

E09 - IIS & Windows Server Backup

Challenge

- Identifier l'utilisateur supprimé dans l'Active Directory.
 - ▮ ▮ ▮ Suppression de l'utilisateur Christophe SEIGNANT
- Ouvrir Windows Server Backup et localiser une sauvegarde contenant l'utilisateur.
 - ▮ ▮ ▮ Restauration du dossier NTDS contenant les objets dont l'user supprimé

```
ApplicationRestore-01-12-2025_11-49-44.log - Bloc-notes
Fichier  Edition  Format  Affichage  Aide
C:\Windows\NTDS\Active Directory\ntds\edb.log restauré
C:\Windows\NTDS\Active Directory\ntds\edb00003.log restauré
C:\Windows\NTDS\Active Directory\ntds\edb.chk restauré
C:\Windows\NTDS\Active Directory\ntds\ntds.dit restauré
Sauvegarde de l'application
ID d'enregistreur : {B2014C9E-8711-4C5C-A5A9-3CF384484757}
Composant : ntds
Sous-titres :
Chemin logique : C:_WINDOWS_NTDS

*-----*
```

Heure de début : 01/12/2025 13:56
Heure de fin : 01/12/2025 13:56
Données transférées : 54,76 Mo

Éléments

Nom	Destination	État
C:\Users\cseignant\ntuser.dat.L...	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\NTUSER.D...	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\NTUSER.D...	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\NTUSER.D...	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\ntuser.ini	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\Recent	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\SendTo	C:\Users\cseignant\	Terminé.
C:\Users\cseignant\Voisinage ...	C:\Users\cseignant\	Terminé.

- Effectuer une restauration de l'état du système.

Sélectionner une date ...
Sélectionner le type d...
Sélectionner l'emplacement...
Confirmation
Statut de la récupération...

☐ Emplacement d'origine

Cette option restaure l'état du système. Vous devez redémarrer l'ordinateur pour effectuer l'opération de récupération.

☐ Effectuer une restauration faisant autorité des fichiers Active Directory

Cette option de récupération va rétablir tout le contenu répliqué sur ce serveur et sur tous les autres serveurs du domaine, y compris SYSVOL. Les autres dossiers répliqués sur ce serveur sont également concernés par cette récupération.

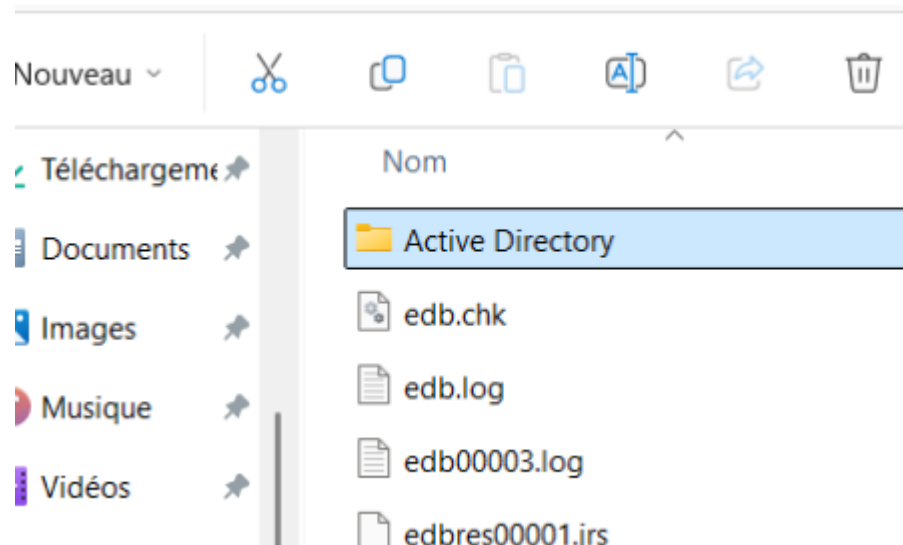
☒ Autre emplacement

Cette option copie l'état du système sous forme d'un jeu de fichiers à l'emplacement spécifié.

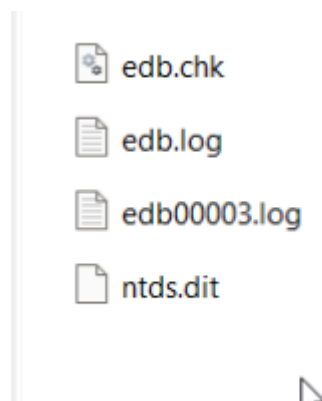
C:\Windows\NTDS Parcourir

☐ Restaurer en tant que fichiers IFM (Installation à partir du support)

Activez cette case à cocher si vous utilisez la fonctionnalité Installation à partir du support (IFM) pour copier les fichiers de l'état du système et installer une nouvelle base de données Active Directory.



Les fichiers à restaurer :



Solution : Redémarrer en "Mode Restauration des services d'annuaire" (Directory Services Restore Mode - DSRM)

Avec la commande : `bcdedit /set safeboot dsrepair`

Copier/coller les fichiers sauvegardés dans NTDS et écraser les anciens.

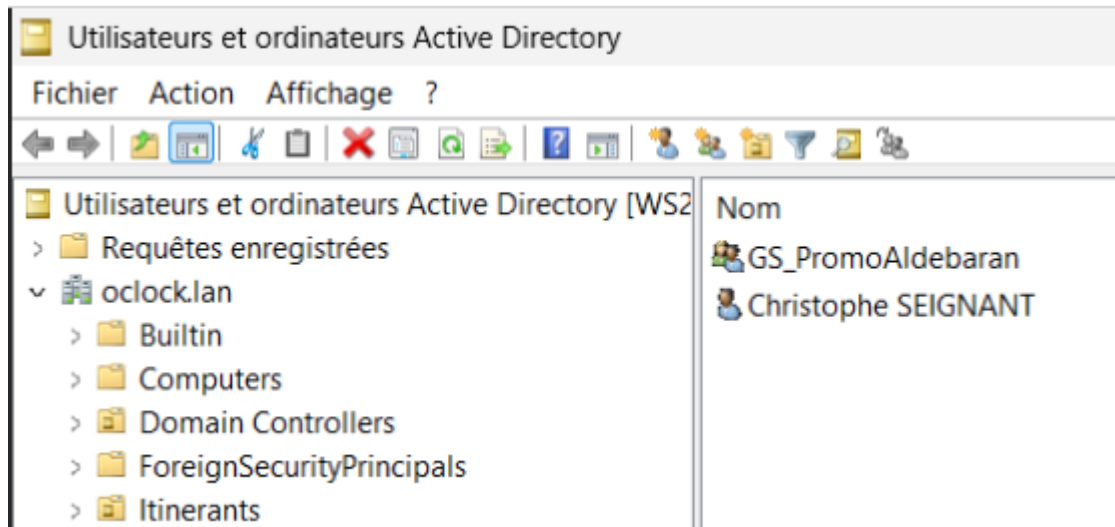
En CMD : bcdedit /deletevalue safeboot pour sortir du mode safe.

```
Administrateur : Command Pr  X  +  v

Microsoft Windows [version 10.0.26100.7171]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>bcdedit /deletevalue safeboot|
```

- Vérifier que l'utilisateur apparaît à nouveau dans l'AD après le redémarrage.



Christophe SEIGNANT est de retour.



- Tester la connexion avec le compte restauré.

