

# TD2 Gestion des accès aux ressources dans un workgroup

**Objectif général :** Administrer des utilisateurs, des groupes dans un workgroup au travers d'environnement Windows 10 et Linux :

- ⇒ Mise en place d'une architecture réseau
- ⇒ Gestion des comptes et des groupes
- ⇒ Sécurisation des accès
- ⇒ Utilisation et configuration de conteneurs

*Ce travail s'effectuera en binôme sur 2 machines physiques gérant chacune 2 machines virtuelles, une Windows 10 (mdp : Azerty@123) et une Linux (login : root) et une linux docker (A récupérer sur le communII)*

## Phase 1 → Contraintes :

Vous allez simuler dans votre groupe de travail, composé de 4 machines, le fonctionnement d'une association. Celle-ci est gérée par un responsable, une secrétaire et 2 bénévoles

- ✓ On utilise des adresses IP privées de la classe C → 192.168.xx.yy , masque 255.255.255.0 ou xx représente le numéro de binôme et yy l'identifiant machine
  - ✓ Le nom des machines est composé des initiales du binôme suivi de cli10, cliw7, srvli puis d'un numéro nn et donc comprend 9 caractères.
  - ✓ Les machines appartiennent à un workgroup dont l'identifiant fait 6 caractères (3 premières lettres de chaque nom de binôme).
  - ✓ Les utilisateurs doivent entrer un mot de passe de 5 caractères minimum qui doit être changé chaque mois.
  - ✓ La création des comptes se fait par l'interface graphique mais également par les commandes NET USER (voir annexe ci-dessous) et Power shell ou ADDUSER sous Linux
  - ✓ Les groupes **administratifs** (membres → le responsable et la secrétaire) et **bénévoles** (membres → les 2 bénévoles) doivent être créés sous linux et sous Windows.
  - ✓ Les membres du groupe **administratifs** ont tous les droits sur les 4 machines.
  - ✓ Intégrer la machine docker dans votre réseau
  - ✓ Voir la version de docker
  - ✓ Charger le conteneur helloworld
  - ✓ Charger une machine debian
  - ✓ Installer le paquet apache
  - ✓ Accéder au site web via un de vos clients Windows
- Faire les tests suivants :
- ✓ Connexion réseau entre les différentes machines
  - ✓ Ouverture de session pour chacun des utilisateurs sur chaque machine
  - ✓ Conformité des mots de passe

Un compte-rendu complété par un schéma *visio* doit être fourni en fin de TP

## Power shell

### New-LocalUser.

Get-help -examples new-localuser

### MS-DOS

### Net User

Ajoute ou modifie des comptes d'utilisateur, ou bien affiche des informations concernant les comptes d'utilisateur.

**net user [nom d'utilisateur [mot de passe | \*] [options]] [/domain]**  
**net user nom d'utilisateur {mot de passe | \*} /add [options]**  
**net user nom d'utilisateur [/delete]**

### Paramètres

*Aucun* → Tapez net user sans paramètres pour afficher la liste des comptes d'utilisateur sur l'ordinateur.

*nom d'utilisateur* → Nom du compte d'utilisateur à ajouter, supprimer, modifier ou afficher. Longueur maximale : 20 caractères.

*mot de passe* → Définit ou change le mot de passe du compte d'utilisateur. Le mot de passe doit satisfaire au critère de longueur minimale établi par l'option /minpwlen de la commande net accounts et ne peut dépasser 14 caractères de long (ou 127 maintenant).

*\** → Crée une invite pour le mot de passe. Ce dernier n'est pas affiché lorsque vous le tapez après l'invite.

*/domain* → Exécute l'opération sur le contrôleur de domaine du domaine principal de l'ordinateur.

Remarque : Cette action est exécutée sur le contrôleur principal de domaine du domaine principal de l'ordinateur. Celui-ci ne correspond pas forcément au domaine sur lequel vous avez ouvert une session.

*/add* Ajoute un compte d'utilisateur à la base de données de comptes d'utilisateur (SAM).

*/delete* Enlève un compte d'utilisateur de la base de données de comptes d'utilisateur (SAM).

*/usercomment:"texte"* Permet à un administrateur d'ajouter ou de changer le "Commentaire utilisateur" pour le compte. Placez le texte entre guillemets (" ").

*/stations de travail:{nom d'ordinateur[...]} | \** Indique les stations de travail (8 maximum) à partir desquelles un utilisateur peut ouvrir une session réseau. Séparez les entrées multiples de la liste par des virgules. Si /stations de travail ne contient pas de liste, ou si la liste est représentée par un astérisque (\*), l'utilisateur peut ouvrir une session à partir de n'importe quel ordinateur.

.....

# adduser

man adduser

## NOM

adduser, addgroup - ajoute un utilisateur ou un groupe au système

## SYNOPSIS

**adduser** [options] [--home REP] [--shell|-s SHELL] [--no-create-home] [--uid ID] [--firstuid ID] [--lastuid ID] [--ingroup GROUPE | --gid ID] [--disabled-password] [--disabled-login] [--gecos GECOS] utilisateur

**adduser** --system [options] [--home REP] [--shell SHELL] [--no-create-home] [--uid ID] [--group | --ingroup GROUPE | --gid ID] [--disabled-password] [--disabled-login] [--gecos GECOS] utilisateur

**adduser** --group [options] [--gid ID] groupe

**addgroup** [options] [--gid ID] groupe

**adduser** --group --system [options] [--gid ID] groupe

**addgroup** --system [options] [--gid ID] groupe

**adduser** [options] utilisateur groupe

## OPTIONS COMMUNES

[--quiet] [--debug] [--force-badname] [--help|-h] [--version] [--conf FILE]

## DESCRIPTION

**adduser** et **addgroup** ajoutent des utilisateurs ou des groupes au système en fonction des options fournies en ligne de commande et des informations contenues dans le fichier de configuration */etc/adduser.conf*. Ce sont des interfaces plus conviviales que les programmes **useradd** et **groupadd**. Elles permettent de choisir des UID ou GID conformes à la charte Debian, de créer un répertoire personnel configuré suivant un modèle (squelette), d'utiliser un script sur mesure, et d'autres fonctionnalités encore. **adduser** et **addgroup** peuvent être exécutées d'une de ces cinq façons :

## Ajouter un utilisateur normal.

Lorsqu'il est exécuté avec un seul argument qui n'est pas une option et sans les options **--system** ou **--group**, **adduser** ajoute un utilisateur normal.

**adduser** choisira le premier identifiant (UID) dans le domaine défini pour les utilisateurs normaux dans le fichier de configuration. L'UID peut être forcé avec l'option **--uid**.

Le domaine spécifié dans le fichier de configuration peut être remplacé avec les options **--firstuid** et **--lastuid**.

Par défaut, chaque utilisateur d'un système Debian GNU/Linux se voit attribué un groupe avec le même nom et le même identifiant numérique. Les groupes d'utilisateurs facilitent la gestion des répertoires qui sont accessibles en écriture pour un groupe : les utilisateurs appropriés sont placés dans le nouveau groupe, le bit SGID du répertoire est positionné, et on s'assure que tous les utilisateurs ont un masque de création des fichiers (« umask ») de 002. Si cette option est désactivée en configurant **USERGROUPS** à *no*, tous les identifiants de groupe des utilisateurs seront **USERS\_GID**. Les groupes des utilisateurs peuvent aussi être forcés en ligne de commande avec l'option **--gid** ou **--ingroup** respectivement pour l'identifiant numérique et le nom du groupe.

**adduser** créera un répertoire personnel en fonction de **DHOME**, **GROUPHOMES** et **LETTERHOMES**. Le répertoire personnel peut être forcé en ligne de commande avec l'option **--home**, et l'interpréteur de commandes (« shell ») avec l'option **--shell**. Le bit SGID du répertoire personnel est positionné si **USERGROUPS** vaut *yes*, de telle sorte que tous les fichiers créés dans le répertoire personnel de l'utilisateur auront le bon groupe.

**adduser** copiera les fichiers de **SKEL** (le squelette) dans le répertoire personnel et demandera les informations pour le champ gecos (utilisées par finger) et un mot de passe. Le champ gecos peut aussi être donné par l'option **--gecos**. Avec l'option **--disabled-login**, le compte est créé mais est désactivé tant que le mot de passe n'est pas configuré. Dans ce cas, les connexions SSH par clef RSA sont toujours possibles.

Si le fichier **/usr/local/sbin/adduser.local** existe, il est exécuté une fois que l'utilisateur a été configuré, de façon à réaliser des opérations propres au système. Les arguments passés à **adduser.local** sont :

## Ajouter un utilisateur système.

Lorsqu'il est appelé avec un seul argument qui n'est pas une option et avec l'option **--system**, **adduser** ajoute un utilisateur système. Si l'utilisateur possède déjà un identifiant dans l'intervalle affecté au système (même si on indique un uid différent), **adduser** quittera avec un message d'avertissement.

**adduser** choisira le premier UID disponible dans l'intervalle spécifié pour les utilisateurs système dans le fichier de configuration. Cet identifiant peut être forcé avec l'option **--uid**.

Par défaut, les utilisateurs système sont placés dans le groupe **nogroup**. Pour placer le nouvel utilisateur système dans un groupe existant, utilisez l'option **--gid** ou **--ingroup**. Pour placer le nouvel utilisateur système dans un groupe avec le même identifiant numérique, utilisez l'option **--group**.

Un répertoire personnel est créé avec les mêmes règles que pour les utilisateurs normaux. Le nouvel utilisateur système aura **/bin/false** comme interpréteur de commandes (à moins qu'un autre interpréteur soit fourni avec l'option **--shell**), et aura un compte désactivé. Les fichiers du squelette ne sont pas copiés.

## Ajouter un groupe utilisateur.

Si **adduser** est appelé avec l'option **--group** et sans l'option **--system**, ou si **addgroup** est appelé, un groupe utilisateur sera ajouté.

Un identifiant numérique GID est choisi dans l'intervalle spécifié pour les identifiants des groupes utilisateur dans le fichier de configuration. L'identifiant peut être forcé avec l'option **--gid**.

Le groupe est créé sans utilisateur.

## Ajouter un groupe système.

Si **addgroup** est appelé avec l'option **--system**, un groupe système sera ajouté.

Un identifiant numérique GID est choisi dans l'intervalle spécifié pour les identifiants des groupes système dans le fichier de configuration. L'identifiant peut être forcé avec l'option **--gid**.

Le groupe est créé sans utilisateur.

## Ajouter un utilisateur existant à un groupe existant.

Lorsqu'il est appelé avec deux arguments n'étant pas des options, **adduser** ajoutera un utilisateur existant à un groupe existant.

### **--system**

Crée un utilisateur système.

### **--uid *ID***

Force le nouvel identifiant utilisateur à un entier donné. **adduser** échouera si cet identifiant est déjà utilisé.

### **--firstuid *ID***

Force la borne inférieure du domaine des identifiants.

### **--lastuid *ID***

Force la borne supérieure du domaine des identifiants.

### **--version**

Affiche la version et le copyright.