

Le compte utilisateur

Active Directory contient beaucoup de types d'objets différents dont le compte utilisateur. Généralement rattaché à une personne physique, ce type permet à cette personne d'être authentifiée par un contrôleur de domaine. L'authentification est faite à l'aide d'un mot de passe saisi par l'utilisateur. Si l'authentification est réussie, l'utilisateur se voit attribuer un jeton qui contient notamment son SID (*Security IDentifier*), unique dans le domaine AD, ainsi que l'ensemble des SID des groupes dont il est membre.

Les comptes utilisateur peuvent être locaux (ils sont dans ce cas stockés dans une base SAM - *Security Account Manager*) ou de domaine (stockés dans Active Directory).


1. Création d'un utilisateur

Cet objet étant référencé dans le schéma, il est possible d'en créer à souhait (dans la limite du nombre d'objets maximum autorisé par votre version d'AD). Cette opération s'effectue à l'aide de la console Utilisateurs et ordinateurs Active Directory. La création peut être automatisée à l'aide de scripts PowerShell ou de la commande **DSADD**.

- Sur **AD1**, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Effectuez un clic droit sur le dossier système **Users** puis, dans le menu contextuel, sélectionnez **Nouveau - Utilisateur**.


Un assistant se lance. Il permet la création de l'objet utilisateur.

- Saisissez **Jean** dans le champ **Prénom** puis **BAK** dans le champ **Nom**.

 Le champ **Nom complet** se remplit à l'aide des deux champs ainsi renseignés.

Les champs **Nom d'ouverture de session de l'utilisateur** et **Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)** contiennent le nom d'ouverture de session qu'utilise l'utilisateur pour ouvrir une session.

- Saisissez **jbak** dans le champ **Nom d'ouverture de session de l'utilisateur**.

 Le deuxième champ se remplit seul, ne le modifiez pas.

Nouvel objet - Utilisateur

Créer dans : Formation.local/Users

Prénom : Jean Initiales :

Nom : BAK

Nom complet : Jean BAK

Nom d'ouverture de session de l'utilisateur : jbak @Formation.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : FORMATION\ jbak

< Précédent Suivant > Annuler

→ Cliquez sur **Suivant**.

→ Saisissez **Pa\$\$w0rd** dans le champ **Mot de passe** puis confirmez-le.

Ce mot de passe a l'avantage de respecter la politique de complexité du mot de passe qui est mise en vigueur pour les utilisateurs du domaine **formation.local**.

→ Décochez l'option **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session** puis cliquez sur **Suivant**.

Nouvel objet - Utilisateur

Créer dans : Formation.local/Users

Mot de passe : Confirmer le mot de passe :

☒ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé


< Précédent Suivant > Annuler

→ Cliquez sur **Terminer** pour lancer la création de l'objet.

2. Propriétés de l'objet utilisateur

Après l'étape de création de l'utilisateur, il convient de paramétrer ses propriétés.

→ Effectuez un clic droit sur l'utilisateur **Jean BAK** puis sélectionnez **Propriétés**.

 Certains onglets nécessitent l'affichage des fonctionnalités avancées. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez sur le menu **Affichage** puis sur **Fonctionnalités avancées**. Seuls les onglets et propriétés les plus utilisés sont détaillés ci-dessous.

- L'onglet **Général** reprend les informations saisies lors de la création de l'objet. Il est possible de les compléter en saisissant la page web, le numéro de téléphone...
- L'onglet **Compte** permet de modifier le nom d'utilisateur mais également les différentes options de compte :
 - L'utilisateur doit changer le mot de passe.
 - Le mot de passe n'expire jamais...

Il est également possible de choisir une date d'expiration pour le compte (très utile pour des personnes en CDD ou des stagiaires) ; lorsque la date est passée, le compte est automatiquement désactivé.

Le déverrouillage du compte peut également être effectué suite à un nombre de tentatives de connexion infructueuses égal à celui configuré dans la stratégie de mot de passe.

Enfin, la configuration des horaires d'accès, qui permet d'autoriser l'ouverture de session sur le domaine dans une fourchette de temps (par exemple, 9h - 18h), et la limitation des postes sur lesquels l'utilisateur a le droit de se connecter sont également deux propriétés configurables dans cet onglet.

Propriétés de : Jean BAK

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Nom d'ouverture de session de l'utilisateur :

jbak @Formation.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

FORMATION\ jbak

Horaires d'accès... Se connecter à...

☐ Déverrouiller le compte

Options de compte :

☐ L'utilisateur devra changer le mot de passe

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

☒ Jamais

☐ Fin de : mardi 15 octobre 2013

OK Annuler Appliquer Aide

- L'onglet **Profil** permet de configurer le chemin du profil de l'utilisateur. Lors de l'ouverture de session, le poste vient récupérer le profil stocké dans le partage réseau. Les modifications sont copiées dans le profil stocké sur le serveur lors de la fermeture de session. Le champ **Script d'ouverture de session** est très souvent utilisé, il permet l'exécution d'un script lorsque la session s'ouvre (il est possible de faire la même opération lorsqu'un poste démarre ou s'arrête. Dans ce cas, l'exécution du script doit être configurée par stratégie de groupe).

Propriétés de : Jean BAK

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Profil utilisateur

Chemin du profil :

Script d'ouverture de session :

Dossier de base

☒ Chemin d'accès local :

☐ Connecter : à :

OK Annuler Appliquer Aide

- L'onglet **Éditeur d'attributs** permet la modification les attributs LDAP de l'objet Utilisateur.

Propriétés de : Jean BAK

| | | | | |
|---------------------------------------|-----------------------------|---------------------|---------------------|---------------------|
| Membre de | Réplication de mot de passe | Appel entrant | Objet | Sécurité |
| Environnement | | Sessions | Contrôle à distance | |
| Général | Adresse | Compte | Profil | Téléphones |
| Organisation | | Certificats publiés | | |
| Profil des services Bureau à distance | | COM+ | | Éditeur d'attributs |

Attributs :

| Attribut | Valeur |
|------------------------------|--------------|
| accountExpires | (jamais) |
| accountNameHistory | <non défini> |
| aCSPolicyName | <non défini> |
| adminCount | <non défini> |
| adminDescription | <non défini> |
| adminDisplayName | <non défini> |
| altSecurityIdentities | <non défini> |
| assistant | <non défini> |
| attributeCertificateAttri... | <non défini> |
| audio | <non défini> |
| badPasswordTime | (jamais) |
| badPwdCount | 0 |
| businessCategory | <non défini> |
| c | <non défini> |

Modifier Filtre

OK Annuler Appliquer Aide

➤ Les fonctionnalités avancées doivent être activées.

- L'onglet **Membre de** sert lors de l'ajout de l'utilisateur à un groupe. L'opération peut être faite par l'intermédiaire de cet onglet ou directement dans les propriétés du groupe concerné.
- L'onglet **Réplication de mot de passe** est utilisé avec un serveur RODC (*Read Only Domain Controller*), il permet de s'assurer que le mot de passe du compte utilisateur a bien été mis en cache sur le serveur en lecture seule.
- L'onglet **Objet** donne le nom canonique de l'objet, composé du nom complet précédé par son conteneur. Si ce dernier est enfant d'un autre conteneur, celui-ci apparaîtra et ainsi de suite jusqu'à la racine du domaine. On peut visualiser la classe d'objets et les date et heure de création ainsi que celles de la dernière modification de l'objet. Le nombre de séquences de mise à jour (USN), qui s'incrémente à chaque modification, est également présent. Enfin la protection contre la suppression accidentelle peut également être activée. Par défaut, cette fonctionnalité est désactivée.

Propriétés de : Jean BAK

| | | | | | | |
|---------------------------------------|-----------------------------|---------------|----------|------------|---------------------|---------------------|
| Environnement | | | Sessions | | Contrôle à distance | |
| Général | Adresse | Compte | Profil | Téléphones | Organisation | Certificats publiés |
| Profil des services Bureau à distance | | | COM+ | | Éditeur d'attributs | |
| Membre de | Réplication de mot de passe | Appel entrant | | Objet | Sécurité | |

Nom canonique de l'objet :

Formation.local/Users/Jean BAK

Classe d'objets : Utilisateur

Créé le : 15/09/2013 17:53:28

Modifié le : 15/09/2013 17:53:28

Nombres de séquences de mise à jour (USN) :

Actuel : 21078

Original : 21073

☐ Protéger l'objet des suppressions accidentelles

OK Annuler Appliquer Aide

Comme pour tout objet Active Directory, une liste ACL est présente et donne des droits de modification, de suppression ou autres à des groupes ou utilisateurs.

3. Création d'un modèle d'utilisateur

Il est fréquent dans une entreprise que plusieurs personnes faisant partie d'un même service aient accès aux mêmes ressources partagées. La liste des groupes dont ils sont membres est donc la même. Afin de faciliter la création d'utilisateurs possédant des propriétés communes, il est possible de créer un utilisateur modèle qui peut être copié. L'utilisateur qui sert de modèle peut être un compte modèle désactivé ou tout simplement un compte activé.

→ Configurez les champs des onglets **Général**, **Adresse**, **Compte**, **Profil** et **Organisation**.

➤ Seuls les champs communs à tous sont copiés. Les autres devront être saisis pendant ou après la création.

→ Effectuez un clic droit sur **Jean BAK** puis, dans le menu contextuel, sélectionnez **Copier**.

→ L'assistant se lance alors. Remplissez les champs **Prénom**, **Nom** puis **Nom d'ouverture de session de l'utilisateur** et **Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)** puis cliquez sur **Suivant**.

Copier l'objet - Utilisateur

Créer dans : Formation.local/Users

Prénom : Stéphane Initiales :

Nom : LETON

Nom complet : Stéphane LETON

Nom d'ouverture de session de l'utilisateur : sleton| @Formation.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : FORMATION\ sleton

< Précédent Suivant > Annuler

→ Saisissez **Pa\$\$w0rd** dans le champ **Mot de passe** puis confirmez-le et cliquez sur **Suivant**.

➤ Les options de compte sont par défaut les mêmes que celles du compte modèle.

→ Validez la création à l'aide du bouton **Terminer**.

Dans l'onglet **Général**, aucun champ n'a été copié depuis le compte modèle.

Les propriétés qui sont copiées sont :

- **Ville** et **Code postal** dans l'onglet **Adresse**.
- Toutes les propriétés à l'exception des noms d'ouverture de session.
- Chemin du profil et script d'ouverture de session.
- **Service** et **Société** dans l'onglet **Organisation**.
- La liste des groupes dans l'onglet **Membre de**.

4. Le jeton d'accès

Lors de la tentative d'ouverture de session, Active Directory se charge de l'authentification et de l'autorisation des utilisateurs et des ordinateurs. L'autorité de sécurité locale (**LSA**, *Local Security Authority*) traite les requêtes d'authentification effectuées via **Kerberos v5** (ou via le protocole **NTLM**).

Lorsque l'utilisateur est authentifié par son contrôleur de domaine, ce dernier génère un jeton d'accès. Il contient le nom de l'utilisateur et son **SID** (*Security Identifier*), ainsi que les groupes dont il est membre et leurs SID. Si cet utilisateur est membre d'un nouveau groupe après la création du jeton, il est nécessaire de fermer puis ouvrir la session une nouvelle fois afin de générer un nouveau jeton qui contiendra le nouveau groupe. Si la régénération n'est pas effectuée, l'utilisateur ne pourra pas accéder à la ressource partagée.

En effet, lors de la tentative d'accès à une ressource, les SID contenus dans le jeton de l'utilisateur sont comparés à ceux présents dans la **DACL** (*Discretionary Access Control List*). Si un SID est trouvé, l'utilisateur se voit accorder l'accès avec les droits configurés dans la liste de contrôle d'accès, sinon l'accès est refusé.

Les groupes dans Active Directory

Afin de faciliter l'administration, il est recommandé d'utiliser des groupes. Il est en effet plus facile d'ajouter le groupe dans l'**ACL** (*Access Control List*) d'une ressource partagée plutôt que d'y rajouter l'ensemble des utilisateurs. Une fois le groupe positionné, l'administration ne se fait plus sur la ressource mais via la console **Utilisateurs et ordinateurs Active Directory** (les opérations étant des ajouts ou suppressions d'utilisateurs, groupes...). De plus, un groupe peut être positionné sur la liste de contrôle d'accès de plusieurs ressources. La création des groupes peut être faite par profils (un groupe Compta qui regroupe les personnes de la comptabilité, DRH...) ou par ressources (G_Compta_r, G_Compta_w...). Le nom du groupe doit, dans la mesure du possible, être le plus parlant possible. J'ai l'habitude de nommer mes groupes de la manière suivante :

- **L'étendue**, ce point est traité plus loin dans le chapitre (**G** pour globale, **U** pour universel ou **DL** pour domaine local).
- **Le nom de la ressource** (Compta, Fax, BALNicolas, RH...).
- **Le droit NTFS** qui va être attribué au groupe (**w** pour écriture, **m** pour modifier, **r** pour lecture...).

Ainsi, si mon groupe se nomme **G_Compta_w**, je peux très vite en déduire que c'est un groupe global positionné sur le dossier partagé Compta et qui donne des droits d'écriture sur la ressource à ses membres.

1. Types de groupes

Il existe dans **Active Directory** deux types de groupes : les **groupes de sécurité** et les **groupes de distribution**. Le premier type de groupes est une entité de sécurité et il possède un SID. Ainsi, il est possible de le positionner sur une liste de contrôle d'accès ou de l'utiliser comme groupe de diffusion par le serveur Exchange. Le groupe possédant un SID, il est présent dans le jeton d'accès de l'utilisateur. Pour cette raison, il est conseillé, si le groupe est utilisé uniquement pour l'envoi de mail, de choisir un groupe de distribution.

Ce dernier type de groupes est utilisé par les applications de messagerie comme groupe de diffusion. Ne possédant pas de SID, les groupes concernés ne peuvent pas être positionnés dans une liste de contrôle d'accès. Un mail envoyé à ce groupe est transféré à l'ensemble des membres.

2. Étendues des groupes

Un groupe peut contenir des utilisateurs, des ordinateurs ou d'autres groupes en fonction de son étendue. En effet, cette dernière a un impact sur les membres et sur la ressource sur laquelle il est positionné. Il existe quatre étendues de groupe :

- **Local** : ce type de groupes se trouve dans la base locale de chaque machine ou serveur (à l'exception des contrôleurs de domaine). Il peut contenir les utilisateurs ou groupes locaux à la machine, des utilisateurs, ordinateurs ou groupes (globaux et universels) d'un domaine de la forêt. Il est utilisé uniquement dans des ACL locales.



Lors de la jonction au domaine d'une station de travail ou d'un serveur, les groupes admins du domaine et utilisateurs du domaine sont respectivement membre des groupes locaux Administrateurs et Utilisateurs de la machine.

- **Domaine local** : utilisé pour gérer les autorisations d'accès aux ressources du domaine, il peut avoir comme membres des utilisateurs, ordinateurs ou groupes globaux et universels de la forêt. Les groupes de domaine local membres de ce groupe doivent être du même domaine. Ce type de groupes peut être positionné uniquement sur des ressources de son domaine.
- **Globale** : contrairement à l'étendue **Domaine local**, les groupes globaux peuvent contenir des utilisateurs, des ordinateurs ou d'autres groupes globaux du même domaine. Les groupes globaux peuvent être positionnés sur

n'importe quelles ressources de la forêt.

- **Universel** : les groupes universels peuvent contenir les utilisateurs, ordinateurs et groupes globaux et universels d'un domaine de la forêt. Il peut être membre d'un groupe de type **Universel** ou **Domaine local**. Le groupe peut être positionné sur les ACL de toutes les ressources de la forêt. Attention à ne pas abuser de ce type de groupe car il est répliqué dans le catalogue global. Un nombre important de groupes universels charge la réplication du catalogue global.

La stratégie de gestion des groupes (**IGDLA**) définie par Microsoft schématise l'imbrication. Cette stratégie consiste à ajouter des **Identités** (utilisateurs et ordinateurs) dans un groupe **Global**, lui-même membre d'un groupe **Domaine Local** (il assure la fonction de gestion de l'accès aux ressources). Ce dernier est positionné dans une **ACL**.

Ainsi, si un nouveau groupe appelé **G_Tech_w** doit avoir accès à la ressource partagée nommée Informatique, il n'est plus nécessaire d'accéder à l'ACL. Un ajout dans le groupe (**DL_Tech_w** celui-ci est bien sûr positionné sur la ressource) donne l'accès souhaité.

3. Identités spéciales dans AD

Active Directory prend en charge les identités spéciales. Les membres de ces groupes sont gérés par le système d'exploitation.

L'affichage ou la modification de ces identités spéciales ne peut être effectué par l'intermédiaire de la console **Utilisateurs et ordinateurs Active Directory**.

Voici une petite liste de ces groupes :

- **Ouverture de session anonyme** : utilisé pour les connexions à une ressource sans avoir fourni un nom d'utilisateur et un mot de passe. Avant Windows Server 2003, ce groupe était membre du groupe Tout le monde, par défaut. Ce n'est plus le cas aujourd'hui.
- **Utilisateurs authentifiés** : contrairement aux utilisateurs anonymes, les membres de ce groupe sont les utilisateurs authentifiés par un contrôleur de domaine. Le compte invité n'est pas contenu dans ce groupe, même s'il dispose d'un mot de passe.
- **Tout le monde** : ce groupe contient comme membres l'ensemble des utilisateurs authentifiés ainsi que le groupe Invité.
- **Interactif** : lorsqu'un utilisateur accède à une ressource sur un ordinateur sur lequel il a ouvert une session localement, il est ajouté à ce groupe. Ce dernier contient également les utilisateurs qui ont ouvert une session via le bureau à distance.
- **Réseau** : contrairement au groupe précédent, celui-ci concerne les utilisateurs qui accèdent à une ressource sur le réseau.

Comme nous avons pu le voir, la gestion de ces groupes ne peut être effectuée par l'administrateur mais ce dernier a la possibilité de les rajouter dans une ACL.

4. Création d'un groupe

→ Sur **AD1**, ouvrez une session en tant qu'administrateur puis lancez la console **Utilisateurs et ordinateurs Active Directory**.

→ Dans la barre d'outils, cliquez sur l'icône permettant l'ajout d'un groupe.



L'icône située à droite de celle permettant la création d'un groupe est grisée, car nous sommes dans un conteneur système et la création d'une unité d'organisation est impossible.



→ Dans le champ **Nom du groupe** saisissez **G_GestionnaireAD_W** puis cliquez sur **OK**.

Nouvel objet - Groupe

Créer dans : Formation.local/Users

Nom du groupe :

G_GestionnaireAD_W

Nom de groupe (antérieur à Windows 2000) :

G_GestionnaireAD_W

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution


OK Annuler

→ Double cliquez sur le groupe qui vient d'être créé.

L'onglet **Général** reprend les informations que nous avons saisies. Le changement de l'étendue peut être fait (en fonction des membres du groupe...) depuis cet onglet. Pour mettre l'étendue en **Domaine local**, il est nécessaire dans un premier temps de la passer en **Universelle**.

Propriétés de : G_GestionnaireAD_W

Général Membres Membre de Géré par Objet Sécurité Éditeur d'attributs

 G_GestionnaireAD_W

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

Remarques :


OK Annuler Appliquer Aide

→ Cliquez sur **Universelle** puis sur **Appliquer**.

→ Sélectionnez **Domaine local** et validez le choix en cliquant sur **Appliquer**.

Propriétés de : G_GestionnaireAD_W

Général Membres Membre de Géré par Objet Sécurité Éditeur d'attributs

 G_GestionnaireAD_W

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

☒ Domaine local

☐ Globale

☐ Universelle

Type de groupe

☒ Sécurité

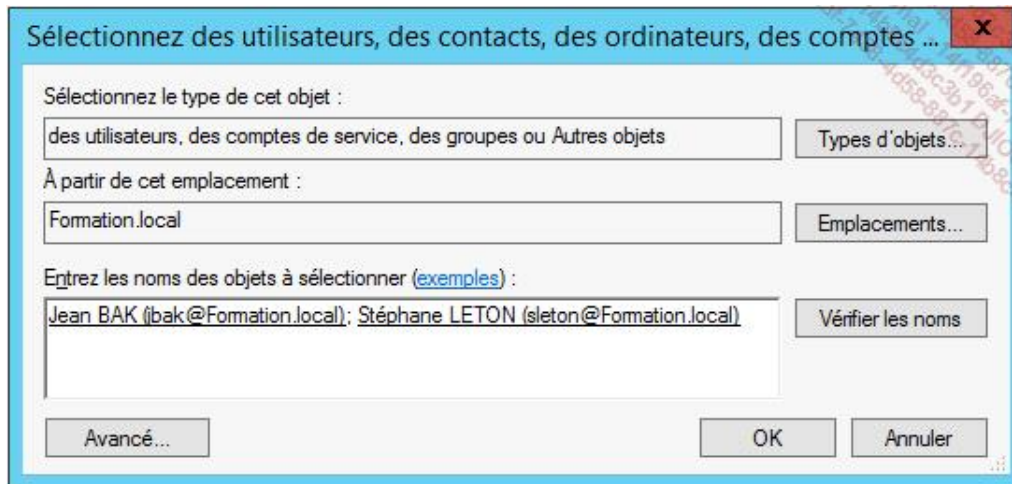
☐ Distribution

Remarques :

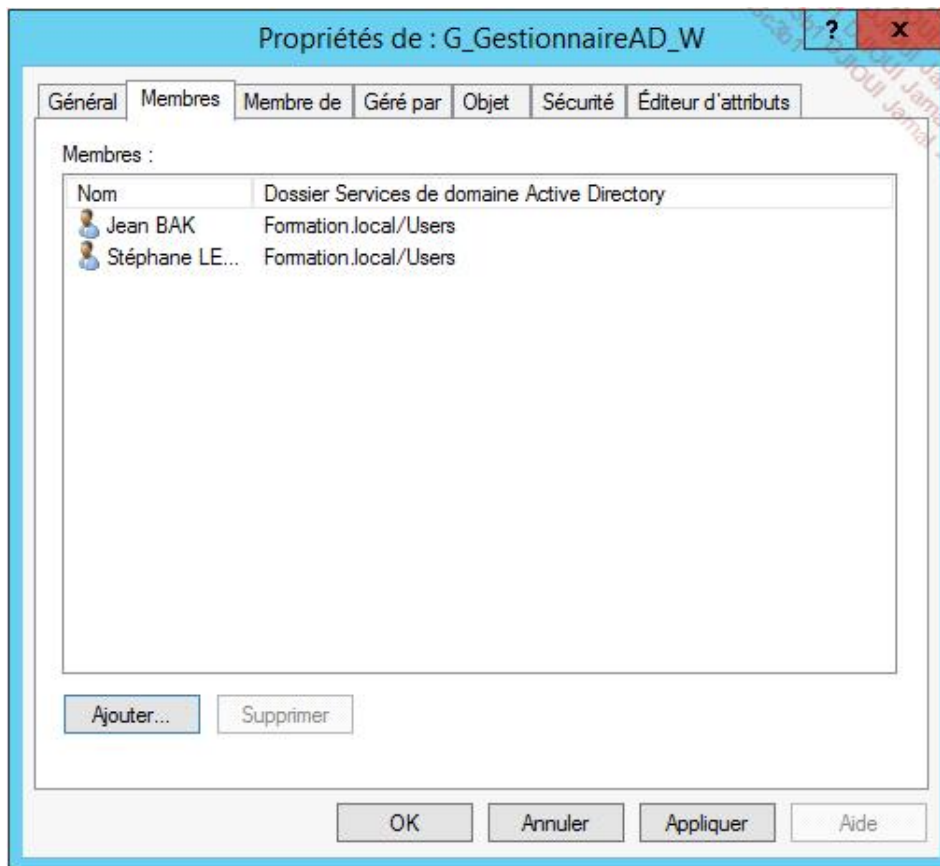
OK Annuler Appliquer Aide

Les onglets **Membres** et **Membre de** permettent de rajouter des objets dans le groupe ou de rendre ce dernier membre d'un autre groupe.

- Cliquez sur l'onglet **Membres** puis sur le bouton **Ajouter**.
- Dans le champ **Entrez les noms des objets à sélectionner**, saisissez **Jbak;Sleton** et cliquez sur **Vérifier les noms**.



- Cliquez sur **OK**.



Comme pour tous les objets AD (unité d'organisation, compte utilisateur, compte ordinateur et groupe), la protection contre la suppression peut être effectuée.

Le compte ordinateur

Par défaut, un ordinateur appartient à un groupe de travail. Pour pouvoir ouvrir une session sur le domaine, l'ordinateur doit appartenir au domaine. À l'identique du compte utilisateur, l'ordinateur possède un nom d'ouverture de session (attribut **sAMAccountName**), un mot de passe et un SID. Ces informations d'identification permettent au compte ordinateur d'être authentifié sur le domaine. Si l'authentification réussit, une relation sécurisée est établie entre le contrôleur de domaine et le poste.

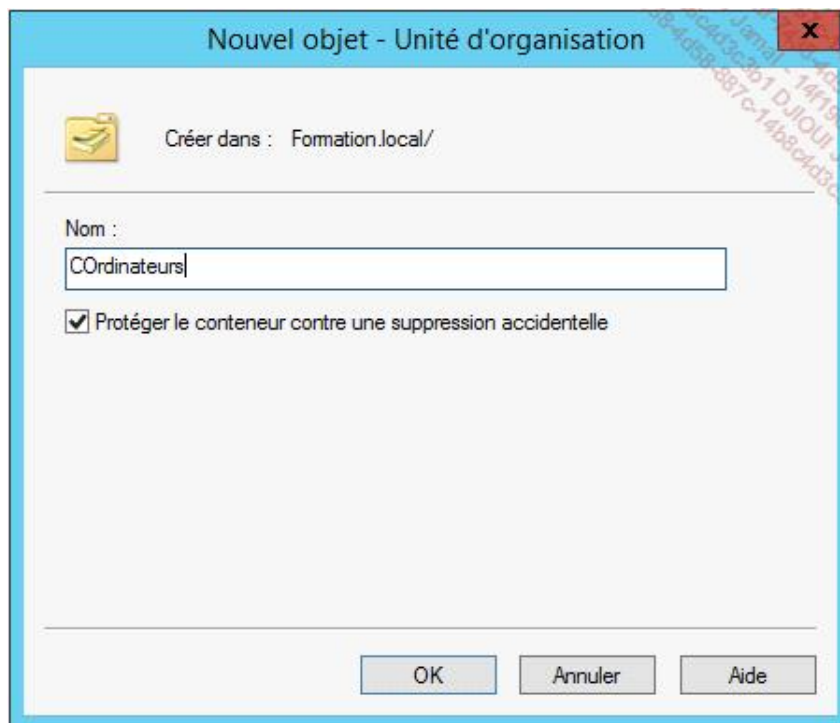
1. Le conteneur Computers

Lorsque l'ordinateur est joint au domaine et si le compte n'existe pas, un compte ordinateur est automatiquement créé dans le conteneur **Computers**. Ce conteneur est un dossier système, aucune stratégie de groupe ne peut être appliquée à celui-ci. Il est donc nécessaire de déplacer le compte de l'ordinateur vers l'unité d'organisation souhaitée.

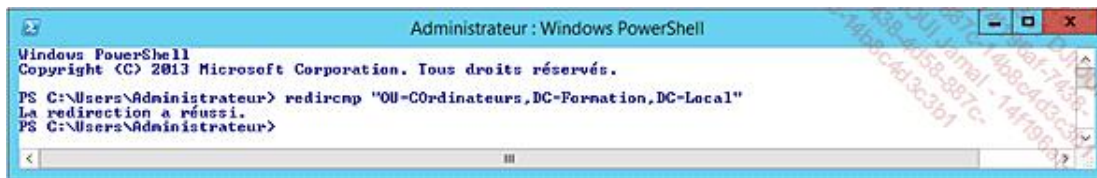
Néanmoins, il est possible d'effectuer la création des nouveaux comptes ordinateur vers un autre conteneur. En effectuant cette opération, le conteneur par défaut peut être une unité d'organisation sur laquelle est positionnée une stratégie de groupe.

Pour effectuer cette opération, la commande **redircmp** est utilisée.

- Sur **AD1**, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Cliquez sur la racine du domaine puis, dans la barre d'outils, cliquez sur l'icône permettant la création d'une unité d'organisation.
- Dans le champ **Nom**, saisissez **COrdinateurs** puis cliquez sur **OK**.



- Lancez une invite de commandes DOS puis saisissez la commande **redircmp "OU=COrdinateurs,DC=formation,DC=local"** puis appuyez sur la touche [Entrée] du clavier.



Lors des prochaines jonctions, les comptes ordinateurs seront créés dans l'OU **Cordinateurs**.

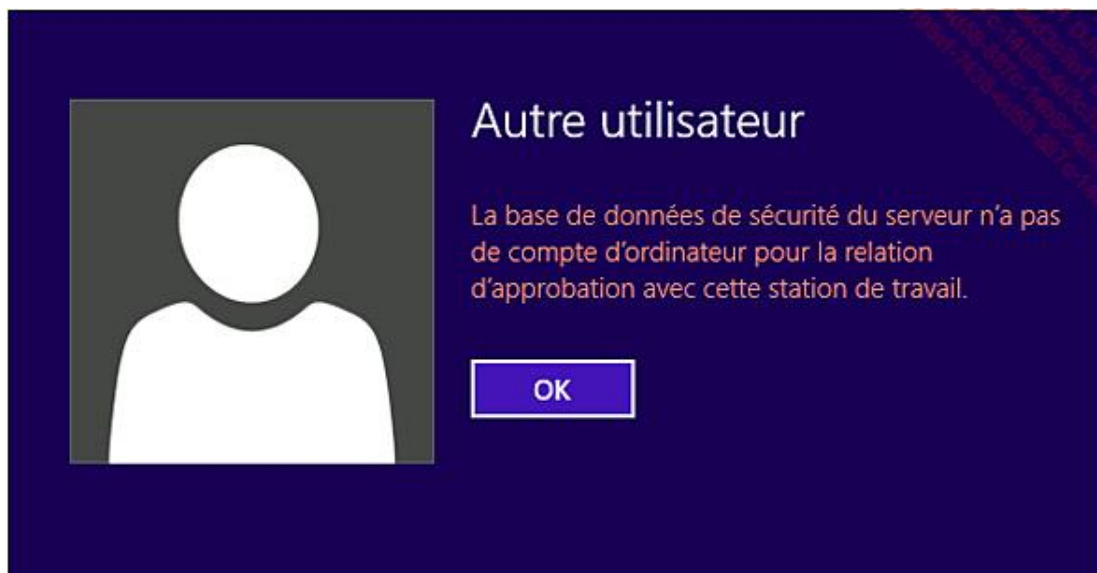
2. Canal sécurisé entre le contrôleur de domaine et le poste

Comme nous l'avons vu plus haut, lors de la jonction au domaine un compte ordinateur est créé. Ce dernier possède un nom d'utilisateur (**sAMAccountName**) et un mot de passe, celui-ci est stocké sous forme de secret **LSA** (autorité de sécurité locale). Un changement de mot de passe est effectué tous les 30 jours. Lors de la connexion au domaine, les informations d'identifications sont utilisées par le service **Netlogon** afin de créer un canal sécurisé avec son contrôleur de domaine.

Dans certains cas, il peut arriver qu'un canal sécurisé soit rompu. Le compte machine n'étant alors plus authentifié, il est impossible d'ouvrir une session sur le domaine. Plusieurs actions peuvent causer cette rupture du canal :

- Restauration d'un contrôleur de domaine.
- Restauration du poste.
- Suppression et recréation du compte ordinateur.

Dans ces cas-là, un message d'erreur s'affiche, informant l'utilisateur qu'il est impossible de trouver un compte ordinateur.



La recréation du canal sécurisée est nécessaire pour ouvrir la session sur le domaine.

Pour réinitialiser le canal sécurisé rompu, il est possible de sortir la machine du domaine en la plaçant dans un groupe de travail. Par la suite, l'ordinateur doit être à nouveau joint au domaine.

Une autre méthode consiste à régénérer le canal à l'aide de l'outil `netdom ou nltest`. L'avantage de cette solution est la conservation du SID et l'appartenance aux groupes.