

MODIFIER LE PARAMETRAGE DIFFIE-HELLMAN

PROBLÈME

Par défaut, NGinx utilise un paramétrage Diffie-Hellman de 1024 bit. Ce paramétrage est maintenant considéré comme faible, cependant BlueMind < 3.5 utilise Java 6 & 7 qui ne supportent pas un paramétrage plus long.

SOLUTION

A partir de BlueMind 3.5, il est possible de générer manuellement un paramétrage plus long :

1. Générer un paramétrage Diffie-Hellman de 2048 bit :

```
| openssl dhparam -out /etc/nginx/bm_dhparam.pem 2048
```

2. Relancer le service :

```
| service nginx restart
```