

Thoughts on Centralized Loghosting March 2006 Unix Users Group

Keith Lehigh
Unix Systems Support Group

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Why Bother?
- System Logging in a Unix World
- The PG-Rated Gory Details
- Logging any service *
- So What Now?
- What about Windows?
- Where to find help and ideas

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Logs can be modified during compromise
- Secure, remote loghost provides a trusted source for investigation
- Loghost can also provide a centralized location to generate statistics on service usage
- Near Realtime logwatching can be done, possibly inline

On The Unix Syslog Service

- **Syslog Facilities & Levels**
 - Facilities are sources of log messages
 - Kern - Mail - Local[0-7] – user defined
 - Levels reflect criticality of messages
 - Debug to crit
- Standard unix syslog has ability to forward log data to remote host via UDP port 514
- Input and Output limited to files or UDP

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Support to read log data from a variety of sources
- Better filtering capabilities than standard syslog
- Support for logging to files, network, or usertty*
- TCP Support and Solaris oddities
- libol required to build current version
 - Provides non-blocking I/O
- Version 2.0 coming soon w/o libol dep
- Builds easily on RHEL and Gentoo

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Global Options
- Statements (with local options available)
 - source - specifies a source of logging data
 - file / unix-dgram / unix-stream / udp / tcp / sun-streams
 - filter - optional user-defined filter(s)
 - facility / level / program / host / match
 - destination - destination for log data
 - file / unix-dgram / unix-stream / udp / tcp / usertty
 - log – combines source, destination and filter

- Lots of per-service examples on website
- Only supports TCP-based protocols
- Provides encrypted tunnel for log data in transit
- Per host certificates provide layered defense
 - Compromise of one host won't reveal logs of all hosts to network sniffing
 - Full Verification provides additional access control

The PG-Rated Gory Details

- Operating System Thoughts
 - (if \$os =~ 'Gentoo-hardened') { \$shappy_count ++; }
 - Loghosting only, minimal accts and remote access
 - Create a watcher group (for admins)
 - /var/log should be mounted as a separate partition
 - Use “nodev,noexec,nosuid” mount options
 - And make it large to avoid DoS attacks
 - Exclude this partition from standard backups *
 - Encrypt the logs before backup

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – Loghost Syslog-ng

- Setup Syslog-ng on Loghost
 - User separation via cmd line opts (and non-priv'd ports)
 - Listen for connections on localhost
 - Choose large port ranges for client connections
 - All syslog-ng connections will be made over localhost
 - Adjust access controls accordingly
 - Let's peek at a syslog-ng.conf

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – SSL Certs

- Setup Signing CA (on loghost perhaps)
 - Setup logging specific openssl.cnf (for defaults)
 - Setup directory and file structure
 - Generate signing certificate
- Generate Cert for Loghost
- Generate Cert for client(s)
- Cert chain and cert file details

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – Stunnel & Access

- Loghost Stunnel Setup
 - Permissions on directories and files
 - Separate range of ports for external connections
 - Tcp-wrappers service names derived from stunnel.conf service names
- Loghost Access Controls
 - Tcp-wrappers
 - Iptables (or system specific firewall)

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – Loghost Details

- Final Loghost details
 - Use least privilege as much as possible
 - Don't share groups or users for any of these services
 - Don't forget log rotation!!

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – Client Stunnel

- Client Stunnel Setup
 - Install certs, remember perms
 - Accept over localhost, Connect over network
 - Install certs
 - Setup stunnel.conf
- Access Controls
 - Firewall and tcp-wrappers

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

Gory Details – Client Syslog-ng

- Client Syslog-ng Setup
 - Connect over localhost
 - Use separate sources where possible
- Test with logger
 - Or use a script to test every facility and priority
- Log Rotation!

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Logging Apache access logs via named pipes
 - Create pipes
 - Ensure syslog-ng starts first (to read the pipes)
 - <Syslog-ng config magic to not mangle log entry>
 - <apache config line>
 - <Forwarding config>
- Some Services just don't like named pipes

- Logwatch
 - look at your data
 - then decide what you want to collect from it
 - then collect it
 - count the stuff you throw away
 - vector the rest to a human's attention
- Simple Event Correlator
- Loghound

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP

- Freeware products limited to UDP
- loganalysis.org has a good page of info
- Event Reporter and Snare
- Stunnel is supported (binaries at stunnel.org)
 - Certs should live in [C:\Program Files\stunnel](#)
- Audit Policy needs to be fine-tuned

Where to find help & ideas

<http://www.loganalysis.org/>

http://www.balabit.com/products/syslog_ng/

<http://www.stunnel.org/>

<http://www.campin.net/syslog-ng/faq.html>

<http://kodu.neti.ee/~risto/sec/>

<http://kodu.neti.ee/~risto/loghound/>

<http://mail.wildlist.org/pipermail/firewall-wizards/2006-February/019241.html>

<http://www.ussg.iu.edu/>

USSG UNIX SYSTEMS
SUPPORT GROUP