

TP 2 ADMINISTRATION AVANCÉE D'UN DOMAINE AD

Partie 1 - Mise en place d'un DC secondaire

L'objectif de cette partie est de mettre en place un second contrôleur de domaine afin d'assurer la redondance et la continuité de service au sein du domaine gp01.lab.ece.

Pour cela, une nouvelle machine virtuelle Windows Server 2025 est déployée, jointe au domaine existant puis promue comme contrôleur de domaine secondaire. Une fois la promotion effectuée, différentes vérifications permettent de confirmer le bon fonctionnement de la réplication entre les deux DC. Enfin, un test d'authentification est réalisé après avoir mis hors ligne le contrôleur de domaine principal afin de vérifier que le second DC peut prendre le relais en cas de panne.

1.Mise en place d'un DC secondaire

La première figure présente l'apparition de SRV-DC2-GP01 dans la console Active Directory Users and Computers, directement dans le conteneur Domain Controllers. On voit ainsi que la promotion du serveur en contrôleur de domaine secondaire a bien été prise en compte.

Son placement dans le site par défaut correspond à la configuration initiale appliquée lors de la mise en place du serveur.

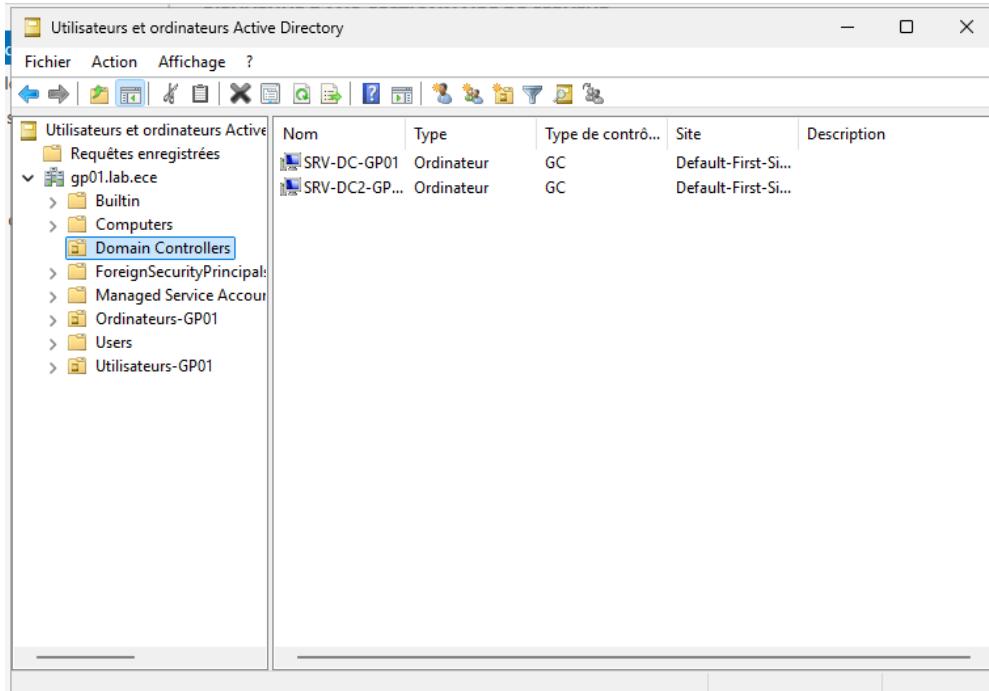


Figure 1: Résumé de l'installation du second DC

La seconde figure correspond à la commande `repadmin /showrepl`, utilisée pour observer la réplication entre SRV-DC2-GP01 et SRV-DC-GP01. Les différentes partitions AD, comme le schéma, la configuration ou encore les zones DNS, s'affichent avec un statut indiquant que les synchronisations se déroulent correctement.

On peut aussi voir ce qu'on appelle “les horodatages” qui permettent de voir que les mises à jour sont récentes et que les deux serveurs échangent bien leurs données.

```
C:\Users\Administrateur.GP01>repadmin /showrepl
Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Default-First-Site-Name\SRV-DC-GP01
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 8c844261-f3aa-42f9-84b9-83b48bd7e369
ID de l'invocation DSA : e76c7a02-c34b-45b6-8bf4-3f4f1a40c832

==== INSTANCES VOISINES ENTRANTES =====

DC=gp01,DC=lab,DC=ece
Default-First-Site-Name\SRV-DC-GP01 via RPC
    GUID de l'objet DSA : e040cb37-3345-4109-8016-c65302c15d06
    La dernière tentative, le 2025-11-16 12:01:27, a réussi.

CN=Configuration,DC=gp01,DC=lab,DC=ece
Default-First-Site-Name\SRV-DC-GP01 via RPC
    GUID de l'objet DSA : e040cb37-3345-4109-8016-c65302c15d06
    La dernière tentative, le 2025-11-16 11:50:27, a réussi.

CN=Schema,CN=Configuration,DC=gp01,DC=lab,DC=ece
Default-First-Site-Name\SRV-DC-GP01 via RPC
    GUID de l'objet DSA : e040cb37-3345-4109-8016-c65302c15d06
    La dernière tentative, le 2025-11-16 11:50:27, a réussi.

DC=DomainDnsZones,DC=gp01,DC=lab,DC=ece
Default-First-Site-Name\SRV-DC-GP01 via RPC
    GUID de l'objet DSA : e040cb37-3345-4109-8016-c65302c15d06
    La dernière tentative, le 2025-11-16 12:04:48, a réussi.

DC=ForestDnsZones,DC=gp01,DC=lab,DC=ece
Default-First-Site-Name\SRV-DC-GP01 via RPC
    GUID de l'objet DSA : e040cb37-3345-4109-8016-c65302c15d06
    La dernière tentative, le 2025-11-16 11:50:27, a réussi.
```

Figure 2: Résultat de la commande repadmin

Dans la troisième figure, la console Active Directory Sites and Services montre les deux serveurs présents dans le site Default-First-Site-Name. Chacun possède son objet NTDS Settings, ce qui permet de visualiser la manière dont ils sont configurés pour communiquer entre eux.

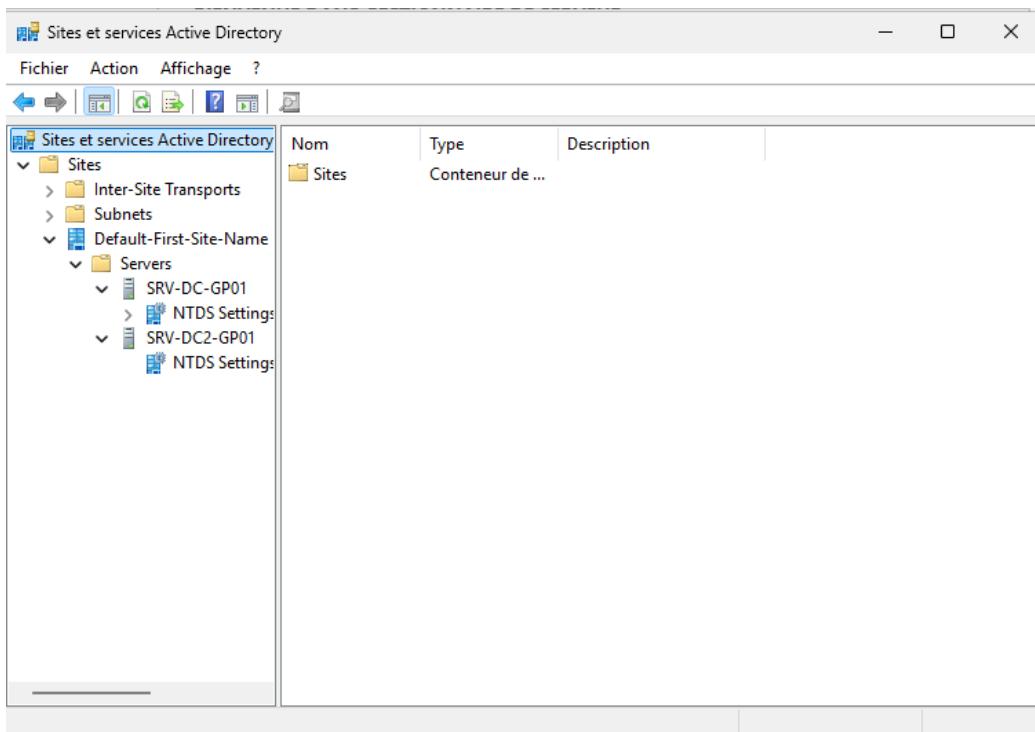


Figure 3: Vue Sites and Services montrant les deux DC

La dernière figure illustre le test réalisé après avoir désactivé temporairement SRV-DC-GP01. En tentant une connexion avec un utilisateur du domaine, on peut vérifier si SRV-DC2-GP01 assure correctement l'authentification en l'absence du DC principal. La connexion réussie montre que le second contrôleur de domaine prend bien le relais, ce qui assure la continuité du service en cas d'indisponibilité du premier serveur.

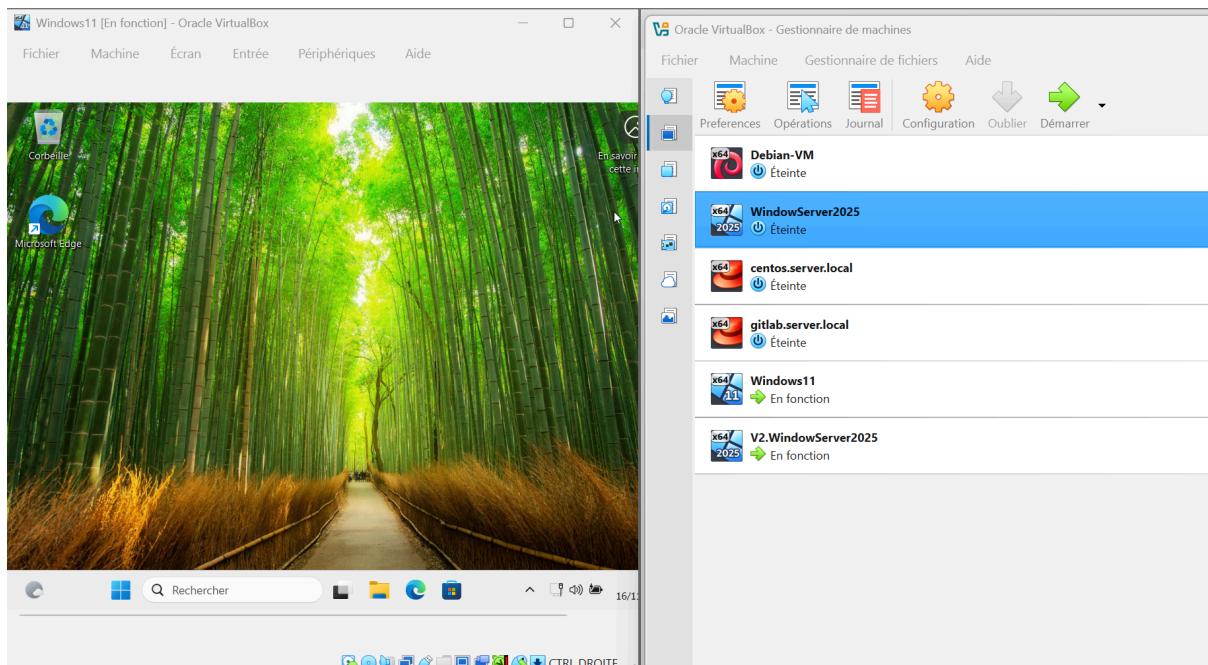


Figure 4: Test de connexion utilisateur lorsque le DC1 est hors ligne

Quels rôles FSMO ont été répliqués automatiquement?

Tous les cinq rôles FSMO (Schema Master, Domain Naming Master, RID Master, PDC Emulator, Infrastructure Master) ont été répliqués vers le nouveau DC, mais ils résident tous sur le DC principal (SRV-DC-GP01) jusqu'à leur transfert.

Quelle différence entre "transfert" et "seizure" des rôles FSMO?

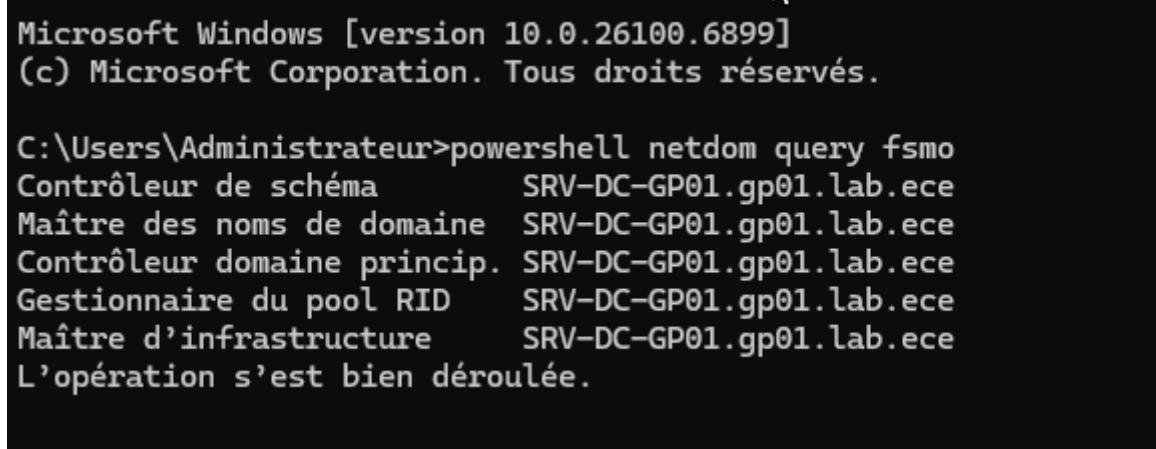
Le transfert est une opération propre et planifiée lorsque le DC maître est en ligne. La seizure est une opération forcée lorsque le DC maître est définitivement hors ligne ou irrécupérable.

Quels sont les avantages d'une topologie multi-DC?

Les avantages d'une topologie multi-DC sont la redondance, la haute disponibilité, la tolérance aux pannes et la répartition de charge pour l'authentification.

Partie 2 - FSMO et gestion des rôles

Le premier objectif est de connaître précisément où se trouvent les rôles FSMO avant de faire la moindre modification. Le résultat permet de vérifier que tous les rôles sont bien sur SRV-DC-GP01 et donc de partir d'une situation claire.



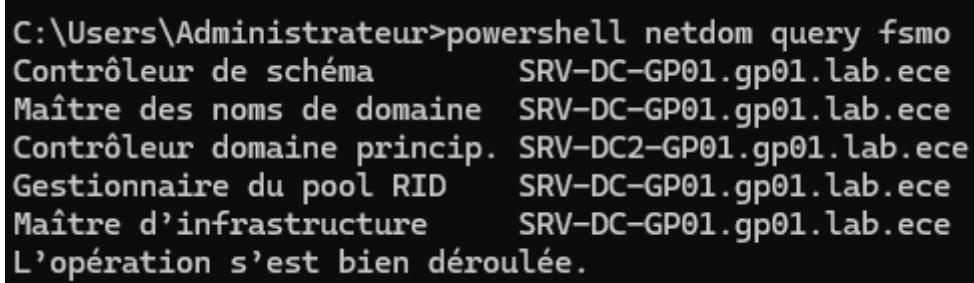
```
Microsoft Windows [version 10.0.26100.6899]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>powershell netdom query fsmo
Contrôleur de schéma          SRV-DC-GP01_gp01.lab.ece
Maître des noms de domaine    SRV-DC-GP01_gp01.lab.ece
Contrôleur domaine princip.  SRV-DC-GP01_gp01.lab.ece
Gestionnaire du pool RID     SRV-DC-GP01_gp01.lab.ece
Maître d'infrastructure       SRV-DC-GP01_gp01.lab.ece
L'opération s'est bien déroulée.
```

Figure 5: Résultat de la commande netdom

La figure 5 montre le résultat de la commande netdom query fsmo. On y voit que l'ensemble des rôles FSMO est détenu par SRV-DC-GP01. Cette étape sert surtout à faire un état des lieux avant toute manipulation, afin de savoir exactement où sont situés les rôles du domaine. Comme la commande s'exécute correctement, on peut travailler sur une base fiable pour la suite du TP.

Dans cette deuxième étape l'objectif est de montrer que le transfert se fait correctement et que le second DC est en capacité d'assumer un rôle FSMO sans perturber le fonctionnement du domaine.



```
C:\Users\Administrateur>powershell netdom query fsmo
Contrôleur de schéma          SRV-DC-GP01_gp01.lab.ece
Maître des noms de domaine    SRV-DC-GP01_gp01.lab.ece
Contrôleur domaine princip.  SRV-DC2-GP01_gp01.lab.ece
Gestionnaire du pool RID     SRV-DC-GP01_gp01.lab.ece
Maître d'infrastructure       SRV-DC-GP01_gp01.lab.ece
L'opération s'est bien déroulée.
```

Figure 6: Résultat de la commande netdom après transfert du rôle de contrôleur de domaine principale à DC2

Sur la figure 6, on voit le résultat de la même commande après le transfert du rôle vers SRV-DC2-GP01. On voit clairement que le rôle de contrôleur de domaine principal a été déplacé, tandis que les autres rôles restent sur SRV-DC-GP01.

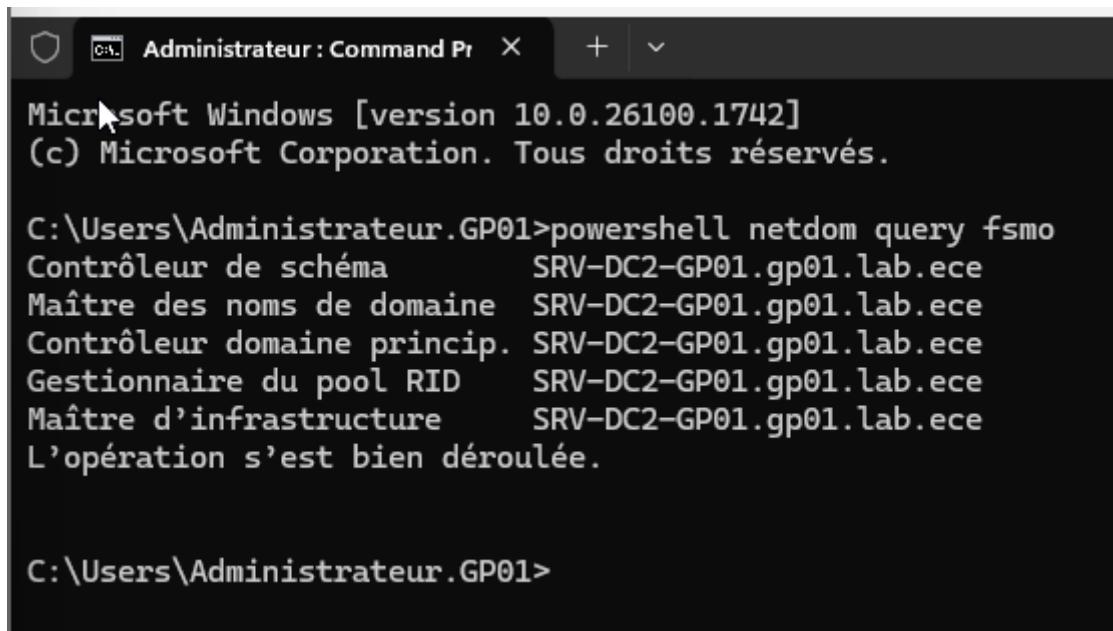
Ensuite on s'assure comment récupérer les rôles FSMO quand le DC principal ne répond plus du tout. Le seizure permet au DC2 de prendre le contrôle de l'ensemble des rôles afin que le domaine reste opérationnel malgré la panne.

```
PS C:\Users\Administrateur.GP01> ntdsutil
C:\WINDOWS\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server SRV-DC2-GP01
Liaison à SRV-DC2-GP01...
Connecté à SRV-DC2-GP01 en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections: quit
fsmo maintenance: |
```

Figure 7: Transfert ou seizure FSMO

La figure 7 nous montre que on est sur le DC secondaire et que on va exécuter les commandes de *seizure*.

La commande netdom query fsmo est relancée et montre que SRV-DC2-GP01 possède désormais l'ensemble des rôles FSMO. Cette vérification assure que le domaine dispose d'un détenteur fonctionnel pour tous les rôles critiques et qu'il peut continuer à opérer correctement. C'est aussi une base stable pour, éventuellement, réintégrer DC1 et redistribuer les rôles par la suite.



The screenshot shows a Windows Command Prompt window titled "Administrateur : Command Prompt". The title bar also includes the text "Microsoft Windows [version 10.0.26100.1742]" and "(c) Microsoft Corporation. Tous droits réservés.". The command entered was "powershell netdom query fsmo". The output lists the current持主 (holders) for various FSMO roles:

Rôle (Role)	Hôte (Holder)
Contrôleur de schéma (Schema Master)	SRV-DC2-GP01_gp01.lab.ece
Maitre des noms de domaine (Domain Name Master)	SRV-DC2-GP01_gp01.lab.ece
Contrôleur domaine princip. (Domain Controller Primary)	SRV-DC2-GP01_gp01.lab.ece
Gestionnaire du pool RID (RID Manager)	SRV-DC2-GP01_gp01.lab.ece
Maitre d'infrastructure (Infrastructure Master)	SRV-DC2-GP01_gp01.lab.ece

Below the role holder information, the message "L'opération s'est bien déroulée." (The operation proceeded well.) is displayed. The prompt at the bottom of the window is "C:\Users\Administrateur.GP01>".

Figure 8: Vérification post-seizure

1. Quels sont les 5 rôles FSMO et leurs fonctions ?

Rôle FSMO	Niveau	Fonction
Schema Master	Forêt	Gère toutes les modifications du schéma (définition de la structure) de l'Active Directory. Il n'y en a qu'un par forêt.
Domain Naming Master	Forêt	Gère l'ajout et la suppression de domaines ou de partitions de l'annuaire dans la forêt. Il n'y en a qu'un par forêt.
PDC Emulator	Domaine	Gère les changements de mots de passe immédiats, la synchronisation du temps, et est le point de contact par défaut pour les clients.
RID Master	Domaine	Alloue des pools d'identificateurs relatifs (RID) uniques à chaque DC pour la création d'objets (SIDs).
Infrastructure Master	Domaine	Met à jour les références d'objets entre les domaines (groupes/utilisateurs) et gère le "Phantom".

2. Dans quel cas justifie-t-on un "seizure" ?

Un seizure (c'est une saisie forcée) est justifié uniquement en cas d'urgence absolue lorsque le détenteur actuel d'un rôle FSMO est définitivement hors ligne ou irrécupérable (panne matérielle, corruption du système d'exploitation, etc.). Cette opération est destructive et ne doit jamais être utilisée si le contrôleur de domaine principal peut être remis en ligne, car elle crée un risque de conflit de rôles.

3. Quelle commande permet de vérifier rapidement la localisation des rôles ?

Pour vérifier rapidement la localisation des rôles, il faut lancer dans l'invite de commande de powershell la commande 'netdom query fsmo'.

Partie 3 – Sauvegarde et restauration d'Active Directory

Dans cette partie, on a mis en place une procédure complète pour sauvegarder et restaurer l'Active Directory. Le but est de vérifier que, si on supprime par erreur un utilisateur ou un groupe, on peut les récupérer grâce à une sauvegarde système.

1. Création de la sauvegarde système avec wbadmin

On a commencé par créer une sauvegarde de l'état du système avant de faire la moindre modification.

Pour ça, on a utilisé la commande wbadmin, qui permet de sauvegarder les éléments essentiels du contrôleur de domaine comme la base AD, le registre et le dossier SYSVOL.

On a exécuté la commande dans PowerShell pour obtenir une sauvegarde fiable, qui servira de point de restauration.

```
PS C:\Users\Administrateur.GP01> wbadmin start backup -backuptarget:E: -include:C: -allcritical -systemstate
wbadmin 1.0 - Outil en ligne de commande de sauvegarde
(C) Copyright Microsoft Corporation. Tous droits réservés.

Récupération des informations de volume...
Cette opération va sauvegarder (\?\Volume{e5df90f4-0000-0000-0000-100000000000}\),(C:),(\?\Volume{e5df90f4-0
000-0000-e0540c000000}\) sur E: .
Voulez-vous démarrer l'opération de sauvegarde ?
[O] Oui [N] Non O

L'opération de sauvegarde sur E: démarre.
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
La Sauvegarde Windows Server met à jour la sauvegarde existante pour supprimer les fichiers
qui ont été supprimés du serveur depuis la dernière sauvegarde.
Cette opération peut prendre quelques minutes.
La sauvegarde du volume (100.00 Mo) a abouti.
Création d'une sauvegarde du volume (C:) en cours, (1%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (4%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (8%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (13%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (17%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (21%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (26%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (30%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (35%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (40%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (44%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (49%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (53%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (58%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (62%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (67%) copiés.
```

```

Création d'une sauvegarde du volume (C:) en cours, (71%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (76%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (80%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (84%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (89%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (93%) copiés.
Création d'une sauvegarde du volume (C:) en cours, (98%) copiés.
La sauvegarde du volume (C:) a abouti.
Création d'une sauvegarde du volume (688.00 Mo) en cours, (36%) copiés.
Création d'une sauvegarde du volume (688.00 Mo) en cours, (100%) copiés.
Récapitulatif de l'opération de sauvegarde :
-----
L'opération de sauvegarde a abouti.
La sauvegarde du volume (100.00 Mo) a abouti.
La sauvegarde du volume (C:) a abouti.
La sauvegarde du volume (688.00 Mo) a abouti.
Journal des fichiers sauvegardés correctement :
C:\WINDOWS\Logs\WindowsServerBackup\Backup-16-11-2025_15-44-05.log
PS C:\Users\Administrateur.GP01> |

```

Figure 9: Exécution de la commande wbadmin

Cette étape garantit qu'on pourra revenir en arrière si nécessaire.

2. Suppression volontaire d'un utilisateur et d'un groupe

Une fois la sauvegarde faite, on a supprimé volontairement un utilisateur et un groupe depuis la console Utilisateur et ordinateurs Active directory.

L'idée est de simuler une erreur d'administration pour ensuite vérifier si la restauration permet bien de récupérer les objets supprimés.

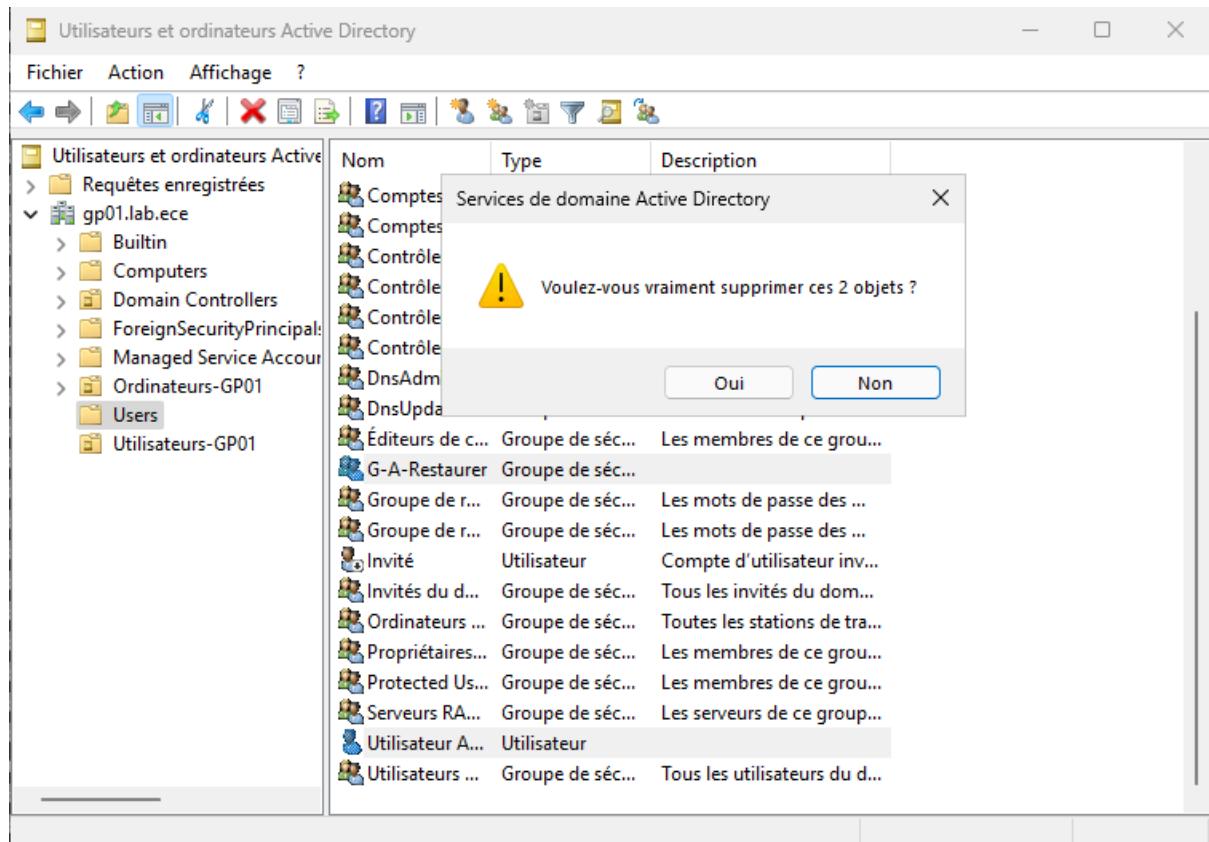


Figure 10: Suppression d'un objet

Cette suppression permettra de vérifier si la restauration permet bien de récupérer les objets disparus.

3. Démarrage en mode DSRM et restauration

Pour restaurer l'Active Directory, on a redémarré le serveur en mode DSRM (Directory Services Restore Mode).

Ce mode désactive les services AD, ce qui permet de restaurer proprement la base de données NTDS, qui signifie New Technology Directory Services, est la base de données centrale des services de domaine Active Directory (AD DS).

Ce fichier, présent sur chaque contrôleur de domaine, stocke l'ensemble des données de l'annuaire, y compris les informations relatives aux utilisateurs, aux ordinateurs et aux groupes, ainsi que des hachages de mots de passe et des clés Kerberos

Une fois connectés avec le mot de passe DSRM, on a utilisé wbadmin pour lancer la restauration à partir de la sauvegarde créée au début.

```
authoritative restore: restore subtree "CN=Users,DC=gp01,DC=lab,DC=ece"
Ouverture de la base de données DIT... Terminé.

Il est actuellement 11-16-25 17:47.09.
Mise à jour la plus récente de la base de données effectuée à 11-16-25 16:38.26.
Incrémentation de l'attribut Numéros de version de 100000.

Dénombrement des données devant être mises à jour...
Nombre d'entrées : 0000000057
Terminé.

57 entrées doivent être mises à jour.

Mise à jour des entrées...
Entrées restantes : 0000000000
Terminé.

57 entrées ont été mises à jour.

Le fichier texte suivant doté d'une liste fiable d'objets restaurés a été créé
et se trouve dans le répertoire de travail :
ar_20251116-174709_objects.txt

Un ou plusieurs des objets spécifiés possèdent des liens inverses vers ce domaine. Les fichiers LDIF suivants
ayant fait l'objet de restaurations de liens ont été créés et se trouvent dans le répertoire de travail :
ar_20251116-174709_links_gp01.lab.ece.ldf

Restauration faisant autorité terminée correctement.

authoritative restore: |
```

Figure 11: Écran du mode DSRM

Le serveur revient alors à l'état exact qu'il avait au moment où la sauvegarde a été faite.

4. Vérification du retour des objets

Après la restauration, on a redémarré le serveur normalement et on est retournés dans la console AD.

On a vérifié si l'utilisateur et le groupe supprimés étaient de nouveau présents, et c'était bien le cas. Cela confirme que la restauration s'est déroulée correctement.

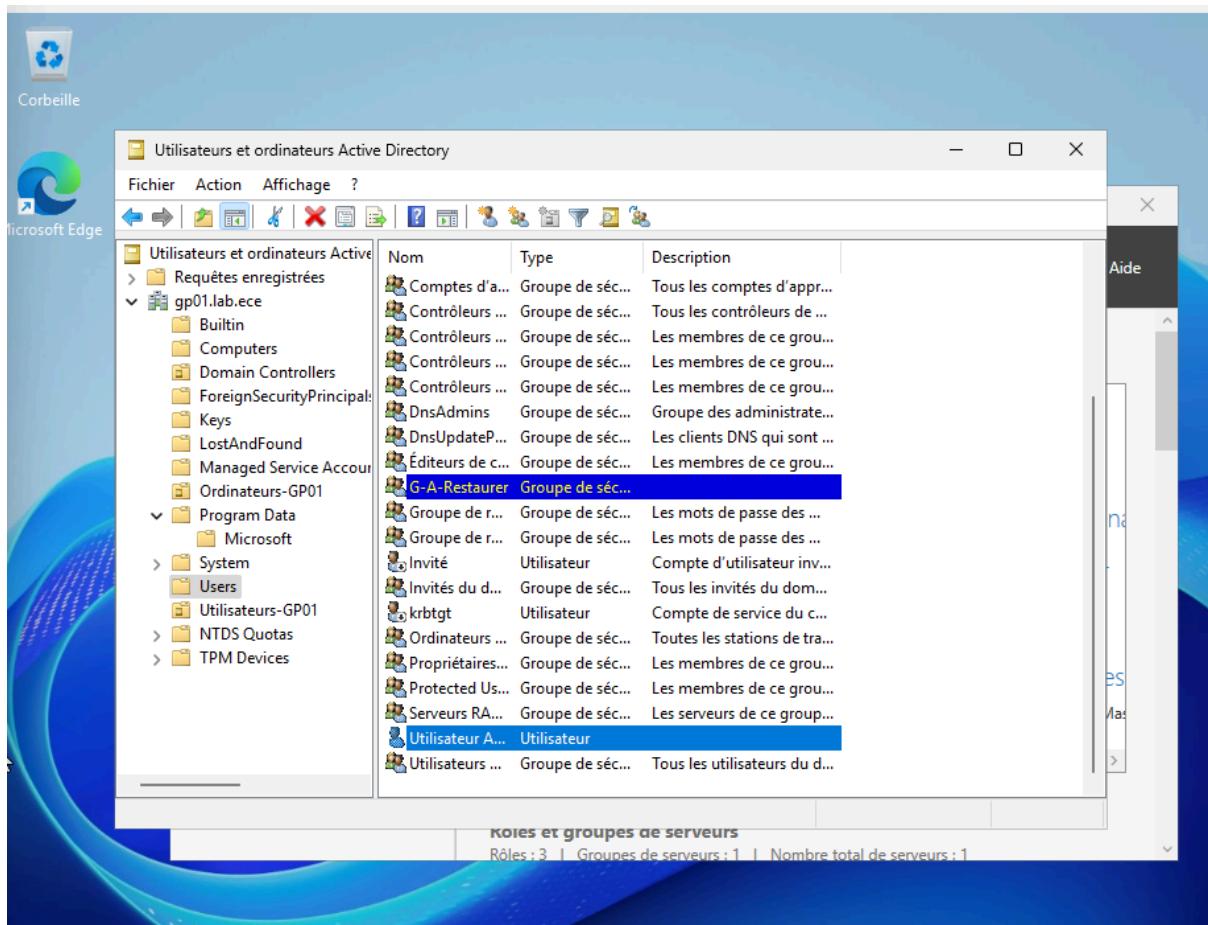


Figure 12: Vérification après restauration

Cette étape montre que la procédure de sauvegarde et de restauration est essentielle pour récupérer rapidement des objets critiques en cas d'erreur.

1. Quelle différence entre restauration autorisée et non autorisée ?

La différence est fondamentale et détermine si les objets restaurés seront réintégrés dans l'annuaire ou si de nouvelles copies de données écraseront l'annuaire existant.

Restauration Non-Autorisée :

- Son but est de rétablir un contrôleur de domaine à un état antérieur, souvent après une panne matérielle ou logicielle. C'est l'étape initiale wbadmin.

- Le DC restauré est considéré comme ayant des données anciennes. Après le redémarrage, il se connecte aux autres DC s'ils existent et met à jour sa copie de l'annuaire.
- Tous les changements survenus sur les autres DC après l'heure de la sauvegarde y compris les suppressions comme vos objets de test sont répliqués sur le DC restauré. L'objet supprimé reste donc supprimé.

Restauration Autorisée :

- Son but est de récupérer des objets Active Directory qui ont été accidentellement supprimés. C'est la deuxième étape (ntdsutil).
- L'administrateur utilise la commande ntdsutil authoritative restore pour marquer les objets restaurés comme étant la version la plus récente et correcte. Cela incrémentera leur Numéro de Version à un niveau très élevé.
- Lorsque le DC redémarre et réplique avec l'annuaire, les autres DC voient que la version de l'objet restauré est plus récente que leur propre marque de suppression et acceptent de restaurer l'objet.

2. Pourquoi le mode DSRM est-il isolé du domaine ?

Le mode DSRM est isolé du domaine parce que, lorsqu'un contrôleur de domaine démarre dans ce mode spécial, les services Active Directory ne sont pas chargés, seuls les services système essentiels sont exécutés.

Cette isolation permet d'effectuer des opérations de maintenance de bas niveau sur la base de données NTDS.DIT sans que celle-ci soit utilisée ou verrouillée par les processus du domaine. Elle rend possible des actions telles que la réinitialisation du mot de passe administrateur du domaine, la restauration de l'état du système via wbadmin ou ntdsutil, ou encore la défragmentation hors ligne de la base de données.

C'est également pour cette raison qu'un compte administrateur local distinct, défini lors de la promotion du contrôleur de domaine, doit être utilisé pour s'authentifier en DSRM.

3. Quelle stratégie recommanderiez-vous pour les sauvegardes AD ?

La stratégie la plus recommandée pour les sauvegardes d'Active Directory est une stratégie hybride combinant plusieurs méthodes complémentaires.

Elle repose d'abord sur des sauvegardes régulières de l'état du système, idéalement chaque jour, ou toutes les douze heures dans des environnements critiques et effectuées sur au moins deux contrôleurs de domaine différents, car c'est le seul moyen fiable de restaurer l'annuaire après une suppression accidentelle ou une panne majeure.

Elle inclut également l'utilisation de la réPLICATION de machines virtuelles via Hyper-V ou VMware, réalisée en continu ou toutes les heures, afin de permettre une reprise rapide après un sinistre matériel, tout en gardant à l'esprit que ces réplicas ne

doivent pas être utilisés pour restaurer des objets supprimés sans précautions, car ils peuvent contenir des données obsolètes.

Enfin, cette stratégie intègre l'activation de la Corbeille Active Directory, qui, bien qu'elle ne constitue pas une sauvegarde à proprement parler, représente une première ligne de défense en permettant de restaurer rapidement des objets supprimés tant que la période de rétention n'est pas dépassée.

Partie 4 – Audit et surveillance

Dans cette partie, on a configuré une stratégie d'audit pour suivre les actions importantes réalisées sur le domaine Active Directory. L'objectif est de surveiller les connexions, les modifications d'objets AD et les changements de stratégie, puis d'observer les événements générés lors de la création d'un compte de test.

1. Création d'une GPO d'audit appliquée aux contrôleurs de domaine

On a commencé par créer une nouvelle GPO dédiée à l'audit et on l'a liée à l'OU contenant les contrôleurs de domaine. L'idée est d'activer plusieurs catégories d'audit afin que les DCs enregistrent toutes les opérations sensibles.

Dans l'éditeur de GPO, on a activé les paramètres suivants :

- Suivi des ouvertures et fermetures de session
Pour enregistrer chaque authentification réussie ou échouée.
- Audit des modifications d'objets Active Directory
Pour garder une trace des créations, suppressions et modifications dans la base AD.
- Audit des changements de stratégie
Pour suivre toute modification appliquée aux stratégies de sécurité ou aux GPO.

The figure displays three tables of audit policies, likely from the Windows Group Policy Management (GPM) console.

Catégories	Configuration
Connexion de compte	Non configuré
Gestion du compte	Non configuré
Suivi détaillé	Non configuré
Accès DS	Configuré
Ouvrir/fermer la session	Configuré
Accès à l'objet	Non configuré
Changement de stratégie	Configuré
Utilisation de privilège	Non configuré
Système	Non configuré
Audit de l'accès global aux objets	Non configuré

Sous-catégorie	Événements d'audit
Auditer la réplication du service d'annuaire détaillé	Non configuré
Auditer l'accès au service d'annuaire	Succès
Auditer les modifications du service d'annuaire	Non configuré
Auditer la réplication du service d'annuaire	Non configuré

Sous-catégorie	Événements d'audit
Auditer le verrouillage du compte	Non configuré
Auditer les revendications utilisateur/de périphériq...	Non configuré
Auditer l'appartenance à un groupe	Non configuré
Auditer le mode étendu IPsec	Non configuré
Auditer le mode principal IPsec	Non configuré
Auditer le mode rapide IPsec	Non configuré
Auditer la fermeture de session	Succès
Auditer l'ouverture de session	Succès
Auditer le serveur NPS (Network Policy Server)	Non configuré
Auditer d'autres événements d'ouverture/fermetur...	Non configuré
Auditer l'ouverture de session spéciale	Non configuré

Sous-catégorie	Événements d'audit
Auditer la modification de la stratégie d'audit	Succès et échec
Auditer la modification de stratégie d'authentificat...	Non configuré
Auditer la modification de la stratégie d'autorisation	Non configuré
Auditer la modification de la stratégie de platefor...	Non configuré
Auditer la modification de la stratégie de niveau r...	Non configuré
Auditer d'autres événements de modification de st...	Non configuré

Figure 13: Paramétrage de la GPO d'audit

Grâce à ces réglages, les contrôleurs de domaine commencent à enregistrer dans le journal de sécurité les événements liés à l'activité du domaine.

2. Crédation du compte "test" et observation des événements

Pour vérifier que la GPO fonctionne bien, on a créé un compte utilisateur nommé test dans Active Directory. Cette action est censée générer plusieurs événements liés à la création d'objet AD.

Ensuite, on est allé dans le Journal des événements > Windows Logs > Security. On a filtré les événements et observé ceux correspondant :

- à la création de compte (ID 4720),
- aux modifications d'attributs,

- aux ajouts dans les groupes,
- et éventuellement aux connexions du compte si on l'utilise.

Les événements présents dans la console confirment que l'audit est actif et que les DC enregistrent correctement toutes les actions surveillées.

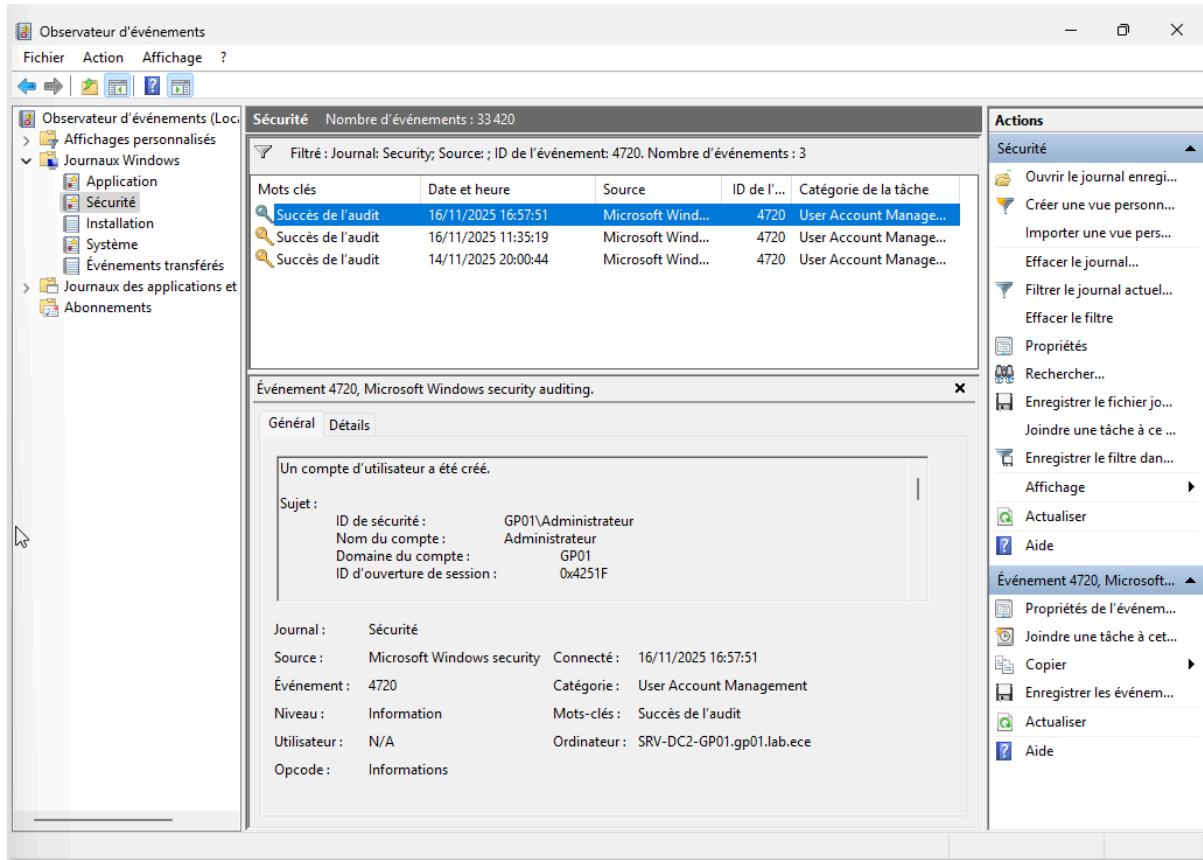


Figure 14: Journal d'événements avec une création/modification de compte

1. Quels événements AD sont critiques à surveiller ?

Les événements les plus critiques à surveiller dans Active Directory sont ceux qui peuvent indiquer une tentative de compromission, une élévation de priviléges ou une perturbation des services. Il est donc essentiel de suivre de près les modifications apportées aux comptes à priviléges, notamment les changements de mot de passe ou d'attributs concernant les administrateurs ou les comptes de service, correspondant à l'événement 4738.

Il faut également surveiller les modifications apportées aux groupes de sécurité sensibles, comme l'ajout (4728) ou la suppression (4729) de membres dans des groupes tels que Domain Admins ou Enterprise Admins. Le transfert ou la saisie des

rôles FSMO doit aussi attirer l'attention, car il peut signaler une opération critique sur l'infrastructure AD.

De même, les tentatives répétées d'ouverture de session échouées, identifiées par l'événement 4625, permettent de détecter des attaques par force brute. Enfin, la création ou la suppression d'objets dans l'annuaire, détectée via les événements 4720 ou 5137, constitue un autre indicateur important, surtout lorsqu'elle est déclenchée par un compte inattendu.

2. Comment automatiser l'analyse de ces journaux ?

Automatiser l'analyse des journaux AD est indispensable en raison du volume très important des événements générés.

Pour cela, il est possible de mettre en place des abonnements aux événements Windows afin de centraliser les journaux de sécurité de tous les contrôleurs de domaine sur un serveur collecteur unique, facilitant ainsi leur consolidation et leur exploitation.

Des scripts PowerShell utilisant la cmdlet *Get-WinEvent* permettent également de filtrer automatiquement les journaux en fonction des événements critiques, comme les ID 4720 ou 4625, et de produire des rapports ou des alertes sans intervention manuelle. Enfin, l'utilisation d'une solution de gestion des logs ou d'un SIEM, telle que Splunk ou ELK, offre une automatisation avancée en permettant d'ingérer, normaliser, analyser et visualiser les données dans des tableaux de bord dédiés.

3. Pourquoi un SIEM est-il souvent nécessaire ?

Un SIEM devient indispensable dans les environnements professionnels car il permet d'effectuer une corrélation avancée des événements, en reliant par exemple une connexion suspecte sur un contrôleur de domaine à un transfert de données anormal sur un autre équipement, ce qu'aucun journal isolé ne peut révéler seul.

Il offre également une normalisation et une centralisation complètes des données issues non seulement des contrôleurs de domaine, mais aussi des pare-feu, routeurs ou applications, ce qui facilite les analyses globales de sécurité.

Enfin, les SIEM modernes intègrent des capacités de détection d'anomalies via des techniques d'IA ou d'apprentissage automatique, permettant d'identifier un comportement utilisateur inhabituel (comme une connexion depuis un pays inédit ou l'accès à des ressources jamais consultées) même si l'événement généré n'est pas explicitement une erreur ou un échec.

Partie 5 - Authentification avancée et RODC

Dans cette partie, on a travaillé sur l'implémentation d'un RODC (Read-Only Domain Controller). L'objectif est de comprendre son fonctionnement, de configurer le cache de mots de passe et d'observer son comportement lors de connexions utilisateurs, ainsi que l'échange Kerberos généré.

1. Création de la VM SRV-RODC-GPXX

On a commencé par créer une nouvelle machine virtuelle nommée SRV-RODC-GP01.

Cette VM est destinée à devenir notre contrôleur de domaine en lecture seule.

On lui a configuré une adresse IP fixe, l'a ajoutée au domaine, puis on a vérifié que la communication avec le DC principal fonctionnait correctement.

2. Promotion de la VM en RODC

Ensuite, on a lancé l'Assistant d'installation des services AD DS pour promouvoir la VM en RODC.

Pendant la promotion, on a sélectionné l'option Contrôleur de domaine en lecture seule (RODC).

On a également configuré le site AD où placer le RODC.

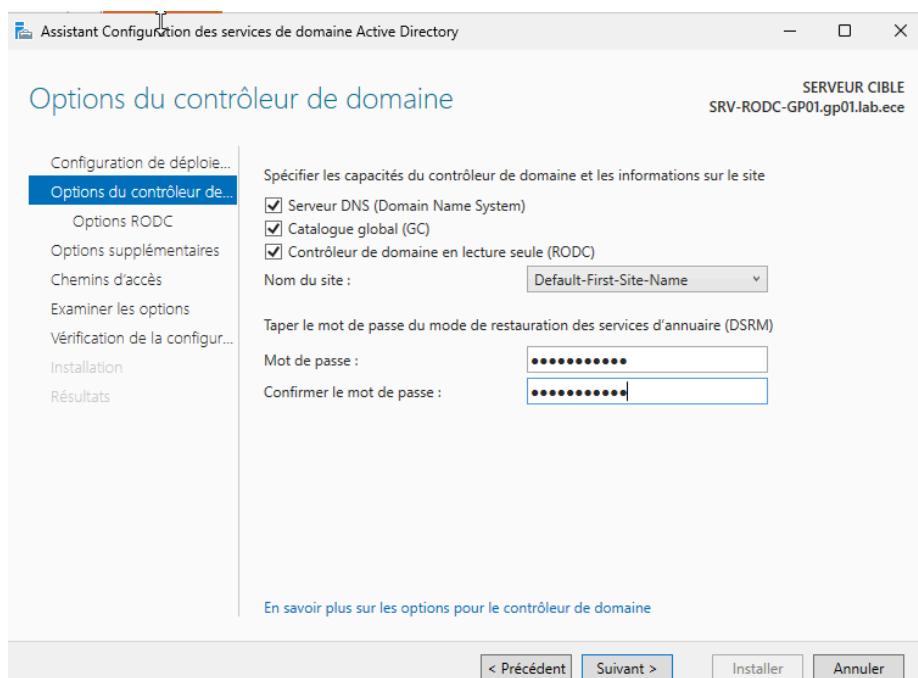


Figure 15: Assistant de promotion RODC

Une fois la promotion terminée, le serveur est devenu un contrôleur de domaine capable de répondre aux authentifications en lecture seule, tout en ayant un comportement particulier concernant les mots de passe.

3. Configuration du cache de mots de passe

L'étape suivante consistait à configurer le Password Replication Policy du RODC. Cela permet de décider quels comptes utilisateurs ou groupes sont autorisés à avoir leur mot de passe mis en cache sur le RODC.

On a défini :

- Une liste d'utilisateurs autorisés → leurs mots de passe peuvent être mis en cache localement.
- Une liste d'utilisateurs non autorisés → leurs mots de passe ne peuvent jamais être stockés.

Cette configuration se fait dans les propriétés du RODC, onglet Stratégie de réPLICATION de mot de passe.

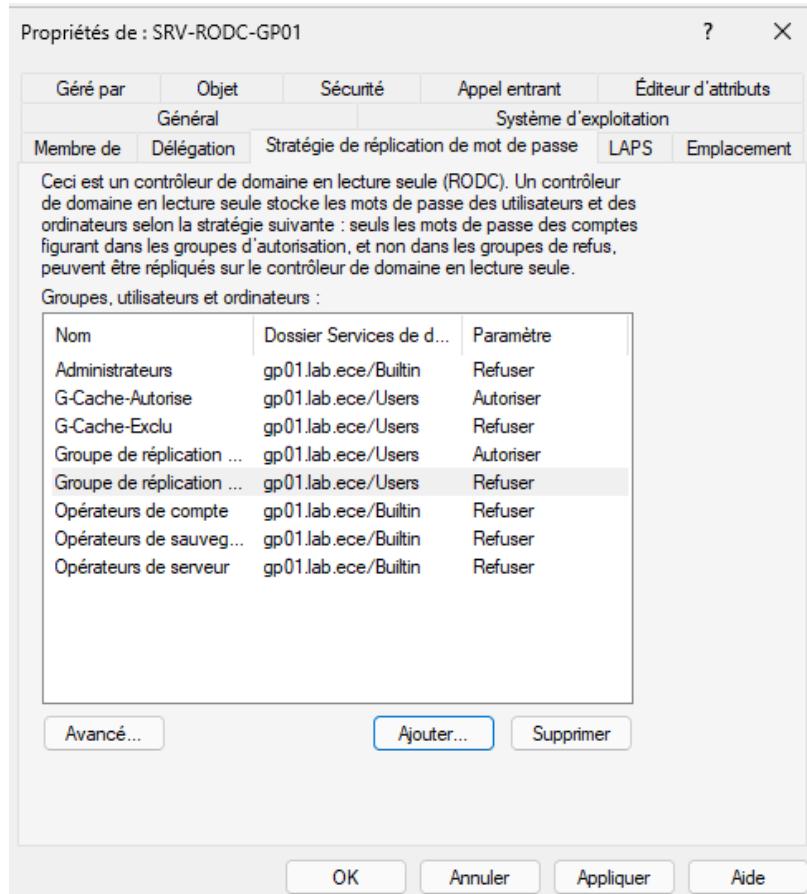


Figure 16: Paramètres de cache de mots de passe

Cela montre les deux groupes configurés. (G-Cache-Autorise / G-Cache-Exclu)

4. Tests de connexion : utilisateur autorisé vs utilisateur non autorisé

Pour vérifier le fonctionnement du PRP, on a réalisé deux tests :

Test 1 – Connexion avec un utilisateur autorisé

On a utilisé un compte qui appartient à la liste autorisée. Le RODC a bien pu authentifier l'utilisateur localement, et on observe que son mot de passe peut être mis en cache.

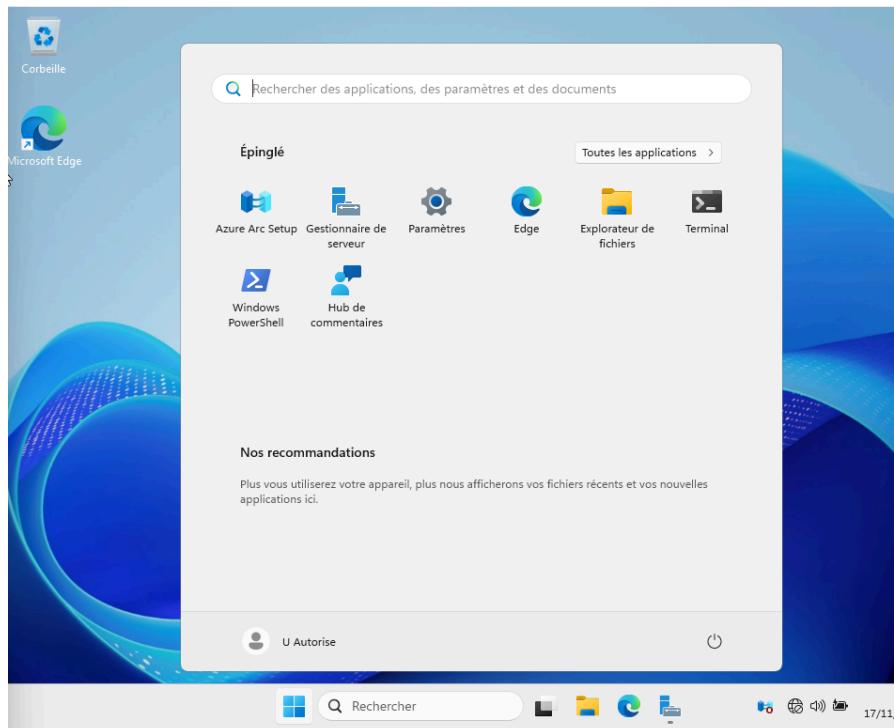


Figure 17: Avec connexion réseau (Utilisateur : U Autorise)

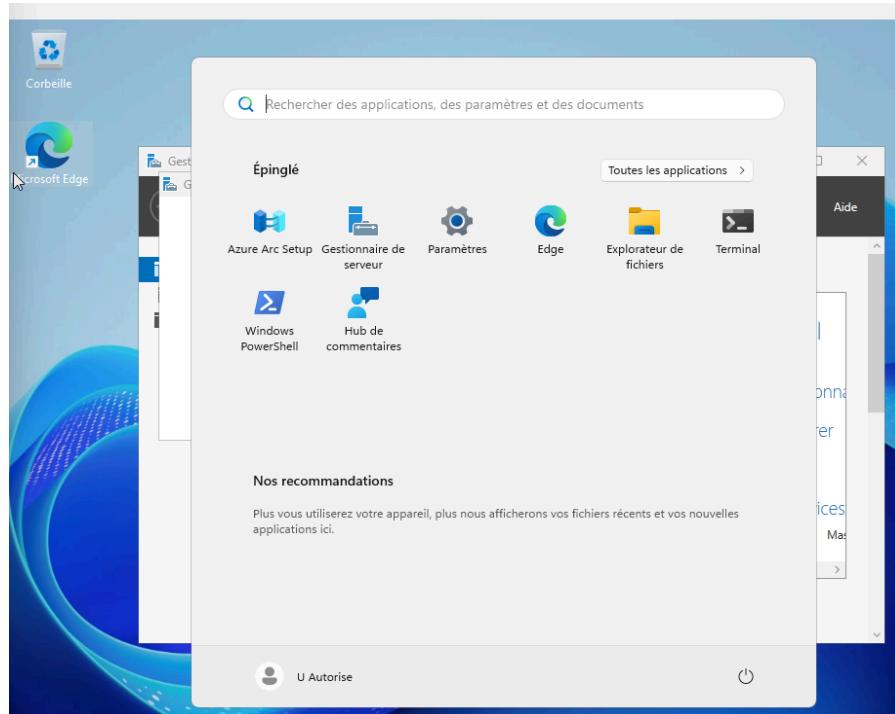


Figure 18: Sans connexion réseau (Utilisateur : U Autorise)

Cela fonctionne car le compte est membre de G-Cache-Autorise. Lors de la première connexion (Réseau Connecté), la PRP autorise le RODC à répliquer et stocker le hachage du mot de passe en cache localement. Lorsque le réseau est coupé, le RODC utilise ce cache pour valider l'utilisateur.

Test 2 – Connexion avec un utilisateur non autorisé

Cette fois, on a essayé un compte explicitement refusé dans la PRP.

Le RODC n'a pas pu mettre le mot de passe en cache et a dû contacter le DC principal pour valider l'authentification.

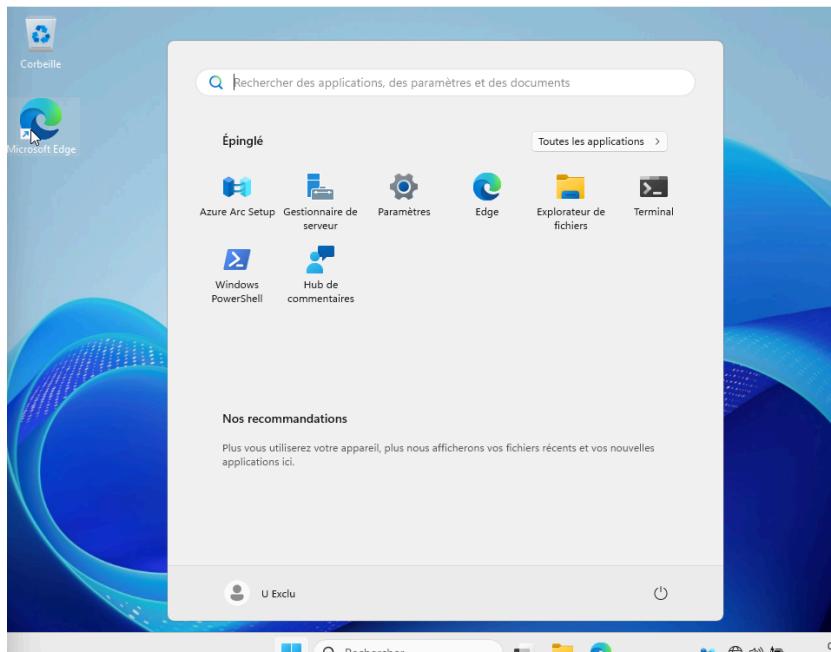


Figure 19: Avec connexion réseau (Utilisateur : U Exclu)

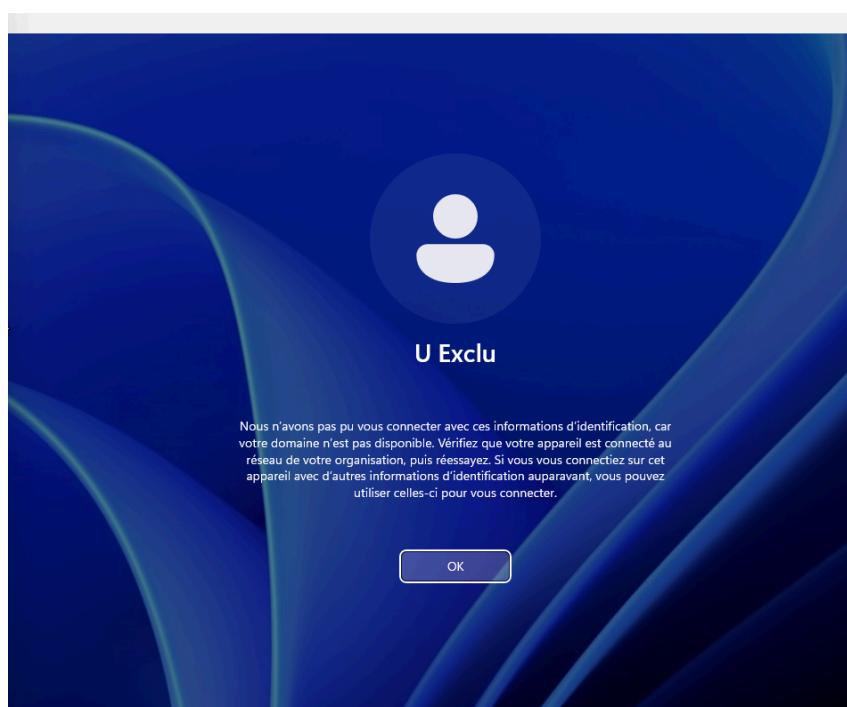


Figure 20: Sans connexion réseau (Utilisateur : U Exclu)

Le compte est membre de G-Cache-Exclu. Lors de sa connexion initiale, la PRP interdit au RODC de stocker son mot de passe en cache. Lorsque le réseau est coupé, le RODC n'a plus accès au DC principal pour l'authentification et ne possède aucune information locale pour valider l'utilisateur.

Ces tests confirment le fonctionnement attendu du RODC (il ne met en cache que les mots de passe explicitement autorisés).

5. Capture d'un échange Kerberos avec Wireshark

Pour compléter l'étude, on a réalisé une capture réseau avec Wireshark afin d'observer l'échange Kerberos lors d'une authentification via le RODC.

Dans la capture, on retrouve :

- Les paquets AS-REQ / AS-REP,
- Puis les paquets TGS-REQ / TGS-REP,
- Avec l'adresse du RODC comme serveur Kerberos.

On peut ainsi visualiser le processus d'obtention du Ticket Granting Ticket (TGT) puis du ticket de service, confirmant que l'authentification passe bien par le RODC mais avec les restrictions propres à son rôle.

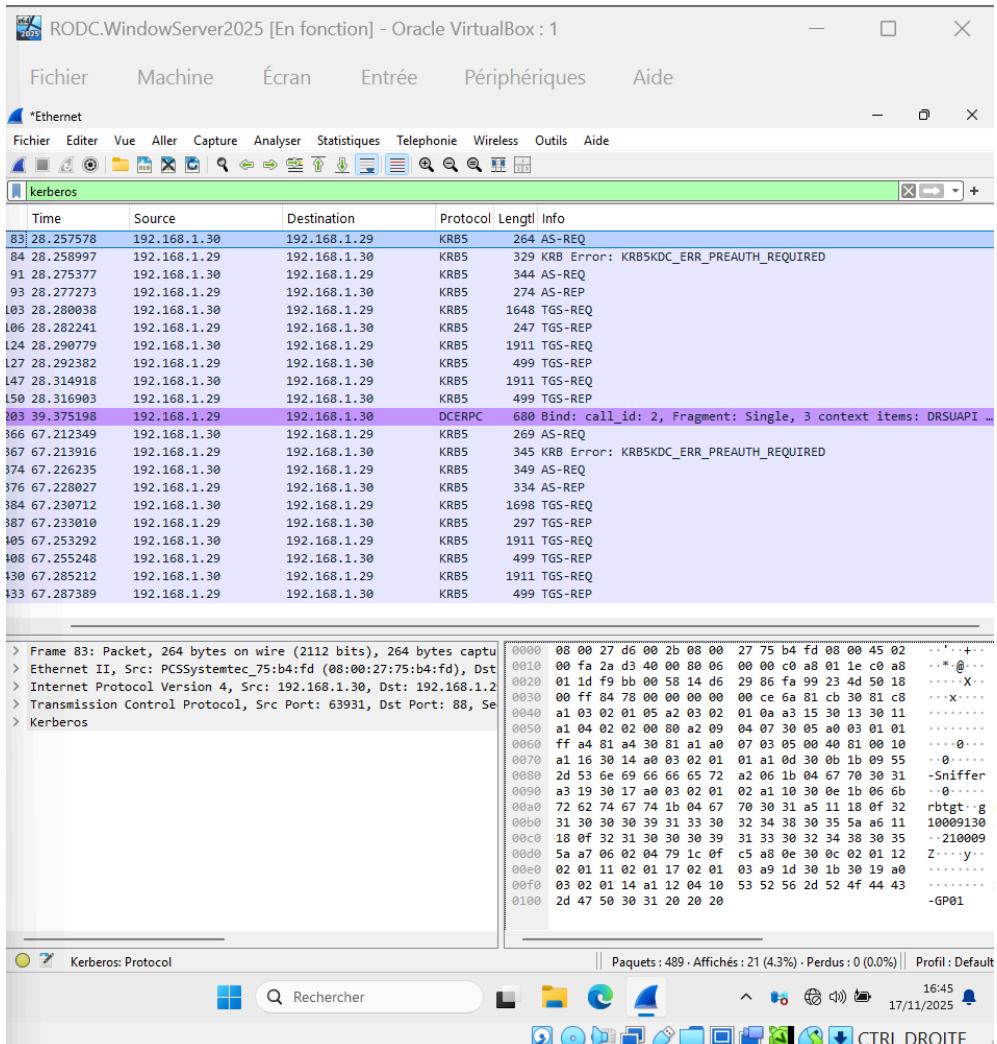


Figure 21: Capture d'un échange Kerberos avec Wireshark

Élément	Valeur dans l'image	Signification
Filtre	kerberos	Confirme que le trafic est bien filtré sur le protocole Kerberos.
Source / Destination	192.168.1.30 (RODC) \$leftrightarrow\$ 192.168.1.28 (DC Principal)	Confirme que l'échange a lieu entre votre RODC et votre DC principal.
Trames Clés	KRB5 AS-REQ et KRB5 AS-REP	L'échange AS-REQ (Authentication Service Request) et AS-REP (Response) est la preuve qu'un client (le RODC au nom de U-Sniffer) a demandé l'authentification au DC principal.
Informations	Le champ décodé montre Sniffer	Confirme que l'utilisateur de test (U-Sniffer) a été utilisé pour déclencher cet échange, prouvant que le mot de passe n'était pas en cache sur le RODC.

Quels sont les avantages d'un RODC ?

Un Read-Only Domain Controller présente plusieurs bénéfices dans des environnements distants ou peu sécurisés. Tout d'abord, une base AD en lecture seule, il est donc impossible de modifier les objets en local. De plus, en cas de vol ou de piratage du serveur, l'AD ne peut pas être altérée. La gestion des mots de passe est aussi un avantage car seuls les comptes autorisés ont leurs mots de passe localement stockés.

Quels comptes ne doivent jamais être mis en cache ?

Les comptes à ne jamais être mis en cache sont :

- Comptes Administrateurs du domaine
- Comptes Built-in privilégiés (Administrator, Domain Admins, Enterprise Admins, Schema Admins)
- Comptes de services sensibles
- Comptes utilisés pour GPO, systèmes critiques, backups, répliques AD
- Comptes ayant accès à des ressources stratégiques (serveurs de bases de données, etc.)

En d'autres termes, tout compte qui possède des priviléges élevés ne doit pas être mis en cache.

Quelle différence observe-t-on entre RODC et DC complet lors d'une authentification ?

La différence principale est que le RODC nécessite un contact avec un DC complet pour valider la première connexion et décider de la mise en cache, alors que le DC complet valide toujours localement.

Partie 6 - Audit de sécurité et durcissement

Après avoir téléchargé PingCastle et Purple Knight depuis un poste du domaine, nous ouvrons les rapports afin d'analyser les résultats.

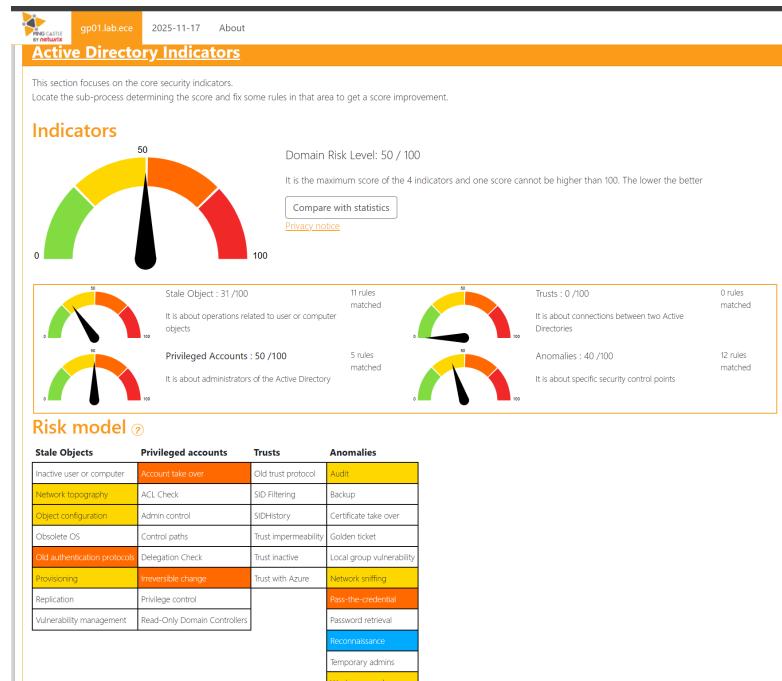


Figure 22: Rapport PingCastle

Dans ce rapport, nous pouvons voir que le risque le plus élevé se situe au niveau des comptes à hauts priviléges, c'est-à-dire les administrateurs. Les deux problèmes que nous observons à ce niveau sont les "Account take over" et "Irreversible change", ce sont deux points sur lesquels il serait important pour une entreprise de travailler.

Regardons maintenant le rapport Purple Knight.

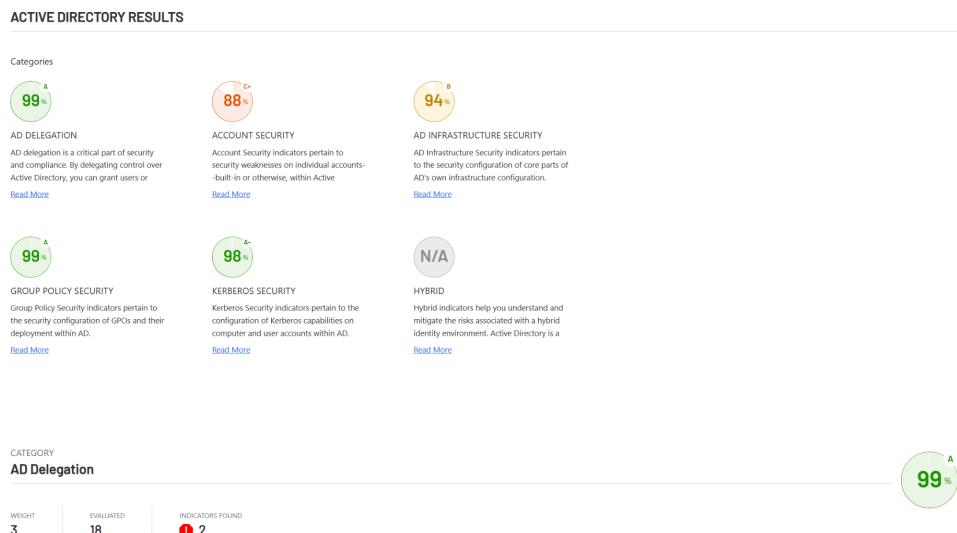


Figure 23: Rapport Purple Knight

Cette fois-ci, nous pouvons voir que les défauts de sécurité sont sur deux axes :

- des failles sur les comptes utilisateurs : mots de passe faibles, comptes à priviléges mal gérés
- infrastructure AD, configuration interne

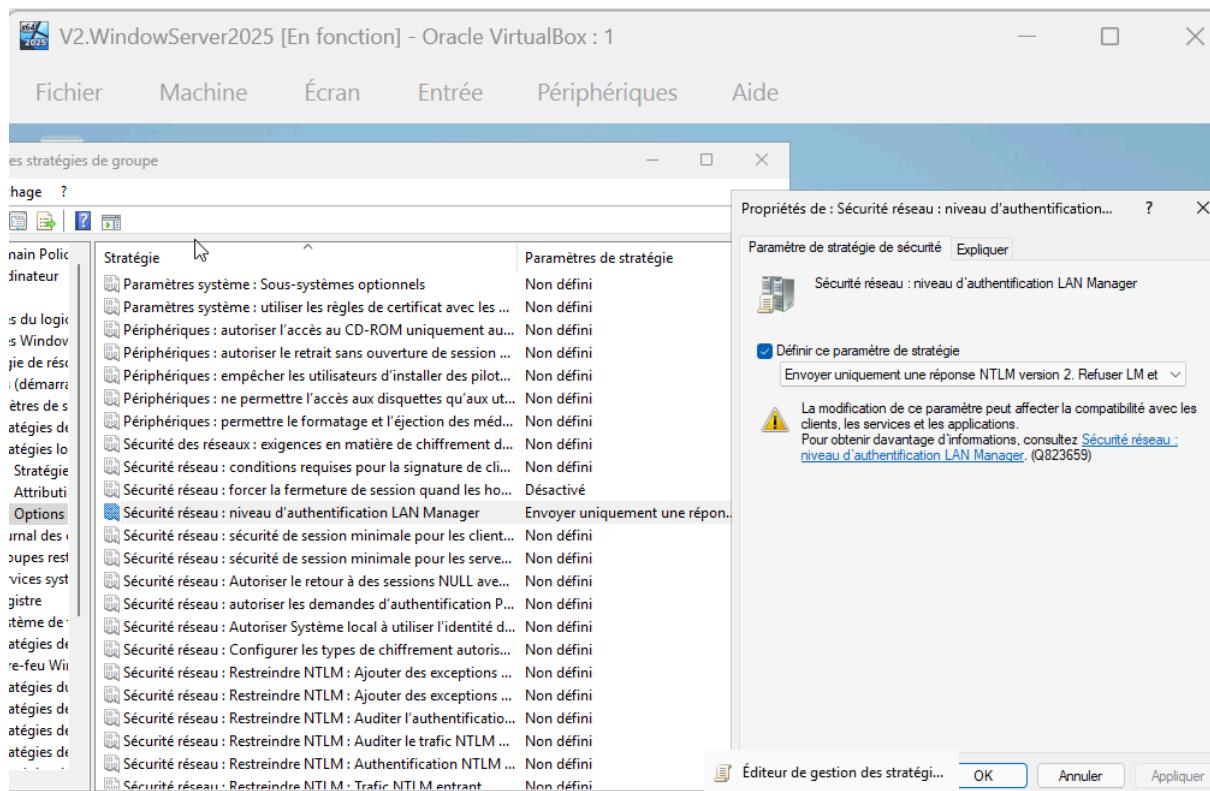


Figure 24: Preuve de la mesure de durcissement appliquée

La mesure de durcissement appliquée est la configuration de "Sécurité réseau : niveau d'authentification LAN Manager" sur Niveau 5 (Envoyer uniquement la réponse NTLMv2. Refuser LM et NTLM), afin d'interdire l'utilisation des protocoles d'authentification obsolètes et faibles comme LM et NTLMv1, réduisant ainsi le risque de vol ou de cassage de mot de passe.

Une fois le durcissement appliqué, nous relançons les analyses de PingCastle et PurpleKnight :

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

- Yellow background: Inactive user or computer, Network topography, Object configuration, Old authentication protocols, Provisioning, Replication, Vulnerability management.
- Orange background: Account take over, Admin control, Control paths, Delegation Check, Irreversible change, Privilege control, Read-Only Domain Controllers.
- Red background: Audit, Backup, Certificate take over, Golden ticket, Local group vulnerability, Network sniffing, Password retrieval, Reconnaissance, Temporary admins, Weak password.

Figure 25: Nouveau Risk Model

Le grand changement se trouve dans la première colonne, dans la case “Old authentication protocols”. Cette case est passée en risque nul ce qui signifie que le durcissement à fonctionné à ce niveau.

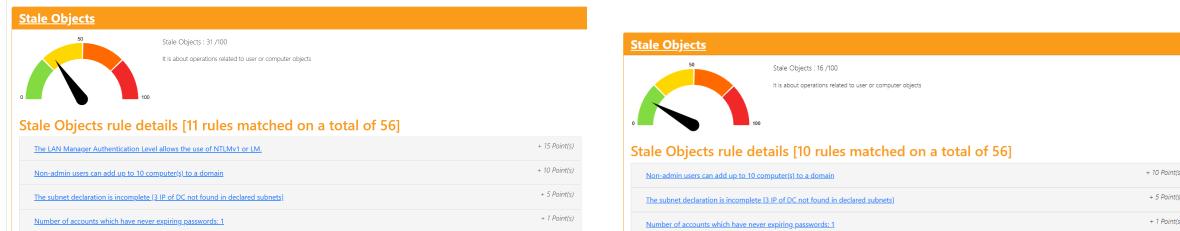


Figure 26: Comparaison avant/après sur le rapport PingCastle (gauche = avant, droite = après)

Dans ce avant/après, nous constatons à nouveau une amélioration, la règle sur le gestionnaire d'authentification LAN a disparu. Cela confirme le durcissement car c'est exactement ce sur quoi il portait.

1. Quelle différence entre PingCastle et Purple Knight dans leur approche d'audit ?

Outil	Approche	Points forts
PingCastle	Audit global de maturité AD, basé sur un scoring de risques	Rapide, simple, vue synthétique (indicateurs rouges/jaunes/verts)
Purple Knight	Audit approfondi de sécurité, orienté vers les techniques d'attaque AD (Kerberos, délégations, ACL)	Très technique, détecte des failles d'exploitation réelles

Ainsi, PingCastle a plus une vision stratégique tandis que Purple Knight a une vision offensive.

2. Quelle mesure de durcissement avez-vous choisie et pourquoi ?

Nous avons choisi la mesure “Sécurité réseau : niveau d'authentification LAN Manager”. C'est la mesure que nous avons choisie car nous avons constaté que le problème principal se trouve au niveau de l'authentification.

3. Quelle évolution constatez-vous dans le score de sécurité ?

Dans la catégorie “Stale Object” de PingCastle, le score évolue de 31 à 16. C'est une évolution due à une règle de sécurité validée grâce au durcissement.

4. Quelles seraient les trois priorités d'un plan de durcissement complet ?

Le premier point à sécuriser est les comptes à priviléges, c'est le Tier 0. C'est l'axe le plus critique relevé par PingCastle et Purple Knight.

Ensuite, il faut durcir les protocoles et configurations d'authentification. Ceci est dans la continuité et la mesure NTLMv2.

Enfin, il serait bon de nettoyer et contrôler l'infrastructure AD

Partie 7 - Architecture, automatisation et vision d'ingénieur

L'architecture de notre domaine simule un environnement d'entreprise simple, mais avec une base solide de résilience. Nous avons déployé deux contrôleurs de domaine principaux, DC1 et DC2, qui travaillent ensemble pour garantir que des services vitaux comme le DNS et l'application des GPO restent toujours disponibles (c'est notre point de redondance principal). L'ajout du RODC nous permet de simuler la gestion d'un site distant, bien qu'il introduise un risque de sécurité potentiel lié au stockage local des identifiants. L'interaction entre nos clients et ces DCs, si elle n'est pas strictement contrôlée, expose l'ensemble à des risques de mouvement latéral, faute d'un vrai modèle de Tiering. Tous les détails de cette structure, incluant les composants, les services et les flux logiques, sont visualisés dans la Figure 27.

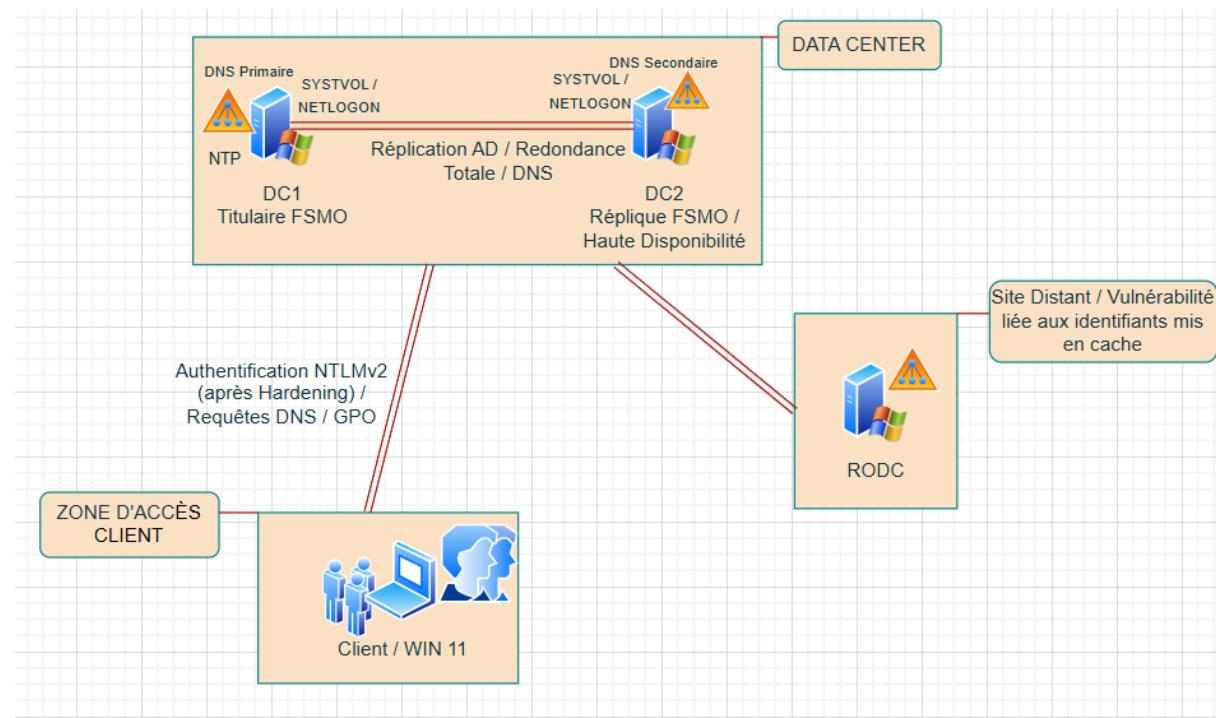


Figure 27: Draw IO schema

Notre audit initial (avec un score PingCastle de 50/100 et un score Purple Knight de 81% avant correction) a révélé que notre domaine souffre de plusieurs failles structurelles héritées de la configuration par défaut de l'Active Directory.

Le problème le plus critique réside dans la gestion des accès privilégiés, nous ne disposons pas de modèle de Tiering (compartimentage). Cela signifie que nos administrateurs se connectent potentiellement avec leurs comptes de haut niveau depuis n'importe quel poste client. Si ce poste client est compromis, un attaquant pourrait facilement intercepter les identifiants, rendant le mouvement latéral vers un Contrôleur de Domaine trivial. Par ailleurs, bien que nous ayons corrigé la faiblesse des protocoles NTLMv1 et du hachage LM, cette faille était présente par défaut et illustre un manque de *hardening* initial. Enfin, le manque de processus automatisé pour le cycle de vie des objets rend difficile le maintien d'une hygiène des comptes et des GPO. Sans ce processus, le risque de voir apparaître des comptes orphelins ou des erreurs dans les stratégies de sécurité devient une menace chronique, diminuant la résilience globale de notre architecture.

Pour résoudre les failles structurelles identifiées dans l'environnement Active Directory, nous proposons trois mesures d'amélioration clés, couvrant les aspects technique, organisationnel et de gouvernance, afin de construire une défense en profondeur.

Type de Mesure	Proposition Détailée	Objectif
Technique	Mise en place d'un Modèle d'Administration en Tiers (Tiering Model). Isoler l'administration de Tier 0 (DC et AD) dans des comptes dédiés, utilisés uniquement depuis des stations de travail P-BA (Privileged Access Workstations) sécurisées, non utilisées pour la navigation.	Empêcher le Mouvement Latéral et isoler les comptes les plus critiques.

Organisationnelle	Politique de Gestion du Cycle de Vie des Comptes. Mettre en place une procédure formelle (avec revues trimestrielles) pour l'approbation, la création, la modification, et surtout la suppression/désactivation des comptes et groupes inutilisés.	Réduire la surface d'attaque en éliminant les comptes orphelins et les droits inutiles (principe du moindre privilège).
Gouvernance	Définition d'une Base de Référence (Baseline) de Sécurité GPO. Adopter un standard reconnu (ex : ANSSI ou CIS Benchmarks) comme niveau de sécurité minimum obligatoire pour les GPO et planifier des audits trimestriels (avec PingCastle/Purple Knight) pour vérifier la conformité.	Assurer une sécurité cohérente et mesurable de l'environnement sur le long terme.

Voici ci-dessous notre script qui permet une automatisation via le powershell. Cette automatisation donne la possibilité de créer des utilisateurs, des groupes et des OU.

```

<#
.SYNOPSIS
    Script d'automatisation de la création d'unités d'organisation, de groupes et d'utilisateurs.
.DESCRIPTION
    Ce script crée une structure d'OU, deux groupes (IT Admins, HR Staff) et deux utilisateurs dans le domaine gp01.lab.ece. Il inclut la gestion des erreurs pour éviter les échecs.
.AUTEUR
    [Marchal Grégoire] Velasco Angel / Sourdin Maxime / Adda Michael
.DATE
    [18/11/2025]
.VERSION
    1.0
#>

# Variables de Configuration
$DomainRoot = "DC=gp01,DC=lab,DC=ece"

$Password = ConvertTo-SecureString "P@ssw0rd4Lab" -AsPlainText -Force

# Création des Unités d'Organisation
Write-Host "[Création des Unités d'Organisation]"
$OUS = @("ECE", "ECE/Users", "ECE/Groups", "ECE/Computers")

foreach ($OU in $OUS) {
    # Construit le chemin AD à partir du nom d'OU
    $PathAD = $OU -split '/' | ForEach-Object { "OU=$_" }
    $PathFinal = "$($PathAD -join ','),$DomainRoot"
    $NameOU = $OU.Split('/')[-1]

    # Vérifie si l'OU existe avant de la créer
    try {
        if (-not (Get-ADOrganizationalUnit -Filter "Name -eq '$NameOU'" -SearchBase $PathFinal -ErrorAction Stop)) {
            New-ADOrganizationalUnit -Name $NameOU -Path $PathFinal
            Write-Host "OU '$OU' créée avec succès."
        } else {
            Write-Host "OU '$OU' existe déjà. Ignoré."
        }
    } catch {
        Write-Error "Impossible de créer l'OU $OU. Erreur: $($_.Exception.Message)"
    }
}

# Création des Groupes
Write-Host "[Création des Groupes]"
$GroupsOU = "OU=Groups,OU=ECE,$DomainRoot"

New-ADGroup -Name "GRP_IT_Admins" -GroupCategory Security -GroupScope Global -Path $GroupsOU -Description "Administrateurs IT globaux" -PassThru | Out-Null
New-ADGroup -Name "GRP_HR_Staff" -GroupCategory Security -GroupScope DomainLocal -Path $GroupsOU -Description "Personnel des Ressources Humaines" -PassThru | Out-Null
Write-Host "Groupes GRP_IT_Admins et GRP_HR_Staff créés."

# Crédit des Utilisateurs
Write-Host "[Création des Utilisateurs]"
$UsersOU = "OU=Users,OU=ECE,$DomainRoot"

$UserData = @(
    @{
        GivenName = "Alice"; Surname = "Dupond"; Sam = "a.dupond"; Groups = @("GRP_HR_Staff")}
    @{
        GivenName = "Bob"; Surname = "Martin"; Sam = "b.martin"; Groups = @("GRP_IT_Admins")}
)

foreach ($User in $UserData) {
    # Crédit de l'utilisateur
    New-ADUser -Name "$($User.GivenName) $($User.Surname)" `-
        -GivenName $User.GivenName `-
        -Surname $User.Surname `-
        -SamAccountName $User.Sam `-
        -Path $UsersOU `-
        -ResetPassword $Password `-
        -Enabled $true `-
        -ChangePasswordAtLogon $true

    Write-Host "Utilisateur $($User.Sam) créé."
}

# Ajout aux groupes
foreach ($Group in $User.Groups) {
    Add-ADGroupMember -Identity $Group -Members $User.Sam
    Write-Host "Ajouté au groupe $group."
}
}

Write-Host "[Script d'automatisation terminé.]"

```

Figure 28 : Code qui automatise la création des users, groups et OU

```

PS C:\Users\Administrateur.GP01> powershell.exe -ExecutionPolicy Bypass -File Creation_AD.ps1
Création des Unités d'Organisation (OU)
OU 'ECE' créée sous DC=gp01,DC=lab,DC=ece.
OU 'ECE/Users' créée sous OU=ECE,DC=gp01,DC=lab,DC=ece.
OU 'ECE/Groups' créée sous OU=ECE,DC=gp01,DC=lab,DC=ece.
OU 'ECE/Computers' créée sous OU=ECE,DC=gp01,DC=lab,DC=ece.

Création des Groupes
Groupes GRP_IT_Admins et GRP_HR_Staff créés.

Création des Utilisateurs
Utilisateur a.dupond créé.
Ajouté au groupe GRP_HR_Staff.
Utilisateur b.martin créé.
Ajouté au groupe GRP_IT_Admins.

Script d'automatisation terminé.
PS C:\Users\Administrateur.GP01>

```

Figure 29: Résultat du code lancé

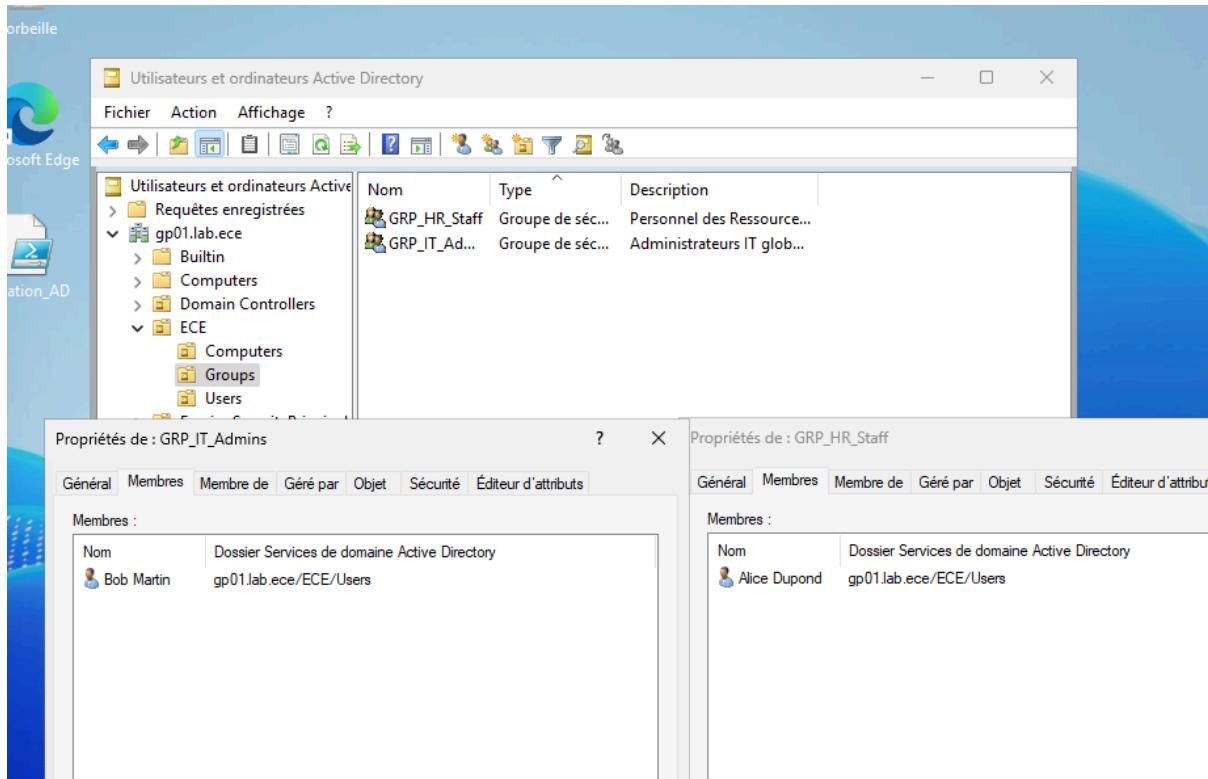


Figure 30: Vérification des créations

Sur les figures ci-dessus, nous avons pu vérifier le bon fonctionnement de notre code d'automatisation de la création des utilisateurs, groupes et OU. On peut observer sur la figure 30 nos ajouts. Nous y retrouvons en outre, la création de l'utilisateur BoB Martin, qui a été ajouté au groupe GRP_IT_Adms, mais également la *création de l'utilisatrice Alice Dupond, qui a été ajoutée au groupe GRP_HR_Staff*. Les deux utilisateurs sont dans l'OU ECE/Users, tandis que les deux groupes sont dans l'OU ECE/Groups.

Comment automatiser entièrement le déploiement de l'infrastructure ?

Pour un déploiement complet (du VM à l'AD fonctionnel), il faut adopter une approche **Infrastructure as Code (IaC)** en plusieurs phases :

- Provisioning (VM et OS) :** Utiliser Terraform ou Packer pour créer les VMs sur l'hyperviseur (VirtualBox, VMWare) et installer le système d'exploitation de base (Windows Server).
- Configuration (Rôles AD) :** Utiliser Ansible ou la Desired State Configuration (DSC) de PowerShell pour installer le rôle ADDS, promouvoir le premier DC et joindre les DC secondaires au domaine.
- Post-Configuration (Baseline et Objets) :** Appliquer la Baseline de sécurité GPO (y compris NTLMv2) de manière programmatique via DSC et exécuter

des scripts PowerShell comme celui ci-dessus pour la création d'objets (OU, Utilisateurs, Groupes).

Quelles étapes inclure dans un runbook ?

Un runbook est un guide opérationnel qui permet à toute équipe de reproduire l'environnement.

1. **Pré-requis :** Configuration réseau (IP, DNS), Ressources (CPU/RAM/Stockage), Images ISO.
2. **Déploiement du DC Primaire :** Installation OS, configuration IP, promotion DC (avec chemins des rôles FSMO).
3. **Déploiement du DC Secondaire / RODC :** Join domaine, installation ADDS, réplication et vérification (DCDiag).
4. **Configuration du Domaine :** Application des GPO de Baseline (sécurité, mots de passe, NTLMv2, audit) et exécution du script PowerShell d'automatisation des objets.
5. **Validation :** Tests de Ping/DNS, exécution complète de DCDiag, validation de la réplication, et exécution de l'audit PingCastle/Purple Knight pour confirmer la conformité à la Baseline (score attendu : 48 / 70% minimum).

1. Pourquoi documenter et automatiser est essentiel dans une architecture d'entreprise ?

Documenter et automatiser permet de garantir la continuité de service, même en cas de changement d'équipe ou d'incident. Cela réduit fortement les erreurs humaines et assure une cohérence dans les déploiements. C'est aussi indispensable pour respecter les normes, faciliter les audits et accélérer les opérations.

2. Quelle différence entre automatisation technique et opérationnelle ?

L'automatisation technique concerne directement les tâches informatiques comme la création d'utilisateurs, le déploiement de serveurs ou les sauvegardes. L'automatisation opérationnelle touche les processus métier, comme les workflows ITSM, les escalades et les procédures internes. Les deux se complètent pour améliorer l'efficacité globale d'un SI.

3. Quels outils professionnels pourraient gérer un environnement AD moderne ?

Pour gérer un AD moderne, on peut utiliser des solutions comme Microsoft Intune, SCCM/MECM ou Azure AD Connect pour la synchronisation hybride. Des outils

comme Ansible, Terraform ou Puppet permettent d'automatiser les configurations, tandis que des SIEM comme Splunk ou Sentinel assurent la surveillance continue.

4. Quelle stratégie adopter pour rendre votre domaine plus résilient et maintenable sur 3 ans ?

Pour renforcer la résilience sur trois ans, il faut miser sur la redondance (plusieurs DC, DNS répliqués) et sur un durcissement continu du domaine. L'automatisation, les bonnes pratiques Kerberos, la rotation des mots de passe et une surveillance active via SIEM améliorent la sécurité. Enfin, des audits réguliers garantissent une évolution maîtrisée de l'infrastructure.