CENTRAL LOGS - WINDOWS SYSLOG

I have previously written about centralizing your server logs (see here and here), now lets enable our windows servers (if you have to support those) to the same process. This is easy and free (unlike most windows solutions), we will be using a small application called *winlogd* which makes life very easy.

Making it work

First thing to do is to download it of course, copy it to your *windows* folder and then the *system32* folder. Then run *"winlogd -i"* to install it as a service. Now lets set it up, open up your favourite registry editor..

```
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\winlogd\Parameters]
  "Facility"="local3"         /* Facility to send logs as */
  "Port"=dword:00000202       /* The UDP port to send to, 514 being the syslog default
*/
  "Server"="192.168.0.6"      /* Change to match your configuration */
```

And make sure that the above details match your particular environment. If you want to see if they took, use *"winlogd --show"* will show the registry settings. Sometimes it may moan about not being able to find *msvcr71.dll*, just search your machine for it, it is probably around somewhere, just copy it into the *system32* folder as well. Finally start the service.

Final Words

That really is it. Short, simple, easy and it works. If only more of IT was like this. Seriously, adding windows boxes to your centralized logging system is a good idea to keep track of stuff. As always, have fun and learn.