

# SME-6.0.0-01

## Changement du port par défaut de SSH

© Michel-André Robillard CLP, MasterCNE

michelandre at micronator.org

Inspiré par un commentaire de "cc\_skavenger" sur un des forum de Contribs.org:  
<http://contribs.org/modules/pbboard/viewtopic.php?t=24818&highlight=>

\*\*\*\*\*

Conventions:

Commande à être entrée à la console

Contenu de fichier

\*\*\*\*\*

Suivre cette démarche pour changer le port SSH, 22 par défaut, pour un autre tel que 2222 ou 22222. Ce howto a été essayé, et fonctionne très bien, sur une version de SME-6.0.0-01.

\*\*\*\*\*

S'assurer que ssh est autorisé dans server-manager: "Sécurité | Accès à distance".

### Paramètres Secure shell

Vous pouvez contrôler l'accès Secure Shell à votre serveur. Le paramètre Public ne doit être activé que expérimentés aux fins de diagnostic et de résolution de problèmes à distance. Nous vous recommandons à « aucun accès » sauf si vous avez une raison bien précise de faire autrement.

<b>Accès Secure shell</b>	Ne permettre l'accès qu'à partir de réseaux locaux ▼
<b>Permettre l'accès à la ligne de commande administrative avec Secure shell</b>	Oui ▼
<b>Permettre l'accès par Secure shell à l'aide des mots de passe standard</b>	Oui ▼

Créer des répertoires nécessaires pour les fragments de gabarit hors-série (custom-template fragments):

```
mkdir -p /etc/e-smith/templates-custom/etc/ssh/sshd_config
mkdir -p /etc/e-smith/templates-custom/etc/rc.d/init.d/masq
```

Copier le fragment standard, qui spécifie le numéro du port SSH, vers un fragment de gabarit hors-série:

```
cp -rip /etc/e-smith/templates/etc/ssh/sshd_config/10Port \
/etc/e-smith/templates-custom/etc/ssh/sshd_config/
```

Éditer le fragment du gabarit hors-série et changer le numéro standard du port SSH (22) pour le nouveau (2222) qu'on veut utiliser à l'avenir.

```
vi /etc/e-smith/templates-custom/etc/ssh/sshd_config/10Port
```

Exemple:

```
##### Modifie par Micronator, le 19 aout 2006 @ 16h44 EDT
##### Mettre l'ancien numéro de port en commentaire pour référence
##### ultérieure.
# Port 22
Port 2222
```

Developper le gabarit avec la commande suivante:

```
/sbin/e-smith/expand-template /etc/ssh/sshd_config
```

Afficher le fichier /etc/ssh/sshd\_config et s'assurer que le port a été changé:

```
vi /etc/ssh/sshd_config
```

```
#-----
# DO NOT MODIFY THIS FILE! It is updated automatically by the
# SME Server software. Instead, modify the source template in
# an /etc/e-smith/templates-custom directory. For more
# information, see http://www.e-smith.org/custom/
#
# copyright (C) 1999-2003 Mitel Networks Corporation
#-----

##### Modifié par Micronator, le 19 août 2006 @ 16h44 EDT
```

```
##### Mettre l'ancien numéro de port en commentaire pour référence
##### Port 22
Port 2222
...
...
```

Ensuite copier le le fragment standard, qui spécifie que l'ancien port 22 est ouvert par le pare-feu, vers le gabarit hors-série de masquarade:

```
cp -rip /etc/e-smith/templates/etc/rc.d/init.d/masq/45AllowSSH \
/etc/e-smith/templates-custom/etc/rc.d/init.d/masq/
```

Éditer le fragment du gabarit hors-série et changer le numéro standard du port SSH 22 pour le nouveau 2222 qu'on veut utiliser à l'avenir.

```
vi /etc/e-smith/templates-custom/etc/rc.d/init.d/masq/45AllowSSH
```

```
{
    my $status = $sshd{status} || "disabled";
    my $access = $sshd{access} || "private";

##### Modifié par Micronator, le 19 août 2006 @ 16h54 EDT
##### Mettre l'ancien numéro de port en commentaire pour référence
### $OUT = allow_tcp_in(22,
    $OUT = allow_tcp_in(2222,
        ($status eq 'enabled') && ($access eq 'public'));
}
```

Developper le gabarit avec la commande suivante:

```
/sbin/e-smith/expand-template /etc/rc.d/init.d/masq
```

Afficher le fichier /etc/rc.d/init.d/masq:

```
vi /etc/rc.d/init.d/masq
```

```
...
...
/sbin/iptables --new-chain $NEW_InboundTCP
/sbin/iptables --append $NEW_InboundTCP \! --destination
$OUTERNET --jump denylog

adjust_tcp_in 113 ACCEPT $NEW_InboundTCP
adjust_tcp_in 21 denylog $NEW_InboundTCP
```

```
adjust_tcp_in 80 ACCEPT $NEW_InboundTCP
adjust_tcp_in 443 ACCEPT $NEW_InboundTCP
adjust_tcp_in 143 ACCEPT $NEW_InboundTCP
adjust_tcp_in 389 denylog $NEW_InboundTCP
adjust_tcp_in 110 ACCEPT $NEW_InboundTCP
adjust_tcp_in 1723 denylog $NEW_InboundTCP
adjust_tcp_in 25 ACCEPT $NEW_InboundTCP
adjust_tcp_in 2222 denylog $NEW_InboundTCP
adjust_tcp_in 23 denylog $NEW_InboundTCP
```

```
/sbin/iptables --replace InboundTCP 1 \
```

```
...
...
```

S'assurer qu'on a bien la ligne suivante (vers ligne 321) avec le nouveau port 2222:

```
adjust_tcp_in 2222 denylog $NEW_InboundTCP
```

Repartir le service ssh:

```
service sshd restart
```

Repartir le pare-feu:

```
service masq restart
```

Voilà, c'est terminé.

\*\*\*\*\*

Il faut maintenant vérifier que tout fonctionne bien en se connectant et en utilisant le nouveau port:

```
[root@dorgee /]# ssh -p 2222 root@192.168.1.1
root@192.168.1.1's password:

Last login: Sat Aug 19 18:48:59 2006 from dorgee.micronator.org
Welcome to SME Server 6.0.1-01

[root@dorgee root]#
```

Si on ne peut se connecter c'est qu'on a fait une erreur quelque part et il faut vérifier les fichiers.

**NOTE:**

Lors d'une copie scp, il faut spécifier le port avec le paramètre `-P` (en majuscule) tel que: `-P 2222`:

```
suse100:/ut # ll
total 37
drwxr-xr-x  2 root root    80 Aug 19 19:22 .
drwxrwxrwx  8 root root   912 Aug 19 19:22 ..
-rw-r--r--  1 root root 36557 Aug 19 19:22 SecureShell.jpg

suse100:/ut # scp -P 2222 SecureShell.jpg root@192.168.1.1:/tmp

root@192.168.1.1's password:
SecureShell.jpg
100%  36KB  35.7KB/s   00:00

suse100:/ut #
```