



# Formation OpenClassrooms Administrateur Systèmes, Réseaux Et Sécurité

## Soutenance Projet-06

Stéphane Perfetti

23/07/2024



# Projet 06

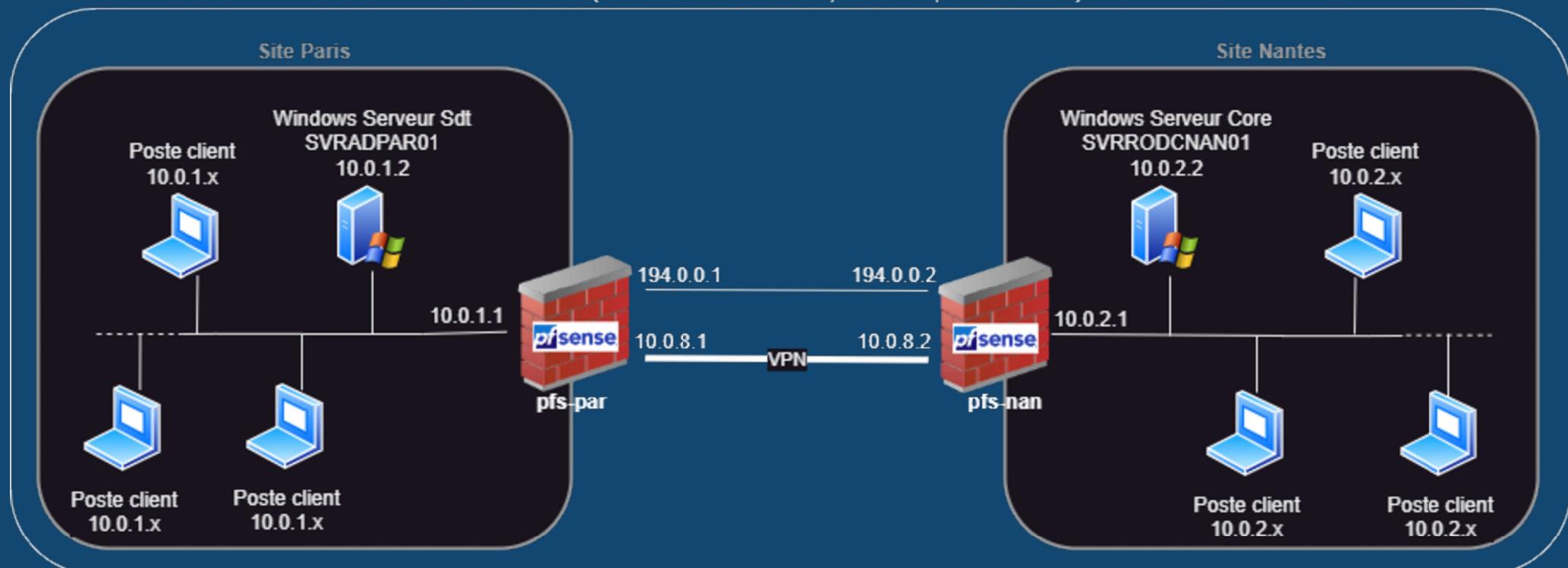
-

## Raccordez une entité et ses postes de travail au SI de votre entreprise

- Scénario :
  - La société OpenBank située à Paris vient d'acquérir de nouveaux locaux à Nantes.
  - Mission: Déployer et à relier informatiquement le site de Nantes au site de Paris.
- Plan d'action :
  - Architecture du laboratoire
  - Configuration de la connexion VPN Site à Site
  - Configurations des Windows Server / Active Directory des sites de Paris et de Nantes
  - Politiques de groupe
  - Sauvegarde sous Google Drive

# Architecture du prototype

VirtualBox (Réseaux Privés: Int Paris; Int Nantes; Ext Site à Site)



# Configuration des Firewall PfSense

- PfSense site Paris: pfs-par

System Information

Name	pfs-par.openbank.com
User	admin@10.0.1.2 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: bc388247fe1f0dfbb970
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64)

Interfaces

WAN	1000baseT <full-duplex>	194.0.0.1
LAN	1000baseT <full-duplex>	10.0.1.1

Netgate Services And Support

Retrieving support information

- PfSense site Nantes: pfs-nan

System Information

Name	pfs-nan.openbank.com
User	admin@10.0.2.3 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: b6d255b8e644594e973f
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64)

Interfaces

WAN	1000baseT <full-duplex>	194.0.0.2
LAN	1000baseT <full-duplex>	10.0.2.1

Netgate Services And Support

Retrieving support information

## Configuration des PfSense:

- Réseaux Int. Paris et Int. Nantes comme interface privées (LAN)
- Réseau Ext. Site à Site comme interface publique (WAN)

# Configuration VPN Site à Site entre Pfsense

- Utilisation du protocole OpenVPN, réseau: 10.0.8.0/30
- Règles de filtrages firewall: autorisant les clients OpenVPN sur l'interface publique (WAN) pfs-par et autorisant les communications au travers du tunnel VPN.

Site Paris

OpenVPN Serveur Config

```
dev ovpns1
verb 3
dev-type tun
dev-node /dev/tun1
writepid /var/run/openvpn_server1.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp4
auth SHA256
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
local 194.0.0.1
ifconfig 10.0.8.1 10.0.8.2
lport 1194
management /var/etc/openvpn/server1.sock unix
max-clients 1
route 10.0.2.0 255.255.255.0
secret /var/etc/openvpn/server1/secret
cipher AES-256-CBC
allow-compression no
resolv-retry infinite
```

Site Nantes

OpenVPN Client Config

```
dev ovpnc1
verb 3
dev-type tun
dev-node /dev/tun1
writepid /var/run/openvpn_client1.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp4
auth SHA256
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
local 194.0.0.2
lport 0
management /var/etc/openvpn/client1.sock unix
remote 194.0.0.1 1194 udp4
ifconfig 10.0.8.2 10.0.8.1
route 10.0.1.0 255.255.255.0
secret /var/etc/openvpn/client1/secret
cipher AES-256-CBC
allow-compression no
resolv-retry infinite
```

The screenshot shows the Pfsense Community Edition web interface. At the top, the navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has tabs for Status, Firewall, Rules, and WAN.

**Status / OpenVPN**

Name	Status	Last Change	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpns1 Site2Site-VPN UDP4:1194	Connected (Success)	Tue Jul 16 15:51:15 2024	10.0.8.1	194.0.0.2	3.56 MiB	8.34 MiB	

**Firewall / Rules / WAN**

Floating **WAN** LAN OpenVPN

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/688 B	IPv4 UDP	*	*	194.0.0.1	1194 (OpenVPN)	*	none	OpenVPN-Site2Site	

**Firewall / Rules / OpenVPN**

Floating WAN LAN **OpenVPN**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/2.46 MiB	IPv4 *	*	*	*	*	*	none		

# Installation/Configuration Windows Servers:

## Site Paris Serveur SVRADPAR01

Informations système

Spécifications de l'appareil

Nom de l'appareil	SVRADPAR01
Processeur	12th Gen Intel(R) Core(TM) i5-12450H 2.50 GHz
Mémoire RAM installée	4,00 Go
ID de périphérique	BE504A98-07B9-4A71-A05D-911BDEA8BAFF
ID de produit	00431-10000-00000-AA222
Type du système	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

[Renommer ce PC](#)

Spécifications de Windows

Édition	Windows Server 2019 Standard Evaluation
Version	1809
Installé le	04/07/2024
Build du système d'exploitation	17763.3650

[Mettre à niveau votre édition de Windows ou modifier la clé de produit  
\(Product Key\)](#)

[Lire le Contrat de services Microsoft qui s'applique à nos services](#)

[Lire les termes du contrat de licence logiciel Microsoft](#)

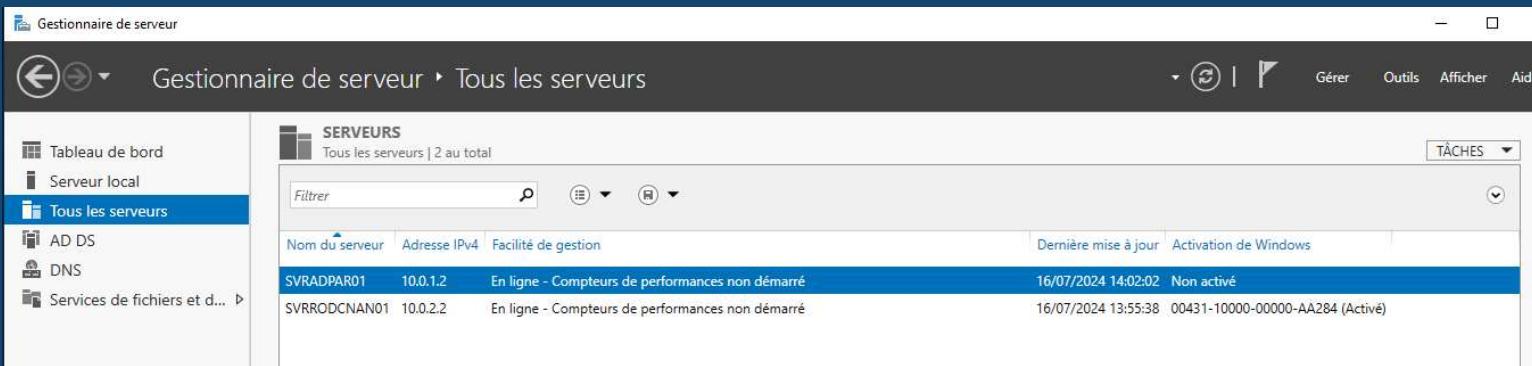
## Site Nantes Serveur SVRRODCNAN01

```
PS C:\Users\Administrateur.OPENBANK> Get-ComputerInfo | select CsName, WindowsProductName, WindowsInstallationType, OsProductType, CsDomain, CsDomainRole
```

CsName	: SVRRODCNAN01
WindowsProductName	: Windows Server 2019 Standard Evaluation
WindowsInstallationType	: Server Core
OsProductType	: DomainController
CsDomain	: openbank.com
CsDomainRole	: BackupDomainController

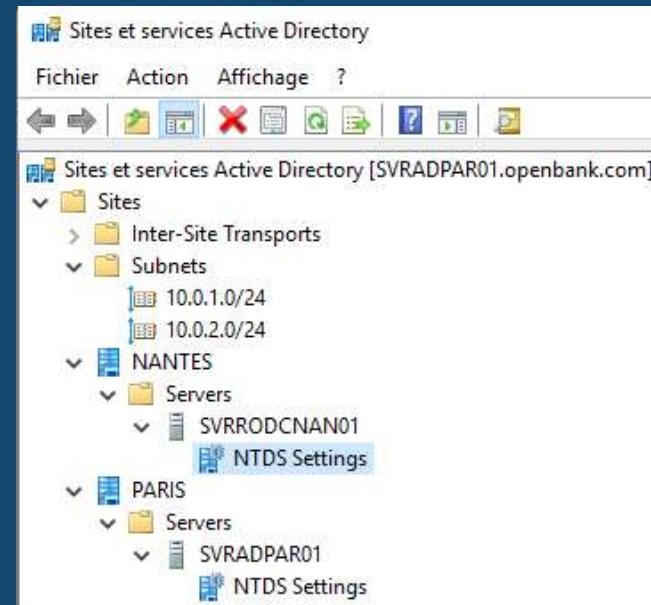
- Site Paris:
  - Installation Windows Server, rôle Active Directory et DNS
  - Création du Contrôleur de domaine principal (lecture/écriture) et du domaine [openbank.com](#)
- Site Nantes:
  - Installation Windows Server Core
  - Intégration au domaine [openbank.com](#)
- Serveur Paris:
  - Ajout du serveur de Nantes dans le gestionnaire de serveur.
  - Installation des rôle Active Directory et DNS sur le serveur de Nantes.
  - Création du Contrôleur de domaine secondaire RODC (lecture seule) sur le serveur de Nantes avec réplication a partir du contrôleur de domaine de Paris.

# Installation/Configuration Windows Server:



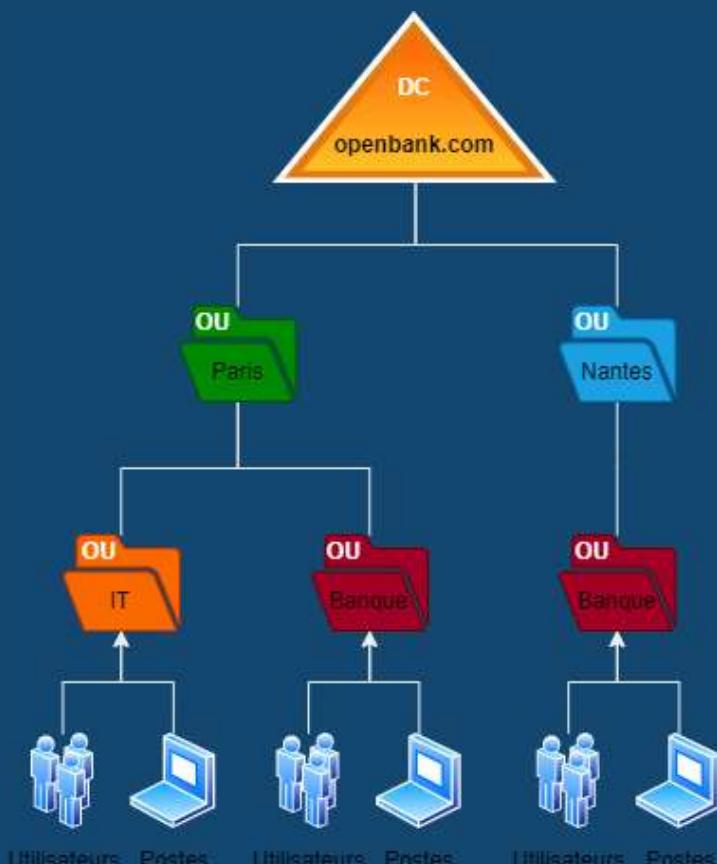
Windows Server des sites de Paris et Nantes fonctionnels et connectés

- Crédation des sites Active Directory Paris et Nantes, association des serveurs AD respectifs.
- Crédation des sous-réseaux pour chaque sites.



# Domaine, Unités d'Organisations et Utilisateurs:

- Création des unités d'organisations (OU) suivant l'organigramme.
- Créations des utilisateurs avec liens hiérarchiques



Interface utilisateur de l'outil "Utilisateurs et ordinateurs Active Directory" :

Arborescence de l'arbre :

- Utilisateurs et ordinateurs Active Directory
- openbank.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - NANTES
    - BANQUE
    - PARIS
      - BANQUE
      - IT
    - Users

Liste des utilisateurs :

Nom	Type	Description
David Azoulay	Utilisateur	
Lucie Garrido	Utilisateur	
Sabrina Ouazani	Utilisateur	

Propriétés de : Sabrina Ouazani

Fenêtre de propriétés pour l'utilisateur Sabrina Ouazani :

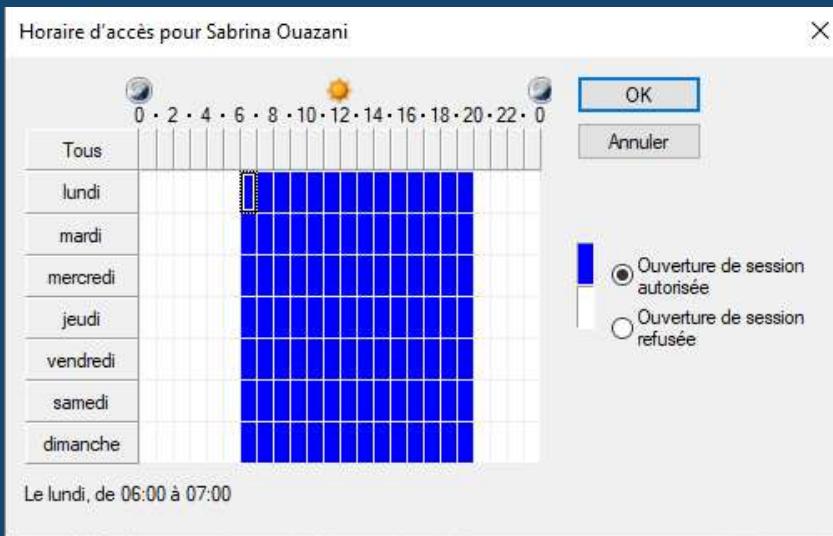
- Général :
  - Fonction : Responsable
  - Service : Banque
  - Société :
  - Gestionnaire : Nom : Louise Chapat
- Collaborateurs : David Azoulay, Lucie Garrido

Buttons : OK, Annuler, Appliquer, Aide

# Politique de groupe:

Besoin: Les employés ont l'interdiction de travailler entre 20h et 6h.

- Réglage individuel pour chaque utilisateur, des horaires de connexions.
- Utilisation d'un script PowerShell pour effectuer un traitement de masse, suivant le nom distingué, l'OU et ou l'utilisateur.



```
<#
.Synopsis
    Script to apply AD-users logon days and hours restrictions
.DESCRIPTION
    This script will search all enabled users into the specified DistinguishedName
    level and apply logon days and hours parameters, except for users present into
    the $OU_EXCLUDE (organisation unit) or $USERS_EXCLUDE (user name) variables.
.EXAMPLE
    PS> .\UserLogonTimeRestriction.ps1
.NOTES
    Version:      1.0
    Author:       Stephane
    Creation Date: 05/07/2024
    Purpose/Change: v1.0: Initial script development
#>

##-[Initialisations]-----
$ErrorActionPreference = "Stop"

##-[Declarations]-
$SEARCHBASE = "DC=openbank,DC=com" # DistinguishedName search level
$OU_EXCLUDE = "*OU=IT*"           # Organisation unit to exclude
$USERS_EXCLUDE = @(
    'Administrateur',
    'Visiteur')
$LOGON_DAYS = "L-D"               # Logon days period
$LOGON_HOURS = "6:00AM-8:00PM"     # Logon hours period

##-[Execution]-----

# Export all enabled users from $SEARCHBASE into csv file
$USERS_CSV = "C:\Windows\temp\users-export.csv"
Get-ADUser -Filter "Enabled -eq 'true'" -SearchBase $SEARCHBASE |>
    Export-Csv $USERS_CSV -NoTypeInformation

$CSV = Import-Csv -Path $USERS_CSV

Foreach ($user in $CSV) {
    if ($user.DistinguishedName -notlike $OU_EXCLUDE -and ($user.Name -notin $USERS_EXCLUDE)) {
        # Configure user logon hours
        net user $user.GivenName /times:$LOGON_DAYS, $LOGON_HOURS -
        Write-Host -ForegroundColor Green "User $user.Name configured."
    }
}
```

# Politique de groupe:

Besoin: Les disques amovibles ne sont pas autorisés, sauf pour le service IT.

→ GPO configuration ordinateur:

- Stratégie: "Toutes les classes de stockage amovible: refuser tous les accès".
- Liaisons: Appliquée au domaine entier.
- Délégation: A l'exception du groupe utilisateur IT.

GPO\_C\_USB-Disable  
Données recueillies le : 18/07/2024 14:35:54

**Général**

**Détails**

**Liaisons**

Emplacement	Appliqué	État du lien	Chemin d'accès
openbank	Non	Activé	openbank.com

Cette liste ne contient que les liaisons du domaine de l'objet de stratégie de groupe.

**Filtrage de sécurité**

**Délégation**

Ces groupes et utilisateurs ont l'autorisation spécifiée pour cet objet de stratégie de groupe.

Nom	Autorisations acceptées	Hérité
OPENBANK\IT	Personnalisé	Non

**Configuration ordinateur (activée)**

**Stratégies**

**Modèles d'administration**

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

**Système/Accès au stockage amovible**

Stratégie	Paramètre
Toutes les classes de stockage amovible : refuser tous les accès	Activé

Paramètres de sécurité pour GPO\_C\_USB-Disable

**Sécurité**

Noms de groupes ou d'utilisateurs :

- CREATEUR PROPRIÉTAIRE
- Utilisateurs authentifiés
- Système
- IT (OPENBANK\IT)

Ajouter... Supprimer

**Autorisations pour IT**

	Autoriser	Refuser
Lire	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Écrire	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Créer tous les objets enfants	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Supprimer tous les objets enfants	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Appliquer la stratégie de groupe	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

Informations sur le contrôle d'accès et les autorisations

OK Annuler Appliquer

# Politique de groupe:

Besoin: L'outil f.lux doit être déployé sur le poste de la collaboratrice Ana Garcia du site de Nantes.

→ GPO configuration utilisateur:

- Stratégies:
  - "Exécution script PowerShell à l'ouverture de session" .
  - "Activer l'exécution des scripts" .
- Liaisons: Appliquée qu'à l'utilisateur Ana.

The screenshot shows the 'GPO\_U\_Install-flux\_Ana-Garcia' configuration page. In the 'Stratégies Windows' section, the 'Scripts' tab is selected. Under 'Ouvrir la session', it says 'For this GPO, Script order: Les scripts Windows PowerShell s'exécuteront en premier.' A single script named 'InstallExe.ps1' is listed with the parameter '\$silentArg'. Below this, the 'Modèles d'administration' section shows a table with two rows: 'Activer l'exécution des scripts' (Activé) and 'Stratégie d'exécution' (Autoriser les scripts locaux et les scripts signés distants).

```
<#
Description: This script will Install silently .exe package from shared
Parameters: None
Example: PS> .\InstallExe.ps1
Notes:
Version:      1.0
Author:       Stephane
Creation Date: 10/07/2024
Purpose/Change: v1.0: Initial script development
#>

#--[Initialisations]-----
$ErrorActionPreference = "Stop"

#--[Declarations]-----
$PackageName = "flux-setup.exe"
$SoftwareName = "f.lux"
$SOFTWARE_VERSION = "4.134"
$SilentArg = "/S"
$PackageFolder = "\\SVRADPAR01\sysvol\openbank.com\App"
$LocalFolder = "C:\TEMP"

#--[Execution]-----
if (Test-Path "$PackageFolder\$PackageName") {
    # Check if software already installed and return his version
    $INSTALLED_VERSION = (Get-Package $SoftwareName -ErrorAction SilentlyContinue).version

    if ((($null -eq $INSTALLED_VERSION) -or ` 
        ($null -ne $INSTALLED_VERSION -and $INSTALLED_VERSION -ne $SOFTWARE_VERSION)) {
        # Copy package on local computer
        New-Item -ItemType Directory -Path $LocalFolder
        Copy-Item "$PackageFolder\$PackageName" $LocalFolder -Force

        # Install package
        if (Test-Path "$LocalFolder\$PackageName") {
            Start-Process -Wait -FilePath "$LocalFolder\$PackageName" -ArgumentList "$SilentArg"
        }
    }

    # Remove package
    Remove-Item "$LocalFolder\$PackageName"
}
else {
    Write-Host "Package $PackageName v.$INSTALLED_VERSION already installed." -ForegroundColor Cyan
}
else {
    Write-Warning "Package $PackageName not found in $PackageFolder\" 
    Exit 0
}
```

# Politique de groupe: Résumé

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console window. The left pane displays a tree view of group policy objects (GPOs) under the 'Forêt : openbank.com' root. The 'Domaines' node contains several GPOs, including 'Default Domain Policy', 'GPO\_C\_Deconnexion-expiration-session', 'GPO\_C\_USB-Disable', and 'GPO\_U\_Install-flux\_Ana-Garcia'. Below 'Domaines' are 'Domain Controllers' and 'NANTES' and 'PARIS' sites, each with their own GPOs. The 'Objets de stratégie de groupe' node also lists these GPOs. The right pane shows a table titled 'Objets de stratégie de groupe dans openbank.com' with the following data:

Nom	État GPO	Filtre WMI	Modifié le	Propriétaire
Default Domain Controllers Policy	Activé	Aucun(e)	04/07/2024 15:11:10	Admins du domaine (OPEN...)
Default Domain Policy	Activé	Aucun(e)	04/07/2024 16:27:40	Admins du domaine (OPEN...)
GPO_C_Deconnexion-expiration-session	Activé	Aucun(e)	11/07/2024 11:42:28	Admins du domaine (OPEN...)
GPO_C_USB-Disable	Activé	Aucun(e)	09/07/2024 11:01:52	Admins du domaine (OPEN...)
GPO_U_FondEcran_Nantes	Activé	Aucun(e)	11/07/2024 00:31:12	Admins du domaine (OPEN...)
GPO_U_FondEcran_Paris	Activé	Aucun(e)	11/07/2024 00:28:54	Admins du domaine (OPEN...)
GPO_U_Install-flux_Ana-Garcia	Activé	Aucun(e)	11/07/2024 11:19:38	Admins du domaine (OPEN...)

# Sauvegarde lecteur D: sous Google Drive:

Création d'un lecteur D: et d'un répertoire partagé 'Share' disponible sous:  
\\SVRADPAR\\share

Possibilité de stocker les répertoires système Active Directory (base de données, fichiers logs, partage SYSVOL)

The screenshot shows the Windows Server Manager interface under 'Services de fichiers et de stockage > Volumes'.  
**VOLUMES**: Lists two volumes: SVRADPAR01 (3) and SVRRODCNAN01 (2).  
**RESSOURCES PARTAGÉES**: Shows a share named D:\\Share.  
**DISQUE**: Details about the physical disk D:\\ on SVRADPAR01.

Volume	Statut	Nom de système...	Allocation	Capacité	Espace libre	Taux de déduplication	Gain de déduplication	Pourcentage u...
SVRADPAR01 (3) \\?\Volume[c04...	Réserve au système	Fixe	549 Mo	133 Mo				
C:		Fixe	49,5 Go	38,2 Go				
D:	Volume-D	Fixe	5,00 Go	4,97 Go				
SVRRODCNAN01 (2) \\?\Volume[34...	Réserve au système	Fixe	549 Mo	134 Mo				
C:		Fixe	49,5 Go	41,3 Go				

Dernière actualisation : 16/07/2024 14:16:24

Partager	Chemin d'accès local	Protocole	Type de disponibilité
Share	D:\\Share	SMB	Non-cluster

DISQUE  
D:\\ sur SVRADPAR01  
VBOX HARDDISK  
Capacité : 5,00 Go  
100% alloué(s) 5,00 Go alloué(s)  
0,00 Go non alloué(s)  
Statut : En ligne  
Type de bus : SATA

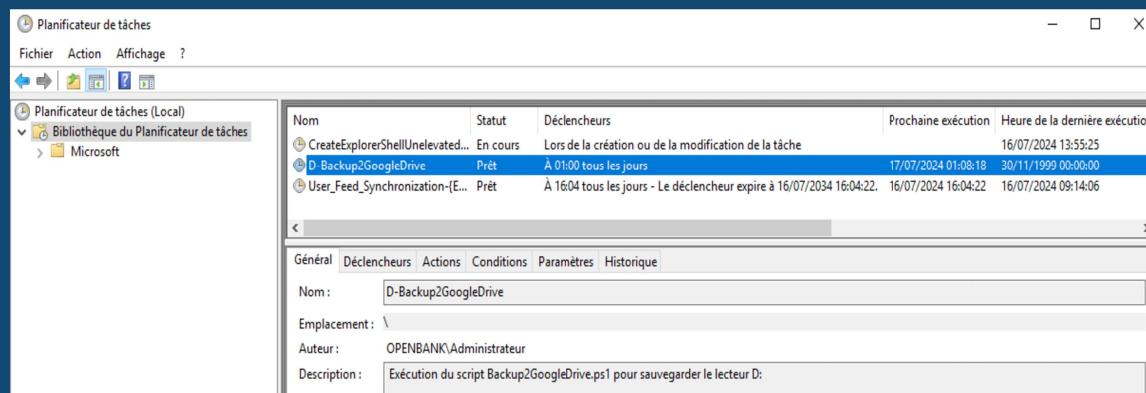
Sauvegarde vers Google Drive (plusieurs possibilités):

- ⚠ • Installer et utiliser le client Google Drive relié au lecteur D:, avec un script PowerShell qui copierait sous D: les données à sauvegarder.  
→ Potentiel risque de sécurité et ne respecterait pas les bonnes pratiques.
- ✓ • Script PowerShell utilisant les API Google Drive pour uploader les données à sauvegarder, avec déclenchement périodique à l'aide du planificateur de tâches.

# Script sauvegarde D: vers Google Drive:

```
Description: PowerShell script to upload data to Google Drive using Google Drive REST Api module.  
Data are being created belong to the API service-account email, need to give permission  
to owner of that account like.  
Data will be available in 'Shared with me' section.  
Require: Module GMGoogleDrive (https://github.com/MVKozlov/GMGoogleDrive/tree/master)  
Google Cloud Project (App), with Drive API enable and a Service Account  
Parameters: None  
Example: PS> .\Backup2Drive.ps1  
Notes:  
Version: 0.1  
Author: Stephane Perfetti  
Creation Date: 11/07/2024  
Purpose/Change: v0.1: Initial script development  
#>  
  
#--[Declarations]-----  
$GoogleAccountEmail = "openbank@gmail.com"  
$ServiceAccountEmail = "backup-serviceaccount@oc-p6-openbank-429304.iam.gserviceaccount.com"  
$ServiceAccountJson = "$PSScriptRoot\Backup-ServiceAccount@oc-p6-openbank.json"  
$Data2Backup = "D:"  
  
#--[Initialisations]-----  
$ErrorActionPreference = "Stop" # Stop; Ignore; Inquire  
Import-Module -Name "$PSScriptRoot\GMGoogleDrive"  
  
1 reference  
function Add-ToLog($logText) {  
    $date = Get-Date -Format "yyyy/mm/dd HH:mm:ss"  
    Add-Content -Value $date - "$env:COMPUTERNAME" - $logText -Path "$PSScriptRoot\log.txt"  
}  
  
#--[Execution]-----  
try {  
    # Get Authentication Token  
    $Token = (Get-GDriveAccessToken `  
        -Path $ServiceAccountJson -JsonServiceAccount `  
        -ImpersonationUser $ServiceAccountEmail).access_token  
  
    # Upload data and get its Id  
    $NewItemId = (Add-GDriveFolder -AccessToken $Token `  
        -Path $Data2Backup -ParentID "root" -Recurse -ShowProgress).id  
  
    # Change permission on uploaded data  
    Add-GDriveItemPermission -AccessToken $Token -ID $NewItemId `  
        -Role writer -Type user -EmailAddress $GoogleAccountEmail  
}  
catch {  
    Write-Error "Erreur: $_" && Add-ToLog("Erreur: $_")  
}
```

- Utilisation d'un projet Google Cloud avec API Google Drive activé, et création d'un compte de service associé.
- Utilisation du module PowerShell 'GMGoogleDrive' pour faciliter l'utilisation de l'API Google Drive.
- Déroulé:
  - Récupération d'un jeton d'authentification.
  - Copie des données sous D:
  - Modification des droits sur les données copiées



# Questions / Réponses

# Voies d'améliorations :