Log File Retention Guidelines

Institute for Advanced Study

July 21, 2011 (revision 206)

Contents

1 Log File Retention Times

The default log retention time is *100 days*, except as shown in Table 1.

Table 1: Log File Retention Times

Log File Type	Retention Time
Web Proxy Campus[a]	24 hours
Web Proxy Resnet[b]	24 hours
Urchin Web Analytics[c]	Indefinitely
Virtual Machine backups[d]	465 days
Logs stored in Databases[e]	13 months

[a] As ratified by SPC on 2010-02-02

[b] As ratified by SPC on 2010-01-14

[c] Contains logs and reports of visits to ias.edu web pages.

[d] VMs may hold 100 days of logs and are backed up for 365 days, so 465 days total. As ratified by SPC 2010-12-03

[e] As ratified by SPC on 2011-07-14

2 Finding Log Files

The EFF provides *logfinder*[1], a python script which is helpful in identifying log files. See `logfinder.py --help` and the included `README` file for usage. *logfinder* can be run in one of two ways:

- `logfinder.py` – Scans open files system-wide.
- `logfinder.py /some/path` – Statically analyzes files in `/some/path` for log-like characteristics.

3 Log File Destruction Procedure

The three-pass DoD 5220.22-M method is suitable. Here are some sample commands to destroy log files on various operations systems[2] to this standard:

- Linux: `shred -ufn3`
- Windows[3]: `sdelete -p 3`
- Mac OS X: `srm -fm`

In general, log files should be selected for deletion according to last modification time. The following command would destroy log files in `/var/log` older than 100 days:

```
find /var/log -type f -mtime +100 -exec shred -ufn3 {} \;
```

4 Related Documents

All Institute Computing policies can be referenced here: `https://security.ias.edu/policies`

- Institute for Advanced Study. *Log File Retention Policy*

[1] http://www.eff.org/osp/logfinder-0.1.tar.gz

[2] Other devices or operating systems may not have such a utility. In these cases destruction via the best and most economical method available is required.

[3] *sdelete* is part of SysInternals.