

# 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

The screenshot shows two windows. The top window is a Notepad titled 'ApplicationRestore-01-12-2025\_11-49-44.log - Bloc-notes' containing a restore log for Active Directory components (ntds.log, edb.chk, ntds.dit) and application logs. It includes details like the recorder ID, component (ntds), and logical path (C:\_WINDOWS\_NTDS). The bottom window is a 'Windows Server Backup' status window showing a completed backup job. It lists the start and end times (01/12/2025 13:56), transferred data (54,76 Mo), and a table of restored items (files and folders) from the C:\Users\cseignant\ directory to the same location, all marked as 'Terminé' (Completed).

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.

Selectionner une date ...  
Selectionner le type d...  
Selectionner l'emplace...  
Confirmation  
Statut de la récupérati...

Emplacement d'origine

Cette option restaure l'état du système. Vous devez redémarrer l'ordinateur pour que 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 contrôleur de 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 base de données Active Directory.

Nouveau ▾



Téléchargement  
Documents  
Images  
Musique  
Vidéos

Nom

Active Directory  
edb.chk  
edb.log  
edb00003.log  
edbres00001.jrs

Les fichiers à restaurer :

edb.chk  
edb.log  
edb00003.log  
ntds.dit

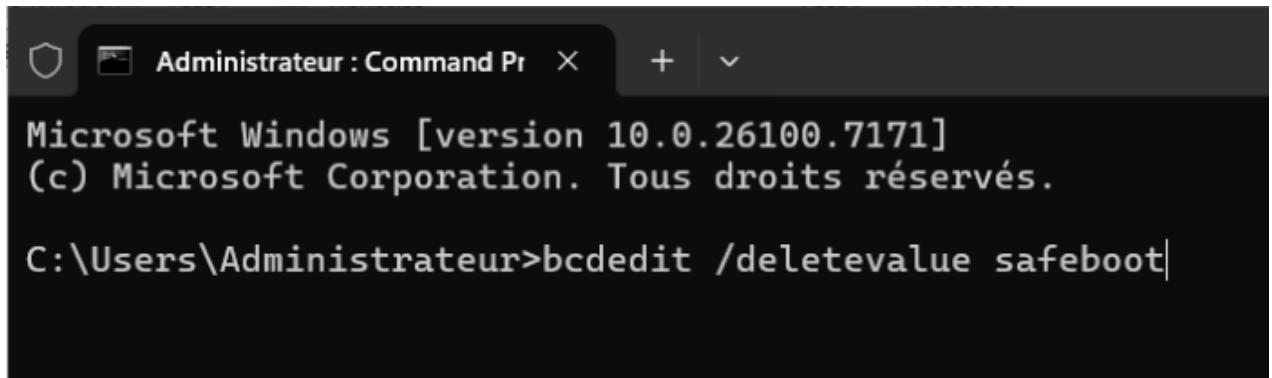


Solution : Redémarrer en "Mode Restauration des services d'annuaire" (Directory Services Restore Mode – DSRM)

Avec la commande : bcdedit /set safeboot dsrepair

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

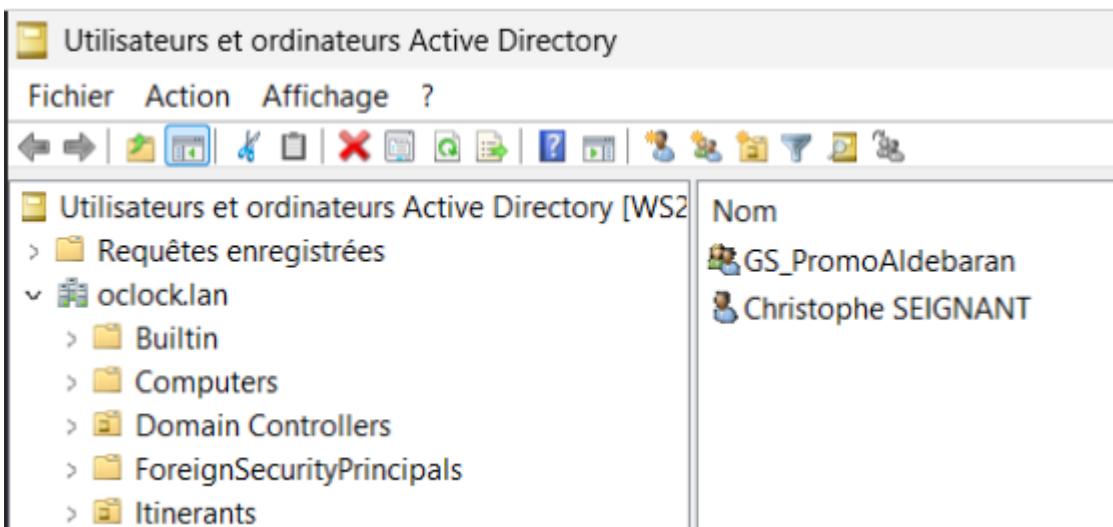
En CMD : bcdedit /deletevalue safeboot pour sortir du mode safe.



```
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.



Nom
GS_PromoAldebaran
Christophe SEIGNANT

Christophe SEIGNANT est de retour.



- Tester la connexion avec le compte restauré.

