Procédure blanchiment de serveur Windows 2016 / 2019 avec l'outil KillDisk.

Table des matières :

Contexte

Le blanchiment de serveur consiste à effacer complètement toutes les données d'un serveur pour le remettre à zéro, comme un formatage sécurisé. Son but principal est de garantir la confidentialité des données, surtout en cas de fin de vie du matériel, de réaffectation ou de suspicion de compromission (piratage, fuite).

Objectifs principaux

- Sécuriser les données sensibles : Éliminer traces de mots de passe, logs, fichiers temporaires ou configurations pour éviter leur récupération par un attaquant ou un nouvel utilisateur.
- Respecter la conformité : cela répond aux exigences RGPD (données personnelles) ou normes de sécurité (ISO 27001) lors de la destruction ou réutilisation d'équipements IT au sein de l'entreprise.
- Préparer une réinstallation propre : Avant une nouvelle installation (ex: Windows Server ou Linux), pour repartir sur une base vierge sans résidus.

Périmètre et prérequis

Matériel accessible via l'IP ou la carte ILO (cf photo)

License Killdisk

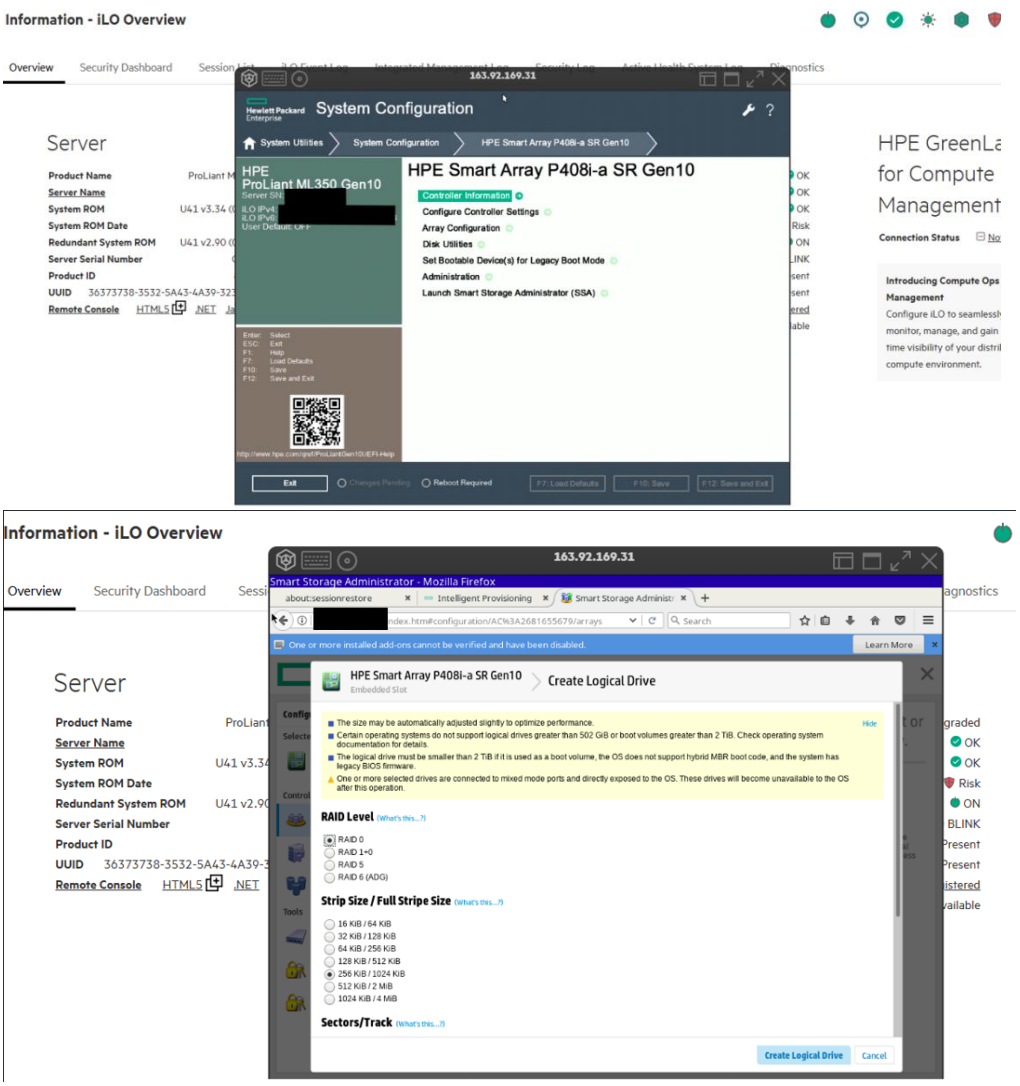
Droit d'administration

Lors d'un blanchiment de serveur, le technicien suit un processus en plusieurs phases pour garantir un effacement sécurisé et conforme.

Les différentes étapes

1.Identifier le serveur à blanchir et compléter les étapes de la procédure.

- Vérifier la propriété des données et les obligations légales (RGPD, archivage légal).
- Définir un calendrier et prévenir les utilisateurs pour éviter les interruptions de service.

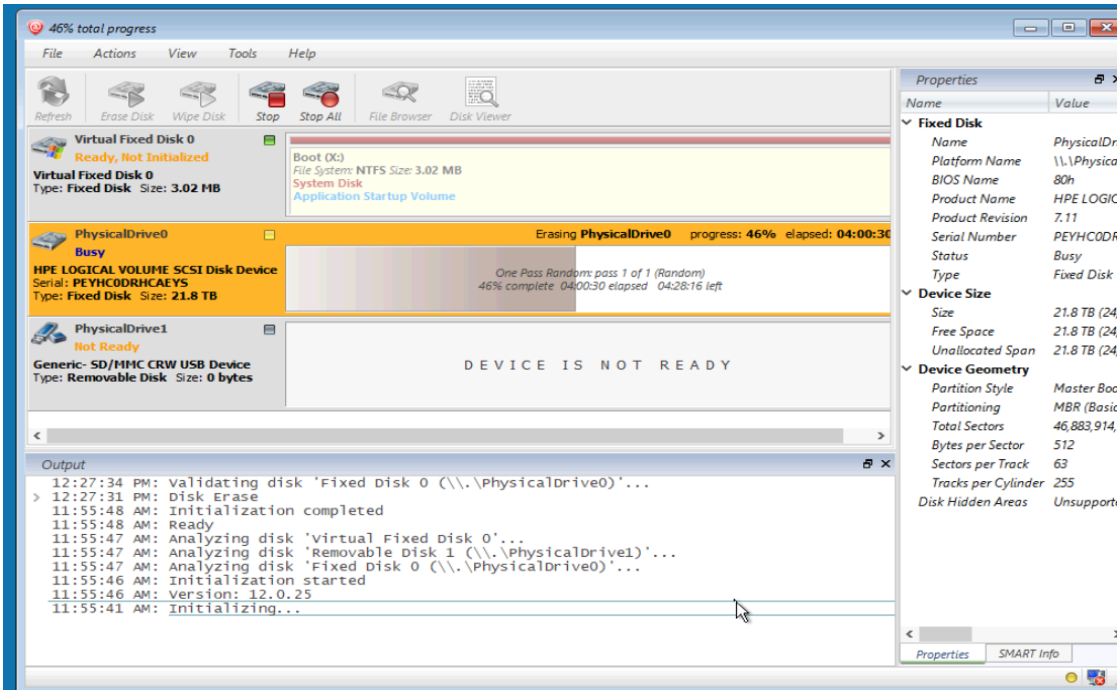
- 

2. Sauvegarde et migration

- Copier tous les fichiers à conserver vers un autre support ou serveur.
- Vérifier l'intégrité des sauvegardes avant de continuer.
- Migrer les services actifs vers une nouvelle infrastructure si nécessaire.

3. Effacement sécurisé des données

Lancer l’outils Killdisk prenant en charge la norme US DoD 5220.22-M et plus de 20 normes internationales d’assainissement des données. (NIST 800-88, DoD 5220.22-M)



4. Déconnexion et retrait

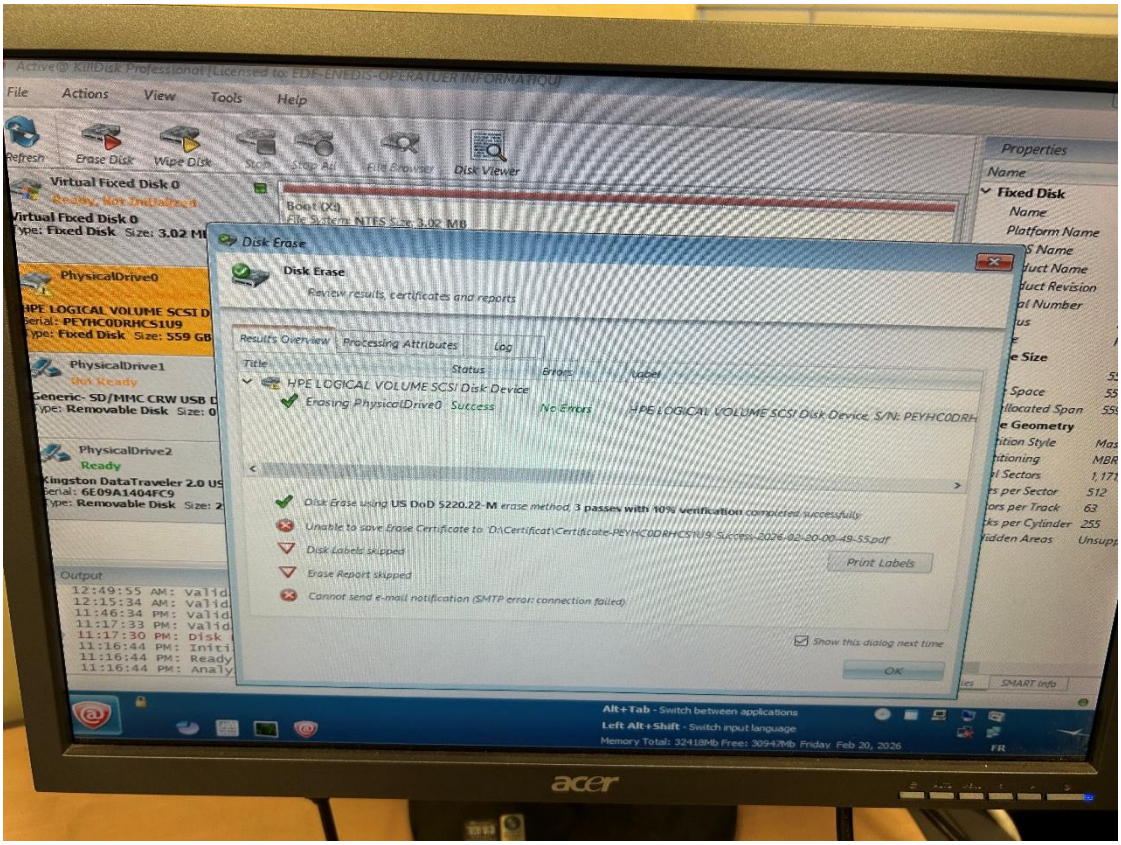
- Révoquer tous les accès utilisateurs et comptes associés.
- Déconnecter physiquement le serveur du réseau.
- Mettre à jour l'inventaire des actifs IT.

5. Destruction ou réaffectation du matériel

- Prise de contact avec le prestataire dans le but de le supprimer.
- Ou réaffecter en interne après blanchiment complet pour des tâches non sensibles.

6. Documentation

- Réception d’un certificat de blanchiment avec : date, méthode utilisée, n° série du disque, nom du technicien.
- Conserver ce document pour audit ou conformité RGPD.

- 
File
Actions
View
Tools
Help
Refresh
Erase Disk
Wipe Disk
Disk Viewer
Properties
Disk Erase
Review results, certificates and reports
Result's Overview
Processing Attributes
Log
Title
Status
Errors
Label
HPE LOGICAL VOLUME SCSI Disk Device
Erasing PhysicalDrive0 Success
No Errors
HPE LOGICAL VOLUME SCSI Disk Device, S/N: PEYHC0DRH
Disk Erase using US DoD 5220.22-M erase method, 3 passes with 10% verification completed successfully
Unable to save Erase Certificate to 'D:\Certificat\Certificate-PEYHC0DRHCS1U9-Success-2026-02-20-00-49-55.pdf'
Disk Labels skipped
Print Labels
Erase Report skipped
Cannot send e-mail notification (SMTP error: connection failed)
Show this dialog next time
OK
Output
Alt+Tab - Switch between applications
Left Alt+Shift - Switch input language
Memory Total: 32418Mb Free: 30947Mb Friday, Feb 20, 2026
acer