Como consultar y manejar fail2ban

Dado el gran numero de intentos de acceso a *detritus*, hemos instalado y configurado *fail2ban*. esta es una herramienta que despues de un numeo de intentos fallidos, bloquea el acceso al servidor durante un tiempo.

Ahora mismo esta configurado de esta manera: Si en un intervalo de **5 minutos** hay **3 intentos** fallidos de acceso, se bloquea el acceso a esa IP duante **6 horas**.

Manipulando

Para saber las IPs que estan *banneadas*,

```
[root@detritus ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed:   0
|  |- Total failed:   57
|  `- Journal matches:    _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned:    2
   |- Total banned:    11
   `- Banned IP list:  195.54.160.180 195.54.160.183
```

Abajo se muestra la lista de IPs bloqueadas. Si una de estas IPs es la nuestra (ver http://whatismyip.com), no podremos entrar al servidor. La unica alternativa es entrar a traves de una IP distinta (brick03, datos en el movil, etc).

Para eliminar la IP de la lista de bloqueo,

```
fail2ban-client set sshd unbanip XXX.XXX.XXX.XXX
```

siendo XXX.XXX.XXX.XXX nuestra IP.