

# **TIC-AMS3 / Administration Microsoft Windows**

## **/ Étape 3 - Users**

- 1) En configuration par défaut, seuls les utilisateurs disposant de privilèges d'administrateur sur l'ordinateur peuvent le joindre à un domaine Active Directory.

Cela signifie que seuls les comptes appartenant au groupe d'utilisateurs Administrateurs locaux sont en mesure d'effectuer cette opération.

Il est toutefois possible de déléguer cette tâche à d'autres utilisateurs en leur accordant des privilèges supplémentaires, mais cela nécessite une configuration manuelle et une planification adéquate des stratégies de sécurité

- 2) Un GUID (Identificateur Unique Global) est un identificateur unique utilisé pour identifier de manière sûre et fiable différents objets et composants dans un système d'exploitation.

Ils sont fréquemment utilisés dans l'infrastructure Active Directory et les services associés pour identifier des objets tels que les utilisateurs, les groupes et les ordinateurs.

Les GUID peuvent également être utilisés pour identifier les composants logiciels dans Windows Server 2016.

Les GUID sont importants pour une gestion et une maintenance faciles du système en permettant une identification fiable des objets et composants

- 3) La suppression d'un utilisateur dans l'Active Directory peut entraîner différents résultats en fonction de la configuration de votre environnement et de vos politiques de sauvegarde et de suppression de données.

Voici les étapes clés qui peuvent se produire lors de la suppression d'un utilisateur :

- Suppression de l'objet utilisateur : L'objet utilisateur est retiré de l'Active Directory et ne peut plus être utilisé pour l'authentification ou d'autres tâches liées à l'annuaire.
- Suppression des autorisations : Les autorisations accordées à l'utilisateur pour accéder aux ressources du réseau, comme les fichiers partagés et les imprimantes, sont également supprimées.
- Suppression des données associées : Les fichiers et dossiers associés à l'utilisateur peuvent être définitivement supprimés en fonction des politiques de suppression de données en place. Cela dépend de la façon dont les fichiers sont stockés et de la configuration du système de fichiers

- 4) Un UPN (User Principal Name) est un nom d'identification unique pour un utilisateur dans un environnement réseau.

Il permet aux utilisateurs de se connecter à différents services avec un seul nom d'utilisateur et un seul mot de passe, sans avoir à les saisir à chaque fois.

Le format standard d'un UPN est "nom\_utilisateur@nom\_domaine", par exemple, "karl@example.com" si l'utilisateur s'appelle "karl" et que le nom de domaine est "example.com".

- 5) Il est impossible de créer deux utilisateurs avec le même nom d'utilisateur dans Active Directory sur Windows Server.

Les noms d'utilisateur sont des identificateurs uniques pour chaque objet utilisateur dans l'Active Directory et ne peuvent pas être répétés.

Lors de la création d'un nouvel objet utilisateur, vous devez fournir un nom d'utilisateur unique qui n'a pas été utilisé auparavant.

Si vous essayez de créer un utilisateur avec un nom d'utilisateur déjà existant, vous recevrez une erreur indiquant que ce nom d'utilisateur est déjà en usage.

Il est crucial de veiller à ce que les noms d'utilisateur soient uniques pour chaque utilisateur dans Active Directory afin de garantir l'intégrité des données et d'éviter les conflits d'identité lors de l'authentification et de l'autorisation.

- 6) Séparer les utilisateurs en Unités Organisationnelles (OU) dans Active Directory sur Windows Server présente de nombreux avantages, notamment en termes d'organisation et de gestion des autorisations d'accès.

Les OUs permettent de regrouper les utilisateurs en fonction de leur appartenance à une organisation ou à un département spécifique, facilitant ainsi la gestion des autorisations pour les différentes ressources du réseau.