Express-Guide
~to~
Basic Setup of
SYSLOG
Centralization of Linux with Windows

by, **ABK** ~ http://www.twitter.com/**aBionic**

::Task Detail::

Setting up a centralized Syslog service to get EventLogs from all Windows Hosts (using a Windows EventLog Agent sending it in Syslog format) being analyzed.

::Background::

Links: http://www.syslog.org

- Syslog is the standard for program message logging initially developed for SendMail. It's now used for general service messages. Some standard settings are
  - Messages refer to a facility (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0, ... , local7)
  - Assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug)

::Execution Method::

This task was mainly composed of three sub-tasks detailed as

- Configuring EventLog Agent(s)
  We used '**`NTSyslog`**' utility as a Syslog Agent on Windows Machines, used to send every event-log to Syslog Server in it's format.
  Pre-Requisite: **`DotNet Framework 3.5 SP1`**
  ::Steps::
  - Install '**`NTSyslog`**'
  - Start '**`NTSyslog Service Control Manager`**'
  - Select '**`Computer`**', set the '**`HostName`**' as desired
  - Select '**`Syslog Daemons`**', enter IP of Syslog Servers (max. 2 allowed)

- In Combo-Box, for '**Application**', '**Security**' and '**System**' set the '**Facility**' you will be configuring your Syslog server to listen for.
- Click to '**Start Service**'
- Close it (this will still run it as a service, just don't kill the process)

- Configuring Syslog Server
  Pre-Requisite: normally syslog is present on all popular POSiX machines, just check you have it or it's newer advancement syslog-ng running at your box

- **::Steps::** ***for 'syslog' to listen for Remote Syslog Messages***
  - Open Syslog's Configuration file in any text editor
    {in Debian default is **/etc/init.d/sysklogd**; in Fedora/CentOS it's **/etc/sysconfig/syslog**}
  - Find for line containing text (within '<>')
    < **SYSLOGD=""** > and change it to text (within '<>')
    < **SYSLOGD="-r -m0"** >

- **::Steps::** ***for 'syslog' to handle the received messages***
  - Add following lines to it to log the messages
    ```
    *.* /var/logs/all_Logs.log
    *.emerg /var/logs/emergency_Logs.log
    *.alert /var/logs/alert_Logs.log
    *.crit /var/logs/critical_Logs.log
    ```
    //suppose you set 'local7' for 'debug' as 'Facility' in NTSyslog;
    //then local7.debug /var/logs/win_local7.log
  - Save and Close your Syslog Configuration file
  - Open '**/etc/logrotate.d/syslog**' file in any text editor
  - To keep logs truncated after some time, add your Log file names with absolute path at starting. Then Save and Close the file.
  - Restart '**SyslogD**' service

- **::Steps::** ***for 'syslog-ng' if required***
  - Normally, its configuration file has following pattern
    - options{}, defining global properties
    - source <gatewaySname>{}, defining sources of Logs and can be more than one
    - destination <localhost>{}, defining location to dump output and it can be anything from file to command and pipe to n/w stream.
    - log{}, co-relating different 'source' and 'destination' entries
  - This pattern will be specified in the respective service you are trying to implement using it, like in our case we set 'source' as all messages received and destination as mysql db

- Setting up Web Application to analyze the collected logs this is just required to analyze the logs collected in a better UI. There are several open-source

options present for it.
PHP-Syslog and PHP-Syslog-NG are two such services which can be deployed as a Web-Service over normal Apache as per instructions attached with it in README.
LogZilla is also a similar newer model of service with a detailed database of its own to provide better understanding of the logs.

::Tools/Technology Used::

- NTSyslog as Syslog Agents on Windows: http://ntsyslog.sourceforge.net/
- syslog/syslog-ng on Linux machine to act as a server: http://www.syslog.org/
- LogZilla as Web GUI to analyze the information: http://www.logzilla.pro/

::Inference::

- Deploying Syslog Server and NTSyslog based hosts was very easy.
- Deploying the open-source Web Services took much effort to get deployed due to its compatibility over certain Linux Distros and Versions giving problems for the interfacing of this service with syslog-ng to collect logs.

::Troubleshooting/Updates::

- ***Problem:*** The actual aim of this task was to analyze the events of all hosts from a central location to analyze any problem occurring. But a problem arise that Syslog Service had an upper limit over Event Description Content, so NTSyslog had to truncate the Description and send. So, due to incomplete description it wasn't feasible to analyze the exact problem.
  Solution:
  I'm working on a Project 'eVuVeR' for this task including all 3 components discussed and more monitoring capabilities... soon to be released.
