Directadmin

- Changer le sender et le return path
- Disable brute force notifications

Changer le sender et le return path

Pour changer le sender du mail système dans directadmin il y a deux possibilités.

Soit via l'interface web soit en modifiant le fichier user.conf

Option 1 par l'interface web :

image.png
Image not found or type unknown

Option 2 par le fichier users.conf :

La valeur peut être modifiée via le fichier :

```
nano /usr/local/directadmin/data/users/admin/user.conf
```

Il suffit de modifier la valeur dans : email=xxxx , l'idéal est de placer la même valeur que le return path.

Exemple : diradmin@hostnode6.behostings.net

```
service directadmin restart
```

Pour changer le return Path

Pour obtenir l'info configurée dans directadmin

```
/usr/local/directadmin/directadmin config-get diradmin_envelope
```

Si la valeur est vide, c'est qu'il n'y pas de return path forcé et donc c'est celui par défaut de directadmin.

Par défaut il y a deux valeurs possibles (ça dépend de la version de directadmin)

- soit root@"hostname"
- soit diradmin@"hostname"

Pour configurer un return path il y a trois possibilités :

```
/usr/local/directadmin/directadmin set diradmin_envelope diradmin@`hostname`
```

ou

```
/usr/local/directadmin/directadmin set diradmin_envelope diradmin@hostnode6.behostings.net
```

ou en éditant le fichier de configuration directadmin

```
nano /usr/local/directadmin/conf/directadmin.conf
et ajouter la valeur : diradmin_envelope=diradmin@hostnode6.behostings.net
```

ensuite , restarter le service directadmin

```
service directadmin restart
```

Disable brute force notifications

Comment empêcher les administrateurs d'être avertis par pour les attaques de type brute force

Si vous êtes inondé de message system de ce genre : Brute-Force Attack detected in service log on

image.png
Image not found or type unknown

DirectAdmin propose un outil de surveillance des brutes force qui envoie des notifications par e-mail à tous les administrateurs lorsque des agressions par force brute sont détectées.

Si vous souhaitez empêcher l'envoi de messages tout en gardant les adresses IP sur liste noire, il suffit de définir une valeur dans le directadmin.conf

```
nano /usr/local/directadmin/conf/directadmin.conf
```

valeur à définir :

```
hide_brute_force_notifications=1
```

ensuite restart du services directadmin

```
service directadmin restart
```