Documentation CRYHOD

Sommaire

Serveur Samba

Samba a été installée sur une base Debian 11 via « apt install samba » sur un serveur AWS qui sera accessible via une adresse FQDN (*********.cnpf.fr) sur l'ip 172.***.***.***.

Configuration du partage

```
 GNU nano 7.2                        /etc/samba/smb.conf
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin

[CRYHOD]
        comment = Dossier configuration et stockage des informations CRYHOD
        path = /CRYHOD
        browsable = yes
        guest ok = yes
        read only = no
        create mask = 0755
```

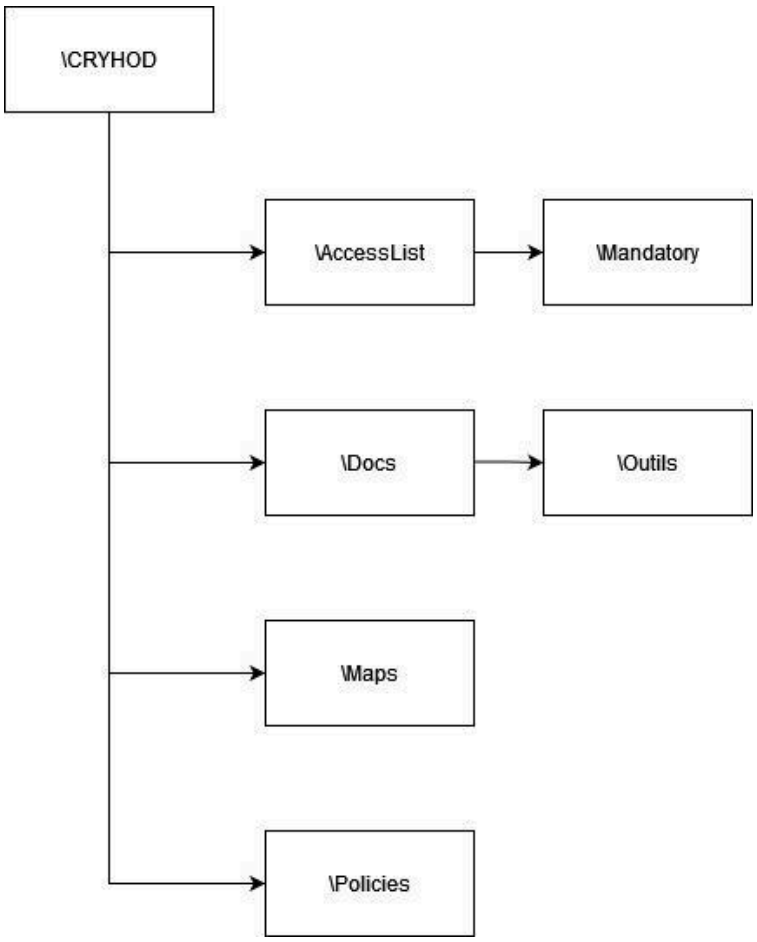
browsable : autorise les clients Windows à parcourir le répertoire partagé en utilisant l'explorateur de fichiers de Windows.

guest ok : permet aux clients de se connecter au répertoire partagé sans fournir de mot de passe.

CRYHOD

Arborescence

Les fichiers qui sont à la base de Cryhod sur le serveur Samba sont les suivants :



AccessList : Dossier qui répertorie les fichiers avec les identifiants et mots de passe de chaque poste client. Le chemin est indiqué via la **P121**.

Mandatory : Dossier qui contient les fichiers de références pour les accès administrateurs et support. Le chemin est indiqué via la **P121** et les fichiers sont identifiés via la **P131**.

Docs : Dossier contenant tous les fichiers autour de CRYHOD.

Outils : Dossier qui contient les fichiers compressé de certains outils mis à disposition par CRYHOD.

Maps : Dossier qui répertorie dans des sous dossiers les fichiers « .cymap » des ordinateurs chiffrer pour que en cas de dépannage les fichiers peuvent alors être utilisé pour créer un laissez passer pour un utilisateur qui a perdu son mot de passe. Le chemin est indiqué via la **P821**

Policies : Dossier qui contient le fichier « Main.xml » qui contient les politiques qui s'applique via la **P070**.

Les fichiers et dossiers générés par les différents postes portent le nom du poste. Lors d'une procédure de secours si un utilisateur perd son mot de passe le nom de la machine est inscrit sur l'écran.

Logiciel annexe

Gpedit.exe : Ce logiciel Microsoft permet dans l'onglet « Configuration ordinateur>Modèles d'administration>Prim'X Technologies>CRYHOD » de configuré et généré une configuration qui peut être par la suite déployé sur le serveur. Cryhod installe aussi un logiciel du nom de « Politiques de Sécurité (CRYHOD) qui est un raccourcie vers le gpedit.

⚠ **Attention : Sur un poste utilisateurs il ne faut jamais modifier les politiques via le gpedit car celle-ci seront prioritaires sur les politiques présentes sur le serveur.**

Console de commandes (CRYHOD) : Terminal qui permet la modification par ligne de commandes des politiques ainsi que l'import et l'export des politiques présent sur le poste.

Préparation des packages (CRYHOD) : Terminal qui permet la modification du .msi.

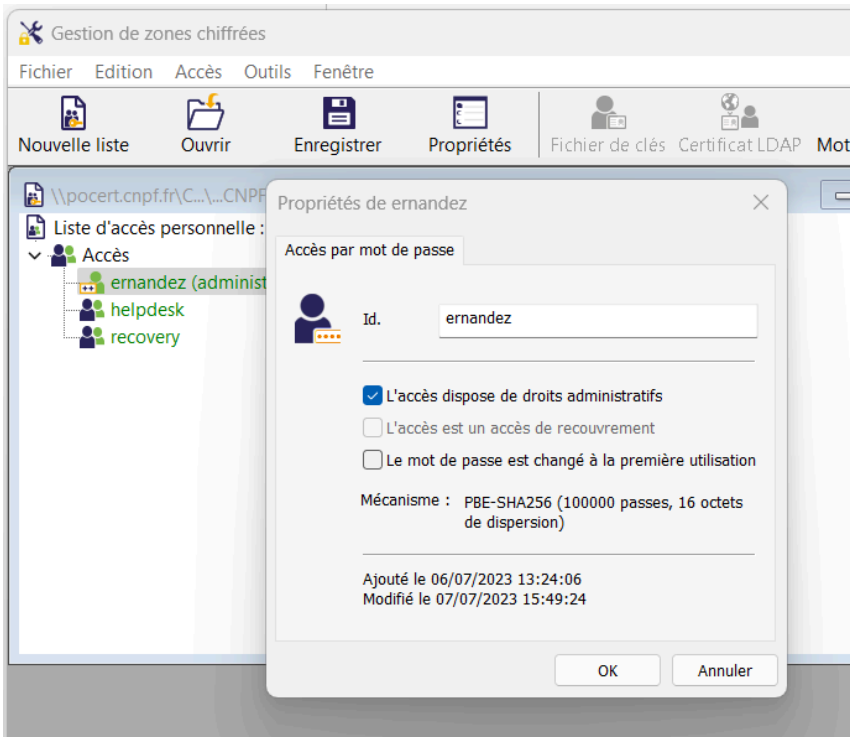
Signature des politiques (CRYHOD) : Logiciel qui permet de signer les politiques mais aussi de les exporter ou les importés de manières graphique. Logiciel utile lors d'une modification des politiques.

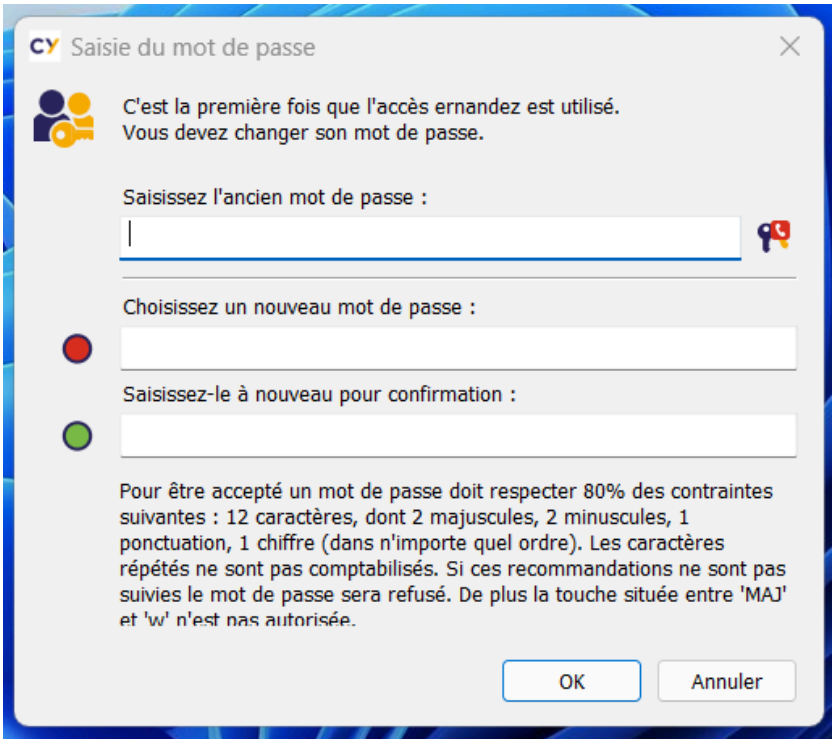
L'outil zceditsa : Outils graphique pour la modification des fichiers d'accès, il permet après que le mot de passe du profil soit rentré de modifier le mot de passe ou d'accéder à plusieurs informations autour du fichier. Ce logiciel permet de créer l'option de changement du mot de passe à la prochaine connexion ce qui peut être utile lors de la création et l'envoi d'un poste à un utilisateur pour qu'il choisisse son propre mot de passe.

Information général

Pour les utilisateurs qui possèdent deux ordinateurs il est possible d'ajouter un accès liste commun pour les identifiants de connexion. En effet dans le centre de chiffrement on peut gérer les accès et soit ajouté un nouvel identifiant de connexion ou utiliser un autre fichier d'identifiant d'un autre poste.

Lors de la préparation d'un poste il est possible d'attribuer un mot de passe temporaire et avec le logiciel **zceditsa** d'utiliser une option sur le fichier d'accès présent sur le serveur pour faire qu'au prochain démarrage le poste demande un nouveau mot de passe à l'utilisateur qui sera alors le définitif pour l'utilisateur.


Gestion de zones chiffrées
Fichier Edition Accès Outils Fenêtre
Nouvelle liste
Ouvrir
Enregistrer
Propriétés
Fichier de clés
Certificat LDAP
Mot
\\pocert.cnpf.fr\C...\...CNPF
Liste d'accès personnelle :
Accès
ernandez (administ
helpdesk
recovery
Propriétés de ernandez
Accès par mot de passe
Id.
ernandez
L'accès dispose de droits administratifs
L'accès est un accès de recouvrement
Le mot de passe est changé à la première utilisation
Mécanisme : PBE-SHA256 (100000 passes, 16 octets de dispersion)
Ajouté le 06/07/2023 13:24:06
Modifié le 07/07/2023 15:49:24
OK
Annuler


Saisie du mot de passe
C'est la première fois que l'accès ernandez est utilisé.
Vous devez changer son mot de passe.
Saisissez l'ancien mot de passe :
Choisissez un nouveau mot de passe :
Saisissez-le à nouveau pour confirmation :
Pour être accepté un mot de passe doit respecter 80% des contraintes suivantes : 12 caractères, dont 2 majuscules, 2 minuscules, 1 ponctuation, 1 chiffre (dans n'importe quel ordre). Les caractères répétés ne sont pas comptabilisés. Si ces recommandations ne sont pas suivies le mot de passe sera refusé. De plus la touche située entre 'MAJ' et 'w' n'est pas autorisée.
OK
Annuler