
Cours - Active Directory - Focus sur l'objet Utilisateur

BTS SIO - B1/U4 Support et mise à disposition des services informatiques

1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution

1. Le compte utilisateur	3
1.1. Création d'un utilisateur	3
1.1.1. Cas pratique	3
1.2. Propriétés de l'objet utilisateur	5
1.3. Création d'un modèle utilisateur	9
1.4. Le jeton d'accès	9
1.5. Création d'un utilisateur en powershell	10

1. Le compte utilisateur

Active Directory contient différents types d'objets, dont le compte utilisateur. Généralement rattaché à une personne physique, ce type d'objet permet d'être authentifié par un contrôleur de domaine. L'utilisateur doit pour cela saisir un login et mot de passe afin de prouver son identité.

Ainsi, si la saisie de l'utilisateur est valide l'authentification est réussie, un jeton est attribué à la personne, qui contient notamment le **SID** (*Security IDentifier*) du compte utilisateur, unique dans le domaine AD, ainsi que l'ensemble des SID des groupes dont il est membre.

Les comptes utilisateurs peuvent être locaux à un poste de travail ou un serveur (ils sont dans ce cas stockés dans une base SA (*Security Account Manager*) ou de domaine (stockés dans Active Directory).

1.1. 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 l'annuaire Active Directory). 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.

1.1.1. Cas pratique

Sur votre serveur AD, 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 votre prénom dans le champ **Prénom**, puis votre nom dans le champ **Nom**.

Le champ Nom complet se remplit à partir 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 utilisé pour ouvrir une session.

Saisissez le nom d'ouverture de session au format **prenom.nom**

Nouvel objet - Utilisateur

Créer dans : bts-sio.local/CCI-BTS-SIO/Utilisateurs/Formaturs

Prénom : Roger Initiales :

Nom : Varnier

Nom complet : Roger Varnier

Nom d'ouverture de session de l'utilisateur :
 roger.varnier @bts-sio.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
 BTS-SIO\ roger.varnier

< Précédent Suivant > Annuler

Cliquez sur **Suivant**.

Saisissez le mot de passe de l'utilisateur dans le champ **Mot de passe** puis confirmez-le.

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 : bts-sio.local/CCI-BTS-SIO/Utilisateurs/Formaturs

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.

Nouvel objet - Utilisateur

Créer dans : bts-sio.local/CCI-BTS-SIO/Utilisateurs/Formaturs

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :

Nom complet : Roger Vamier

Nom de connexion de l'utilisateur : roger.vamier@bts-sio.local

< Précédent Terminer Annuler

1.2. 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 que vous venez de créer, 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 telles que :
 - 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 utiles pour les personnes en CDD ou les stagiaires); lorsque la date est passée, le compte est automatiquement désactivé.

Le verrouillage du compte peut également être effectué par suite d'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, 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 : Roger Varnier

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

Nom d'ouverture de session de l'utilisateur :

roger.varnier @bts-sio.local

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

BTS-SIO\ roger.varnier

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 8 décembre 2020

OK Annuler Appliquer Aide

- L'onglet Profil permet de configurer le chemin du profil de l'utilisateur. Lors de l'ouverture de session, le système d'exploitation vient récupérer le profil stocké sur un partage réseau. Par la suite, il est copié sur le poste sur lequel l'utilisateur a ouvert une session. Les modifications sont copiées dans le profil stocké sur le serveur lors de la fermeture de session. Le champ **Script d'ouverture de session** permet l'exécution d'un script lors de l'ouverture de session sur un poste de travail ou un serveur. Dans ce cas, l'exécution du script doit être configurée par une stratégie de groupe.

Propriétés de : Roger Varnier ? X

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

Profil utilisateur

Chemin du profil :

Script d'ouverture de session :

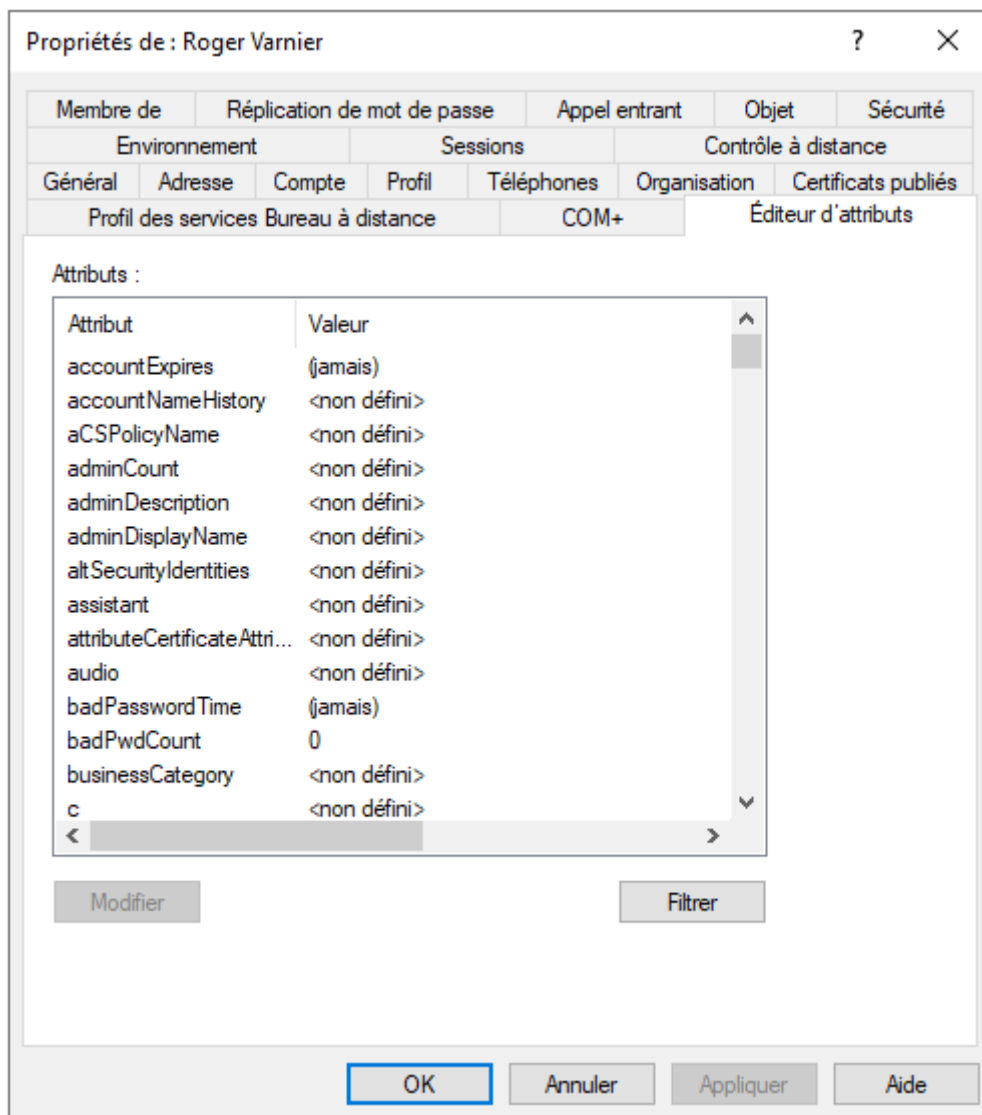
Dossier de base

☒ Chemin d'accès local :

☐ Connecter : à :

OK Annuler Appliquer Aide

- L'onglet **Editeur d'attributs** permet la visualisation et/ou la modification des attributs LDAP de l'objet.



- L'onglet **Membre de** permet de visualiser les groupes dont l'objet est membre. Il est même d'ajouter de nouveaux groupes à l'utilisateur.
- L'onglet **Réplication de mots 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. Et ainsi permettre à l'utilisateur de se connecter même en cas de coupure du réseau Wan. Par défaut, la fonctionnalité de mise en cache est désactivée.
- L'onglet **Objet** permet d'obtenir le nom canonique de l'objet. Ce dernier est composé du nom complet de l'objet 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 également visualiser la classe de l'objet ainsi que les date et heure de création et dernière modification. Le nombre de séquences de mise à jour (*Update Sequence Numbers - USNs*), 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 : Roger Varnier ? X

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 :

bts-sio.local/CCI-BTS-SIO/Utilisateurs/Fomateurs/Roger Varnier

Classe d'objets : Utilisateur

Créé le : 08/11/2020 17:39:20

Modifié le : 08/11/2020 17:39:20

Nombres de séquences de mise à jour (USN) :

Actuel : 12813

Original : 12808

☐ Protéger l'objet des suppressions accidentelles

OK Annuler Appliquer Aide

1.3. Création d'un modèle utilisateur

Cette partie fait l'objet d'un exercice à réaliser par les étudiants durant le cours.

1.4. Le jeton d'accès

Lors de l'ouverture d'une session, Active Directory se charge de l'authentification des utilisateurs et ordinateurs. L'autorité de sécurité locale (LSA, *Local Security Authority*) traite les requêtes d'authentification effectuées, pour cela Kerberos v5 est utilisée. Le protocole NTLM / NTLMv2 peut également être utilisé.

Après avoir authentifié un utilisateur, le contrôleur de domaine qui a effectué l'opération génère un jeton d'accès. Ce dernier contient le SID (*Security Identifier*) de l'utilisateur ainsi que le SID des groupes dont l'utilisateur est membre. Lors de l'ajout dans un nouveau groupe (après la création du jeton), il est nécessaire de fermer puis rouvrir la session. Ceci permet d'effectuer une nouvelle fois l'étape de génération du jeton et de posséder le SID du nouveau groupe. Si la régénération n'est pas effectuée, l'utilisateur ne pourra pas accéder à la ressource partagée.

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.

1.5. Création d'un utilisateur en powershell

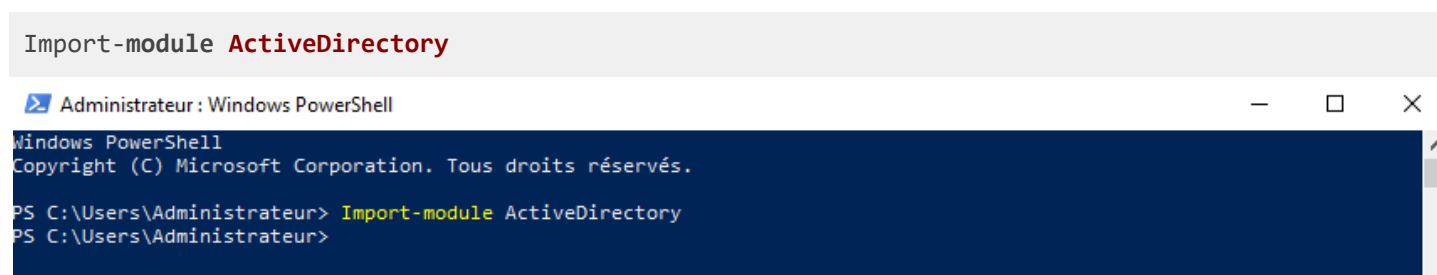
La création d'utilisateurs Active Directory en PowerShell permet d'automatiser la création d'un ou plusieurs objets. Il est possible d'utiliser un fichier CSV avec un script PowerShell afin de créer un grand nombre d'utilisateurs.

La commande permettant la création d'un objet utilisateur dans un annuaire AD est **NewADUser**.

Les syntaxes ci-dessous peuvent être utilisées afin de créer un utilisateur.

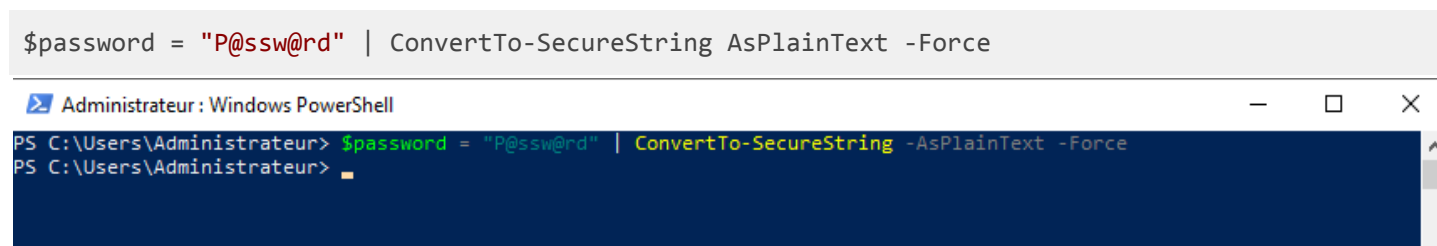
Dans un premier temps, le module AD doit être importé, cela permet l'utilisation de commandes liées à l'annuaire AD (récupération des attributs LDAP d'un compte, création d'un utilisateur...). Ce module est présent sur les contrôleurs de domaine.

```
Import-module ActiveDirectory
```



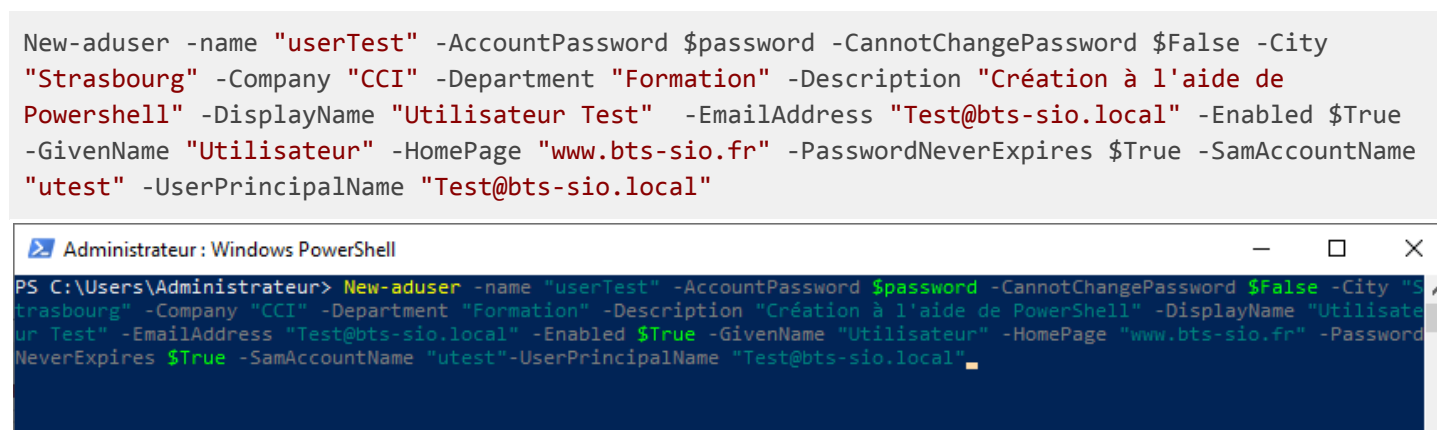
Nous allons ensuite utiliser une variable nommée password, qui nous servira à stocker le mot de passe de l'utilisateur. néanmoins avant d'être stocké dans la variable, le mot de passe devra être converti en chaîne de caractère sécurisée.

```
$password = "P@ssw@rd" | ConvertTo-SecureString AsPlainText -Force
```



L'instruction New-aduser peut maintenant être utilisée afin de procéder à la création du compte utilisateur. Le paramètre **CannotChangePassword** positionné à False autorise l'utilisateur à changer le mot de passe.

```
New-aduser -name "userTest" -AccountPassword $password -CannotChangePassword $False -City "Strasbourg" -Company "CCI" -Department "Formation" -Description "Création à l'aide de Powershell" -DisplayName "Utilisateur Test" -EmailAddress "Test@bts-sio.local" -Enabled $True -GivenName "Utilisateur" -HomePage "www.bts-sio.fr" -PasswordNeverExpires $True -SamAccountName "utest" -UserPrincipalName "Test@bts-sio.local"
```



L'utilisateur est correctement créé.

Utilisateurs et ordinateurs Active Directory [SRVDCLOCA]

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory [SRVDCLOCA]

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Administrateurs clés	Groupe de sécurité - Global	Les membres de ce groupe peuvent effectuer des actions administratives sur des objets clés dans le domaine.
Administrateurs clés Enterprise	Groupe de sécurité - Universel	Les membres de ce groupe peuvent effectuer des actions administratives sur des objets clés dans la forêt.
Administrateurs de l'entreprise	Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
Administrateurs DHCP	Groupe de sécurité - Domaine local	Les membres qui ont un accès d'administrateur au service DHCP
Administrateurs du schéma	Groupe de sécurité - Universel	Administrateurs désignés du schéma
Admins du domaine	Groupe de sécurité - Global	Administrateurs désignés du domaine
Contrôleurs de domaine	Groupe de sécurité - Global	Tous les contrôleurs de domaine du domaine
Contrôleurs de domaine clonables	Groupe de sécurité - Global	Les membres de ce groupe qui sont des contrôleurs de domaine peuvent être clonés.
Contrôleurs de domaine d'entreprise en lecture seule	Groupe de sécurité - Universel	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans l'entreprise.
Contrôleurs de domaine en lecture seule	Groupe de sécurité - Global	Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans le domaine
DnsAdmins	Groupe de sécurité - Domaine local	Groupe des administrateurs DNS
DnsUpdateProxy	Groupe de sécurité - Global	Les clients DNS qui sont autorisés à effectuer des mises à jour dynamiques en tant que clients différents (tels que les serveurs DHCP).
Éditeurs de certificats	Groupe de sécurité - Domaine local	Les membres de ce groupe ont l'autorisation de publier des certificats dans le répertoire
Groupe de réplication dont le mot de passe RODC est autorisé	Groupe de sécurité - Domaine local	Les mots de passe des membres de ce groupe peuvent être répliqués sur tous les contrôleurs de domaine en lecture seule du domaine.
Groupe de réplication dont le mot de passe RODC est refusé	Groupe de sécurité - Domaine local	Les mots de passe des membres de ce groupe ne peuvent pas être répliqués sur des contrôleurs de domaine en lecture seule du domaine.
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe de sécurité - Global	Tous les invités du domaine
krbtgt	Utilisateur	Compte de service du centre de distribution de clés
Ordinateurs du domaine	Groupe de sécurité - Global	Toutes les stations de travail et les serveurs joints au domaine
Propriétaires créateurs de la stratégie de groupe	Groupe de sécurité - Global	Les membres de ce groupe peuvent modifier la stratégie de groupe pour le domaine.
Protected Users	Groupe de sécurité - Global	Les membres de ce groupe bénéficient de protections supplémentaires contre les atteintes à la sécurité en matière d'authentification.
Serveurs RAS et IAS	Groupe de sécurité - Domaine local	Les serveurs de ce groupe peuvent accéder aux propriétés d'accès distant des utilisateurs
UsersTest	Utilisateur	Création à l'aide de PowerShell
Utilisateurs DHCP	Groupe de sécurité - Domaine local	Les membres qui ont un accès en consultation seule au service DHCP
Utilisateurs du domaine	Groupe de sécurité - Global	Tous les utilisateurs du domaine