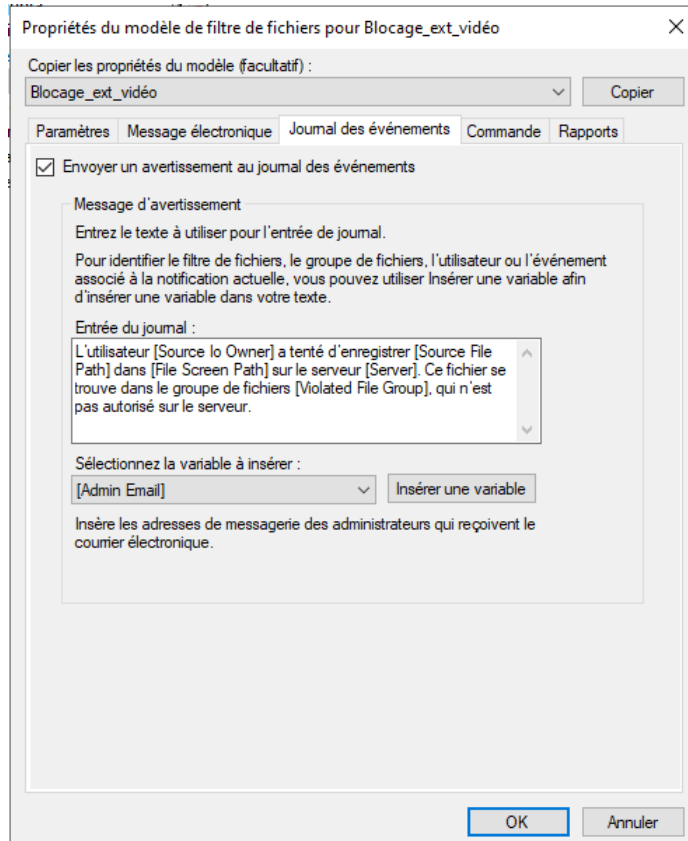

Procédure : filtre

Objectif : Apprendre à utiliser les filtres

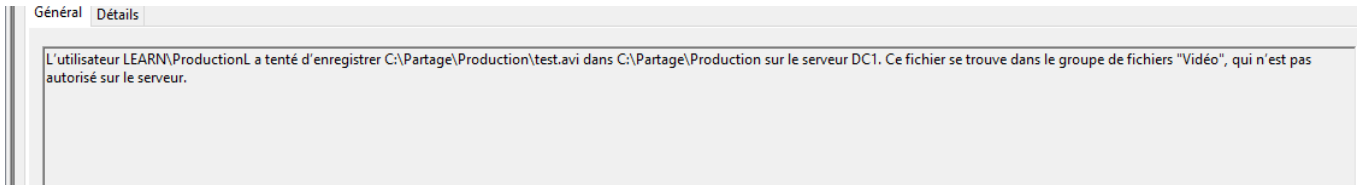
- I. Dans la même fenêtre que pour les quota (c'est-à-dire Gestionnaire de ressources du serveur de fichiers)
Dans la partie Gestion du filtrage de fichiers, créer dans Modèles de filtres de fichiers, un modèle



II. Sans oublier l'alertes dans le journal d'évènement



III. TEST





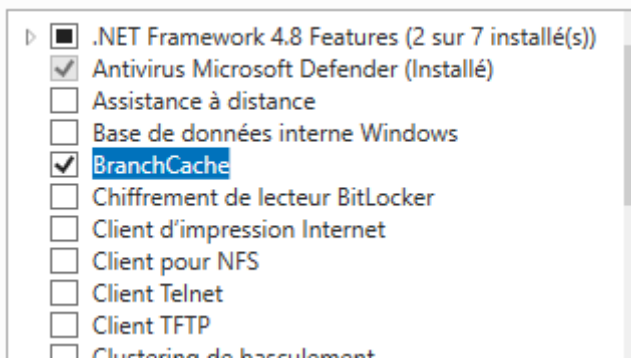
Procédure : Branchcache

Objectif : Installer un serveur de cache

I. Installer le rôle Branchcache sur le serveur DC1

Services de fichiers et de stockage
Services de fichiers et iSCSI
BranchCache pour fichiers réseau

II. Installer Branchcache sur le serveur cache1 et l'activer, intégrer le serveur au Domain



III. Activer Branchcache GPO et la Publication de hachages pour Branchcache

Paramètre	État	Commentaire
Activer BranchCache	Activé	Non
Définir le mode de cache distribué de BranchCache	Non configuré	Non
Définir le mode de cache hébergé de BranchCache	Non configuré	Non
Activer la découverte automatique du cache hébergé par le ...	Non configuré	Non
Configurer les serveurs de cache hébergé	Non configuré	Non
Configurer BranchCache pour les fichiers réseau	Non configuré	Non
Définir le pourcentage d'espace disque utilisé pour la mémo...	Non configuré	Non
Définir l'âge des segments dans le cache de données	Non configuré	Non
Configurer la prise en charge de la version BranchCache du ...	Non configuré	Non

Paramètre	État	Commentaire
Ordre des suites de chiffrement	Non configuré	Non
Publication de hachages pour BranchCache	Activé	Non
Prise en charge de la version de hachage pour BranchCache	Non configuré	Non
Respecter l'ordre des suites de chiffrement	Non configuré	Non

IV. Commande PowerShell sur Cache1

```
PS C:\Windows\system32>
PS C:\Windows\system32> Enable-BCHostedServer -RegisterSCP
PS C:\Windows\system32> Get-BCStatus

BranchCacheIsEnabled      : True
BranchCacheServiceStatus  : Running
BranchCacheServiceStartType : Automatic

ClientConfiguration:

    CurrentClientMode      : LocalCache
    HostedCacheServerList  :
    HostedCacheDiscoveryEnabled : False

ContentServerConfiguration:

    ContentServerIsEnabled : True

HostedCacheServerConfiguration:

    HostedCacheServerIsEnabled      : True
    ClientAuthenticationMode        : Domain
    HostedCacheScpRegistrationEnabled : True

NetworkConfiguration:

    ContentRetrievalUrlReservationEnabled : True
    HostedCacheHttpUrlReservationEnabled  : True
    HostedCacheHttpsUrlReservationEnabled : True
    ContentRetrievalFirewallRulesEnabled  : True
    PeerDiscoveryFirewallRulesEnabled     : False
    HostedCacheServerFirewallRulesEnabled : True
    HostedCacheClientFirewallRulesEnabled : True
```

V. TEST

```
PS C:\Windows\system32> Get-BCClientConfiguration

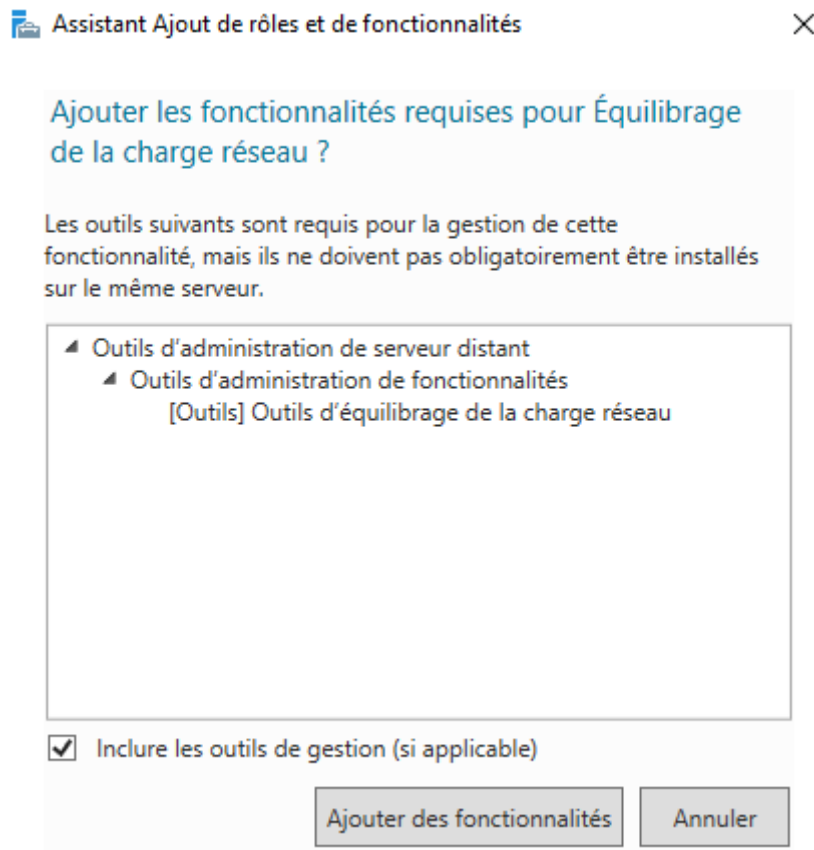
CurrentClientMode      : HostedCacheClient
HostedCacheServerList  : {10.1.1.3}
HostedCacheDiscoveryEnabled : False
```



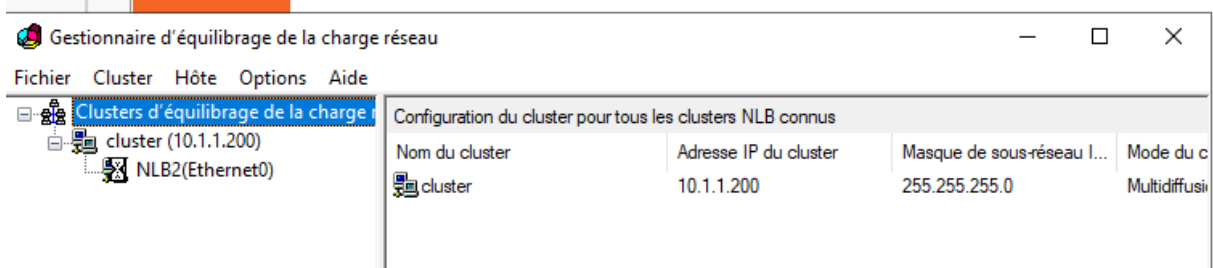
Procédure : Network Load Balancing

Objectif : Installer et configurer la répartition de charge

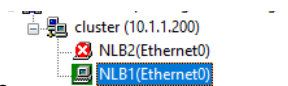
I. Installer la fonctionnalité Network Load Balancing Tools



II. Créer un cluster regroupant les 2 Windows server derrière l'ip 10.1.1.200/24



NB : Il faut ici ajouter les deux hôtes



III. Faites un ping en continue sur l'adresse 10.1.1.200 et éteindre un des serveurs

```
C:\Users\Administrateur>ping 10.1.1.200 -t
```

IV. TEST

Administrateur : Invite de commandes - ping 10.1.1.200 -t

```
Microsoft Windows [version 10.0.20348.587]  
(c) Microsoft Corporation. Tous droits réservés.  
C:\Users\Administrateur>ping 10.1.1.200 -t  
Envoi d'une requête 'Ping' 10.1.1.200 avec 32 octets de données:  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps=8 ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps<1ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps=1 ms TTL=128  
Réponse de 10.1.1.200 : octets=32 temps=1 ms TTL=128
```

On peut voir que NLB1 est arrêté mais ça ping bien

Pareil pour NLB2

Gestionnaire d'équilibrage de la charge réseau

Fichier Cluster Hôte Options Aide

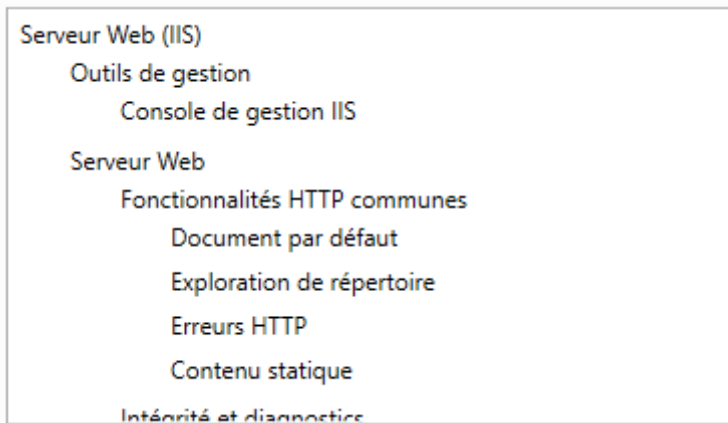
Clusters d'équilibrage de la charge

- cluster (10.1.1.200)
 - NLB2(Ethernet0)
 - NLB1(Ethernet0)

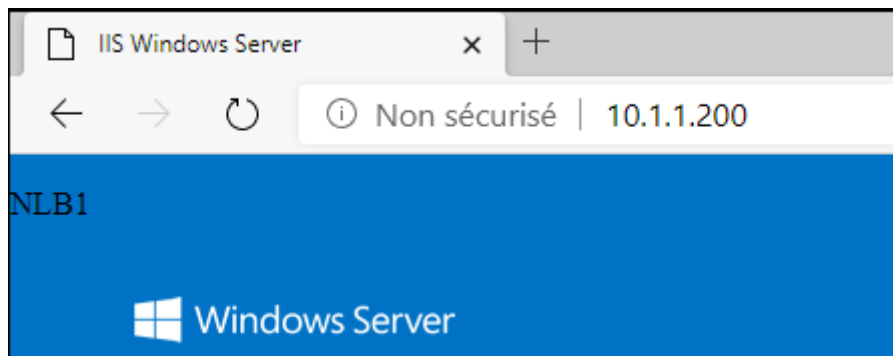
Règles de port configurées sur NLB1 (Ethernet0)						
Adresse IP du cluster	État	Début	Fin	Protocole	Mode	
Tous	Activé	0	65535	Les deux	Plusieurs	

Suite du TP

V. On ajoute le rôle IIS sur les deux serveurs

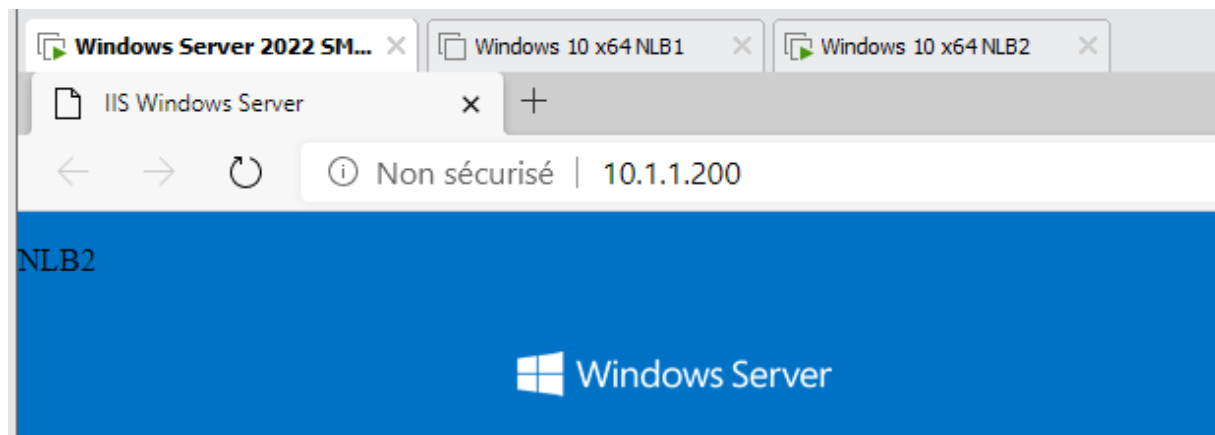


VI. Puis dans le dossier on rajoute NLB1 et NLB2 dans le html puis on test en utilisant un navigateur en saisissant 10.1.1.200

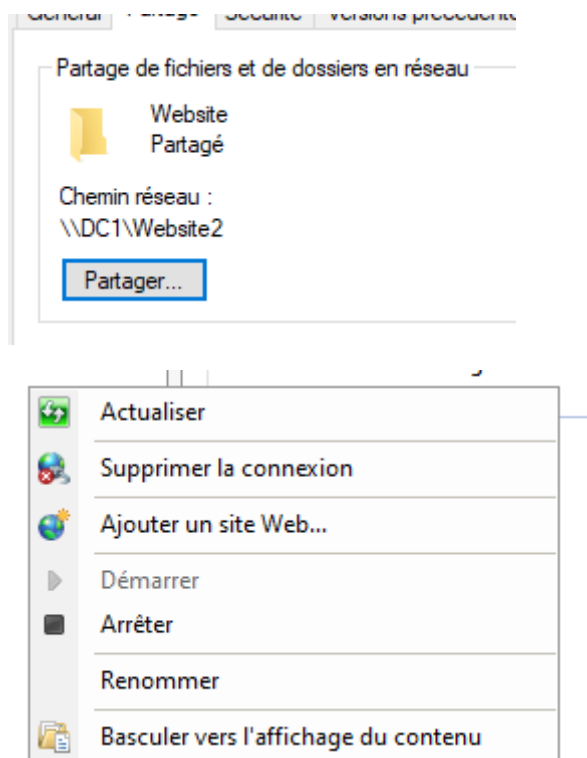


VII. Je coupe NLB1 et je test

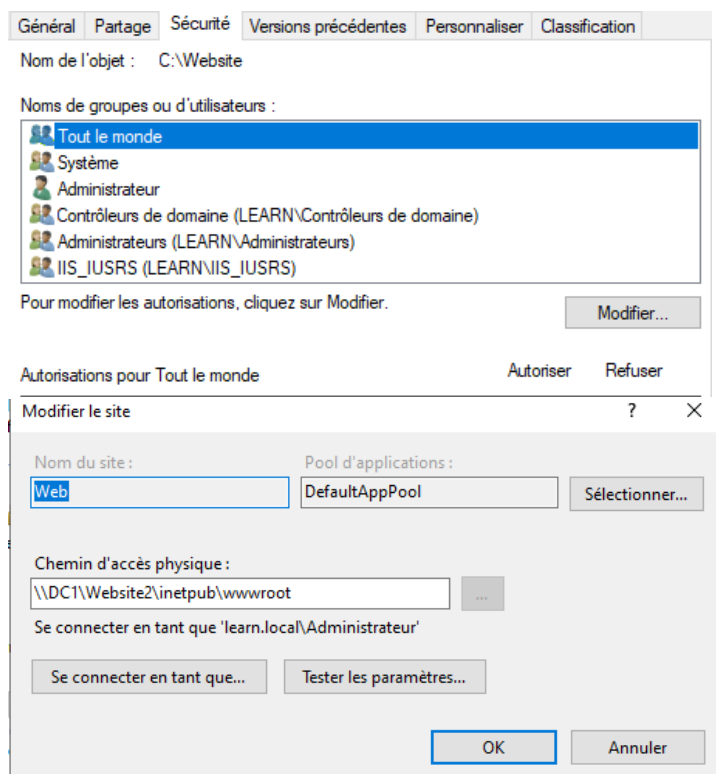
C'est bien NLB2 qui a repris



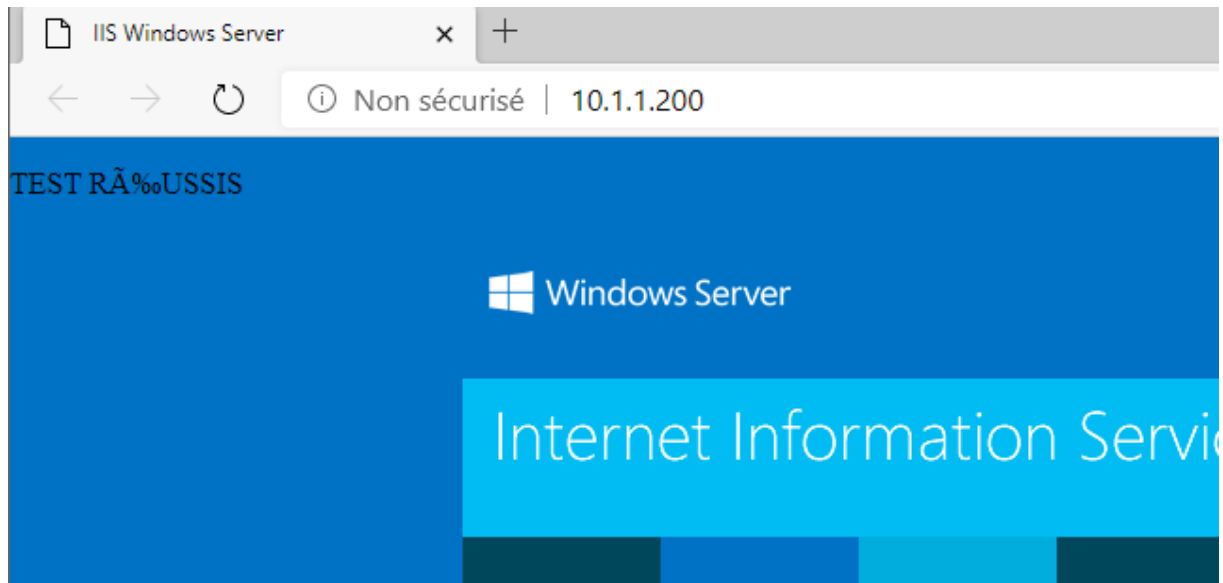
VIII. Suite du TP création d'un dossier partagé et ajout d'un site web



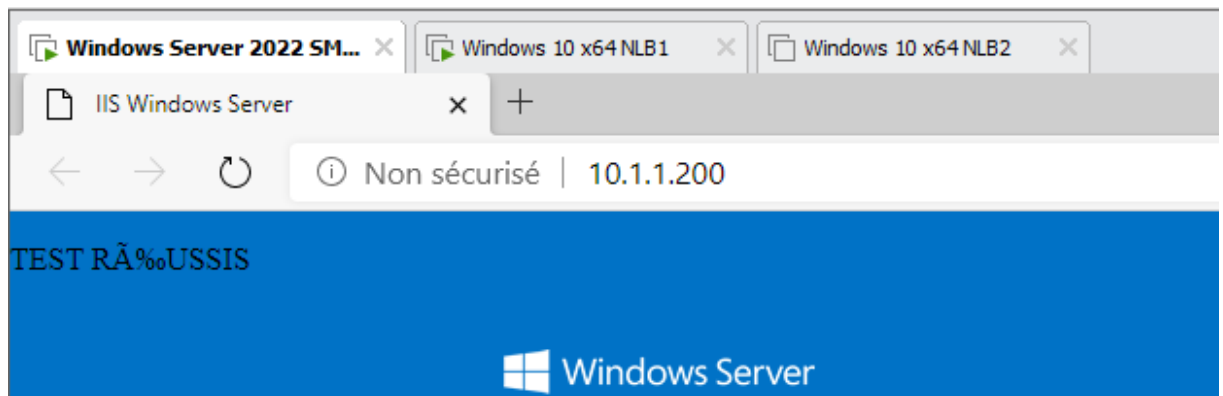
IX. Lors de la création saisir le chemin du partage [\\DC1\Website2](#) et mettre les droits de lecture



X. Si on se connecte en 10.1.1.200 sur une machine cliente on voit bien le site internet



Si on fait tomber le NLB2 on voit bien que le serveur Web reste en place

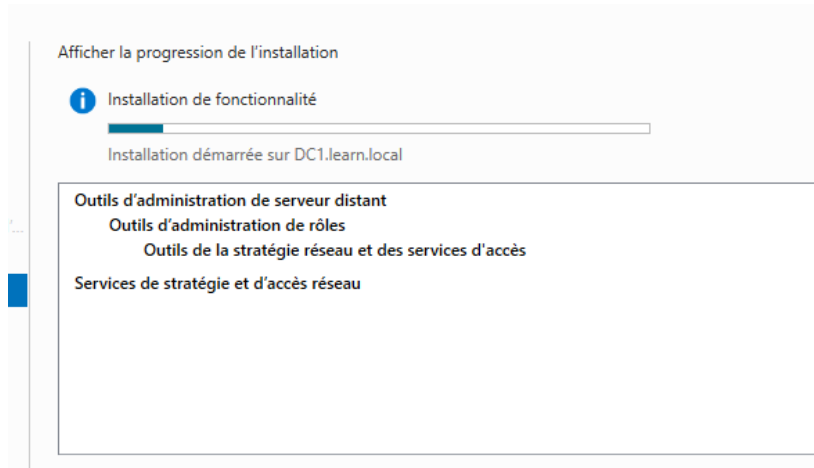




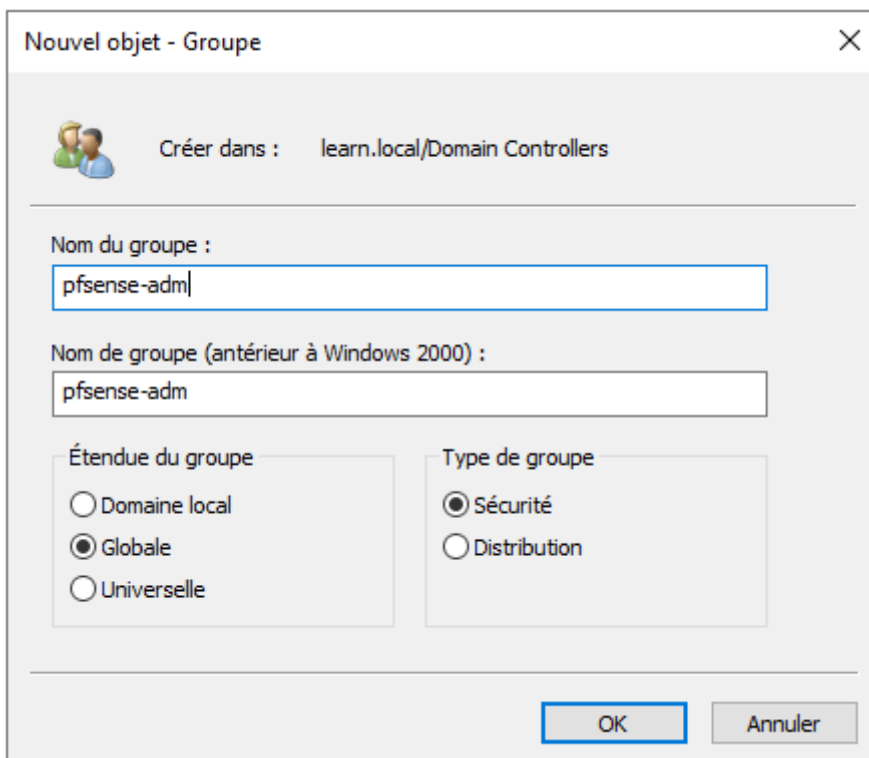
Procédure : NPS

Objectif : Apprendre à utiliser la stratégie NPS

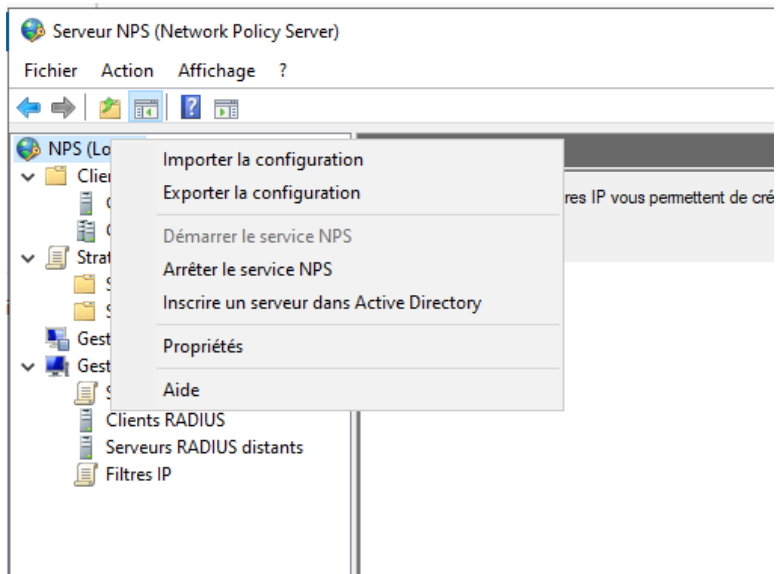
I. Installer le rôle NPS sur votre serveur



II. Sur l'AD créer un groupe de sécurité



III. Sur votre serveur NPS sélectionner Inscrire un serveur dans AD



IV. Ajouter FW1 en tant que client RADIUS

Nom convivial	Adresse IP	Fabricant du périphérique	État
FW1	10.1.1.8	RADIUS Standard	Activé

V. Activer l'authentification PAP

Nouvelle stratégie réseau ×

Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
- L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
- L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

VI. Ajouter un class « pfsense-adm »

Ajouter un attribut RADIUS standard

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :
Tous

Attributs :

- Nom
- Acct-Interim-Interval
- Callback-Number
- Class
- Filter-Id
- Framed-Apple-Talk-Link
- Framed-Apple-Talk-Network

Description :
Spécifie la classification des enregistrements de comptabilité.

Ajouter... Fermer

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Class	pfsense-adm

VII. Configuration pfsense

Server Settings

Descriptive name RADIUS NPS

Type RADIUS

RADIUS Server Settings

Protocol PAP

Hostname or IP address 10.1.1.1

Shared Secret

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout
This value controls how long, in seconds, that the RADIUS server will wait for a response from the client. If the value is blank, the default value is 5 seconds. NOTE: If using an interactive authentication method, this value controls how long it will take the user to receive and enter their password.

RADIUS NAS IP WAN - 10.10.0.217

VIII. TEST

User Administrateur authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server RADIUS NPS
Select the authentication server to test against.

Username Administrateur

Password

Debug Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

IX. Mettre les droits pour le groupe

Group Privileges

Group: pfsense-admin

Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted sc
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPOE Dialin
- WebCfG - AJAX: Get Queue Stats
- WebCfG - AJAX: Get Service Providers
- WebCfG - AJAX: Get Stats
- WebCfG - All pages**
- WebCfG - Crash reporter
- WebCfG - Dashboard (all)
- WebCfG - Dashboard widgets (direct access).
- WebCfG - Diagnostics: ARP Table

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

Privilege information

The following privileges effectively give administrator-level access to users in the group: execute general commands, edit system files, modify users, change passwords or similar.

User - System: Copy files (scp)

X. Je me connecte avec le compte dans le groupe pfsense-admin

System Information

Name	pfSense.home.arpa
User	Administrateur@10.1.1.127 (RADIUS/RADIUS NPS)
System	VMware Virtual Machine Netgate Device ID: cf54e33fca10f2a19fdf
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.1-RELEASE (amd64) built on Wed Nov 15 17:06:00 UTC 2023 FreeBSD 14.0-CURRENT Version 2.7.2 is available. Version information updated at Tue Jun 18 14:33:41 UTC 2024
CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.






- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate | Courrier postal
- Visit Netgate.com

```
Message from syslogd@pfSense at Jun 18 14:39:51 ...
php-fpm[400]: /index.php: Successful login for user 'Administrateur' from: 10.1.1.127 (RADIUS/RADIUS NPS)
```






<https://techexpert.tips/fr/pfsense-fr/pfsense-authentification-radius-a-laide-de-freeradius/>

XI. Suite du TP, configurer un VPN SSL






Création d'un certificat

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CALEARN	✓	self-signed	1	CN=calearn, C=FR Valid From: Wed, 19 Jun 2024 10:38:15 +0000 Valid Until: Sat, 17 Jun 2034 10:38:15 +0000		    




Création de règles dans le Firewall

<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN calearn wizard	    
--------------------------	---	-------	-------------	---	---	----------------	-------------------	---	------	------------------------------	---




Et dans le firewall Openvpn

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	*	*	*	none	OpenVPN calearn wizard	    

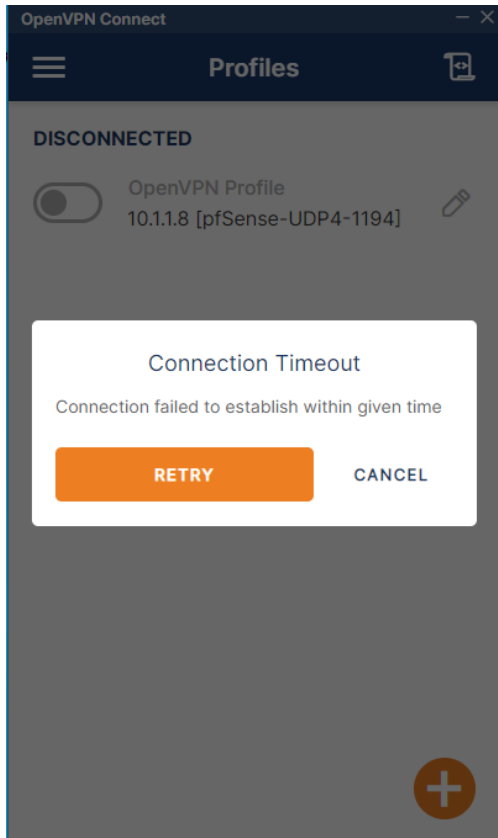
Configuration de openvpn

VPN / OpenVPN / Servers   

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.1.1.8/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	calearn	  

TEST



Cryptographic Settings

TLS Configuration Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority CALEARN


Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate vpn (Server: Yes, CA: CALEARN)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length 2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. 

ECDH Curve Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA



Procédure : Audit

Objectif : Activer les audits pour la gestion des comptes utilisateurs AD

1. Faire une GPO pour avoir un audit lors de la création d'un utilisateur

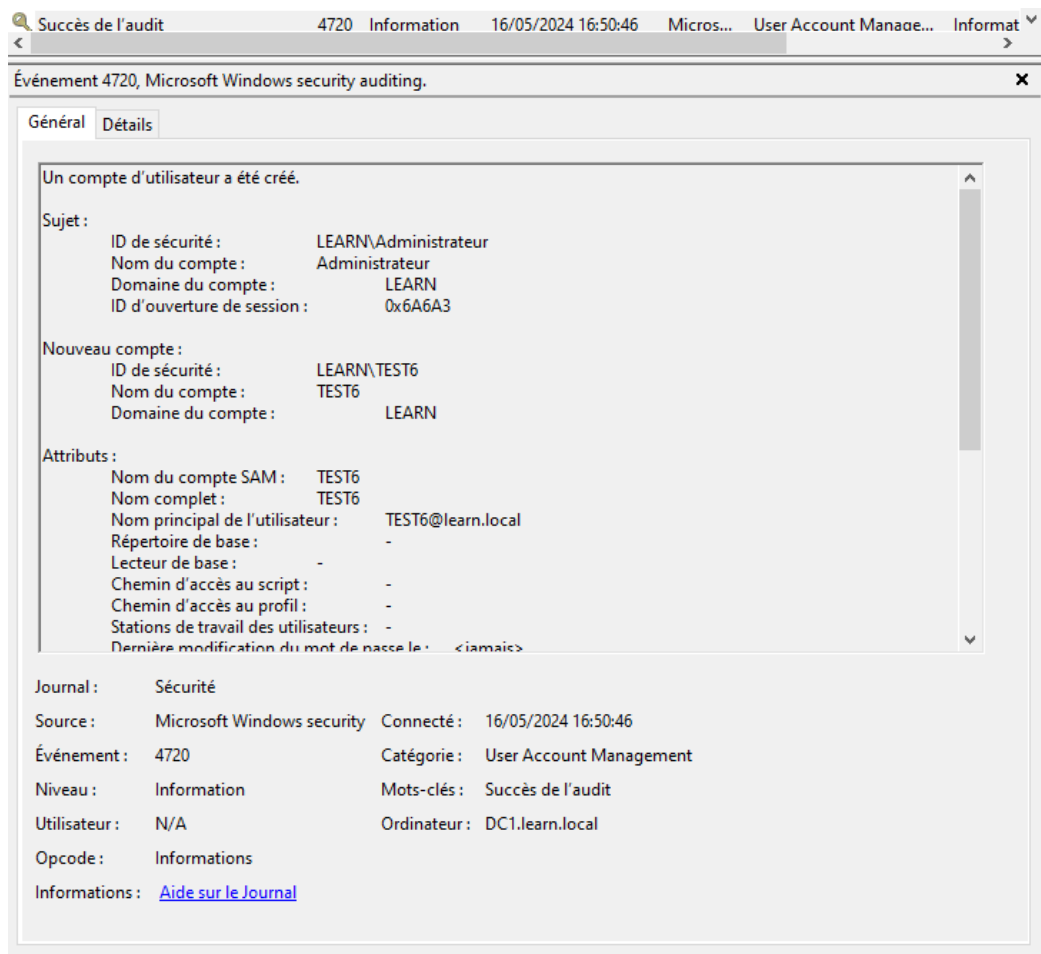
The screenshot shows the Group Policy Editor interface. The left pane displays the hierarchy: Gestion de stratégie de groupe > Forêt : learn.local > Domaines > learn.local > Audits AD usr > Configuration ordinateur > Stratégies > Paramètres de stratégie de sécurité > Auditer la gestion des comptes. The right pane shows the 'Audits AD usr' details, with the 'Liaisons' field set to 'learn.local'. Below this, a table lists various audit settings:

Stratégie	Paramètres de stratégie
Auditer l'accès au service d'annuaire	Non défini
Auditer l'accès aux objets	Non défini
Auditer l'utilisation des privilèges	Non défini
Auditer la gestion des comptes	Réussite
Auditer le suivi des processus	Non défini
Auditer les événements de connexion	Non défini
Auditer les événements de connexion aux comptes	Non défini
Auditer les événements système	Non défini

A 'Propriétés de : Auditer la gestion des comptes' dialog box is open, showing the 'Paramètre de stratégie de sécurité' tab. It displays the following configuration:

- Définir ces paramètres de stratégie
- Auditer les tentatives des types suivants :
 - Réussite
 - Échec

2. TEST



Succès de l'audit 4720 Information 16/05/2024 16:50:46 Micros... User Account Manae... Informat

Événement 4720, Microsoft Windows security auditing.

Général Détails

Un compte d'utilisateur a été créé.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x6A6A3

Nouveau compte :

- ID de sécurité : LEARN\TEST6
- Nom du compte : TEST6
- Domaine du compte : LEARN

Attributs :

- Nom du compte SAM : TEST6
- Nom complet : TEST6
- Nom principal de l'utilisateur : TEST6@learn.local
- Répertoire de base : -
- Lecteur de base : -
- Chemin d'accès au script : -
- Chemin d'accès au profil : -
- Stations de travail des utilisateurs : -
- Dernière modification du mot de passe le : < jamais >

Journal : Sécurité

Source : Microsoft Windows security Connecté : 16/05/2024 16:50:46

Événement : 4720 Catégorie : User Account Management

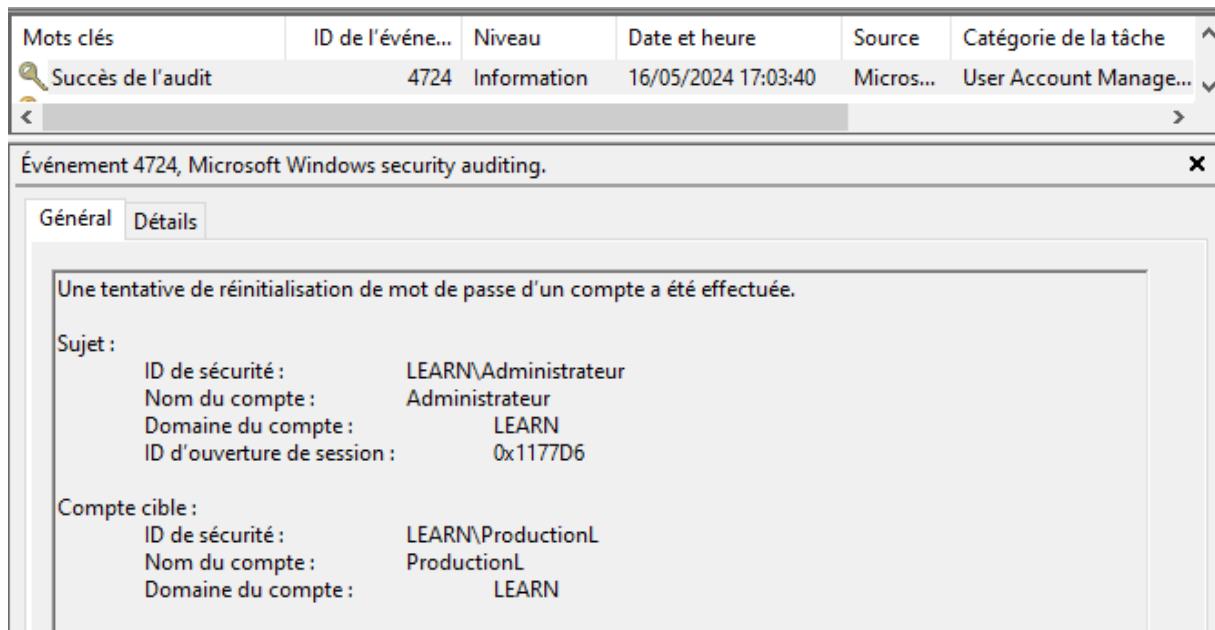
Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : DC1.learn.local

Opcode : Informations

Informations : [Aide sur le Journal](#)

3. TEST – Modifier le mot de passe de production



Mots clés ID de l'événement Niveau Date et heure Source Catégorie de la tâche

Succès de l'audit 4724 Information 16/05/2024 17:03:40 Micros... User Account Manae...

Événement 4724, Microsoft Windows security auditing.

Général Détails

Une tentative de réinitialisation de mot de passe d'un compte a été effectuée.

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x1177D6

Compte cible :

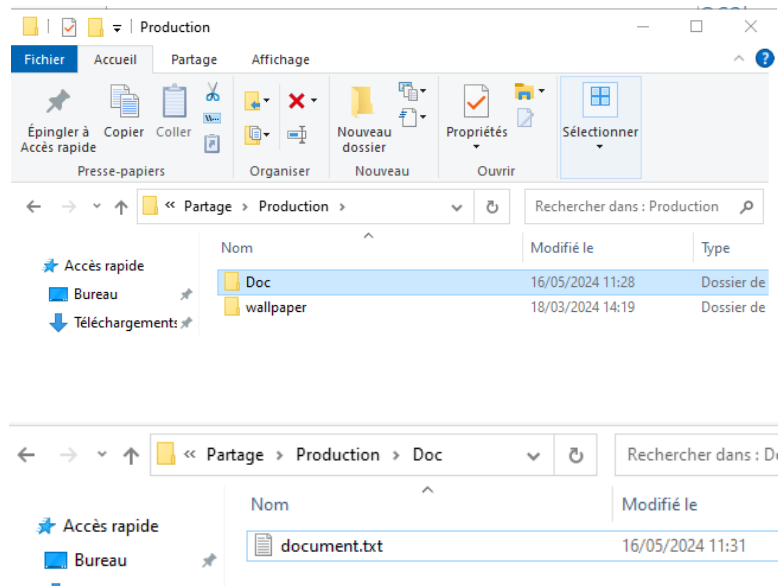
- ID de sécurité : LEARN\ProductionL
- Nom du compte : ProductionL
- Domaine du compte : LEARN



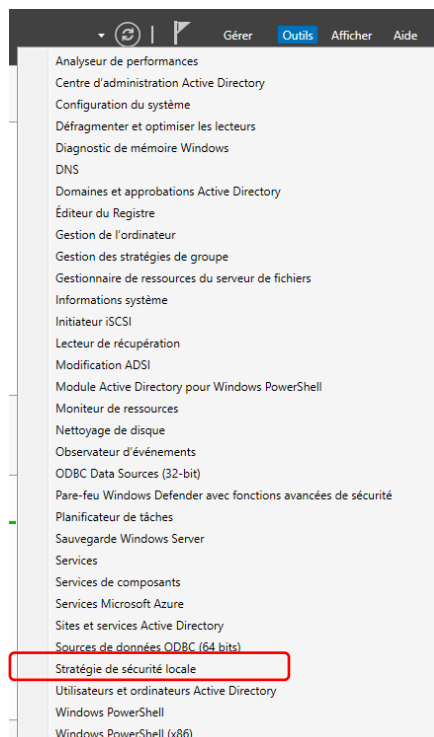
Procédure : Audit

Objectif : Créé un audit sur un dossier

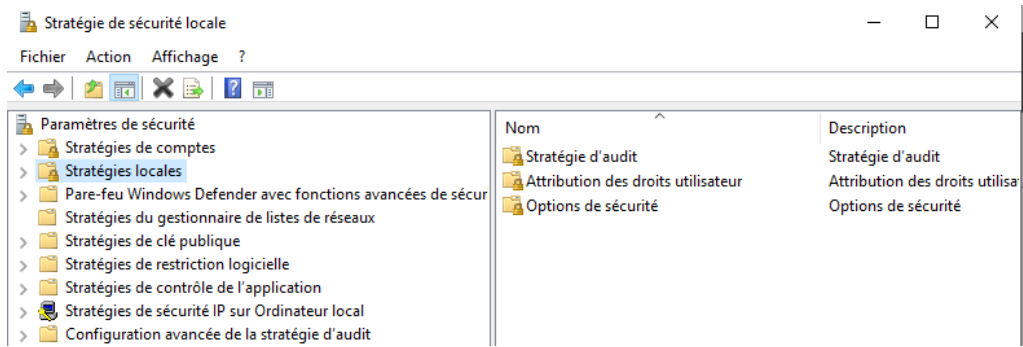
1. Le sous-dossier Doc est crée dans le dossier Production, ainsi que le document text



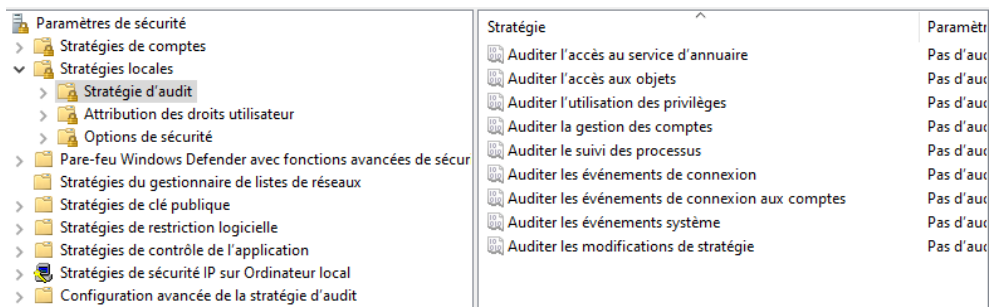
2. Création d'un audit sur le dossier production



Puis aller sur Stratégie de sécurité locale



Puis sur Stratégie d'audit

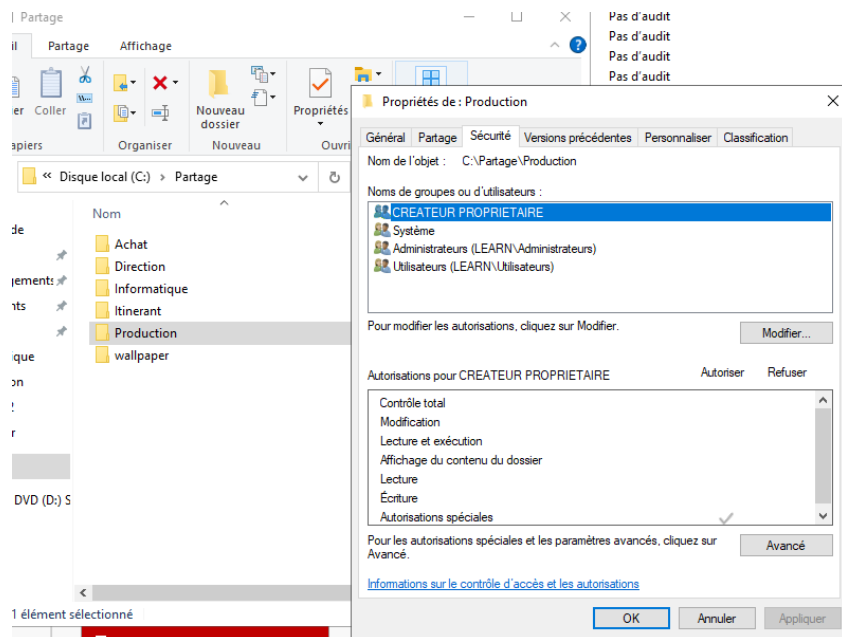


Ensuite Auditer l'accès aux objets

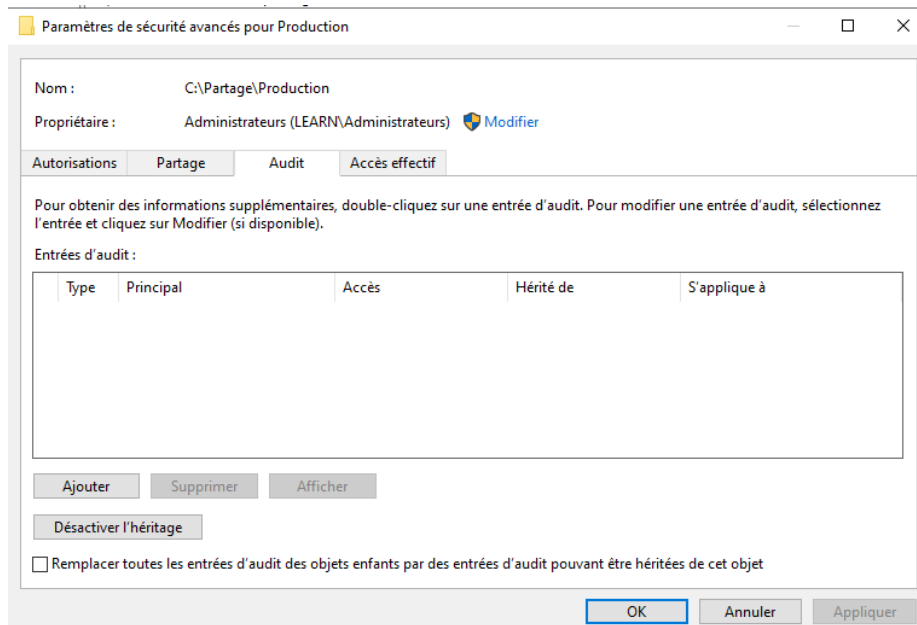
3. Définir les objets à auditer

Clic droit sur le dossier production, propriétés

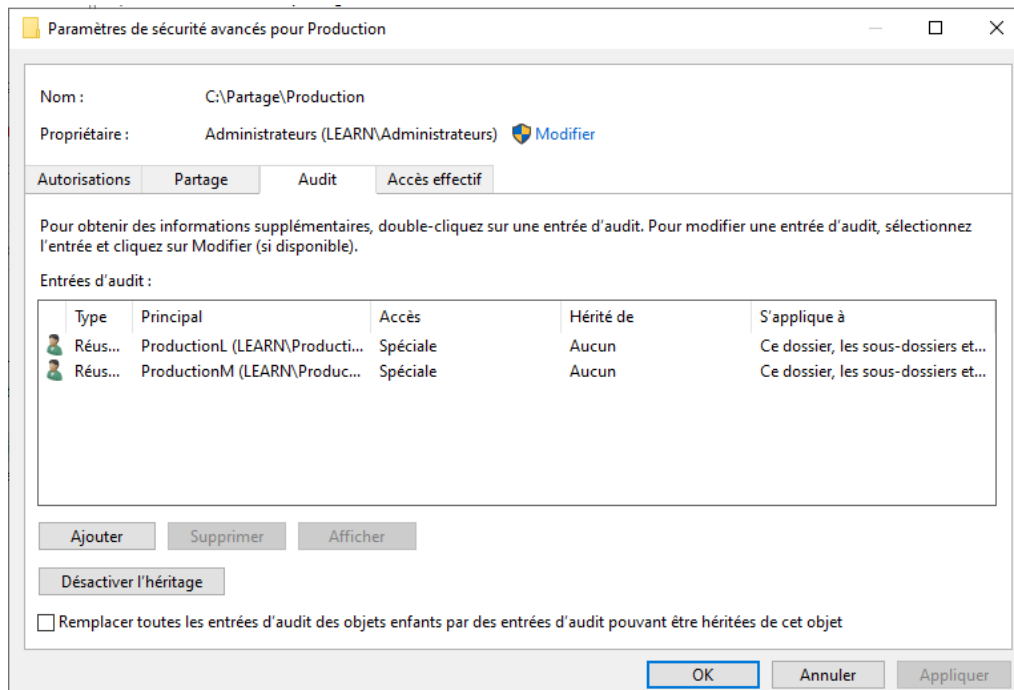
Aller dans l'onglet sécurité puis paramètre avancer



Aller dans l'onglet Audit



Crée un audit pour chaque utilisateur



4. TEST

Filtré : Journal: Security; Source: ; ID de l'événement: 4659. Nombre d'événements : 1

Mots clés	Niveau	Date et heure	Source	ID de l'...	Catégo...	Code opérationnel	Nom source de l'évén...
Succès de l'audit	Information	16/05/2024 12:42:25	Micros...	4659	File Sys...	Informations	

Événement 4659, Microsoft Windows security auditing.

Général Détails

Un handle vers un objet a été demandé dans un but de suppression.

Sujet :

ID de sécurité : LEARN\ProductionM
Nom du compte : ProductionM
Domaine du compte : LEARN
ID d'ouverture de session : 0xE2C66

Objet :

Serveur de l'objet : Security
Type d'objet : File
Nom de l'objet : C:\Partage\Production\Doc\document.txt
ID du handle : 0x0

Informations sur le processus :
ID du processus : 0x4

Informations sur la demande d'accès :
ID de la transaction : {00000000-0000-0000-0000-000000000000}
Accès : DELETE
ReadAttributes

Journal : Sécurité
Source : Microsoft Windows security Connecté : 16/05/2024 12:42:25
Événement : 4659 Catégorie : File System
Niveau : Information Mots-clés : Succès de l'audit
Utilisateur : N/A Ordinateur : DC1.learn.local
Opcode : Informations
Informations : [Aide sur le Journal](#)

5. Audit Direction

Refaire à partir de la 3 pour le dossier direction

Paramètres de sécurité avancés pour Direction

Nom : C:\Partage\Direction
Propriétaire : Administrateurs (LEARN\Administrateurs) [Modifier](#)

Autorisations Partage Audit **Accès effectif**

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'audit. Pour modifier une entrée d'audit, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'audit :

Type	P..	Accès	Hérité de	S'applique à
Réus...	U..	Parcours/exécution	Aucun	Ce dossier, les sous-dossiers et...

Remplacer toutes les entrées d'audit des objets enfants par des entrées d'audit pouvant être héritées de cet objet

6. TEST

The screenshot displays the Windows Event Viewer interface. At the top, a table lists event details:

Mots clés	ID de l'événement	Niveau	Date
Échec de l'audit	4656	Information	16/0

Below the table, the 'Événement 4656, Microsoft Windows security auditing.' window is open, showing the 'Général' tab. The main text reads: 'Un handle vers un objet a été demandé.'

Sujet :

- ID de sécurité : LEARN\Administrateur
- Nom du compte : Administrateur
- Domaine du compte : LEARN
- ID d'ouverture de session : 0x660B0

Objet :

- Serveur de l'objet : Security
- Type d'objet : File
- Nom de l'objet : C:\Windows\System32\secpol.msc
- ID du handle : 0x0
- Attributs de ressource : -

Informations sur le processus :

- ID du processus : 0x190
- Nom du processus : C:\Windows\System32\mmc.exe

Informations sur la demande d'accès :

- ID de la transaction : {00000000-0000-0000-0000-000000000000}
- Accès : READ_CONTROL, SYNCHRONIZE, Écriture données (ou ajout fichier)

Journal : Sécurité

Source : Microsoft Windows security **Connecté :** 16/05/2024 14:19:50

Événement : 4656 **Catégorie :** File System

Niveau : Information **Mots-clés :** Échec de l'audit

Utilisateur : N/A **Ordinateur :** DC1.learn.local

Opcode : Informations

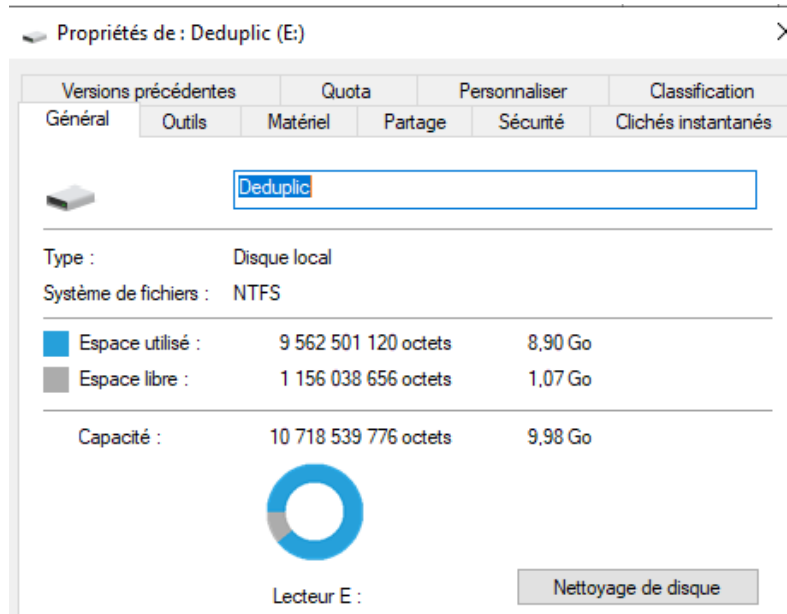
Informations : [Aide sur le Journal](#)



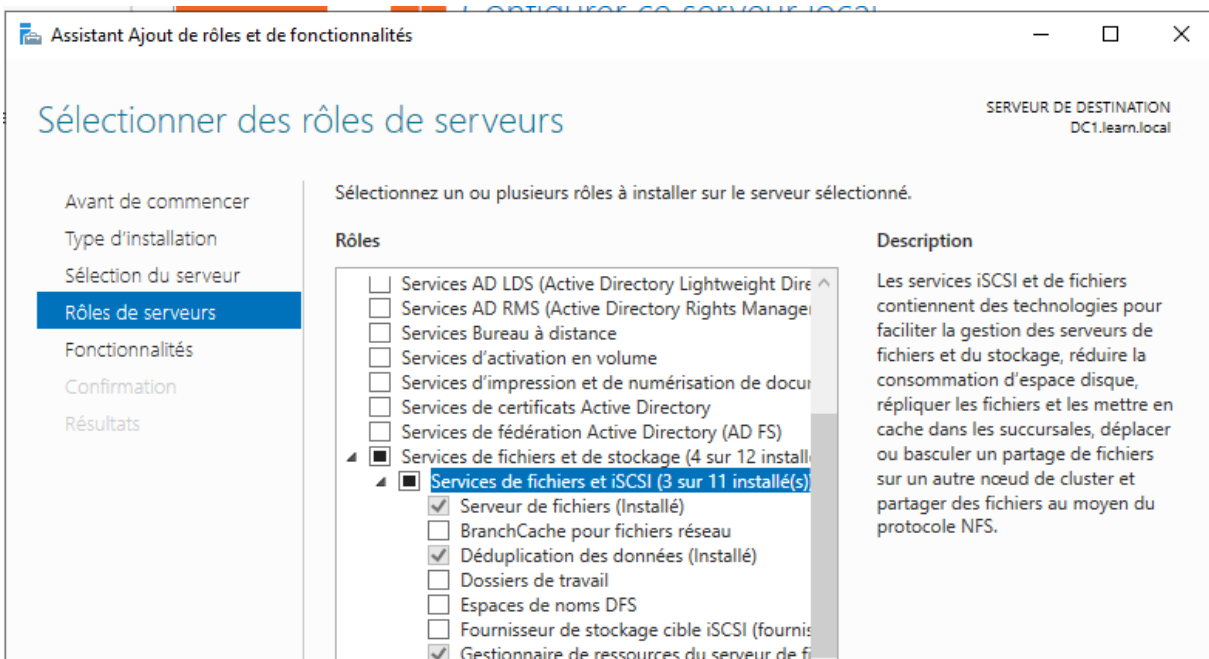
Procédure : Déduplication

Objectif : Apprendre à utiliser la déduplication

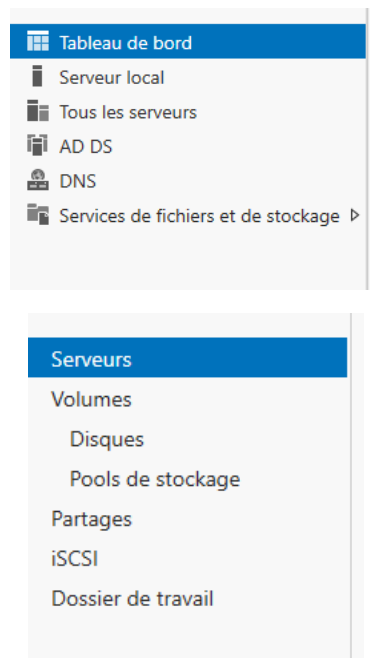
1. Après la création d'un disque dur de 10Go et son remplissage



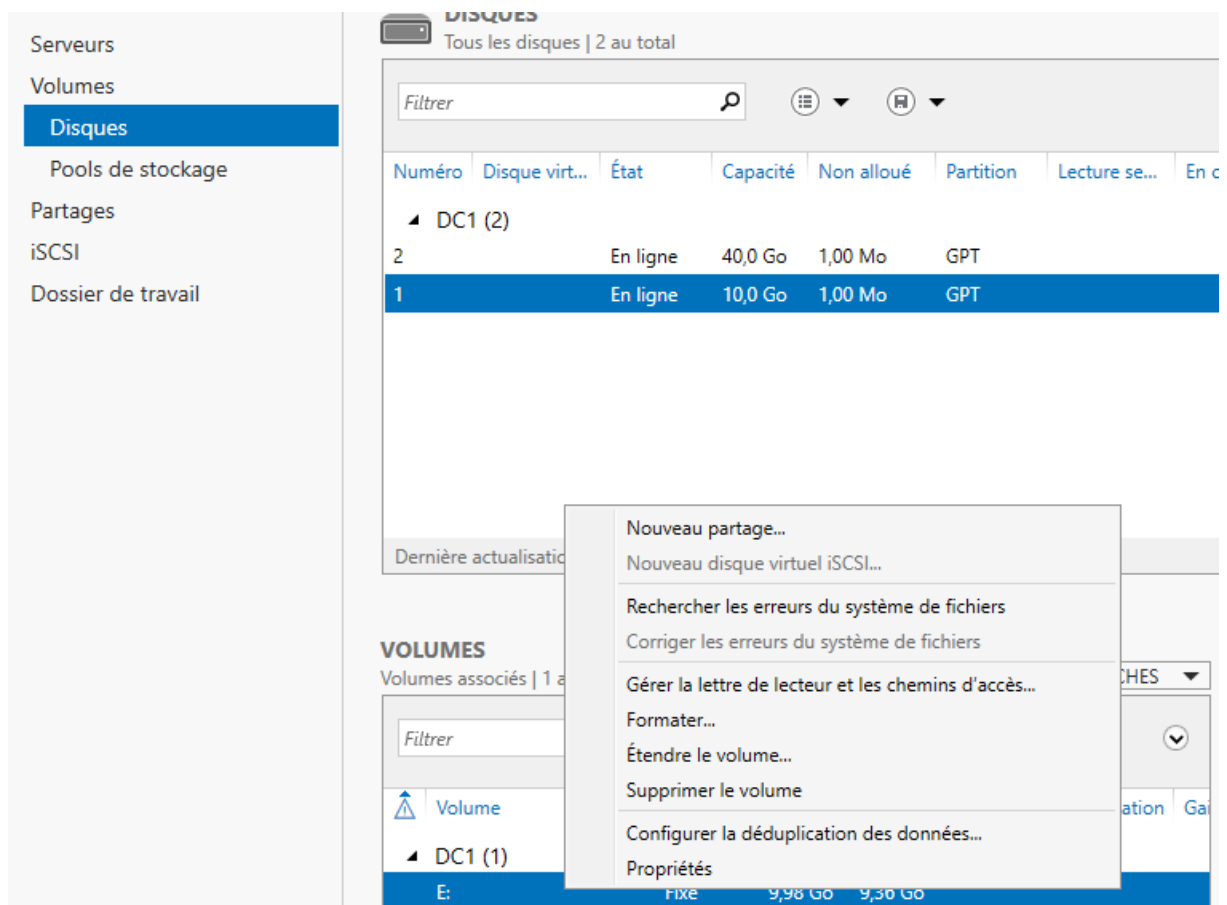
2. Ensuite installer le rôle déduplication



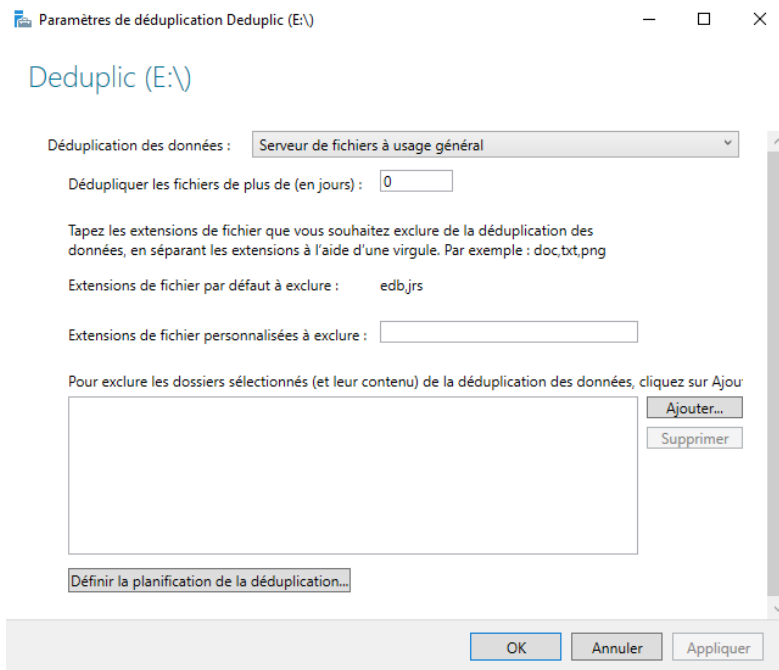
3. Aller dans Services de fichiers et de stockage, puis disque



4. Clic droit sur le disque de 10Go, puis configurer la déduplication des données



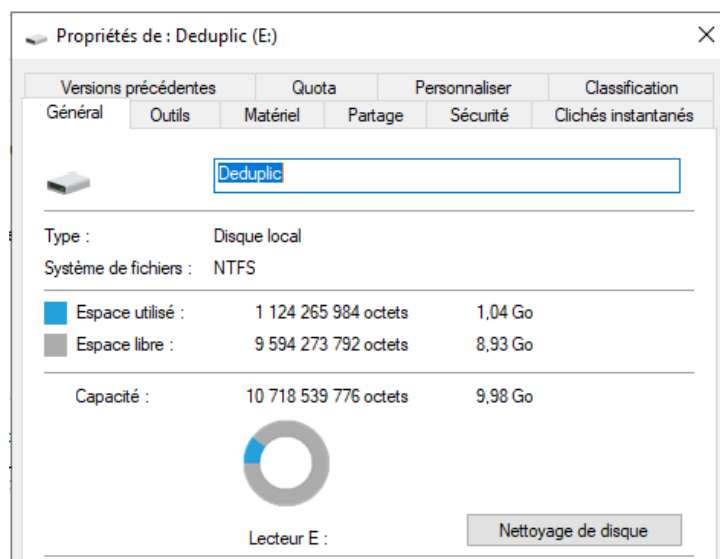
5. Choisir Serveur et fichiers à usage général



6. TEST

On peut forcer la déduplication depuis le planificateur d'évènement -> Microsoft -> Windows -> déduplication et sur la ligne BackgroundOptimization clic droit exécuter

Nom	Statut
BackgroundOptimization	En c...
WeeklyGarbageCollection	Prêt
WeeklyScrubbing	Prêt

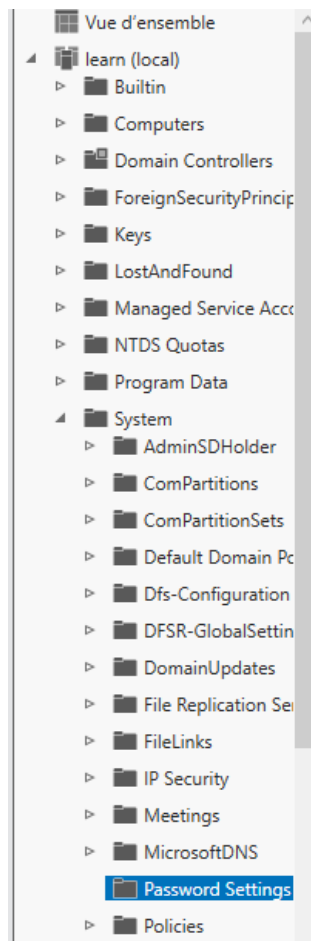




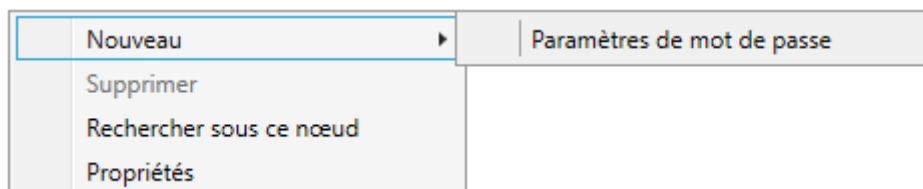
Procédure :

Objectif :

1. Dans l'AD allez sur le centre administration



2. Crée un nouveau paramètre de mot de passe



3. Mettre les paramètres recommandés mais limiter les tentatives à 3 et réinitialiser le compteur et déverrouiller le compte au bout de 5min

Nom : *	<input type="text" value="poL_mdp_general"/>	Options d'âge du mot de passe :	
Priorité : *	<input type="text" value="1"/>	<input checked="" type="checkbox"/> Appliquer l'âge minimal de mot de passe	
<input checked="" type="checkbox"/> Appliquer la longueur minimale du mot de passe		L'utilisateur ne peut pas changer le mot de passe d'ici à (jours) :	* <input type="text" value="1"/>
Longueur minimale du mot de passe (caractères) :	* <input type="text" value="7"/>	<input checked="" type="checkbox"/> Appliquer l'âge maximal de mot de passe	
<input checked="" type="checkbox"/> Appliquer l'historique des mots de passe		L'utilisateur doit changer le mot de passe après (jours) :	* <input type="text" value="42"/>
Nombre de mots de passe mémorisés :	* <input type="text" value="24"/>	<input checked="" type="checkbox"/> Appliquer la stratégie de verrouillage des comptes :	
<input checked="" type="checkbox"/> Le mot de passe doit respecter des exigences de complexité		Nombre de tentatives de connexion échouées autorisé :	* <input type="text" value="3"/>
<input type="checkbox"/> Stocker le mot de passe en utilisant un chiffrement réversible		Réinitialiser le nombre de tentatives de connexion échouées après (mins) :	* <input type="text" value="5"/>
<input checked="" type="checkbox"/> Protéger contre la suppression accidentelle		Le compte va être verrouillé	
Description :	<input type="text"/>	<input checked="" type="radio"/> Pendant une durée de (mins) :	* <input type="text" value="5"/>
		<input type="radio"/> Jusqu'à ce qu'un administrateur déverrouille manuellement le compte	

On n'oublie pas de l'appliquer au compte production et Achat



Partie 2

1. Créez une nouvelle stratégie de mot de passe

Paramètres de mot de passe

Nom :	* Pol_mdp_dir	Options d'âge du mot de passe :	
Priorité :	* 1	<input checked="" type="checkbox"/> Appliquer l'âge minimal de mot de passe	
<input checked="" type="checkbox"/> Appliquer la longueur minimale du mot de passe		L'utilisateur ne peut pas changer le mot de passe d'ici à (jours) :	* 1
Longueur minimale du mot de passe (caractères) :	* 12	<input checked="" type="checkbox"/> Appliquer l'âge maximal de mot de passe	
<input checked="" type="checkbox"/> Appliquer l'historique des mots de passe		L'utilisateur doit changer le mot de passe après (jours) :	* 42
Nombre de mots de passe mémorisés :	* 24	<input checked="" type="checkbox"/> Appliquer la stratégie de verrouillage des comptes :	
<input checked="" type="checkbox"/> Le mot de passe doit respecter des exigences de complexité		Nombre de tentatives de connexion échouées autorisées :	* 3
<input type="checkbox"/> Stocker le mot de passe en utilisant un chiffrement réversible		Réinitialiser le nombre de tentatives de connexion échouées après (mins) :	* 30
<input checked="" type="checkbox"/> Protéger contre la suppression accidentelle		Le compte va être verrouillé	
Description :		<input type="radio"/> Pendant une durée de (mins) :	* 30
		<input checked="" type="radio"/> Jusqu'à ce qu'un administrateur déverrouille manuellement le compte	

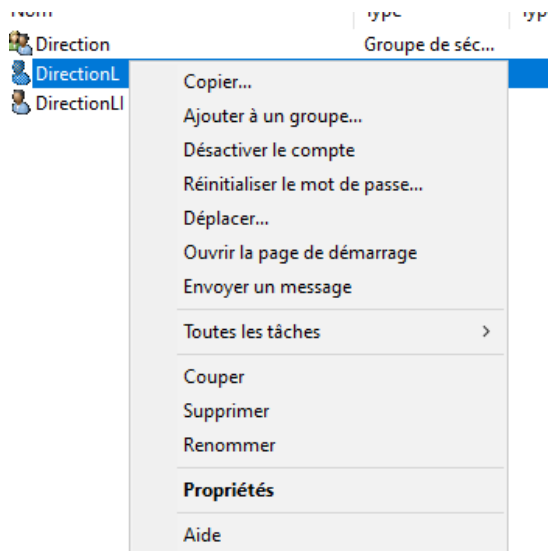
2. Le compte est bien bloqué au bout de 3 essais



3. Déblocage

Dans Utilisateurs et Ordinateurs de l'active directory

Clic droit sur l'utilisateur puis propriété, dans compte apparait



Déverrouiller le compte. Ce compte est actuellement verrouillé sur ce contrôleur de domaine Active Directory.

Coché la case puis appliquer et ok

Le compte est déverrouillé

