CHAMBREUIL
Maxime

Procédure d'installation du serveur Big Brother 1.9c sous Linux

Juillet / Août 2002

I. Installation

Voici les pré-conditions de l'installation du serveur BB sous Linux :

- Vous devez connaître la distribution (redhat), le nom de la machine (redhat.csi.fr), son adresse IP (10.10.20.1).
- Vous devez connaître le mot de passe root de la machine et avoir un utilisateur bbserver
- Un serveur web doit tourné sur la machine et vous devez connaître le répertoire racine du serveur (/usr/local/apache/htdocs).
- Une petite reconfiguration du serveur web est nécessaire pour l'exécution des scripts (exemple avec Apache). Dans le fichier httpd.conf, il faut rajouter un ScriptAlias :

```
<IfModule mod_alias.c>

        ScriptAlias /bbcgi/  « /home/bbserver/bb19c/cgi/ »

        <Directory « /home/bbserver/bb19c/cgi/ »>
                AllowOverride None
                Options None
                Order allow,deny
                allow from all
        </Directory>
</IfModule>
```

et une extension au AddHandler :

```
AddHandler cgi-script   .cgi   .sh
```

Après avoir récupéré le tarball sur http://www.bb4.com et l'avoir téléchargé dans votre répertoire /home/bbserver, à la console, veuillez taper :

```
$cd /home/bbserver
$tar –zxf bbLinux-1.9c.tar
$tar –xf  bb19c.tar
$cd bb19c
$mkdir cgi
$cd install
$su
```

Vous devez ensuite entrer le mot de passe root et créez un lien symbolique :

```
$ln –s /home/bbserver/bb19c/www  /usr/local/apache/htdocs/bb
```

Avant de continuer, il faut savoir l'option de configuration spécifique à votre distribution. Pour la connaître, taper :

$ls /home/bbserver/bb19c/install/

Vous devriez voir plusieurs fichiers bbsys et Makefile avec des extensions différentes. L'extension correspondant à votre distribution est votre option de configuration : redhat. Taper ensuite :

$./bbconfig redhat

La configuration est lancée, et certaines questions seront posées :

- Etes vous d'accord avec les termes de la licence ? : Y
- Interdire l'exécution par le root ? : Y (1)
- Quel sera le nom de l'utilisateur de BB ? : bbserver
- Garder ancienne structure de fichier ? : N (2)
- Utilisé FQDN ? : Y (3)
- Quelle machine sera le BBDISPLAY ? redhat.csi.fr (4)
- Quelle machine sera le BBPAGER ? redhat.csi.fr (5)
- La machine locale est-elle le BBDISPLAY ? : Y
- La machine locale est-elle le BBPAGER ? : Y
- Entrer le destinataire par defaut : bbserver@redhat.csi.fr
- Entrer l'URL des pages web à afficher : /bb
- Entrer le répertoire des scripts CGI[1] : /home/bbserver/bb19c/cgi
- Entrer l'URL des scripts CGI : /bbcgi
- Entrer le nom de l'utilisateur qui exécute le démon http nobody
- Entrer son groupe : nobody

(1) : Pour des questions de sécurité, il est prudent de ne pas utiliser l'utilisateur ayant tous les droits pour l'utilisation de Big Brother.
(2) : Si on veut garder l'ancienne structure de fichier, des problèmes peuvent arriver lors d'une extension Big Brother.
(3) : Permet l'utilisation des noms tel que nom_machine.domaine.fr
(4) : BBDISPLAY : Machine affichant les résultats ou serveur d'affichage
(5) : BBPAGER : désigne le serveur de pager

L'installation étant terminée passons à la compilation :

$ cd ../src
$ make
$ make install
$ cd /home/bbserver
$ chown –R bbserver bbvar bb19c

[1] CGI :Common Gateway Interface : La Common Gateway Interface (CGI) est une norme définissant l'interfaçage d'applications externes avec des serveurs d'information

```
$ su  bbserver
$cd /home/bbserver/bb19c/etc
$emacs bb-hosts
```

Dans le fichier bb-hosts, vous devez mettre toutes les lignes existantes en commentaire (un # en début de chaque ligne) et rajouter :

```
10.10.20.1              redhat.csi.fr # BBDISPLAY BBNET BBPAGER
```

Vous enregistrez et vous tapez :

```
$../runbb.sh start
```

Voila le serveur BB est installé et tourne (les résultats sont visibles sur http://redhat.csi.fr/bb/), il ne reste plus qu'à le configurer.

Veuillez noter que l'installation d'un client BB sur la même machine Linux que le serveur est inutile : le serveur BB joue le rôle de client pour la machine sur laquelle il est installé.

II. Configuration

Utilisation des scripts existants

Dans chaque client, des scripts existent déjà et sont très utiles pour la supervision des éléments basiques comme la connexion, la charge cpu…Voici donc une petite liste des scripts existants ainsi que les paramètres possibles à changer dans les fichiers correspondant .

La connexion

Ce service vérifie donc l'état de la connexion entre le serveur et la machine cliente. C'est à travers la fonction ping que ce service existe. A temps espacé, le serveur « ping » les clients, si ceux-ci répondent, la connexion est bonne ; sinon un problème est arrivé. Le script existant se nomme : bb-ping.sh dans le dossier /home/bbserver/bb19c/bin.

La charge CPU

Un élément quasi-obligatoire dans la supervision de réseau et système est la charge CPU. Le script bb-cpu.sh nous aide à voir la charge cpu d'une machine, son nombre d'utilisateurs et le nombre de processus s'exécutant.

Les seuils de warning et de panic sont à régler dans le fichier bbdef.sh.

La capacité des disques

Dans une machine l'espace disponible est une donnée très importante et qui peut évoluer très vite. Il est donc très important de vouloir la surveiller. Grâce à la commande df sous linux, ce script recense toutes les partitions des disques existant sur la machine, en nous indiquant son nom, l'espace libre, utilisé et total.

Le fichier bb-dftab nous sert à configurer les différents seuils.

Les fichiers de log

Représentés sur la page résultat par la colonne msgs, le script msgs et le fichier de configuration bb-msgstab sont utiles à la surveillance des fichiers de log. Ces fichiers sont également appelés « fichiers journaux » et recensent tous les messages d'erreur qui ont pu se produire.

La configuration est effectuée dans bb-msgtab, on y trouve les mots provoquant une alerte, ceux provoquant une alerte maximale (panic) et les mots à ignorer

Format dans ce fichier:

<nomMachine> : fichier log : : chaîne warning :chaîne panic: chaîne à ignorer

Pour mettre plusieurs chaînes déclenchant une alerte, il faut séparer celles-ci par un « ; ».

Les processus en cours

Ce script est très intéressant car il permet de fixer une limite aux processus tournant sur les machines. Si ces limites sont dépassées, l'administrateur se trouve mis au courant.

Comme dans la plupart des cas, le script se trouve dans le dossier bin (bb-proc.sh) et le fichier de configuration dans le dossier etc (bb-proctab).

Format :

<nomMachine> : liste pour alerte jaune : liste pour alerte rouge

La liste des processus à surveiller connaît une syntaxe particulière :

Exemple :

Httpd ;999	Exactement 999 instances de httpd en cours
Httpd ;=999	Au moins 999 instances en cours
Httpd ;<=999	Moins de ou exactement 999 d'instances httpd en cours
Httpd ;>999	Plus ou ……
Httpd ;<999	Moins de 999……

Httpd,>999 Plus de 999……

Autres services…

Il est également possible de tester les différents serveurs. En effet, grâce à Big Brother nous pouvons connaître l'état des services dns, ftp, nntp, smtp, pop3 et enfin http. Il suffit de rajouter le nom du protocole sur la ligne de la machine dans <install>/bb19c/etc/bb-hosts

Déclarer un script externe

Dans le fichier bb-host.cfg, au niveau de la ligne du client concerné, on rajoute le contenu de la variable « svcname », qui se trouve dans le fichier de configuration du script.

Des script externes sont disponibles à cette adresse : http://www.deadcat.net/

Alerter par E-mail

La configuration de la notification par e-mail se fait grâce à 2 fichiers, qui se trouvent dans <install>/bb19c/etc : « bbwarnrules.cfg » et « bbwarnsetup.cfg ».

➢ Configuration de « bbwarnrules.cfg »

Le fichier « bbwarnrules » contient, comme son nom l'indique, les règles d'alertes ou les conditions d'envois d'une notification. Une règle d'alerte est une ligne formée sur l'architecture suivante :

hôtes supervisés ; hôtes à ne pas superviser ; services contrôlées ; services à ne pas contrôler ; jour ; heure ; destinataire

Exemple :

host1 host2;;conn disk;;2;0600-2000; mailuser@mailhost
vérifie sur les machines host1 et host2, les services « connexion » et « espace disque », le mardi entre 6h et 20h et envoie un e-mail à l'adresse : mailuser@mailhost

**;exhost3;*;disk;0-6; 0900-1230 1330-1800;* mailuser@mailhost
vérifie sur toutes les machines sauf « exhost3 », tous les services sauf l'espace disque, du dimanche au samedi, de 9h à 12h30 et de 13h30 à 18h et envoie un e-mail à l'adresse : mailuser@mailhost

➢ Configuration de « bbwarnsetup.cfg »

Ce fichier contient les paramètres d'envoi de l'e-mail. Voici les principales options à configurer :

bbwarn: Pour activer la notification d'alerte (TRUE ou FALSE)

pagedelay: Délai en minute entre 2 envois d'e-mails successifs
pagelevels : Spécifie les niveaux d'alertes pour l'envoi d'un mail (red, purple , yellow)
pagelevelsmail : Spécifie la couleur pour laquelle l'e-mail sera envoyé à l'adresse déclarée dans la règle du fichier bbwarnrules.cfg (yellow, etc…)
pagerecovered: Pour activer la notification lorsqu'un service revient à la normale (TRUE ou FALSE)
pagetype: Spécifie de quel côté le temps entre 2 mails est compté :

L'option RCPT se place du côté du destinataire : Il ne sera pas averti d'une nouvelle alerte tant que le délai spécifié à l'option pagedelay ne sera pas écoulé, quelque soit l'erreur d'un service sur un hôte quelconque.

L'option EVENT se place du côté de l'événement : Le destinataire ne sera pas averti d'une nouvelle alerte d'un événement (c'est-à-dire la combinaison d'un hôte et d'un service) tant que le pagedelay ne sera pas écoulé. Cette option génère le plus d'e-mails.

L'option HOST se place du côté de l'hôte : Le destinataire ne sera pas averti d'une nouvelle alerte sur cet hôte tant que le pagedelay ne sera pas écoulé.

L'option GROUP se place du côté du groupe d'affichage : Le destinataire ne sera pas averti d'une nouvelle alerte provenant du groupe (spécifié au niveau du fichier bb-hosts.cfg) tant que le pagedelay ne sera pas écoulé. Les hôtes qui n'appartiennent à aucun groupe appartiennent par défaut au groupe « global-grp ».

pagemaster: Adresse e-mail au cas ou l'alerte ne peut être envoyé sur l'adresse e-mail spécifiée dans bbwarnrules.cfg. Si ca reste vide, l'alerte peut ne pas être envoyée.

briefrcpt : Adresse e-mail du destinataire, qui recevra une description succincte du problème : on sait qu'un processus est arrêté mais on ne sait pas lequel.

III. Sécurisation

Dans le répertoire /home/bbserver/bb19c/etc, vous avez un fichier security.DIST. Vous le copiez en le renommant « security » :

```
$cd /home/bbserver/bb19c/etc
$cp security.DIST security
```

Puis, vous l'éditez pour rajouter les IP des machines ayant le droit de se connecter au serveur BB :

```
$emacs security
```

La syntaxe est expliquée dans le fichier. Une fois que vous avez fait vos changements, vous enregistrez et vous relancer le serveur BB :

```
$/home/bbserver/bb19c/runbb.sh restart
```