# 15 Questions à retenir CCP2

## Qu'est-ce qu'un rôle FSMO ?

Un rôle FSMO (Flexible Single Master Operation) est la possibilité pour un contrôleur de domaine, sur un domaine Active Directory, de pouvoir effectuer des tâches particulières. Il existe 5 rôles FSMO :

- Maître de schéma
- Maître d'attribution de nom de domaine
- Maître RID
- Maître d'infrastructure
- Émulateur PDC

## En quoi la réplication entre contrôleurs de domaine est primordiale sur un domaine ?

Elle est essentielle pour garantir la cohérence et la disponibilité des données d'annuaire dans un environnement réseau. Elle permet aussi de s'assurer que toutes les modifications (comme les ajouts d'utilisateurs, les modifications de mots de passe, et les politiques de groupe) sont uniformément réparties à travers tous les contrôleurs de domaine, assurant ainsi que les utilisateurs ont accès aux informations les plus à jour, peu importe à quel contrôleur de domaine ils se connectent.

De plus, elle amène de la tolérance de panne.

## Entre les RAID 0, 1, et 5, quel est celui qui amène la meilleure sécurité ?

- Le RAID 0 fait du stripping, il divise les données en 2 sur 2 disques au minimum. Si on perd un disque, on perd l'ensemble des données.
- Le RAID 1 fait du mirroring, il copie les données sur 2 disques distincts au minimum. Si on perd un disque, on ne perd aucune donnée.
- Le RAID 5 répartit les données sur un ensemble de disques, au minimum 3, dont au moins un est un disque de parité, c'est-à-dire qu'il ne contient pas de données, mais sert à la récupération de données dans le cas d'un défaut sur l'un des 2 autres disques. Si on perd un disque, on ne perd aucune donnée.
- Les RAID 1 et 5 sont les plus sécurisés, mais le RAID 5 a un avantage en termes de lecture/écriture et de part l'ajout de disques de parité.

De plus cela dépend du nombre de disques :

- Pour 2 disques durs, le RAID 1 est le plus sécurisé
- A partir de 3 disques, le RAID 5 est le plus sécurisé.

## Quels sont les outils disponibles sur les serveurs Windows pour gérer les journaux d'événements ?

- **L'observateur d'événements (Event Viewer) :** Interface graphique pour afficher, filtrer et exporter les journaux
- **PowerShell :** avec des commandes comme Get-EventLog ou Get-WinEvent pour interroger et analyser les journaux

- **Le système d'abonnement :** il permet de centraliser les journaux de plusieurs serveurs sur un même serveur

## Qu'est-ce qu'une GPO ?

Une GPO (Group Policy Object) est un ensemble de règles dans Active Directory pour gérer et sécuriser les utilisateurs et ordinateurs d'un domaine.

## Est-ce une bonne pratique de partager des fichiers ou des dossiers sur un partage réseau, en mettant des permissions NTFS sur des utilisateurs ?

Sur le principe oui car :

- Le fait de mettre une ressource sur un partage réseau permet de la rendre accessible aux personnes autorisées
- Le fait d'utiliser les permissions NTFS permet d'affiner les droits (Lecture et Écriture) sur les objets cibles comme des fichiers ou des dossiers

Néanmoins, c'est une bien meilleure pratique d'utiliser les permissions NTFS sur des groupes d'utilisateurs que directement sur des utilisateurs.

## Si l'utilisateur jdoe existe sur un domaine Active Directory, sur une machine spécifique, utilisera-t-il le même bureau que l'utilisateur local jdoe ?

Non car ce sont 2 comptes différents :

- Pour le compte jdoe du domaine, son profil est stocké dans C:\Users\jdoe.Domaine
- Pour le compte jdoe en local sur la machine, son profil est stocké sur la machine, dans C:\Users\jdoe, sans aucun lien avec l'Active Directory

Attention, si le compte du domaine se connecte en premier, il utilisera le dossier de profil C:\Users\jdoe

Il n'est pas recommandé d'avoir des utilisateurs locaux qui portent les mêmes caractéristiques d'identification que des utilisateurs du domaine pour éviter l'écrasement de données locales.

## Active Directory contient-il une base de données hiérarchique ou relationnelle ? Explique avec au moins un exemple.

Active Directory est une base de données hiérarchique. Exemple avec l'utilisateur jdoe qui est (exemple) dans l'OU DSI, elle-même dans l'OU Utilisateurs, elle-même sous la racine du domaine. Le DistinguishedName de cet utilisateur sera : CN=jdoe,OU=DSI,OU=Utilisateurs, DC=MyLab,DC=fr).

À la différence avec une base de données relationnelle, les objets ne sont pas liés par des clés étrangères, mais par une structure en arbre avec un héritage des permissions et des configurations.

## Comment mettre en place une politique de mots de passe sur un domaine Active Directory ?

On peut utiliser la GPO “Default Domain Policy” qui permet d’avoir un paramétrage global sur l’AD.

On peut aussi utiliser les FGPP (Fine Grained Password Policy) qui permettent de définir plusieurs stratégies de mot de passe pour différents groupes d’utilisateurs.

## Qu'est-ce qu'un objet Active Directory ?

Un objet Active Directory est une entité stockée dans la base AD. Il existe plusieurs classes d’objets qui définissent leur nature, comme les utilisateurs, les ordinateurs, les groupes, les OU, etc.

## Explique le concept d'attribut d'objet Active Directory

Un attribut d’objet Active Directory est une donnée associée à un objet (utilisateur, groupe, etc.) Il sert à décrire et organiser les objets dans l’annuaire (ex : nom, e-mail, service…).

## Est-ce une bonne pratique de supprimer un compte utilisateur le lendemain du départ d'un collaborateur d'une société ?

Non ce n’est pas une bonne pratique. Il vaut mieux :

- Désactiver le compte
- Déplacer l’objet utilisateur AD dans une autre OU (de quarantaine)
- Modifier le mot de passe
- Transférer les droits de groupe, de messagerie, etc. si nécessaire
- Programmer (automatiquement ou non) la suppression du compte au bout de 90 jours.

## Qu'est-ce qu'une réplication Active Directory ?

La réplication Active Directory, c’est le transfert automatique des données entre les contrôleurs de domaine pour que tous aient les mêmes informations (utilisateurs, mots de passe, groupes…).
Elle permet de garder l’annuaire à jour partout dans le réseau, même si plusieurs serveurs le gèrent.

## Est-ce que tous les contrôleurs de domaine d'un domaine Active Directory doivent être des serveurs graphiques ?

Non, Ils peuvent fonctionner en Server Core, sans interface graphique, ce qui réduit les ressources et améliore la sécurité. L’administration se fait via PowerShell, RSAT (Remote Server Administration Tools) ou ligne de commande.

## Comment gérer l'administration d'un serveur core ?

On peut l’administrer en local, en CLI :

- Avec le menu SConfig
- En ligne de commandes PowerShell ou cmd

Mais également à distance :

- En ligne de commandes PowerShell remote
- Avec du Bureau à distance
- En utilisant la console Server Manager qui permet de prendre la main avec une MMC (Microsoft Management Console) graphique