

Petite présentation école :

Contexte :

Le mode dégradé est un poste physique déployé sur chaque établissement, il permet de consulter les données importantes du DPI et éventuellement déclencher l'impression de ces données en cas d'incident réseau.

Il permet aux collaborateurs en établissement de continuer à exercer leurs fonctions même en cas de panne majeur réseaux

Dire qu'il n'y avait pas de MD en HAD

Mission :

Terminé le 06/12 initialement

20/12

- 1- Faire un AUDIT des configuration physique (clavier, souris, écran, onduleur, imprimante, et poste)
- 2- Passage des postes de distribution (Poste SCCM) en poste mode dégradé, et point de distribution.

Etapes :

- 1- Appelle des différents établissements pour demander la config.
- 2- Remonter les infos sur la config des poste MD à ma responsable pour pouvoir passer les commandes des différentes pièces manquantes (écran...)
- 3- Connexion via bomgar PMAD pour :
 - Renommer le poste de LNADPSCCM0000 ou LNAMD1000 (Quitter le domaine et le rejoindre, déplacement du poste dans l'ad dans la bonne OU)
 - Refaire le point de distribution SCCM
 - Créer un compte utilisateur local
 - Créer un répertoire accessible depuis le bureau
 - Partager le répertoire avec groupe AD
 - Réservation DHCP pour l'IP spécifique des postes
 - Ajouter les postes mode dégradé à la supervision

Script de mise en service de poste mode dégradé :

Création de groupe AD

```
1 $idEtab = Read-Host "ID Etablissement tel qu'il est renseigné dans LNA Data ? (1005, X075...)"
2
3 $groupMembers = "svc_vtom_mhcare_md"
4 $groupOU = "OU=Mode_degrade,OU=Domaines locaux,OU=Groupes,DC=noble-age,DC=fr"
5
6 $groupName = "GLS_PERM_$(($idEtab)_Mode-Degrade_RW"
7 $groupDescription = "Groupe permettant d'accéder au partage sur le mode dégradé $idEtab en RW"
8
9 $groupOK = Get-ADGroup -Filter {Name -eq $groupName}
10
11 if (!$groupOK) {
12
13     New-ADGroup -Name $groupName -Description $groupDescription -GroupScope DomainLocal -GroupCategory Security
14     Add-ADGroupMember -Identity $groupName -Members $groupMembers
15
16 } else {Write-Host "$(get-date) ERROR - Le groupe AD $groupName existe déjà" -ForegroundColor Red}
```

- 1- Saisie de l'ID de l'établissement
- 2- Définition des variables pour le groupe
- 3- Vérification de l'existence du groupe
- 4- Création du groupe si inexistant
- 5- Message d'erreur si le groupe existe déjà

Creation de session locale sur le poste, création du fichier des modes dégradés

```
1 ##### pré requis : disposer de la fonction Connect-PSSession dispo dans le wiki
2
3 $idEtab = Read-Host "Entrez l'ID Etablissement tel qu'il est renseigné dans LNA Data ? (1005, X075...)"
4 $computerName = Read-Host "Entrez le nom du poste modé dégradé que vous souhaitez paramétrer :"
5 $password = Read-Host "Entrez le mot de passe du compte Mode_Degrade dédié à MHCARE (dispo dans LockSelf) " -AsSecureString
6
7 $mdUsername="Mode_Degrade"
8 $mdFullUsername = "Mode Degrade MHCare"
9 $mdUserDescription = "Mode Degrade MHCare"
10 $groupName = "GLS_PERM_${$idEtab}_Mode-Degrade_RW"
11
12 $mdFilePath="C:\Users\Mode_Degrade\Desktop\Mode_degrade_MHCARE"
13 $mdShareName = "Mode_Degrade_MHCARE$"
14
15 $session = connect-PSSession $computerName
16
17 $results = invoke-command -session $session -scriptblock {
18
19     New-LocalUser -Name $Using:mdUsername -Password $Using:password -FullName $Using:mdFullUsername -Description $Using:mdUserDescription
20
21 }
22
23 $choiceUser = Read-Host "$(get-date) INFO - Redémarrez le poste mode dégradé, puis ouvrez une session avec l'utilisateur $Using:mdUsername"
24
25 if($choiceUser -eq "OK"){
26     $session = connect-PSSession $computerName
27     $results = invoke-command -session $session -scriptblock {
28         New-Item -ItemType Directory -Path $Using:mdFilePath
29         New-SmbShare -Name $Using:mdShareName -Path $Using:mdFilePath -ChangeAccess "Tout le monde"
30         $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("NOBLE-AGE\$($Using:groupName)", "FullControl", "Allow")
31         $acl = Get-Acl $Using:mdFilePath
32         $acl.AddAccessRule($rule)
33         Set-Acl -Path $Using:mdFilePath -AclObject $acl
34
35     }
36 }else{"$(get-date) INFO - Saisie <> OK > arret du script"}
```

Le script effectue les actions suivantes :

1. Demande à l'utilisateur de fournir un ID d'établissement, un nom de poste et un mot de passe pour l'utilisateur "Mode_Degrade".
2. Crée un utilisateur local "Mode_Degrade" sur le poste spécifié.
3. Demande à l'utilisateur de redémarrer et de se connecter avec cet utilisateur pour initialiser le profil.
4. Si l'utilisateur confirme, le script crée un dossier partagé et lui attribue des permissions spécifiques.
5. Si l'utilisateur ne confirme pas, le script s'arrête avec un message d'information.

L'objectif de ce script est de préparer un poste pour un accès en mode dégradé et de configurer un dossier partagé avec des droits d'accès spécifiques.

Problèmes rencontrés :

- ⇒ Réservation IP impossible sur le DHCP, pourtant rien sur le DHCP à l'adresse ou le poste était censé être, recherche sur le DHCP et sur l'outil de connexion à distance, après avoir remarqué qu'un poste avait bien l'IP mais qu'ils n'apparaissaient pas sur le DHCP, alors que pourtant sur SCCM il était bien marqué que c'est le DHCP qui lui avait fourni l'IP
 - ⇒ Enfin pour remédier à ce problème j'ai fait une réservation sur une IP non utilisée, me suis connecté au poste et fait un « IPCONFIG / renew » pour qu'il prenne l'IP que je lui avais réservé, ensuite j'ai créé une autre réservation pour le poste MD donc l'IP qui était bloqué par l'autre poste, pareil je me suis connecté sur le post pour faire un /renew, et enfin j'ai supprimé la réservation du poste qui bloquait l'IP pour qu'il ne reste pas en IP fixe
-
- ⇒ Première contrainte, ils ne trouvaient pas le poste sur le site (dans la baie, ou dans un bureau important tel que directrice etc...). Ou personnel compétent pas disponible
 - ⇒ Problème BOMGAR l'outil de connexion à distance ne fonctionnait pas sur certains postes, résolu grâce à une MAJ
-
- ⇒ Postes qui se mettait en veille (pas censé le faire), je ne savais pas que c'était une GPO qui empêchait les postes mode dégradé de se mettre en veille donc je ne pouvais plus me connecter aux postes.
 - ⇒ Une fois compris cela j'ai mis dans le groupe correspondant et le problème était résolu

J'ai fait le point avec le chef de projet et l'équipe, pour présenter ce que j'ai réalisé et ce qu'il nous reste à faire, tout ça reparti dans un grand Excel avec les missions de chaque personne participant au projet

Synthèse :

En tout le projet aura duré environ 1 mois durant lesquelles j'ai abordé plusieurs compétences, sur le réseau, Windows, ainsi que la gestion du temps et de projet, ce projet était intéressant sur le plan des techniques, et sur le plan humain sur la partie coopérations entre collègues et leurs conseils pour avancer efficacement.

```
$idEtab = Read-Host "Entrez l'ID Etablissement tel qu'il est renseigné dans LNA Data ?  
(1005, X075...)"  
  
$computerName = Read-Host "Entrez le nom du poste modé dégradé que vous souhaitez paramétrer :"  
  
$password = Read-Host "Entrez le mot de passe du compte Mode_Degrade dédié à MHCARE (dispo dans LockSelf) " -AsSecureString  
  
$mdUsername="Mode_Degrade"  
$mdFullUsername = "Mode Degrade MHCare"  
$mdUserDescription = "Mode Degrade MHCare"  
$groupName = "GLS_PERM_$(($idEtab)_Mode-Degrade_RW"  
  
$mdFilePath="C:\Users\Mode_Degrade\Desktop\Mode_degrade_MHCARE"  
$mdShareName = "Mode_Degrade_MHCARE$"  
  
$results = invoke-command -scriptblock {  
  
    New-LocalUser -Name $Using:mdUsername -Password :password -FullName  
    :mdFullUsername -Description :mdUserDescription -AccountNeverExpires -  
    UserMayNotChangePassword
```

```
}
```

```
$choiceUser = Read-Host "$(get-date) INFO - Redémarrez le poste mode dégradé, puis ouvrez une session avec l'utilisateur .\Mode_Degrade et le mot de passe associé pour créer le profil (attendre que le bureau soit disponible), puis saisissez OK pour créer le répertoire partagé"
```

```
if($choiceUser -eq "OK"){

    $results = invoke-command -session $session -scriptblock {

        New-Item -ItemType Directory -Path :mdFilePath

        New-SmbShare -Name :mdShareName -Path :mdFilePath -ChangeAccess "Tout le monde"

        $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("NOBLE-AGE\$($Using:groupName)", "Modify", "ContainerInherit,ObjectInherit", "None", "Allow")

        $acl = Get-Acl :mdFilePath

        $acl.AddAccessRule($rule)

        Set-Acl -Path :mdFilePath -AclObject $acl

    }

} else{"$(get-date) INFO - Saisie <> OK > arret du script"}
```

HAD	Matériel complet sur site	Configuration MD et point de distribution	Commentaires
1040	KO	OK	Attente livraison
1065	OK	OK	
1067	OK	OK	
1066	OK	OK	Poste introuvable sur site mais ping OK
1053	KO	OK	Attente livraison + Poste introuvable sur site mais ping OK
1072	OK	OK	Poste introuvable sur site mais ping OK
1088	ETIC		Standby
Z083	OK	OK	
1091	OK	OK	Point de distribution en cours avec l'équipe réseaux car WIFI sur site
1071	OK	OK	