Cahier des charges

Configurer la haute disponibilité d'un serveur web avec heartbeat

Existant :

Serveur 1: Serveur web entièrement configuré, avec apache2, site web par défaut opérationnel : www.webhost.sio

Serveur 2: Serveur dns autonome avec zone webhost.sio configurée (hôtes www, et dns)

Client :système windows XP, navigateur au choix

Définition des besoins

On souhaite que le service web continue à être opérationnel si le premier serveur tombe en panne. On va pour cela configurer un deuxième serveur web à l'identique et utiliser le service heartbeat qui permettra au deuxième serveur de prendre le relai en cas de panne du premier.
Heartbeat utilise une adresse ip virtuelle pour le service qui sera créée automatiquement sur le serveur actif.

Objectif à atteindre

Les deux serveurs web se nommeront www1.webhost.sio et www2.webhost.sio. Le site web sera accessible par le nom www.webhost.sio (qui pointe sur l'IP virtuelle). Si le serveur principal www1.webhost.sio tombe en panne, le deuxième serveur prendra le relai de manière totalement transparente.

Documents à produire et à mettre en ligne sur le serveur.

1. Plan d'adressage IP de la maquette de test
2. Mode opératoire pour l'installation et la configuration
3. Documentation des tests

Etapes :

Modification du hostname du serveur primaire :

Fichier /etc/hostname : www1, redémarrer

Installation du serveur secondaire

Installation du système ubuntu-server
installation de apache2
modification du hostname : www2

configuration de la résolution de nom :

Modifier la configuration de la zone webhost.sio (ajout ou modif des hôtes www1, www2, www)
Tester la résolution des trois noms.

installation de heartbeat sur les deux serveurs

```
apt-get update
apt-get install heartbeat
```

Configuration de heartbeat

La configuration doit être faite sur le premier et recopiée sur le deuxième
Les fichiers de configuration sont dans /etc/ha.d
3 fichiers doivent être configurés : authkeys, ha.cf et haressources
documentation : http://www-igm.univ-mlv.fr/~dr/XPOSE2006/JEREMIE_LEGRAND_HAUTE_DOSPO/pratique2.htm
Un exemple de ces trois fichiers est fourni avec la documentation de heartbeat dans /usr/share/doc/heartbeat
(les fichiers ayant une extension gz doivent être dézippés avec gunzip)

Fichier authkeys : (configuration de la communication chiffrée des deux serveurs)

```
auth 2
2 sha1 test-ha
```

Il faut ensuite changer les permission de ce fichier :

```
chmod 600 authkeys
```

Fichier ha.cf

```
logfile /var/log/ha-log
logfacility local0
keepalive 2
deadtime 15
warntime 10
initdead 120
udpport 694
bcast eth0
auto_failback on
node www1
node www2
```

Fichier haressources

```
www1 <adresse IP virtuelle du service> apache2
```

Copie de la configuration de heartbeat sur le deuxième serveur

```
scp -r /etc/ha.d www2.webhost.sio:/etc/
```

Création et échange des paires de clés sur les deux serveurs

génération de la clé sur le premier serveur

```
ssh-keygen -t dsa
```

copie de la clé sur l'autre serveur dans le fichier authorized_keys:

```
scp /root/.ssh/id_dsa.pub www2.webhost.sio:/root/.ssh/authorized_keys
```

test de la connexion ssh par clé :

```
ssh ww1.webhost.sio
```

Si tout va bien aucun mot de passe n'est demandé

redémarrage de heartbeat sur les deux serveurs :

```
/etc/init.d/heartbeat restart
```

vérification des logs : `cat /var/log/ha-log`

Tests à partir du client XP