Réinitialisation du mot de passe (Clavister)

Pour réinitialiser un mot de passe, il faut impérativement posséder au moins un moyen de connexion au Clavister. Ce moyen peut être via incontrol ou via la console. Il faut ouvrir un shell de commandes sur le pare-feu.

Étape 1 : Ouverture de la base d'utilisateur

Dans un premier temps, se mettre dans le contexte du LocalUserDatabase avec les utilisateurs du pare-feu. Vous pouvez identifier la liste des bases d'utilisateurs locaux via la commande show.

```
FW1:/> show LocalUserDatabase

   Name        Comments
   ----------  --------
   AdminUsers  <empty>
<code>

Dans l'exemple ci-dessus, le pare-feu possède une seule base de
d'utilisateur appelé "AdminUsers".

Une fois la base d'utilisateur identifié, il faut "changer de contexte" pour
rentrer dans cette base. Cette opération revient à ouvrir la base
d'utilisateur pour la manipuler. Elle s'effectue via la commande cc.

<code>
FW1:/> cc LocalUserDatabase AdminUsers
FW1:/AdminUsers>
```

Après le changement de contexte, le nom de la base s'affiche dans le prompt.

Étape 2 : Création d'un utilisateur administrateur

Dans le contexte de la base de donnée des utilisateurs, il est possible d'utiliser les commandes show, add, set et delete pour manipuler les utilisateurs. Ici nous allons créer un utilisateur administrateur appelé “Admin”, avec le mot de passe “secret”.

```
FW1:/AdminUsers> add User Admin Password=secret Groups=administrators
```

Étape 3 : Retour au contexte par défaut

Une fois les manipulations effectuées, vous pouvez quitter le contexte de la banque de donnée utilisateur pour revenir au contexte par défaut. Cette opération revient à fermer la banque de donnée.

Elle s'effectue avec la commande cc.

```
FW1:/AdminUsers> cc
FW1:/>
```

Étape 4 : Sauvegarde et application des changements

Une fois toutes les opérations prêtes, il faut activer les changements.

Le Clavister possède une protection anti-lockout. C'est une protection qui permet d'éviter de perdre le contrôle du pare-feu. La philosophie de Clavister est que vous avez, une fois une configuration activé, 30 secondes pour prouver que vous avez toujours accès à la configuration d'une façon ou d'une autre. Si dans les 30 secondes le Clavister n'a pas moyen d'être sûr d'être toujours administrable, il revient automatiquement à sa configuration précédente.

Dans le cas des lignes de commandes, l'application de la configuration et la preuve “anti-lockout” se font via les commandes activate et commit. La commande activate permet d'activer la configuration.

```
FW1:/> activate
```

La commande activate va activer la configuration. Le pare-feu fait un “soft-restart” de ses services pour activer la configuration. La ligne de commande n'est pas perdu pendant l'opération. Le redémarrage des services prend environ trois secondes. Vous avez ensuite 30 secondes pour taper la commande commit et valider de façon permanente la nouvelle configuration.

```
FW1:/> commit
```

La nouvelle configuration est maintenant persistante. Vous pouvez désormais vous connecter via le nouvel utilisateur sur l'interface web.